IFI Policy Recommendation

IFI Policy Recommendation No.34　March 2025

日本・米国・カナダの協力による研究セキュリティ施策に関する提言

渡部 俊也

東京大学未来ビジョン研究センター 教授

東京大学未来ビジョン研究センター
Institute for Future Initiatives
The University of Tokyo

政策提言

日本、米国、カナダの協力による研究セキュリティ施策に関する提言

１．提言の骨子

2025 年 1 月 21 日に実施された日本、米国、カナダの大学および政府の参加者による国際会議「日米加大学研究セキュリティ・インテグリティ国際ワークショップ」（未来ビジョン研究センター主催）における議論を踏まえ、3 か国の協力による研究セキュリティ施策として下記を提言する。

１．日本・米国・カナダの大学と政府は、アカデミアの自由で国際的な研究の在り方に対して、基本的に同じ価値観を有しており、かつ現下に生じている研究インテグリティに対するリスクの存在を共有していること、3 か国それぞれの、大学コンソシアムやそれに相当する組織、およびそれを支援する政府が相互に協力を行い、そのアプローチ方法を共有することは有益であることから、具体的な協力体制についての議論がなされるべきである。

２．研究インテグリティと研究セキュリティの概念については、G7 に設けられたワーキンググループ（G7 Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group）において整理が試みられたものであるが、特に研究セキュリティについては各国で定義が明確化されているとはいいがたく、今一度日米カナダで統一した概念を確認して、その考え方に対する信頼感を高め、それを研究現場と共有していくことが必要である。

３．研究インテグリティと研究セキュリティについて同じ概念を共有することが、その目標に向かう際に全く同じやり方を行うことを意味するものではなく、各国の実情に沿った実施方法を採用することが推奨される。その際にもお互いのアプローチの相違を認識しながら進めることが望ましい。

これらを踏まえながら、様々なリスク、さらに意図せざる共著の問題や、ペーパーミリングへの対処などについても取り組む国際的協力体制を充実させていくことが重要である。さらにこれらの取り組みの方向性については、日米カナダだけではなく、G7 の各国でも同様に合意できるものと考えられるため、2025 年の G 7 サミット（カナダ政府が議長国を務めアルバータ州のカナナスキスで開催する予定）において、政府間の連携を深め、価値観を同じくする大学が認識を共有し、具体的に自由な研究と知の探求などを最大限に活かせる環境整備を進める機会とすべきである。

２．本提言に至る経緯

本提言に至る源流は 2015 年 1 月 28 日に未来ビジョン研究センターの前身である政策ビジョン研究センターが主催して実施した国際会議国際シンポジウム「グローバル競争の中での自立した大学のあり方

社会との連携とガバナンス・コンプライアンス」”International Conference on “The role of independent universities in global competition: collaboration with society, governance and compliance”[1]にさかのぼる（参考資料１）。

この会議は 2015 年 1 月 28 日、東京大学政策ビジョン研究センターと政策シンクネットの共催で開催されたもので、世界 9 カ国から 15 名のゲストが招かれ、「産学連携」「機微技術と大学」「研究不正と利益相反」「社会との連携のための人材育成」の 4 つのパネル討論が行われた。従来、産学連携と研究不正の問題は個別に議論されることが多かったが、本シンポジウムでは両者の密接な関連性が指摘され、大学が社会との関係を強化する中で、研究不正や利益相反の問題が増加する傾向があることが強調された。米国の例では、1980 年のバイ・ドール法制定により、産学技術移転が活発化したが、同時に研究不正や利益相反の問題が顕在化した。同様の現象は、日本においても 1999 年の日本版バイ・ドール法制定以降に見られる。産学連携の推進に伴い、研究者や大学が社会の信頼を維持するためには、Research Integrity の概念が不可欠であることを示したものである。大学が社会との連携を強化する中で、産学連携の促進と研究不正の防止を両立させるためには、これらを別々の施策として捉えるのではなく、一体的に考えることが重要であるとの結論に至った。

本シンポジウムでは、当時、研究公正と訳され、捏造、改ざん、盗用を防止する狭い意味で用いられていた Research Integrity を、より幅広く「研究者と社会との契約」と位置づけ、単なる制度や規制の問題ではなく、関係者全員が自発的に実践すべきものであるとする主張は、本提言の Research Security の概念につながるという意味で重要である。

後述するように、大学が守らなければならないのは社会との契約としての Research Integrity であり、そのための施策として研究倫理に加え、この会議で指摘されているように産学連携の活発化とともに重要になった産学利益相反などを管理する Research Integrity Management が必要となり、そして今回提言で論ずる Research Security Management が必要となったという文脈で整理することができると考えている。

外国政府や機関との連携において生じる技術流出等に関するリスクの問題については 2019 年 2 月に公開された政策提言「米国大学が行うハイリスクパートナリング管理の実態と日本の大学への示唆」（参考資料２）において一旦の整理が行われた。米国ハーバード大学のハイリスクパートナリング管理の実態を調査し、日本の大学への示唆を提供することを目的として提言を行ったものである。2018 年に成立した米国の NDAA2019（国家防衛権限法）により、米国大学が特定の外国企業との提携が制限され、制裁対象企業と関係を持つと政府研究資金を受け取れなくなったことが背景となっている。しかし重要なのはハーバード大学等では、NDAA2019 以前からリスクのある企業との連携を厳格に管理し、情報流出やレピュテーションリスクを回避する体制を整えていたことである。このことは主要米国大学が政府の規制によって受動的に対応したというより、制裁以前から外国企業のデューデリジェンスを行い、産学利益相反と同様、ステイクホルダーへの説明責任上、その連携の正当性を説明できるかどうかを判断しようとしていたことが注目される。すなわち法令遵守を超えて、その周辺にあるグレーゾーンの領域のパートナリングについては NDAA 規制以前から行っており、「我々はそのリスクを理解していて適切に管理して対処している」とする姿勢のもと、リスクを低減させる管理を行っていたのである。NDAA 以降もそのマネジメントが強化され継続している。2019 年 1 月の時点で米国の 10 を超える大学が

[1] https://www.u-tokyo.ac.jp/focus/ja/articles/t_z0313_00008.html

Guidelines for Sensitive Negotiations に基づく管理を行っている。

このマネジメントの手法は産学連携の利益相反管理と類似しており、リスクをゼロにしようとすれば産学連携そのものを禁止することにつながるが、社会との関係を発展させるために、産学連携自身は推進し、そこに発生するリスクを管理し最小限にまで低減させようとする姿勢とみることができる。そのようなマネジメントが行われる背景としては、前述した Research Integrity の管理による維持発展のために行われている。ハイリスクパートナリングの管理についても、外国組織との関係を断てばリスクはゼロになる が、国際的な大学のありようを発展させるため、外国組織との関係を維持、発展させつつ、そこに発生するリスクを最小限に低減させる自主的なマネジメントが行われていると理解すべきであろう。

2019 年 9 月には、「米国の大学とスタートアップのリスクマネジメント― 日本の大学とスタートアップが先端技術分野で米国と連携するための条件とは ―」（政策ビジョン研究センター）と称して会議が実施された。この会議においては当時米国において Foreign influence という用語を用いて、産学利益相反の概念を外国政府等による影響まで延伸した概念が用いられるようになった経緯や、そのための実務的対処について議論が行われた。Foreign influence という用語が使われてはいるが、先の提言「米国大学が行うハイリスクパートナリング管理の実態と日本の大学への示唆」に示した考え方での対処を実務的に整理することとなった。

このような経緯をへて、米国では外国政府や外国企業との影響下におけるリスクの事例が検討され、蓄積されていく。この際、リスクが顕在化した事例においては、未公開の研究情報である知的財産が窃盗された事例が複数報告されることとなる。

そのうち代表的な事件としては、2015 年、2019 年のゲストとして招いた Ara Tahmassin 博士が、後述する裁判においても大学側の責任者となった事案があげられる。この事件は、ハーバード大学の化学・化学生物学部長であったチャールズ・リーバー教授が中国政府の「千人計画」への関与を米当局に虚偽報告したとして、2020 年 1 月に逮捕されたものである。その裁判で明らかになった事実としては、2011 年に中国の武漢理工大学と契約を結び、月額 5 万ドル（約 550 万円）の給与と、同大学にナノテクノロジーの研究所を設立するための資金として 150 万ドル以上を受け取っていたとされているが、同時に米国立衛生研究所（NIH）や国防総省から合計 1500 万ドル以上の研究助成金を受け取っていたにもかかわらず、これらの外国からの資金提供を申告していなかった。2021 年 12 月、ボストンの連邦地裁の陪審団は、リーバー教授に対し、虚偽陳述や税の虚偽申告など 6 つの罪で有罪の評決を下ししている。この事件に関連して中国人研究者 2 名も起訴されているが、1 人はボストン大学でロボット工学を研究していたイエ・ヤンジン被告であり、人民解放軍の軍人であることを隠していたとされている。もう 1 人はがんの研究者であったジェン・ザオソン被告で、ボストンのローガン国際空港で生体サンプル 21 個を所持していたところを逮捕されている。

これらの事件において以前から懸念されていた High Risk Partnering や Foreign Influence が実際に知的財産の窃盗につながっていることが示されていく。米国で生じた別の事例では、基礎研究に従事している研究室に所属した留学生が、その研究室が行おうとする実験の詳細な計画や実験装置などの情報を用いて、出身国に設けた研究室で秘密裏に全く同じ実験を行なっていた事案なども報告されている。Mirror Research あるいは Shadow Laboratory と称されるこのようなケースは他の事例でも発覚しており、基礎研究であったとしてもその過程にある守られるべき知的財産の窃盗として問題視された。こ

れらの事例が示しているように、論文として公開されない実験方法やノウハウ、または応用に関する情報など公になっていない情報は管理されるべきであり、研究グループに参加する人の管理や、共同研究などを行う場合の連携先についても管理対象とするべきということが強調されるようになっていく。

日本でも最近、国立研究機関において出身国において会社を設立して、無届の取締役兼業を行い、発明情報を送信して、兼業先から特許を出願したことが疑われる事案も発生している。さらに最近では研究室の成果にたいして投資をちらつかせ会社設立を持ち掛けて技術を取得しようとすることが疑われるケースなども生じている。

これらのケースでは、おおむね公開情報からリスクが把握できることが分かっている。したがってこれらのリスクに対する対処としては公開情報による調査（Open Source Due Diligence）が有効であるとされるようになったのである。

ここに至って学術研究における知的財産の窃盗を防ぐための Research Security の概念と、その対策としての Open Source Due Diligence などの Risk Identification とその対策としての Risk Mitigation の考え方が確立されていくことになる。

このような背景を踏まえ、昨年 6 月 24 日に Open Source Due Diligence をトピックとする会議「研究セキュリティとオープンソース・デューデリジェンスに関する国際フォーラム」を行い、さらに 2025 年 1 月 21 日には、日本、米国、カナダの政府と大学からなる「日米加大学研究セキュリティ・インテグリティ国際ワークショップ」が行われた。

本提言はその会議の提言として示された内容を、背景も含めて整理したものである。

３．用語と概念の整理

本提言で用いられる用語と施策の概念について以下に記載する。

①リサーチセキュリティの概念

本提言は「研究セキュリティ（Research Security）」に関するものである。しかし研究セキュリティ（Research Security）は新しい概念であるため、文脈や組織によってさまざまに使われてきた。以下にその代表的なものを上げる

1. G7 の定義

カナダ政府が主導し G7 に設けられた「グローバルな研究エコシステムにおけるセキュリティとインテグリティ（SIGRE）ワーキンググループ」は、2022 年 6 月に「研究セキュリティと研究インテグリティに関する G7 共通の価値観と原則」[2]を公表している。この文書では、研究セキュリティを「経済的、戦略的なリスクや国家的、国際的な安全保障のリスクをもたらす行為者や行動から研究コミュニティを保護する活動」と定義している。具体的には、研究に対する不適切な影響、干渉、悪用のリスクや、国家、軍隊、非国家主体、組織犯罪活動によるアイデア、研究成果、知的財産の窃取などが含まれるとされる

[2] https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/international-research-security-resources/g7-common-values-and-principles-research-security-and-research-integrity

2. 米国国立科学財団（NSF）の定義[3]

NSF は、研究セキュリティを「国家または経済安全保障を害する研究開発の不正流用、それに関連する研究インテグリティの侵害、外国政府による干渉から、研究活動を守ること」と定義している。

3. 日本政府の定義[4]

日本においては、2024 年 12 月に文部科学省より発出された「大学等の研究セキュリティ確保に向けた文部科学省関係施策における具体的な取組の方向性」においては、外国への技術流出等につながる、外部からの不当な影響・干渉のリスクから研究を守ることとされている。

