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～

2024 年６月４日
経済安全保障法制に関する有識者会議

０．はじめに

- 経済安全保障法制に関する有識者会議分野別検討会合（官民技術協力）において、国際動向や国際化への対応を念頭に、経済安全保障上の重要技術に関して、国が支援を行う研究開発プログラム（主に政府機関からの委託、補助によって行われるもの）においてどのような技術流出防止策、リスクマネジメントが必要になるのか、３回にわたり検討してきた[1]。
- まず、はじめに、Ｇ７や同志国等での議論も踏まえ、経済安全保障上の重要技術における国際協力を深化・拡大させていくために、国が支援を行う研究開発プログラムに関して、主に研究成果の公開を前提とした研究を行う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議論を行った[2]。
- 次に、流出した際に経済安全保障上の影響が大きい重要技術に関して、国が支援を行う研究開発プログラムのうち、その成果を企業等で社会実装することを見据えたものを念頭に、国際化への対応、産業競争力の強化のため、その社会実装と技術流出防止に必要な対応を検討した[3]。その際、同志国等の対応やサプライチェーン強靭化、企業等での営業秘密管理における技術流出防止策も参考にした。
- 最後にとりまとめの議論を行った。それらの結果について、以下のとおりとりまとめる。

１．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について

（１）背景・現状

- 技術は我が国の自律性・不可欠性の重要な一部を構成するものであり、我が国の科学技術力の向上のためにも、オープンで自由な研究環境を確保し、国際協力をよりいっそう

---

[1] 第２回（３月２６日）：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
第３回（４月１２日）：経済安全保障上の重要技術に係る研究開発成果の社会実装と技術流出対策の検討
第４回（５月２０日）：第２回・第３回検討会合における議論の取りまとめについて

[2] 競争的研究費を投入する研究開発プログラムにおいて政府方針に基づく研究インテグリティの取組が徹底されること、競争的研究費を投入する研究開発プログラムのうち、リスクの高い研究領域を含む特定の領域において、ⅰ．国際共同研究の実施において相手国から求められる場合や、ⅱ．同志国等と対等な立場で研究を実施するために必要な場合に、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を実施すること（その他、パイロット、トップランナーとして、先行的に実施することも含む）等について検討。

[3] 我が国の技術優位性の強化を目指す技術領域及び将来の我が国の技術優位性の創出を目指す技術領域における社会実装を見据えた研究開発成果の技術流出防止のため、入口から出口までの段階に応じた対策等について検討。

推進する必要がある。

- 一方で、研究活動の国際化、オープン化に伴う研究の不正流用や技術流出のリスクも指摘されており、こういったリスクへの対処は経済安全保障上の喫緊の課題となっている。
- 国際社会では、近年、各国が経済安全保障上の重要技術についての政策を公表し、2か国間、複数国間の協議の場においても、経済安全保障上の重要技術についての議論が盛んに行われており、同志国等の間で協力の重要性、必要性が高まっている。
- こうした中、Ｇ７では「研究セキュリティとインテグリティにおけるＧ７共通の価値観と原則[4]」において、研究インテグリティを「研究の正当性、社会的関連性、責任及び質を確保して守るための職業的価値観、原則及びベストプラクティスの順守」と定義し、「個人が自信をもって研究知識を向上させ、研究結果を普及できる状況を確保」し、「公正で革新的、オープンで、信頼性のある研究環境の中で協力するための基盤を形成するもの」とされている。また、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」とし、「リスクにターゲットを絞った研究セキュリティの施策は、学問の自由、研究インテグリティ、オープンサイエンス、透明性、相互利益のための信頼性のある協力体制の基盤を強化できる」としており、研究セキュリティと研究インテグリティの双方に取り組むことを推奨している。
- 今年２月にとりまとめられたＧ７の作業部会の報告書[5]では、研究セキュリティ・インテグリティのベストプラクティスが、①リスクにさらされている研究領域の特定と情報共有、②「デュー・ディリジェンス（Due Diligence）[6]」を実施し、透明性及び関連情報の開示を確保することにより、リスクのある活動の領域を特定。標準的な組織慣行として、個々の研究プロジェクトについてリスク軽減策を実施、③研究関係者間で研究セキュリティ・インテグリティに関する対話・情報共有を行うための場及び認識を増進させるリソースの確立、の柱に沿って整理されている。
- 特に、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にあたっては、海外

---

[4] https://ised-isde.canada.ca/site/science/sites/default/files/attachments/2023/1135-g7-common-values-and-principles-on-research-security-and-research-integrity_.pdf

[5] “G7 Best Practice for Secure & Open Research”, Secure and Integrity of the Global Research Ecosystem (SIGRE) Working Group, 2024.