これらの定義は、共通して研究活動を外部からの脅威や不正行為から保護し、研究の健全性や公正性を維持することを目的としている。この点従来の Research Integrity Management として位置づけられる研究倫理管理などにおいては、Integrity を棄損することなく維持するために、自らを律することが中心になるが、Research Security Management においては、悪意のある他者（G7 では Bad Faith Actor という用語で説明されている ）からの知的財産の窃盗を防ぐことが中心となる点で異なる。

表現や焦点は異なるものの、悪意ある他者に対する備えを行うことで研究コミュニティを保護する重要性が強調されることは共通であると思われるが、日本の定義はやや広く研究インテグリティを含んでいる点整理が必要ではないかとの意見もみられる。

本提言では後述する今回の会議における議論を踏まえ、研究セキュリティの定義を再度確認する必要があるとしている。

②リサーチセキュリティを担保する方法

このような研究セキュリティ（Research Security） を担保するための管理としては、大きく分けてリスクの発見（Risk Identification） とリスクの低減（Risk Mitigation）があげられる。以下にそれぞれの概念について述べる。

リスクの発見（Risk Identification）：研究セキュリティにおけるリスクの発見とは、研究データや知的財産の保護を脅かす要因を特定するプロセスであるとされている。内部リスクとしては、研究者・学生の意図的または偶発的な情報漏洩の他、研究データの不適切な取り扱い、悪意のある内部関係者による情報持ち出し、研究室や研究機関のシステムに対する不正アクセスなどがある。また外部リスクとしてはサイバー攻撃、などに加え国家・産業スパイによる知的財産の窃取、物理的セキュリティリスク、研究室やデータセンターへの不正侵入、研究機材・試料の盗難や破壊などもあげられる。特にパートナリングや研究者の配属などにおいてリスクが生じていないかを、Due Diligence を通じて確認することが重要であるとされる。この際に重要となる Open Source Due Diligence については、後述する 2024 年 6 月の会議に関する報告において詳しく述べる。

リスクの低減（Risk Mitigation）：リスク低減とは、特定されたリスクに対して適切な対策を講じ、被害の発生確率や影響を最小限に抑えるための手段である。これには技術的対策や、研究データやシステ

[3] https://www.nsf.gov/news/nsf-announces-guidelines-agency-research-security
[4] https://www.mext.go.jp/content/20241219-mxt_kagkoku-000039301_2-1rrr.pdf

ムへのアクセスを最小限に制限（ゼロトラストセキュリティの導入）、多要素認証（MFA）やログ監視の実施、データ保護・暗号化、サイバーセキュリティ対策などの対策に加え、組織的対策として情報管理ポリシーの策定と徹底、研究室やデータセンターへの入退室管理（IC カードや生体認証の導入）などがあるとされるが、サイバー対策や物理的対策以上に人を通じた流出を防止するための管理が重要であるといわれる。この場合の Risk Mitigation の施策としては、パートナリングする分野を限定することや、特別のモニタリングを加えること、採用する場合も同様、従事する研究分野を限定したり、モニタリング対象とするなども行われる。このようなリスク低減措置を行ってもなお許容できるリスクでないと判断される場合は、パートナリングや採用そのものを断念するということもあり得る。

これらのプロセスが研究セキュリティマネジメントにおいて必須であるとしたときに、オープンソースの情報を補完するリスク情報を幅広く国際的に共有することは有益である。また Risk Mitigation においてもその判断の相場観などを、カナダや米国の大学の事例を共有しながら醸成していくことは有益である。このような観点も加味して、2 つの国際会議を実施した。以下にその概要を記載する。

４．研究セキュリティに関する２つの国際会議報告

これらの経緯を経て、以下 2 つの国際会議が実施された。その要約と、最終的にカナダ、米国の大学と政府との議論の場で提案された提言について述べる。

①　「研究セキュリティとオープンソース・デューデリジェンスに関する国際フォーラム」[5]（参考資料３）

2024 年 6 月 24 日に行われたオープンソース・デューデリジェンス（Open Source Due Diligence）をトピックとする国際フォーラムについて以下に述べる。

この会議は、研究セキュリティとオープンソース・デューデリジェンスに関する国際フォーラムとして、日米カナダの政府、大学および企業を招待者として議論が行われたものである。会議では、日本政府の経済安全保障政策の最新動向、G7 における研究セキュリティとインテグリティに関する取り組み、カナダにおける研究セキュリティの実践例が紹介されたほか、日米の事業者によるオープンソース・デューデリジェンスに関する具体的な実施方法の紹介があった。その後カナダ政府の研究セキュリティに関する政策、日本の大学の研究セキュリティの課題などの紹介の後、日本の大学のコンソシアムによる取り組みなどに関してパネル討論において意見交換が行われた。

その中で紹介されたカナダの大学における研究セキュリティの取り組みについては、トロント大学のポール・ジャレット氏から紹介された。カナダ政府は、研究セキュリティセンターを設置し、大学への助言や政府助成金に係るデューデリジェンスを実施している。機微な研究分野や指定研究機関リストを定め、リスクの高い研究領域や組織を特定していることや大学は研究セキュリティチーム（チーム・カナダ）を設置し、研究パートナーに対するデューデリジェンスやリスク評価を行っていることが紹介された。またトロント大学では、国家安全保障の専門家によるデューデリジェンスチームを設置し、他大学とのコンソシアムを形成してベストプラクティスを共有している。カナダの事例を踏まえた今後の課題と

[5] https://ifi.u-tokyo.ac.jp/event/18558/

して、大学のコンソシアム結成、ガイドラインの策定、米国・カナダとの連携、スタートアップ支援、セキュリティ・クリアランスの活用など、今後の課題が提起された。あわせて経済安全保障政策の政府の立場からは、大学への追加的な支援やリソースの提供など、総合的な施策の必要性が指摘された。 具体的には、カナダに倣い日本版の「チーム・ジャパン」に相当するコンソシアムを結成し、政府の支援を受けながらガイドラインや手順書を作成することが提案されたが、あわせて外部の知見や情報を活用し、大学の負担を軽減することが重要であると強調されるとともに、米国・カナダとの情報共有や共同での取り組みも有効であると指摘された。 さらに、ペーパーミリングと呼ばれる論文の不当な作成と、不当な論文に基づく大学の誤った（高）評価への対応、大学発スタートアップへのデューデリジェンス支援の必要性や、セキュリティクリアランスホルダーによるガバナンス体制の構築も課題として挙げられた。これらに取り組むため今後、定期的に国際会議を開催し、具体的な施策を検討することが提案された。加えて 大学発スタートアップへのデューデリジェンス支援体制を構築することや、これらの一般研究においてもセキュリティクリアランスホルダーが関与したガバナンス体制が有効であることが提案された。

最後にこれらの議論をさらに発展させるため、米国も加えた議論の場を 2024 年度内に持つことが提案された。

② 「日米加大学研究セキュリティ・インテグリティ国際ワークショップ」2025 年 1 月 21 日[6]（参考資料４）

前述した会議を受けて 2025 年 1 月 21 日に行われたワークショップの概要について述べる。本ワークショップの目的は、研究の安全性と完全性（インテグリティ）を確保するための国内外の協力の在り方を議論し、実践的なアプローチを共有することにあった。科学技術とイノベーションの発展には、国際的な共同研究が不可欠である。しかし、近年、研究成果の流出や悪用のリスクが高まり、各国政府や大学が対応策を求められるようになった。特に、研究の透明性とセキュリティのバランスを取ることが課題となっており、日本、米国、カナダはそれぞれの政策や取り組みを紹介しながら、今後の協力体制について議論した。

ワークショップの中心議題の一つが、研究セキュリティとインテグリティの確保である。「インテグリティ（Integrity）」という言葉は、日本語では明確な訳語がないが、研究者と社会の契約としての意味を持つ。研究の透明性を担保し、公正で信頼できる環境を維持することが求められる。一方で、「セキュリティ（Security）」の観点からは、研究成果や技術情報が悪用されるリスクを防ぐための対策が不可欠である。

近年、日本国内外で研究不正や技術流出の問題が指摘されている。例えば、意図せざる共著問題：研究者が知らない間に共同研究者として名前を利用されるケース。利益相反の懸念：企業との共同研究において、特定の企業利益のために研究結果が歪められるリスク。技術情報の流出：研究データやノウハウが国外に不正に持ち出される問題。これらの問題に対応するため、北海道大学、東京大学、京都大学、大阪大学、九州大学など 9 つの主要大学がコンソシアムを設立し、国際的な連携を強化することが決定されたことが報告された。

会議では 米国における研究セキュリティの取り組みが共有された。ハーバード大学の事例としては米

[6] https://ifi.u-tokyo.ac.jp/event/19210/

国の大学は、研究セキュリティの管理を強化しており、ハーバード大学ではデューデリジェンス・ガイドラインを策定し、研究者の雇用や共同研究のリスク評価を行っている。ハーバード大学の対策としては、研究者の Due Diligence（過去の共同研究や資金提供元のチェック）、研究データの保護強化（クラウドやアクセス権限の管理）、研究倫理とコンプライアンス研修（定期的なトレーニング実施）などである

また米国政府の研究セキュリティに関する政策として、米国政府は、国家安全保障大統領覚書第 33 号（SPM33）を通じて、大学に対して研究セキュリティ計画の策定を義務付けている。これにより、輸出管理の強化（軍事転用可能な技術の管理）、知的財産保護（特許申請前のデータ流出防止）、政府機関との連携（大学と政府の情報共有）が進められている。

他方 カナダの研究セキュリティと「チームカナダ」の取り組みについても紹介された。カナダ政府は年間 2,500 万ドルの研究セキュリティ基金を設立し、大学に対する資金提供を行っている。この基金は、セキュリティチームの設立（大学内に専門チームを配置）、サイバーセキュリティ対策（デジタルフォレンジック分析の導入）、国際連携の強化（日米の大学との共同対策）に充てられるとの報告があった。

大学の取り組みとしては、カナダの研究セキュリティ強化のため、カナダ国内の 66 大学が参加しチームカナダが発足している。この組織では、情報共有とリスク評価、研究者向けトレーニングの実施、政府機関との連携強化を推進している。

５．２つの会議を受けての提言

「日米加大学研究セキュリティ・インテグリティ国際ワークショップ」の最終とりまとめ都提言として、下記が提案された。

第一は、日米カナダの大学と政府は、アカデミアの自由で国際的な研究の在り方に対して、基本的に同じ価値観を有しており、かつ現下に生じている研究インテグリティに対するリスクの存在を共有していること、その点この 3 か国がそれぞれの、大学コンソシアムやそれに相当する組織、およびそれを支援する政府が相互に協力を行いそのアプローチ方法を共有することはとても有益であることが認識された。具体的な協力体制についての議論が重要である。

第二に研究インテグリティと研究セキュリティの概念については G7 のワーキンググループでも整理を試みたものではあるが、特に研究セキュリティについては、今一度日米カナダで統一した概念を確認してその考え方にたいする信頼感を高め、それを研究現場と共有していくことが大事である。

第三に、研究インテグリティと研究セキュリティについて同じ概念を共有したからといって、その目標に向かう際に全く同じやり方を行うことではなく、日米カナダのそれぞれの取り組みを共有しながら、他方自分に合ったやり方、違いを認識しながら進めること望ましいことが強調すべきである

これらを踏まえながら、様々なリスク、さらに意図せざる共著の問題や、ペーパーミリングへの対処などについても取り組む国際的協力体制をつくっていくことが重要である。さらにこれらの取り組みの方向性については、日米カナダだけではなく、G7 の各国でも同様と考えられるため、2025 年の G７サミッ

ト（カナダ政府が議長国を務めアルバータ州のカナナスキスで開催する予定）において、政府間の連携を深めて価値観を同じくする大学の機能、具体的には自由な研究と知の探求などを最大限に活かせる環境整備を進める機会とすべきである。

６．備考：その後の日本の取り組み

本提言に至る過程における議論を踏まえて、チームカナダ及び米国大学との情報共有等の協力とキャパシティビルディングなどを担う大学セキュリティコンソシアムが結成されている。これは北海道大学、東北大学、東京大学、東京科学大学、電気通信大学、名古屋大学、京都大学、大阪大学、九州大学の 9 大学が参加した取り組みである（任意団体、設立 2025 年 1 月 14 日）（参考資料５）。また政府においては、研究セキュリティ・インテグリティに関するリスクマネジメント体制整備支援事業が開始される予定で公募[7]も始まっている。今後これらの施策を土台として本提言で示された国際協力を進めていくことが期待される。

[7] https://www8.cao.go.jp/cstp/kokusaiteki/integrity/kobo_r7.html

国際シンポジウム「グローバル競争の中での自立した大学のあり方　社会との連携とガバナンス・コンプライアンス」開催報告

未来ビジョン研究センター

掲載日：2015年2月27日

実施日： 2015年01月28日

文：東京大学政策ビジョン研究センター副センター長・教授　渡部俊也（本シンポジウム オーガナイザー）

東京大学政策ビジョン研究センターと政策シンクネット主催で、「社会と連携する大学のあり方」について議論をすることを目的とした国際シンポジウム「グローバル競争の中での自立した大学のあり方：社会との連携とガバナンス・コンプライアンス」が開催されました。世界9ヶ国の大学から15人のゲストを招いて「産学連携」「機微技術と大学」「研究不正と利益相反」「社会との連携のための人材育成」の4つのパネル討論が行われました。

かねてより産学連携をトピックとした会議は少なからずあったと思いますし、また最近問題が頻出するようになった研究不正や大学の研究にまつわる利益相反を扱う会議も増えてきています。しかしこれらの議論は、今までは異なるトピックスとして別々に行われてきたのではないかと思います。どうやって大学の技術をイノベーションに効果的に生かしていくかという、産学連携や技術移転推進施策はポジティブな話題であり、総合科学技術イノベーション政策で取り組まれてきた中核的な課題です。科学技術政策の推進に伴って国税を投じた研究費も増加しており、研究面での大学と政府との関係もより深まっています。

これは日本だけでなく産学技術移転を主導してきた米国や、規制緩和の流れから産学連携が進展したイギリス、日本で最近注目されている橋渡し機能を組み込んだシステムを有するドイツなどにも見られる世界的な傾向で、今回の会議でもアイルランドのような小国でも大学からの技術移転を政府主導で進めて成果を出している事例（Alison Campbell博士）が報告されました。一方で政府が大学への予算をカットして産学連携も沈滞しているオーストラリアの事例（Kevin Cullen博士）なども紹介され、改善すべきであるとする問題提起なされたように、大学と社会との関係は各国政府の政策による大きな影響を受けています。同時にインターネットや情報技術の発展によりコミュニティーとの連携も容易になったことで、大学研究者が独自に社会との連携を深めることも盛んになりました。この結果、産業界だけでなく大学と社会との関係は政府や一般社会との関係を含むより緊密なものになったと言えます。日本でも1990年代の後半以降進められた産学連携推進施策によって進展した産業界、政府や一般社会との関係は、日本の大学が戦後長い間象牙の塔であった時代があったことからすれば隔世の感があります。

一方で、日本では最近STAP細胞問題に象徴される研究不正にまつわる事件が増加しています。こちらは科学への信頼の失墜につながりかねない深刻な課題として取り上げられています。かつては研究不正の問題というのは一部専門家だけが関心を寄せる課題でしたが、ここに来て一般社会が懸念を抱く問題になっています。同時に比較的最近、研究成果の不適切な利用の可能性という問題も生じてきました。その例としては日本の研究者が参加したバイオ関係の研究論文発表が、テロに利用される可能性があるとして、米国政府機関によって公開制限を受けるというケースが生じました。過去にも原子力やミサイル技術に転用できる制御技術など、いわいるDual Use（規模技術）と呼ばれる技術情報の取り扱いについては、輸出管理面から法的規制が加えられてきましたが、これらの技術ではそれなりの設備が必要であるなどの技術開発上の制約から管理は比較的容易であったといえます。しかし、この事例のようなバイオ合成技術においては、知識そのものが悪用されることによって大きなリスクとなることから、基礎研究成果の公表の是非という問題が発生しているものです（Paul Keim博士）。最近日本でも防衛研究に産学連携が活用されるなど科学技術研究の軍事転用の問題にも世間の注目が集まるようになってきています。いずれも大学や公的研究機関の活動と社会との接点において生まれた新たな課題であると考えてよいと思います。

実はこれらの問題を掘り下げていくと、単に大学と社会の関係に生まれたという共通点だけではく、それ以上にこのポジティブ、ネガティブな2つの現象は、相互に因果が絡み合っている事象であることに気づかされます。今回の会議で示された事実として、米国においても日本においても、大学が社会との関係を緊密化した時期と研究不正や利益相反の問題が増加した時期はぴったり一致しているのです。米国では1980年に政府資金による研究成果の移転を促進するためバイ・ドール法が制定され、その結果として産学技術移転が盛んになりましたが、日本でも同様に1999年の日本版バイ・ドール法の制定以降、研究不正や利益相反の問題が顕在化して、現在も増加しています。その因果は複雑で、たとえば大学や研究機関と企業などとの2つの異なるミッションを有する機関と、金銭的な関係を結ぶ、あるいは双方の機関に責務を負うことで生じる利益相反は、研究不正の有力な促進要因として働くことが知られています。

また各国の科学技術政策の推進に伴い、優れた研究成果を求める競争環境の激化が研究不正の原因になることが分かっています。同時に最近は科学技術政策の目的がイノベーション促進としての性格を強めていることもあり、大学や研究機関は組織として、または研究者個人も、益々複雑な金銭的あるいは責務を含むさまざまな利害関係を構築するようになりました。研究不正や利益相反の疑いによって、大学や研究機関が社会からの期待が裏切られれば、それはその組織だけでなく、そこで研究に従事する研究者にとっても大きな損失であり、そのことは研究活動や産学連携の減退にもつながります。そういう意味でこの会議で扱ったポジティブ、ネガティブと称した2つの現象は、コインの表裏であり、科学技術イノベーション政策の側面から見れば車の両輪であるともいえます。この2つの現象に対して科学技術イノベーション政策はどのように扱い、どのように導いていけば、望ましい姿に近づけるのでしょうか。

米国では、このコインの表裏の現象、社会との連携の活発化と研究不正などの問題点が同時に深刻になってきたときに、盛んに使われるようになった概念があります。それはResearch Integrityという言葉で表されるものです。現在米国ではOffice of Research Integrityという政府機関があり研究不正に関する監視や情報収集などを行っていますが、日本語ではこの機関を研究公正局と訳すことが多いようです。一般的に「公正」であれば英語ではJusticeですが、このIntegrityは単なる「公正」というよりもはるかに幅広い概念を有していて、たとえばmisconduct を防止してIntegrityを維持するというような使われ方をします。Integrity の語源は「完全な」を意味するラテン語の Integer だといわれています。使われ方によって「高潔さ」「真摯さ」「正直で誠実」などとも訳されていますが、特にここでいうResearch Integrityはこれらの訳語がそのまま当てはまらない、日本語に訳しにくい概念です。ここではとりあえず「大学や研究機関が維持しなければならない社会から見て欠陥のない状態」を指すと考えたいと思います。

今回の会議では、Research Integrityという概念は、1980年以降、社会との連携を急速に進めた米国の大学が、その存在価値を維持するために生み出した、あるいは生み出さざるを得なかった概念であるのではないかという意見も示されました（上山隆大教授）。調べてみるとこのResearch Integrityという言葉も、やはりバイ・ドール法が施行された1980年代以降に盛んに使われるようになっています。今回のゲストであるハーバード大学のコンプライアンスオフィサーであるAra Tahmassian博士は、発表資料の中でこのResearch Integrityを「研究者と社会との契約である」“Research Integrity is a contract between researchers and the society."と称しています。つまりはコインの表裏ともに、そこでなすべきことはすべて社会との契約の一側面であるということになります。そして、「そしてそれは強制することはできず、関係者が自ら実践すべきことである。」“It cannot be enforced, it must be practiced by all involved."とも述べていることは重要だと思います。

我々は社会との連携を深める大学とそこで遭遇する問題について、たとえば「産学連携の推進」と「利益相反の防止」という別々の施策で捉えてきたものと思われます。産学連携の促進と研究不正の防止は別々の組織が担当して、これらを大学経営の問題として捉えることは少なかったのではないかと思われます。しかしこの2つの事象は別々なものではなく、社会との連携を深める大学が「Integrityを確立する」ことであるという意味で、社会と連携する大学のあり方そのものとして考えるべきなのではないでしょうか。

今回の会議は慶応義塾大学と連携して、大学や研究機関全般を対象としたシンポジウムという位置づけで実施いたしました。過去今回のテーマと関係するイベントとしては、国立大学のあり方に焦点を当てたシンポジウム「国立大学法人法施行から10年–大学改革とイノベーションへの貢献」を2013年10月12日に実施し、法人化後10年社会との連携を深める国立大学のあり方を議論しております。その議論の帰結として「国立大学法人は、産学連携政策を含む現在の大学に関係する多様な政策の統合主体として役割を果たすべきである。」という提言をいたしました。それは2004年以降はじまった大学法人として産学連携に従事する際に、政府主導で産業界の多様なニーズに応えるためのさまざまな政策制度に対応しようとしてきたため、結果的に効率の悪い対応を余儀なくされた面もあったことが背景にあります。そのことを踏まえ「大学の独立したマネジメントによって科学技術政策や産学連携政策等、大学が関わる多様な政策の統合をも実現することが期待される。政府も政策立案と実装に際して、このような大学の役割と機能にもっと注目するべきである」として「独立性が求められる大学が自ら社会との関係性のあり方を提案する試みは、さらに具体的な10年計画の姿を明らかにしていくために、2014年4月に法人化10周年を迎えるまでの活動に引き継がれる」と結んでいます。

今回の国際会議は、議論の対象は国立大学だけでなく、広く世界の大学や研究機関を対象としたものですが、「Integrityを確立することによって社会との連携をよりいっそう深めることが可能となる大学の将来像」を見出すことができたのではないか、という意味において国立か私立か、大学か研究機関かという領域を超えて、2013年の会議を引き継ぐ位置づけでもあったということもできると思います。

そうであれば今後10年、そして次期科学技術イノベーション政策においては、社会との連携を深める大学と公的研究機関のIntegrityの確立のための諸政策が盛り込まれる必要があるということに帰結します。企業とは異なる大学の特徴を自立的に発展させた形でのIntegrity をより高める産学連携のあり方と制度、利益相反の対策や研究不正の防止を目的とするのではなくIntegrityを確立する大学や研究機関の取り組みと、これを支援する諸施策など、このような考え方のもとに具体的な政策を検討することが必要と思われます。

本会議を契機としてこのような政策の検討をさらに具体的に進展させるために、引き続き「大学と社会」の研究をさらに深めていきたいと思います。

photos: Ryoma. K

本シンポジウムの全映像データは、東大TVおよび iTunes にてご覧いただけます。
東大TV：討論・報告「グローバル競争の中での自立した大学のあり方」の動画 日本語 英語
iTunes： 国際シンポジウム「グローバル競争の中での自立した大学のあり方」（日本語）配信者: 東京大学

開催概要

国際シンポジウム「グローバル競争の中での自立した大学のあり方：社会との連携とガバナンス・コンプライアンス イベント詳細（配布資料・発表資料掲載）

【日時】 2015年1月28日（水）9:30-17:30

【会場】 東京大学本郷キャンパス 鉄門記念講堂（医学部教育研究棟14階）

【主催】 東京大学政策ビジョン研究センター、政策シンクネット

【共催】 大学技術移転協議会

【参加費】 無料

【言語】 日英同時通訳

参考リンク

国際シンポジウム「グローバル競争の中での自立した大学のあり方 - 社会との連携とガバナンス・コンプライアンス」（2015年1月28日開催）

バイドール制度の各国比較（古谷真帆 / 渡部俊也）Pari WP 14 No. 17

シンポジウム「国立大学法人法施行から10年 - 大学改革とイノベーションへの貢献」（2013年10月12日開催）

政策提言「国立大学法人法施行から10年 - 大学改革とイノベーションへの貢献」

社会との連携とコンプライアンスという両輪 - 渡部俊也教授に聞く

関連URL：http://pari.u-tokyo.ac.jp/event/smp150128_rep.html

国際シンポジウム「グローバル競争の中での自立した大学のあり方」にて

政策提言
米国大学が行うハイリスクパートナリング管理の実態と日本の大学への示唆（暫定版）[1]

産学および社会連携システム研究ユニット
代表 渡部俊也

2019/2/27

1. はじめに

本稿は、米国ハーバード大学が実施しているハイリスクパートナリング(High Risk Partnering)のマネジメントについての調査結果を参考に、最近の技術に関する安全保障をめぐる国際情勢の変化が、大学の産学連携にどのような影響を及ぼすのか、また大学はこれに対してどのような施策を取るべきなのかについて検討したものである。

本稿の検討のベースとなっている大学のリスクマネジメントについての考え方としては、2015年1月28日に実施した国際シンポジウム「グローバル競争の中での自立した大学のあり方：社会との連携とガバナンス・コンプライアンス」[2]において議論された Research Integrity に基づく大学のマネジメントである[3]。このシンポジウムにおいては、企業との連携で生じる利益相反や安全保障輸出管理などのリスクマネジメントの問題への対処として、Research Integrity に基づく考え方が議論された。本稿で扱う安全保障管理にかかわる問題への対処も、同様の考え方に基づく。

またもう一つ本論のベースとなっている、より実務的なレポートとしては、2015年3月に発表した「大学と社会政策提言：知的財産制度と産学連携に関する論点」（東京大学政策ビジョン研究センター大学と社会に関する研究ユニット）[4]がある。こちらはさらに具体的に外国企業との連携や技術移転の際に生じる論点について整理を行い、実務的な提言を行ったものである。

すでにこの提言を発表したのち、4年近くが経過した。その過程で、後述する2018年のNDAA法などに象徴されるような、米国の安全保障政策の変化がおきたことで、追加の検討が必要になっている。しかし現時点でこの政策提言そのものについて変更をおこなうべき事由が発生したとは考えてはいない。むしろ現下の新たな情勢をうけて、2015年の提言をベースに、これらの情勢に対応するために追加的にリスクマネジメントが必要になってきているとする立場にたっている。そのため本稿は、2015年の国際シンポジウム及び同年に行われた提言を発展させ、新たな情勢に対応するための追加的なマネジメントを提言するものである。

2. 米国大学のハイリスクパートナリング管理と、2018年以降の安全保障管理強化への対応

2.1 ハーバード大学のハイリスクパートナリング管理

米国の安全保障政策における技術情報の取り扱いについての大きな転換点は、2018年に成立したNDAA (National Defense Authorization Act) [5]である。8月13日に成立した同法では、国防上問題視する５つの企業グループと米国政府の取引制限を盛り込んだものである。この規制の決定以降、米国大学は、制裁リストに記載されている企業とのあらゆる契約が存在すると、米国の政府研究費が得られなくなることから、寄付研究を含むあらゆる契約を行うことが事実上できなくなった。その後、米国政府の制裁対象は、半導体分野をはじめとして、NDAAに明示された対象企業以外にも範囲を拡大しており[6]、また同時に大学の研究室における研究者や大学院生によるスパイ活動も問題視していることは注目すべきである[7][8]。

このような米国の安全保障面での技術管理の強化は、様々な影響を大学におよぼしている。ここでは主にハーバード大学における当該分野におけるリスクマネジメントの状況とNDAAへの対応を事例として、その考え方や対応について述べる[9]。2018年8月のNDAA法成立以降、制裁リストに掲載されている企業とは、何等か関係を有することで政府の研究資金の獲得ができなくなることになったため、同リストに記載のある企業との一切の契約に対して解除通告を行っている。この対応そのものは明示的に政府が示した規制に対する対応であるが、NDAA以前からハーバード大学では、FBIや政府関係機関の情報などから、8月にNDAAの制裁リストに記載された企業に対して、連携することによるリスクが高いとして（この際のリスクの評価については後述する）、これらの企業との関係をリスクマネジメント対象として管理を行ってきた。

法令で明示的に禁止されていないにもかかわらず、ハーバード大がこのような管理を行う理由としては、①非公知である大学の保有する重要技術情報または知財の流出リスクへの対応と、②そのようなリスクがあるとみられている企業との連携を行うことに対するレプテーションリスクの2点であると説明されている。前者に関しては、非公知情報を問題にしているのであるから、研究成果が公開されパブリックドメインを経由して技術情報が伝達されることについて規制をすることはない。したがってこれらリスクが高いと考えられる企業からの寄付や Sponsored Research をうけたとしても、公開された研究成果について結果の報告を行うことは問題がないが、その過程で非公知の技術情報やノウハウなどが伝達されることは認めていなかった。同様先方企業のメンバーが研究室を訪問する際、またはハーバードの研究者が先方の施設等を訪問してクローズドの講演などを行う際にも、非公知情報の提供がなされることは認めていない。

このような考え方に基づき、ハーバード大学を含む米国有力大学でのハイリスクパートナリングへの対応は、ハーバード大学へのヒアリングの結果、おおむね下記のような対応が行われてきたことがわかっている。

① 当該企業との連携についてはコンプライアンス機関の評価を受け許可を求めるとともに、コプライアンス機関は、その後も連携を実施する上でのアドバイスを行っている（職務規則上、該当する事案があれば自己申告や相談を行うことが義務付けられている。その情報をもとに、コンプライアンス機関は当事者にヒアリングするなどを行ってアセスメントを行い、必要なアドバイスを行う）

② 当該企業からの研究に対する純粋な寄付（何ら制約を課さない、知的財産権の保持、未公開の研究情報の提供を行わない）は実施可能としている

③ 上記の知的財産権の保持、未公開の研究情報の提供を行わないなどの条件を満たす当該企業との Sponsored Research は実施されている。または、契約上同種の条件が満たされる

場合は Contract Research も認められる可能性がある

④ 非独占的条件での技術移転や知財ライセンスは実施することがある

⑤ 当該企業との連携における情報機器装置の提供については学内のネットワーク等との接続を規制している（情報機器の接続を求めないのも、非公知情報の取得が可能である可能性を排除する意図によるもの）

⑥ 当該企業を含む訪問者に対しては、知財保護などを規定した定型の訪問者契約にサインさせることを求める（Visitor's participation agreement による）

⑦ 当該企業に限らず、大学発ベンチャーや起業家への支援資金を大学が受け取って実施することはない（投資規制を意識したものという側面もあるが、大学発ベンチャーが大学法人とは別個の法人であるから関与しないという側面が強いが、一方大学スタートアップが、大学の技術のライセンスを求めている場合はそのスタートアップに対する投資がどこから行われているかについて、例えば、中国の産業投資ファンドである場合などについては慎重に調査を行っている）

などである。加えて、

⑧ またいわゆる孔子学院（中国が海外の大学などの教育機関と提携し、中国語や中国文化の教育及び宣伝、中華人民共和国との友好を目的に設立した機関）の受け入れは行わない（いわゆる孔子学院についての対応に関しては、技術情報の流出を懸念したものというよりは、学問の自由に対する規制を含むことが問題にされたもので、①には該当しないが、②に関係するとみてよい。経緯としては 2014年6 月に、American Association of University Professors が「孔子学院は中国国家の手足として機能しており、『学問の自由』が無視されている」と批判し関係を絶つよう各大学に勧告したことを契機としている）[10]。

ハーバード大学では、これら特定の企業との交流や連携をハイリスクパートナリング（High Risk Partnering）とみなしてマネジメント対象としている。

これらの企業との連携に制約を課する際、交流を制約される研究者に対する説明としては、FBI などの提供情報を示して説明が行われている。基本的には客観的な情報をもとに、リスクの存在を説明し、そのリスクに対しての合理的対処としてモニタリングや忌避などの管理を説明するとしている。

2.2 2018年NDAA法案成立後の対応

このような対応状況に加え2018年のNDAA法成立の影響により、上記の事情に加え新たな対策がなされている。まだ細部の政策が確定する以前のNDAA成立当初から、その動向や今後の見通しなどについてハーバードのコンプライアンス部門は調査分析を行っており、逐次大学幹部に報告を行ってきた。

この後のアクションの第一としては、NDAA制裁企業に対しては、寄付研究を含むすべての関係は、これらの企業との Procurement とみなされることから、その猶予期間内での契約解除通知を行っている。この点リスクを低減させるという従来のマネジメントから、リスクを事実上ゼロとするゼロトレランスの規制対応へ移行することになったといえる。ただし引き続き制裁リストにない外国企業との間の連携についても、自主的に評価を行いリスクのアセスメントを行うという仕組みは継続され、NDAA以

降はこのような管理をさらに充実させ強化している。具体的にはNDAA制裁リスト以外の外国企業についてもリスクが高いと思われる企業との連携に関しては新たに Guidelines for Sensitive Negotiations を策定して対応を行うことを検討しており、これがNDAA後の新たなアクションの 2 番目となる。ここで記載する Guidelines for Sensitive Negotiations についてはハーバード大学から一般に公表された資料はないが、Ara Tahmassian, Ph.D.（Chief Research Compliance Officer, Harvard University）へ 2018年に行った複数回のインタビューによって得られた概要を以下に解説する。

ここでリスクとみなされているのは、従来と同じく重要非公知技術情報（知財）の流出とレプテーションリスクの 2 つである。以降この Guidelines for Sensitive Negotiations の考え方について、概要を述べる。

まずここでいうハイリスクパートナーシップとして扱われるケースは

① 研究者からの申告などに対する大学によるアセスメントの結果
② 研究機関スポンサー、ドナー、大学の知的財産権への資金提供者からの指摘
③ 国家安全保障上の懸念から第三者（国家安全保障機関や外部資金提供者など）による行政または規制上の決定

などにより指定する

最近の事案としては、トルコのサウジアラビア総領事館で殺害されたと報じられるジャマル・カショギ記者の事件に関与したとされるサウジアラビアに関しても、サウジアラビアの投資資金がはいったプロジェクトがアセスメントの対象となった。このように、ハイリスクの認定のきっかけは政府機関だけでなく、研究機関スポンサー、ドナー、大学の知的財産権への資金提供者からの指摘もあるとされており、サウジアラビアのケースは後者であったものと思われる。

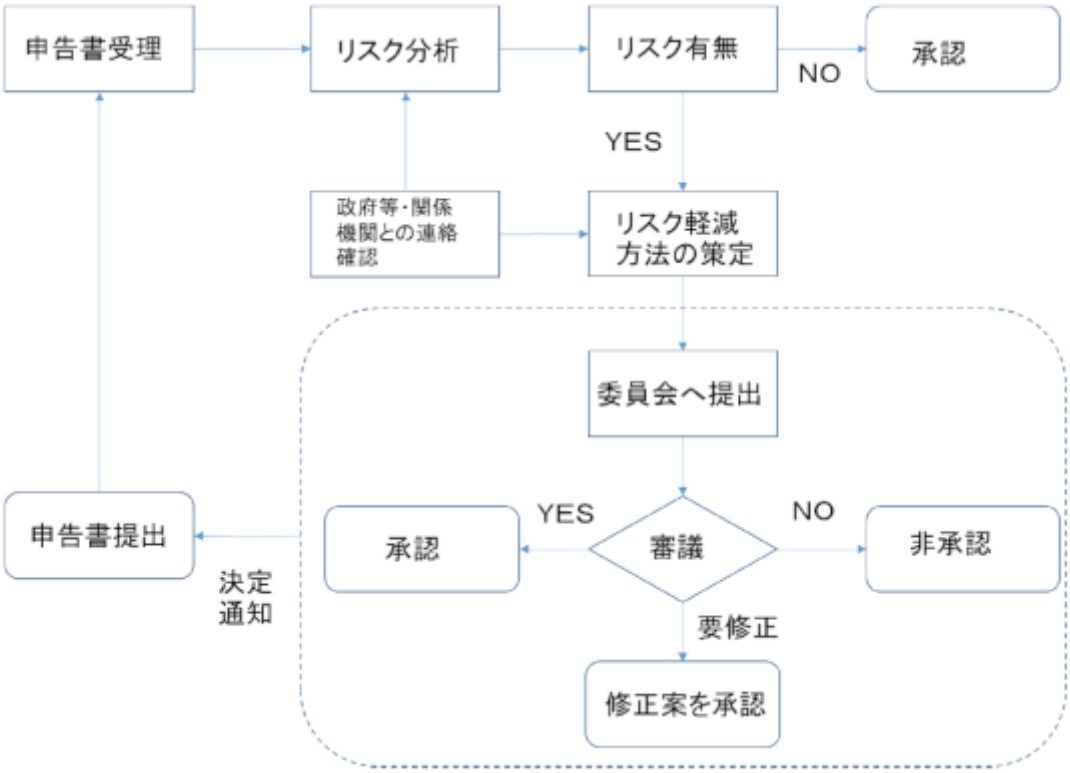


図1 ハイリスクパートナーシップマネジメントのプロセス（Ara Tahmassian, Ph.D.による）

Guidelines for Sensitive Negotiations は、NDAA制裁企業以外に、中国の千人計画への参加研究者に関するリスク管理を意識した部分（受け入れ組織リスト）なども掲載されている。千人計画の研究人材は、企業に加えて清華大学、北京大学など中国の有力大学も多く受け入れていることから、リストにはこれらの大学も含まれている。米国大学においてもオープンな学術交流を行う立場から、中国の大学との関係を、ゼロトレランスで規制することは現実的ではなく、アセスメントとモニタリングによる管理によってリスク低減を図ることがより現実的であるとして、ケースバイケースのマネジメントを行う方針が示されている。

このように米国有力大学では、法令遵守に加えて、その周辺にあるグレーゾーンの領域のパートナリングについてはNDAA規制以前から行っており、「我々はそのリスクを理解していて適切に管理して対処している」とする姿勢のもと、リスクを低減させるためのハイリスクパートナリングの管理を行ってきており、NDAA以降もそのマネジメントが強化され継続している。2019年1月の時点で米国の10を超える大学が Guidelines for Sensitive Negotiations に基づく管理を行っている。

このマネジメントの手法は産学連携の利益相反管理と類似しており、リスクをゼロにしようとすれば産学連携そのものを禁止することにつながるが、社会との関係を発展させるために、産学連携自身は推進し、そこに発生するリスクを管理し最小限にまで低減させようとする姿勢とみることができる。そのようなマネジメントが行われる背景としては、前述した Research Integrity Management （大学や研究機関が維持しなければならない社会から見て欠陥のない状態）の管理による維持発展という考え方がある。

ハイリスクパートナリングの管理についても、外国組織との関係を断てばリスクはゼロになる が、国際的な大学のありようを発展させるため、外国組織との関係を維持、発展させつつ、そこに発生するリスクを最小限に低減させる自主的なマネジメントが行われていると理解すべきであろう。

3. 日本の大学における海外組織との産学連携の状況と輸出管理の状況と今後の施策

3.1 最近の国際情勢が日本の大学の研究に与える影響

ここまで述べた米国の安全保障政策における技術情報や投資規制などが、大学法人または研究者、さらには大学発ベンチャー等にどのような影響を及ぼすのかについて検討した。

その第一として、米国輸出管理規則（Export Administration Regulations: EAR）による再輸出規制に違反するとして制裁を受ける可能性があることに注意するべきである。米国商務省産業安全保障局は、日本の外為法等の管理と同様、デュアルユース品目の製品の輸出の管理・規制として、米国輸出管理規則（Export Administration Regulations: EAR）が定められているが、この米国の輸出管理関連法規は、管轄権の及ばない他国での取引にも域外適用される。この再輸出に関する EAR 規制対象品目（Items subject to EAR）としては、米国国外にあるすべての米国原産品目、米国原産品目を組み込んだ非米国産の品目が対象とされており具体的には輸出規制リスト（Commerce Control List: CCL）に該当する米国原産品が組み込まれた（incorporated）外国製品、CCLに該当する米国原産のソフトウェアが組み込まれた（bundled）外国製品、CCLに該当する米国原産のソフトウェアが組み込まれた（commingled）外国製のソフトウェア、CCLに該当する米国原産の技術が組み込まれた（commingled）外国製技術の4つが対象となる。

日本の大学等が特に注意しなければならないのはこの4番目の米国原産技術が組み込まれたに相当するケースである。これは例えば米国企業や米国の大学等の研究機関のプロジェクト等に参加するなどが

行われた場合、輸出規制リストにある米国の技術を受領したとみなされるケースにおいて発生しうる問題である。米国の企業等との連携を行ったり、米国のプロジェクトに参加している一方、同じ技術分野で中国等の機関との研究に従事する場合は特に注意が必要であ る。これは、10月に米国政府が中国の福建省晋華集成電路（JHICC）への半導体輸出を禁止し、同社の事業に協力しようとしていた台湾のUMCにも制裁を加えたことからみても、米国政府が米国原産重要技術を対象とする技術協力を、日本を含むどこの国籍の組織や人であっても、中国の機関に対して行うことに対して問題視していることがわかる。

これらは米国の域外規制に関係した懸念事項であるが、同時に米国は日本政府に対しても、米国同様の規制を求めてきていることが想定される。米国政府からの公式の発表はないものの、米国の報道（米紙ウォールストリート・ジャーナル）、11月23日、米国が同盟国に対し、中国通信機器大手ファーウェイ（華為技術）の製品を使用しないよう求めていると報じている。イランへの制裁のケースでも同様の要請は行われており、これらの要請に対しては日本政府としても何等か対応がなされる可能性がある。日本政府はこののち、「IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ（平成30年12月10日）」を発出しており、対応した規制を行ったとみてよい。日本政府として今後どこまで規制を行うかが重要であり、法令による規制が行われるのであれば、コンプライアンス上それに従う必要がある。

論理的には、現行外為法のリスト規制の対象を米国NDAA法が指摘する Emerging Technology まで拡大されることや、キャッチオール規制の懸念機関に例えば千人計画の人材受け入れ機関を加えるなどが想定されるが、前者は機械学習など広範な技術領域を含み、また後者の千人計画の人材受け入れ機関として多くの大学なども含まれることから、一挙に規制範囲が拡大し、事実上学術面であっても大学間の交流や研究協力は困難になる。その点米国大学で実施しているケースバイケースのマネジメントが実効的に機能すれば、一律規制するよりも現実的な対応施策であるということも言える。

さらに米国大学が、NDAAによる規制強化に対応する場合、日本の大学と米国大学との研究協力や情報共有などにも影響を及ぼしえる。米国大学並みのリスク管理が行われていない大学とは、従前のような米国大学や研究機関との非公知研究情報の共有がむつかしくなり、連携に支障が生じる可能性がある。

3.2 日本の大学の外国におけるデュアルユース技術開発に対する姿勢

日本の大学は、従来安全保障輸出管理に関する法令遵守に加えて、法令で規制されていない場合でも、いわゆる軍事研究とは距離を置く姿勢をとってきた。 日本学術会議は2017年3月24日に「軍事的安全保障研究に関する声明」を発表しており、過去に表明した「軍事目的のための科学研究を行わない声明」を引き継ぐことを表明し、また 2015年に創設された防衛装備庁の「安全保障技術研究推進制度」は政府による研究への介入が著しく問題が多いとしている [11]。すなわちその研究で開発される技術内容の如何によらず、研究費を提供する組織の意図や介入の可能性を問題視したものであることには留意すべきであろう。

日本学術会議からは、海外の軍事研究機関との研究交流に対して何等かコメントが表明されたことはないが、上記2017年3月の声明に示された姿勢を鑑みれば、海外の機関の軍事に利用する意図をもった研究には、当然かかわるべきでないことになる。

一方学術界としては、研究成果が公開されて、パブリックドメインを介して結果的に様々な譲渡に利用されることを問題にしていない。米国大学でも同様、研究成果を論文等で公開する自由が確保されて

いることが学術研究においては最も重要であるとみなされている。この点、2011年11月に起きた医科研の河岡教授の研究成果の公表の是非について一連の議論は重要である。強毒性の鳥インフルエンザウイルス「Ｈ５Ｎ１」に関する国際チームの研究論文について、米科学誌サイエンスが掲載を見合わせたというものであり、米バイオセーフティー委員会がテロリストによる悪用を理由に論文中の実験データを公表しないよう両誌に勧告したことによるものである。これに対して2012年1月20日、河岡教授ら39人の研究者が60日間の研究自主停止を宣言すると発表する一方、「パンデミック防止のため鳥インフルエンザ・ウイルス感染に関する研究は継続されなければならない」とする意見が表明され、その後ＷＨＯにおける専門家会議などを経て、公開のメリットが大きいとして全文公開が勧告されている[12]。公開がワクチンの開発に有益であるとする考え方による判断であった。

一方大学で研究開発された成果が論文等で公開されたとしても、その研究を実施する上でノウハウが存在しているなどの場合、さらに論文で公開されていないデータなどの非公知情報を含む場合であって、その技術がデュアルユース技術とみなされる場合は、情報管理において重要な責任が生じることになる。このようなケースでは大学における営業秘密管理が必要であり、その情報の提供相手には慎重な対応が必要である。先述した国際情勢からして、リスト規制やキャッチオール規制の対象にはなっていない場合であっても、リスクの有無を評価するなどのマネジメントが必要になる場合があることを認識する必要があるものと思われる。

3.3 日本の大学への示唆

エネルギー、地球環境問題など、人類社会が抱える現下の様々な問題は、国内外の様々な機関と連携することによってはじめて研究が可能になり問題解決のアプローチを見いだせる可能性が生じる。その点大学等の研究機関が国内外の機関と連携して活動することは極めて重要であり、その自由が制約されることは、学術研究においての危機的状況であると考えるべきである。例えば SDGs の実現のための研究に際しては、新興国、発展途上国を含む様々な機関との協力が欠かせない。このような連携を最大限生かして人類社会のための学術研究を推進するために、これらの国々の企業との連携も一律に制約されることは望ましくない。

一方本稿で述べたようなデュアルユースの技術開発につながる研究を、研究成果の軍事転用を意図する企業等と連携することや、非公知の重要技術情報を軍事転用の可能性のある形で流出するような事態は避けなければならない。さらに米国の最近の動向などから見ても、研究者にリスクが及ぶ可能性も否定できない状況から、必ずしも日本の法令で規制されている用途や相手先でなくても、国内外の情報に照らして、連携する際のリスクを評価して管理することも必要である。つまりは、安全保障輸出管理に関する法令遵守を確実に履行することに加え、連携相手によって は、研究者のリスク、そして大学法人にとってのリスクの双方の観点からみて、何等かリスクが懸念される場合は、そのリスクの低減を図るか、忌避を選択するという管理が必要と考えられる。

具体的リスクとしては、米国から非ホワイト国の技術窃盗に協力したとして、または米国安全保障輸出管理上の再輸出規制によって制裁を受ける可能性が生じているほか、レプテーションリスクの問題もある。このような背景から、日本の大学法人においても、米国大学で実施している、法令遵守のみの輸出管理に加えて、ハイリスクパートナリングの管理を行うことは有効であると考えられる。

これはまさしく米国有力大学で、法令遵守に加えて、その周辺にあるグレーゾーンの領域のパートナリングについて、「我々はそのリスクを理解していて適切に管理して対処している」とする姿勢を日本の大学も示すことを意味する。これは法令で明確に強制されなくてもみずからの Research Integrity を維持発展しようとする自立した大学の在り方の一つであるというべきである。

一方日本の安全保障輸出管理制度が、このような幅広のリスク管理の必要性を想定していないということではない。対象国・地域が輸出貿易管理令に示されるホワイト国と指定される欧米を中心とする国に対しては、キャッチオール規制は対象外となっているが、非ホワイト国については、特に懸念される企業・組織等として外国ユーザーリストに含まれていない場合でも、需要者と用途を確認した結果、軍用に用いられるおそれがある場合は管理対象となることは留意すべきである。また平成29年に発表された「安全保障貿易に係る機微技術管理ガイダンス（大学・研究機関用）第三版」においては、必須項目に加えて、法令で直接義務づけられておらず、取り組まなかった場合に法令違反に問われるわけではないが、違反の未然防止のために有益であると考えられる取組を「推奨」項目として記載しており、より幅広な管理が期待されていることにも注意をする必要がある。

これらの日本法令の運用の考え方においても、法令で明確に強制されなくても「みずからの Integrity を維持発展しようとする自立した大学の在り方」としてのハイリスクパートナリングにおけるリスクマネジメントが検討されるべきであろう。

注

1. 本提言は変化の激しい国際情勢に対応したものであり、今後の状況の変化により加筆等を行う可能性があるため暫定版としている。
2. 渡部俊也「国際シンポジウム開催報告」
3. Integrity は一般的には公正と訳されることが多いが、本稿で扱う大学のリスクマネジメントに対する姿勢を表す文脈でははるかに幅広い概念を有していて、たとえば misconduct を防止して Integrity を維持するというような使われ方がなされる。Integrity の語源は「完全な」を意味するラテン語の Integer であり、ここでの Research Integrity は「大学や研究機関が維持しなければならない社会から見て欠陥のない状態」を指す。「研究者と社会との契約である」“Research Integrity is a contract between researchers and the society.” であり、そこでなすべきことはすべて社会との契約の一側面であり、「そしてそれは強制することはできず、関係者が自ら実践すべきことである。」“It cannot be enforced, it must be practiced by all involved.” という表現に見られるように、他者から強制されるものではなく、リスクを理解し自らの問題としてそれに自主的に対処する姿勢につながる。
4. 渡部俊也「大学と社会政策提言 知的財産制度と産学連携に関する論点」
5. https://www.congress.gov/bill/115th-congress/house-bill/5515/text
6. Department of Commerce logo U.S. Department of Commerce のプレスリリース 参照
7. https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf
8. 最近の米国の安全保障に関する規制強化については筆者による整理「最近の米国等の安全保障政策における技術情報の取り扱い（非公開原稿）」にまとめている（大学機関への個別配布可）
9. 本稿に記載されたハーバード大学の事例については、Ara Tahmassian, Ph.D.（Chief Research Compliance Officer, Harvard University）へ2018年に行った複数回のインタビューおよびメールによる情報提供に基づいたものである。
10. https://www.aaup.org/article/confucius-institutes-threaten-academic-freedom#.XGDGkVwzZdh
11. http://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-23-s243.pdf
12. https://www.natureasia.com/ja-jp/nmicrobiol/interview/6

関連リンク

- 産学及び社会連携システム研究ユニット

研究セキュリティとオープンソース・デューデリジェンスに関する国際フォーラム
International Forum on Research Security and Open Source Due Diligence

開催内容　開催報告

【概要】
この会議は、研究セキュリティとオープンソースデューデリジェンスに関する国際フォーラムとして、日米カナダの政府、大学および企業の招待者による議論が行われました。会議では、日本政府の経済安全保障政策の最新動向、G7における研究セキュリティとインテグリティに関する取り組み、カナダにおける研究セキュリティの実践例が紹介されたほか、日米の事業者によるオープンソースデューデリジェンスに関する具体的な実施方法の紹介がありました。その後カナダ政府の研究セキュリティに関する政策、日本の大学の研究セキュリティの課題などの紹介の後、日本の大学のコンソシアムによる取り組みなどに関してパネル討論において意見交換が行われました。

【各セッションの主な内容】
日本政府の経済安全保障政策
内閣府の飯田審議官から、日本政府の経済安全保障政策について説明がありました。日本

は国家安全保障戦略に基づき、サプライチェーンや重要技術、インフラ、データ保護などの分野で経済安全保障政策を推進しています。具体的な取り組みとして、外為法による輸出管理、インフラ事業者への規制、重要技術の特許非公開制度、セキュリティ・クリアランス制度の導入などが紹介されました。また、研究セキュリティについては、大学や企業に対し、国が支援を行う研究開発プログラムを実施するにあたり、リスクに応じて、リスク管理やデューデリジェンスの実施を求める旨の有識者会議の提言について紹介がありました。

G7における研究セキュリティとインテグリティの取り組み

内閣府の塩崎審議官から、G7における研究セキュリティとインテグリティに関する取り組みが紹介されました。G7では、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置し、共通の原則やベストプラクティスを策定しました。研究インテグリティとは、研究の正当性や社会的妥当性を確保することであり、研究セキュリティとは経済的・戦略的リスクから研究コミュニティを保護する活動と定義されています。日本政府としても、大学等における研究の健全性確保に向けた対応方針を決定し、取り組みを進めています。

カナダ政府の方針

カナダ大使館のアニータ・パン一等書記官から、カナダ政府の研究セキュリティ政策が紹介されました。研究者と懸念組織との関係を注視しつつ、オープンな研究環境を維持する方針が説明されました。研究分野が機微技術分野であり、かつ懸念組織との関係があれば、政府の研究助成金が受けられなくなる可能性があることが明らかになりました。一方で、できるだけオープンで協力的な体制を維持したいとの考えも示されました。

カナダの大学における研究セキュリティの取り組み

トロント大学のポール・ジャレット氏から、カナダの大学における研究セキュリティの取組みが紹介されました。カナダ政府は、研究セキュリティセンターを設置し、大学への助言や政府助成金に係るデューデリジェンスを実施しています。機微な研究分野や指定研究機関リストを定め、リスクの高い研究領域や組織を特定しています。大学は研究セキュリティチーム（チーム・カナダ）を設置し、研究パートナーに対するデューデリジェンスやリスク評価を行っています。トロント大学では、国家安全保障の専門家によるデューデリジェンスチームを設置し、他大学とのコンソシアムを形成してベストプラクティスを共有しています。

日米の企業が行っているデューデリジェンスの具体的方法と支援方法

三菱電機の伊藤執行役員から、従業員のメールモニタリングによる情報漏えいリスクの検知について説明がありました。フェーズに応じた対策を講じており、AIを活用したモニタ

リングの導入が進められていることが分かりました。 FRONTEOの久光部長からは、オープンソースインテリジェンスを活用した研究者や組織のリスク評価サービスが紹介されました。研究者ネットワーク解析、株主支配ネットワーク解析、サプライチェーンネットワーク解析などのツールを組み合わせて、大学のリスク管理に活用できる可能性が示唆されました。 ストライダー・テクノロジー社のジョンストン戦略担当役員からは、オープンソース情報を活用して、懸念国が標的とし得る人材、技術、供給網等に対するリスクを評価し、学問の自由を維持しつつ大学が能動的にリスク管理を講じることができるサービスについて紹介されました。共同研究等を実施する際、関係者の軍事機関と潜在的な脅威を事前に特定することなどにより、大学の研究セキュリティ全般の拡充に向けて支援できる可能性が説明されました。

日本の大学における現状と課題

名古屋大学の佐宗副総長から、外国人留学生や研究者の受け入れ時の審査、在籍者のモニタリング、退職後のフォローアップなどの現状と課題が説明されました。外為法に基づく審査は年間2000件程度行われていますが、人的リソースが不足しているため、十分な調査ができていない状況が報告されました。また、研究テーマの変更時のモニタリングや、退職後の情報漏えいリスクへの対応が課題として挙げられました。

文科省の取り組み

文部科学省の西條審議官から、研究インテグリティ確保に向けた政府の取り組みが説明されました。大学の自主的な取り組みを尊重しつつ、ガイドラインの策定やベストプラクティスの共有などの支援策が検討されていることが明らかになりました。また、国立研究開発法人に比べて大学の取り組みが遅れている現状も指摘されました。

今後の課題

パネル討論を経て、大学のコンソシアム結成、ガイドラインの策定、米国・カナダとの連携、スタートアップ支援、セキュリティ・クリアランスの活用など、今後の課題が提起されました。あわせて経済安全保障政策の政府の立場からは、大学への追加的な支援やリソースの提供など、総合的な施策の必要性が指摘されました。 具体的には、カナダに倣い日本版の「チーム・ジャパン」に相当するコンソシアムを結成し、政府の支援を受けながらガイドラインや手順書を作成することが提案されました。外部の知見や情報を活用し、大学の負担を軽減することが重要であると強調されました。また、米国・カナダとの情報共有や共同での取り組みも有効であると指摘されました。 さらに、ペーパーミリングと呼ばれる論文の不当な作成と、不当な論文に基づく大学の誤った（高）評価への対応、大学発スタートアップへのデューデリジェンス支援の必要性や、セキュリティクリアランスホルダーによるガバナンス体制の構築も課題として挙げられました。今後、国際会議を開催

し、具体的な施策を検討することが提案されました。加えて 大学発スタートアップへのデューデリジェンス支援体制を構築することや、これらの一般研究においてもセキュリティクリアランスホルダーが関与したガバナンス体制が有効であることが提案されました。

フォーラム アンケート集計(pdf)

一覧へ戻る

参考資料４

「日米韓大学研究セキュリティ・インテグリティ国際ワークショップ」報告

1. ワークショップの概要と目的

2025 年 1 月 21 日、日本・米国・カナダの大学や政府関係者が参加する「日米加大学研究セキュリティ・インテグリティ国際ワークショップ」が開催された。本ワークショップの目的は、研究の安全性と完全性（インテグリティ）を確保するための国内外の協力の在り方を議論し、実践的なアプローチを共有することにある。

1.1 研究セキュリティの重要性

科学技術とイノベーションの発展には、国際的な共同研究が不可欠である。しかし、近年、研究成果の流出や悪用のリスクが高まり、各国政府や大学が対応策を求められるようになった。特に、研究の透明性とセキュリティのバランスを取ることが課題となっており、日本、米国、カナダはそれぞれの政策や取り組みを紹介しながら、今後の協力体制について議論した。

1.2 あいさつと基調報告

東京大学の齊藤理事の開会挨拶に続き、日本政府の経済安全保障担当大臣兼内閣府特命担当大臣（科学技術政策）である城内衆議院議員からビデオメッセージを寄せられた。

2. 大学研究セキュリティ・インテグリティコンソシアムの設立

2.1 研究セキュリティとインテグリティの概念

ワークショップの中心議題の一つが、研究セキュリティとインテグリティの確保である。「インテグリティ（Integrity）」という言葉は、日本語では明確な訳語がないが、研究者と社会の契約としての意味を持つ。研究の透明性を担保し、公正で信頼できる環境を維持することが求められる。
一方で、「セキュリティ（Security）」は、研究インテグリティを確保するために、研究成果や技術情報が悪用されるリスクから研究コミュニティを保護する活動であり、これらのリスクの認識と低減への対策が不可欠である。

2.2 コンソシアム設立の背景

近年、日本国内外で研究不正や技術流出の問題が指摘されている。例えば、以下のような問題である。
① 利益相反の懸念：企業との共同研究において、特定の海外の機関のために研究結果が歪められるリスク
② 技術情報の流出：研究データやノウハウが国外に不正に持ち出される問題
③ 意図せざる共著問題：研究者が知らない間に共同研究者として外国機関に名前を利用されるケース
これらの問題に対応するため、東京大学をはじめとする国立大学を中心とした 9 つの主要大学がコンソシアムを創設し、参加する大学の研究セキュリティ・インテグリティの対応能力の向上、リスク情報やベストプラクティスの共有、更には国際的な連携を強化する目的でその活動が開始された。

3. 米国における研究セキュリティの取り組み

3.1 ハーバード大学の事例

米国の大学は、研究セキュリティの管理を強化しており、ハーバード大学ではデューデリジェンス・ガイドラインを策定し、研究者の雇用や共同研究のリスク評価を行っている。

・ハーバード大学の対策

ハーバード大学の研究セキュリティのとりくみとして下記が進められていることが報告された
- 研究者の背景調査（過去の共同研究や資金提供元のチェック）
- 研究データの保護強化（クラウドやアクセス権限の管理）
- 研究倫理とコンプライアンス研修（定期的なトレーニング実施）

3.2 米国政府の政策

米国政府は、国家安全保障大統領覚書第 33 号（SPM33）を通じて、大学に対して研究セキュリティ計画の策定を義務付けている。これにより、
- 輸出管理の強化（軍事転用可能な技術の管理）
- 知的財産保護（特許申請前のデータ流出防止）
- 政府機関との連携（大学と政府の情報共有）

が進められていることが報告された。

4. カナダの研究セキュリティと「チームカナダ」の取り組み

4.1 研究セキュリティ基金

カナダ政府は年間 2,500 万ドルの研究セキュリティ基金を設立し、大学に対する資金提供を行っている。この基金は、
- セキュリティチームの設立（大学内に専門チームを配置）
- サイバーセキュリティ対策（デジタルフォレンジック分析の導入）
- 国際連携の強化（日米の大学との共同対策）

に充てられることが報告された。

4.2 チームカナダの役割

カナダの研究セキュリティ強化のため、チームカナダが発足。カナダ国内の 66 大学が参加し、
- 情報共有とリスク評価
- 研究者向けトレーニングの実施
- 政府機関との連携強化

を推進していることが報告された。

4.3 カナダ政府の取組み

カナダ政府のアプローチとしては、研究の開放性や共同研究の促進を前提としつつ、以下の観点を原則としたガイドラインを整備している。
- リスクベースアプローチ

- 適切な科学（の振興）
- 透明性
- 差別、ハラスメント、強制的でないこと
- 研究コミュニティとの協働的な発展

また、政府関係省、研究機関、FA などが役割分担と連携をして大学の取組みをサポートするとともに、今後の国際協力の重要性について強調がなされた。

5. ケーススタディ：研究セキュリティの実際の問題

5.1 スマートシティ監視技術の流用
カナダの大学が国際企業と共同で開発した AI 交通監視技術が、意図せず国家監視プログラムに転用されるリスクが発生。学術研究の目的が、政治的な利用に変質する危険性が浮き彫りとなった。

5.2 監視気球プロジェクト
カナダの大学が進めた気候モニタリング気球プロジェクトに、軍の関連企業が資金提供をしていたことが判明し、プロジェクトが中止された。研究資金の出所を確認することの重要性が強調された。

6. パネルディスカッション

パネルディスカッションでは、日米加の政府、大学をパネリストとして、研究セキュリティ・インテグリティへの対応策、大学間、政府間協力の在り方等について議論を行い、次のような論点が提示された。

- 既存の取組を活かしつつ、横断的につなぐ統合的なアプローチの重要性と、統括的な責任者による対応の重要性
- ルールベースアプローチではなく、リスクベースアプローチによる対応
- 研究者自らの研究を保護し、悪意のある者による成果の利用を防ぐための政府によるツール提供や、各国の対応アプローチの差を許容したうえでの「責任ある国際化」を目指すことの重要性
- 「研究セキュリティ文化」の醸成
- 研究セキュリティ確保のための基本原則（共通の価値観に基づく開放的な研究環境を守ること、大学における国際連携の促進のために必要不可欠であること、ゼロリスクを目指すのではなく適切な範囲でリスクの軽減を目指すこと、いかなる差別を生まないこと）の認識の共有の重要性
- 教職員だけでなく学生や大学を構成する人材への意識啓発、継続教育、体制づくりのための人材づくりやどのような能力の人材が必要かといった能力の深堀り
- 価値観を同じくする各国との連携、経験・ベストプラクティス共有の重要性

7. 今後の展望と課題

7.1 研究セキュリティのバランス
研究の自由を確保しながら、不正な技術流出を防ぐための仕組みづくりが求められる。

7.2 透明性の向上

大学は研究資金の出所や共同研究の透明性を高める必要がある。

7.3 国際協力の深化
日米加の連携を強化し、研究倫理の標準化と情報共有の枠組みを作ることが重要。

8. まとめ

今回のワークショップでは、研究セキュリティに関する国際的な取り組みが議論された。各国の事例を参考にしながら、日本もコンソシアムが設立されたところであるが、大学間・政府間の協力を強化する必要がある。今後も、研究の自由と安全性のバランスを取るための施策が求められる。

会議を受けての提言

第一に、日米加の大学と政府は、アカデミアの自由および国際的な研究の在り方について、基本的に同じ価値観を有しており、現下に生じている研究インテグリティに対するリスクの存在を共有している。この点において、これら三か国が、それぞれの大学コンソーシアムやそれに相当する組織、およびそれを支援する政府が相互に協力し、そのアプローチ方法を共有することは極めて有益である。この認識を共有することができた。具体的な協力体制については、今後議論を行い、その枠組みを検討していく必要がある。

第二に、本日も議論があった研究インテグリティと研究セキュリティの概念についてである。これは G7 のワーキンググループにおいても整理が試みられたものであるが、特に研究セキュリティについては、今一度、日米加において統一した概念を確認し、その考え方に対する信頼感を高め、それを研究現場と共有していくことが重要である。

第三に、研究インテグリティと研究セキュリティについて共通の概念を共有したからといって、その目標に向かう際に全く同じやり方を採用する必要はない。日米加のそれぞれの取り組みを共有しつつ、各国の事情に適した方法を採用し、違いを認識しながら進めることが望ましい。この点についても強調すべきである。

第四に、日米加の安全保障協力は、先進的な研究協力の深化に資するべきである。安全保障は信頼の基盤であり、これを強化することが研究協力の発展に寄与する。

また、会議の質疑の中でセキュリティクリアランスに関する話題が提起された。同制度はまもなく施行されるので注目されているが、今回の議論は基本的に基礎研究（ファンダメンタルリサーチ）に関するものであり、クリアランスは必要ない範囲で行われるものである。そのため、適正調査ではなく、オープンソース DD が手法として採用される。ただし、アメリカのエコシステムにおいては、400 万人のクリアランスホルダーまたはその経験者がファンダメンタルリサーチにも貢献している。このようなエコシステムを日本がどのように構築するかが今後の課題となる。今後、そのようなゴールを意識して政策を検討していく必要がある。

これらを踏まえ、本日指摘された事例や、昨年 6 月のシンポジウムにおいて指摘された個々の問題、本日の事例紹介におけるリスク、新たな問題として意図せざる共著の問題やペーパーミリングへの対処についても、国際的な協力体制を構築することが重要である。

これらの取り組みの方向性については、日米加のみならず、G7 各国にも同様の課題が存在する。今年の G7 サミットでは、カナダ政府が議長国を務め、アルバータ州カナナスキスで開催されると聞いている。この機会に政府間の連携を深め、自由な研究と知の探求を最大限に活かせる環境整備を進めるべきである。

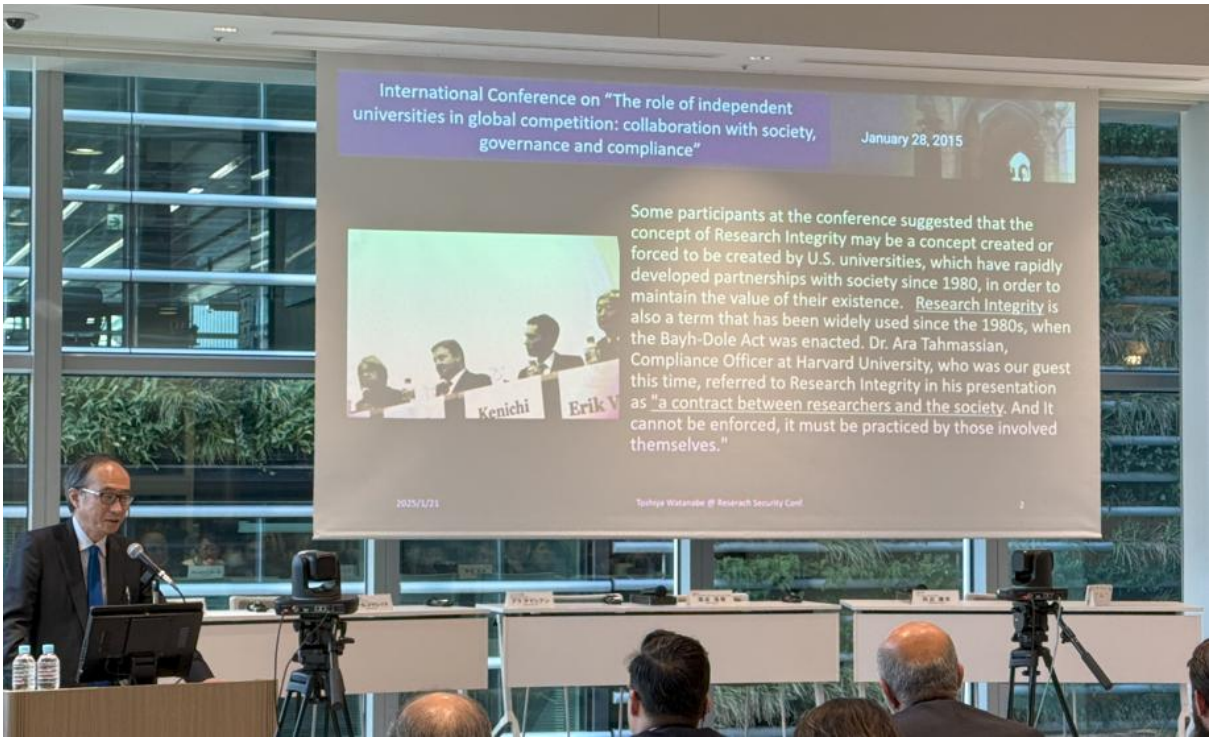
本日の議論は、大学の取り組みやコンソーシアムの今後の活動について、多くの参考となる内容を含んでいた。人材育成、研修、啓発、体制構築など課題は多い。特に、誰がこの分野のエキスパートとなるのかについての議論は重要である。規制の枠組みでは対応しきれない部分を、現場でどのようにマネジメントしていくかが課題となる。そのために、アラ博士が言及したように、大学自身が研究コミュニティとの関係において信頼醸成を行うことが必要であり、それを政府が支援することが最も重要な課題である。

また、研究セキュリティの専門家を対象とした合同研修を実施するための共有プログラムやプロセス、合意形成が求められる。さらに、国内外の大学間の情報共有の仕組みを構築することも必要である。

これらについて、本日伺った各国の取り組みを踏まえ、「走りながら」という表現もあったように、今後もより良い方法を検討していく必要がある。

個々の取り組みを進めつつ、今回の会議の前に、本日のゲストから、日本のコンソーシアムは内部会議のみならず、より多くの関係者が参加可能な公開年次総会を開催すべきであるという意見をいただいた。まさに、コンソーシアムはこのような開かれた取り組みを推進すべきである。その際に、再度皆様にお会いできることを楽しみにしている。

ビデオメッセージ　城内実（経済安全保障担当大臣）



報告　渡部俊也（東京大学未来ビジョン研究センター教授、東京科学大研究イノベーション本部教授）

パネル討論の様子

アラタマシアン博士（ハーバード大学コンプライアンスオフィサー）

ビデオは　米国国務省デービッド・ビッグス氏、前列にアラタマシアン博士（左）、文部科学省大臣官房審議官(科学技術・学術政策局担当）高谷浩樹氏（中央)、モデレーター　東京大学産学協創推進本部 田辺雄史氏（右）

カナダ外務省 オーウェン・サウンダース氏

参考資料5

日本における大学研究セキュリティ・インテグリティコンソシアムの設立：その背景と狙い

Establishment of the University Research Security and Integrity Consortium in Japan: Background and Aims

東京大学　副学長　未来ビジョン研究センター　教授
Vice president & Professor of UTokyo
東京科学大学　副学長　研究イノベーション本部　教授
Vice president & Professor of Science Tokyo
渡部俊也　Toshiya Watanabe

経緯 Background

1. 2024年6月に政府機関、海外大学等を招いた国際フォーラムを開催し、各組織での取組について議論。The international forum was held in June 2024, inviting government agencies, overseas universities, and other organizations to discuss initiatives at each organization.
2. 諸外国で進展する研究パートナーに対するオープンソースデューデリジェンス（OSDD）を、我が国でも実施していくうえでの諸課題や取組方針を提示。The issues and policies for implementing Open Source Due Diligence (OSDD) for research partners in Japan, which has been progressing in other countries have been discussed.
3. これらの取組みに関し、個別大学での対応がリソース（体制、資金等）面の不足により困難に直面するなか、カナダの事例を参考に、効率的な対応や能力向上を可能とする仕組み（コンソーシアム）の検討を開始。As individual universities are facing difficulties in addressing these issues due to a lack of resources (systems, funds, etc.), we have started to consider a system (consortium) that will enable efficient response and capacity building, with reference to the Canadian case study.
4. 2024年9月より関係大学（9大学）による議論を開始し、同体制の役割や機能、検討すべき課題、体制を運営する際に必要な規程などを整備。Discussions by the universities involved (9 universities) will begin in September 2024 to develop the roles and functions of the system, issues to be considered, and regulations necessary for operating the system.
5. 2025年1月14日に設立総会を実施 General meeting for establishment of consortium was held on January 14, 2025

※ 関連して、政府においては2024年6月4日に経済安全保障上の重要技術に関する技術流出防止策についての提言が発表される

In relation to these issues, the government has issues a proposal on June 4, 2024 on measures to prevent technology outflows related to technologies of economic security importance.

Annex 2:
G7 Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group

Mandate & Purpose of the Working Group
The Working Group on the Security and Integrity of the Research Ecosystem (SIGRE) was established in the 2021 G7 Research Compact.

The Working Group serves three main purposes:
1) To review existing principles of research security and integrity to understand whether they sufficiently account for security considerations, developing additional principles where they do not.
2) To identify voluntary standards of conduct and best practices by which such principles of research security and research integrity can be embedded.
3) To strengthen the exchange of best practices across the research community on research security and integrity considerations by establishing a virtual academy and a toolkit.

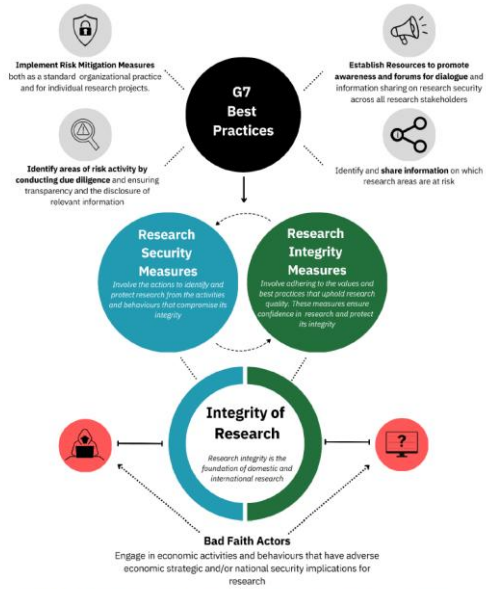
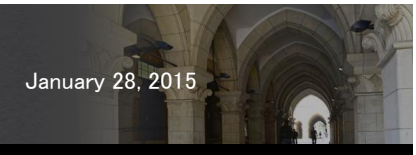


Figure 1: A graphic depicting how the G7 Best Practices support both research security and research integrity.

International Conference on “The role of independent universities in global competition: collaboration with society, governance and compliance”



Some participants at the conference suggested that the concept of Research Integrity may be a concept created or forced to be created by U.S. universities, which have rapidly developed partnerships with society since 1980, in order to maintain the value of their existence.Research Integrity is also a term that has been widely used since the 1980s, when the Bayh-Dole Act was enacted. Dr. Ara Tahmassian, Compliance Officer at Harvard University, who was our guest this time, referred to Research Integrity in his presentation as "a contract between researchers and the society. And It cannot be enforced, it must be practiced by those involved themselves."

Discussion at the International Forum (to be held in June 2024)

Team Canada

64

participating academic institutions in Canada, each contributing university research security staff

Exchange Information

Establish Best-Practices

Liaise with Government

13

U of T-Affiliated hospitals and incubators participating in a U of T-led Toronto area research security group

フォーラムで指摘された今後の課題　Future issues identified at the forum

- パネル討論を経て、大学のコンソシアム結成、ガイドラインの策定、米国・カナダとの連携、スタートアップ支援、セキュリティ・クリアランスの活用など、今後の課題が提起。After a panel discussion, the following issues were raised for the future: formation of a consortium of universities, development of guidelines, collaboration with the U.S. and Canada, start-up support, and use of security clearances.
- あわせて経済安全保障政策の政府の立場からは、大学への追加的な支援やリソースの提供など、総合的な施策の必要性が指摘。政府においてガイドライン等の整備を検討。In addition, the government's position on economic security policy points to the need for comprehensive measures, including additional support and resources for universities. The government will consider the development of guidelines and other such measures.
- 具体的には、カナダに倣い日本版の「チーム・ジャパン」に相当するコンソシアムを結成する等が提案。その際外部の知見や情報を活用し、大学の負担を軽減することが重要。Specifically, it is proposed to form a consortium equivalent to a Japanese version of "Team Japan," modeled after Canada's. In doing so, it is important to reduce the burden on universities by utilizing outside knowledge and information. It is important to reduce the burden on universities by utilizing outside knowledge and information.
- 米国・カナダとの情報共有や共同での取り組みも有効であり、国際会議を開催し、具体的な施策を検討することが提案。Information sharing and joint efforts with the U.S. and Canada are also effective, and it is suggested that an international conference be held to discuss specific measures.
- さらに、ペーパーミリングと呼ばれる論文の不当な作成と、不当な論文に基づく大学の誤った（高）評価への対応、大学発スタートアップへのデューデリジェンス支援の必要性や、セキュリティクリアランスホルダーによるガバナンス体制の構築も課題であり、それらへの支援等が必要。In addition, addressing the unfair preparation of papers called paper milling and the false (high) reputation of universities based on unfair papers, the need for due diligence support for university startups, and the establishment of a governance system with security clearance holders are also issues, and support for these and other issues are needed.

技術流出対策に関する政府の取組　Measures for technology leakage by the government

経済安全保障上の重要技術に関する技術流出防止策についての提言
（国が支援を行う研究開発プログラムにおける対応）
Recommendations about the Countermeasures for the Leakage of Critical Technologies (measures for government-supported R&D program)

■ 技術流出対策について、経済安全保障法制に関する有識者会議に付し、国際動向や国際化への対応を念頭に、下記について議論
Referred countermeasures for the leakage of critical technologies to the Experts' Meeting on Economic Security Legislation
Considering international trends and internationalization of research activities, those experts had mainly discussed two issues;

- **大学や研究機関等において、どのような研究セキュリティ・インテグリティ対策が必要となるか**
what measures for research security and integrity will be required　in academic research community
- **企業等で成果を社会実装することを目指した重要技術**について、**技術流出防止にどのような対応が必要か**
what measures are needed to prevent leakage of critical technologies for social implementation, in private companies, etc.

■ 上記の議論を踏まえ、2024年６月４日、有識者会議で、経済安全保障上の重要技術に関する技術流出防止策についての提言を策定
Based on these discussions, the meeting concluded policy recommendation on June 4, 2024.

国家間における経済安全保障上の重要技術の共同研究の推進（主に大学・研究機関等）
Promotion of international collaborative R&D for critical technologies (mainly for academic research community)

- オープンで自由な研究環境を確保し、経済安全保障上の重要技術に関し国際協力を一層推進するため、これまで実施してきた研究インテグリティの取組を基礎として、その取組を徹底し、これを実効性のある実施に繋げることが、**研究セキュリティの取組**として重要。
  To ensure an openness and freedom of R&D environment and further promote international collaborative research for economic security, it is important to thoroughly implement research integrity initiatives based on those implemented so far, and they need to be implemented effectively for **research security initiatives**.
- 同志国等と対等な立場で国際協力を推進するために必要な施策として、オープンソース・デュー・ディリジェンスやリスク軽減策など、リスクに応じた段階的な取組について検討することを推奨
  The recommendations suggest conducting research security measures depending on the level of risk including implementation of open-source due diligence and risk mitigation measures to promote international cooperation equally with like-minded countries.

①国が主導する研究開発プログラムについて、**ガイドラインやチェックリストの策定・普及**を通じて所要の確認を徹底させるなど、実効性のある対応策を実施
Regarding **nationally funded R&D programs**, we will consider practical and valid measures such as **thoroughly checking the necessary actions by developing and disseminating guidelines or checklists**

②リスクの高い研究領域を含む特定の領域の国際共同研究等において、「**諸外国の先進的な取組と同等の研究セキュリティの取組**」として、例えばオープンソース・デュー・ディリジェンス等の充実によるリスクマネージメントなどを実施
In terms of specific sensitive R&D areas at high risk, it is necessary **to implement research security activities equivalent to advanced measures implemented by like-minded countries**. (e.g. introduction of risk management including open-source due diligence)

議論 Discussion

1. 新たなリスク対応について、何らかの方法で以下のような「相場感」を用意。In order to deal with new risks, a kind of “market view” should be prepared, including the following points
   - ① リスクマネジメント（特にデューディリジェンス）を行う趣旨、コンセプト (1) The purpose and concept of risk management (especially due diligence)
   - ② 共同研究相手、受入れ相手のデューデリジェンスが必要であること。(2) The need for due diligence of joint research partners and host institutions
   - ③ 対象者の範囲の原則（学内には様々なステータスの研究者が存在しているが、どこまでを見るべきなのか、その概念はどうあるべきか） (3) The principle of the scope of the target (there are researchers of various statuses within the university, but to what extent should we look, and what should the concept be?)
   - ④ 確認すべき事項、確認すべきではない事項 (4) Matters that should be confirmed and matters that should not be confirmed
   - ⑤ 学内、あるいは対象者への説明方針 (5) Policy for explaining to the university or the target

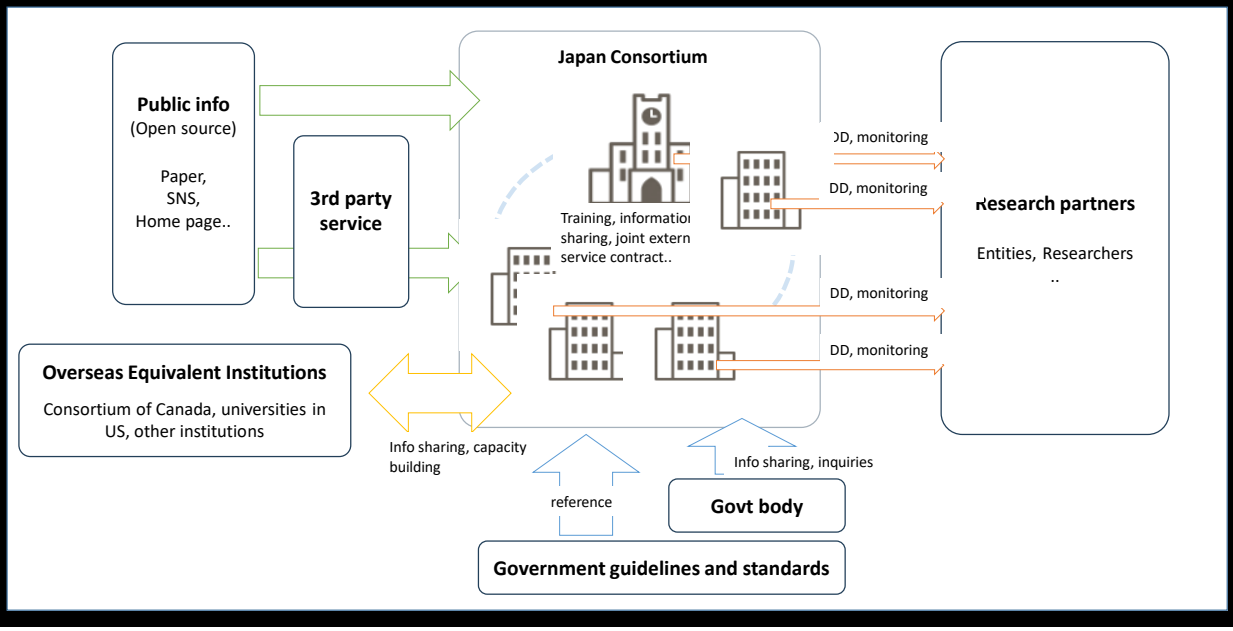
   ある程度統一された「相場感」が用意され、やり方がわかれば、各大学の自主的な取組みによる「適切な」対応の両立が可能。If a certain degree of uniformity is achieved in terms of “market view” and the approach process is understood, it will be possible to the independent initiatives of each university with “appropriate” responses.
2. さらには、海外事例も参考に、効率的な運用体制を我が国大学全体で整備。Furthermore, with reference to overseas examples, an efficient operational system should be developed across all universities in Japan

   ①ある程度秘密が確保された上での事例（手口）の共有. Sharing of cases (methods) with a certain degree of confidentiality ensuredUse of external services with high cost-effectiveness, such as consortium-style services

   ②コンソーシアム形式等、費用対効果の高い外部サービスの利用　Use of external services with high cost-effectiveness, as consortium-style services

- 研究セキュリティ・インテグリティ確保のため、共同研究や研究者受入れの際に、先方の意図や懸念の有無の確認及び必要に応じたモニタリングの手続き（デューデリジェンス（DD））をオープンソース情報を用いて実施することが必要。G7等の諸外国でも近年この動きが加速。
- 海外機関等との共同研究を公正性を確保しつつ推進し、新たな発明、イノベーションを創出し、大学の研究活動を活性化させる上で、将来的に海外機関等から求められ得るDDについて、G7諸国に歩調を合わせた体制整備が急務。
- 個別大学での自主的な実施には限界のある新たな取組であることから、大学間連携によるコンソーシアムを形成し、能力の獲得・向上、懸念情報の共有、DDの実施支援、海外連携等を推進するとともに、政府からの支援を受け入れる体制を整備。
- In order to ensure research security and integrity, when conducting joint research or accepting researchers, it is necessary to confirm the existence of the other party's intentions or concerns and conduct monitoring procedures (due diligence (DD)) as necessary, using open source information.
- In order to promote joint research with overseas institutions while ensuring fairness, create new inventions and innovations, and revitalize university research activities, there is an urgent need to establish a system in line with G7 countries for DD that may be required by overseas institutions in the future.
- Since it is a new initiative with limitations to be implemented by individual universities on their own, a consortium should be formed through inter-university collaboration to acquire and improve capabilities, share information on concerns, support implementation of DD, promote overseas collaboration, and develop a system to accept support from the government.

University Research Security and Integrity Consortium (URSIC)



University Research Security and Integrity Consortium (URSIC) Overview

1. Objective

To appropriately ensure and improve the research security and integrity of Japanese universities and to contribute to the creation of an internationally reliable research environment through collaboration among universities and with equivalent institutions or related initiatives overseas.

2. Outline of Constitution

Activities: Research and surveys, education and training, collection and sharing of risk information, cooperation with external organizations, and policy proposals to the government

Organization: General Assembly (all members), Executive Committee (composed of initial members), Secretariat (same as on the left)

Rights and obligations: Active involvement in and contribution to education, training and information sharing, and able to use of obtained knowledge and information within the university

Membership fee: Free for the time being (volunteer)

3. Initial members (all appointed as members of the Executive Committee and Secretariat)

Hokkaido Univ, Tohoku Univ, Univ of Tokyo (Chairman and Secretariat leader),
Tokyo University of Science, Univ of Electro-Communications, Nagoya Univ,
Kyoto Univ, Osaka Univ, Kyushu Univ

4. Nature of organization Voluntary organization

5. Establishment January 14, 2025

6. Future plans

- Expansion of the scope of activities, including determination of institutional bylaws and activity policy details, explanation to relevant quarters, collection of operational details and contents for human resource development and information sharing, and acceptance of universities wishing to join the URSIC.
- Strengthen relationships mainly with Canada and the U.S. to incorporate leading initiatives, and consolidate information by functioning as a liaison with equivalent institutions overseas.

大学研究セキュリティ・インテグリティコンソシアム(URSIC)　概要

1. 目的

研究セキュリティ・インテグリティに関連する取組について、大学間、更には海外同等機関との連携を通じて、我が国大学の研究セキュリティ・インテグリティを適切に確保・向上するとともに、国際的に信頼性のある研究環境の構築に寄与する。

2. 会則概要

① 活動内容：調査研究、教育・訓練、リスク情報の収集と共有、外部機関との連携、政府への政策提言
② 体制：総会（全会員）、幹事会（初期メンバーにより構成）、事務局（同左）
③ 権利義務：教育・訓練、情報共有に係る積極的な関与・貢献や得られた知見、情報の学内での利用
④ 会費：当面無料（ボランティア）

3. 初期メンバー（すべて幹事会、事務局のメンバーに就任）

北海道大学、東北大学、東京大学（会長、事務局リーダー）、東京科学大学、電気通信大学、名古屋大学、京都大学、大阪大学、九州大学

4. 団体の性格 任意団体

5. 設立 2025年1月14日

6. 今後の予定

① 制度細則、活動方針詳細の決定、関係方面への説明、人材育成や情報共有の運用詳細やコンテンツ収集、コンソシアム入会希望大学の受け入れなど、活動範囲を拡大。
② 主にカナダ、米国との関係を強化し、先行的な取組を取り入れていくとともに、海外の同等機関との連携窓口として機能することで、情報の集約を図る。

14