[6] 一般的には、企業買収や合併の際の対象企業の財務状況調査等、企業が、実際の及び潜在的な自社の負の影響を特定、防止、軽減するとともにどのように対処したかについて説明するプロセス（「OECD 責任ある企業行動に関する多国籍企業行動指針日本語仮訳」参照）であるが、研究セキュリティ・インテグリティの文脈では、例えば、豪州のガイドライン（https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector）において、「十分な情報がない状況での決定をする際のリスク軽減に役立つ関連情報を得るために全ての合理的な措置が講じられるプロセス（仮訳）」（Due Diligence - A process where all reasonable steps are taken to obtain relevant information that will help reduce the risk of making an uninformed decision.）とされている。

の国家や非国家による研究への不当な干渉を防止する研究セキュリティの観点からの取組が重要であり、責任ある国際協力を推進していく必要がある。

- 主要国も、研究セキュリティの取組を推進しており、2024 年に入り 1 月には EU、カナダが研究セキュリティに関連する政策を発表している。また、2024 年 4 月の日米首脳会談における日米首脳共同声明「未来のためのグローバル・パートナー」においても、重要・新興技術の振興及び保護等によって、日米の技術的な優位性を高めるとともに、我々の経済安全保障を強化するとの文言[7]が盛り込まれている。
- 日本ではこれまで内閣府（科学技術・イノベーション推進事務局）を中心に「研究活動の国際化、オープン化に伴う新たなリスクに対応する研究インテグリティの確保に係る対応方針[8]」に基づいて取組が行われてきたが、産業技術総合研究所の外国籍研究者による機密情報漏洩事案の発生（2023 年 6 月）、宇宙航空研究開発機構に対するサイバー攻撃（2023 年 11 月）もあり、研究セキュリティの観点からも取組の強化・徹底が求められている。

（２）研究セキュリティに係る各国の動向

- 外国からの不当な影響への対応の必要性については各国とも認識している一方、研究セキュリティといった言葉の捉え方は各国で異なっており、米国のように政府文書で明確に定義を定めている国、カナダや EU のように政府文書で言及している国、英国や豪州のように類似の概念に基づいて取組を進めている国など様々である。また、各国の政策文書には科学的発見とイノベーション促進の基盤として、学問の自由や研究活動の開放性が不可欠である旨、記載されており、各国とも国際協力を適切に進めるために研究セキュリティが必要であると位置づけている。
- 米国では、2021 年「米国政府支援の研究開発に関する国家安全保障戦略についての国家安全保障大統領覚書 33 号」（NSPM-33）や 2022 年「NSPM-33 実施ガイダンス」において、研究セキュリティが明確に定義されるとともに、情報開示の要件とプロセスの強化、リスクの特定と分析等、自国政府が支援する研究開発を外国政府の干渉や搾取から守るための行動についての指示がなされた。また、2022 年「CHIPS・科学法」も併せ、国防省やエネルギー省等の関係連邦省庁や、米国科学財団（NSF）等の資金配分機関において、研究セキュリティを確保するための各種取組が進められている。

---

[7] Leading on Innovation, Economic Security, and Climate Action
The United States and Japan aim to maximally align our economic, technology, and related strategies to advance innovation, strengthen our industrial bases, promote resilient and reliable supply chains, and build the strategic emerging industries of the future while pursuing deep emissions reductions this decade. Building on our efforts in the U.S.-Japan Competitiveness and Resilience (CoRe) Partnership, including through the U.S.-Japan Economic Policy Consultative Committee (our economic "2+2"), **we intend to sharpen our innovative edge and strengthen our economic security, including by promoting and protecting critical and emerging technologies.**

[8] https://www8.cao.go.jp/cstp/kokusaiteki/integrity/integrity_housin.pdf

- カナダでは、2021 年、政府より「研究パートナーシップに関する国家セキュリティ指針」を発表し、この方針を実施するための予算措置が 2022 年度からなされるなど、研究セキュリティ関連の取組を進めているところ。2024 年には、政府より 11 の「機微技術研究分野リスト（Sensitive Technology Research Areas)」と「指定研究機関リスト（Named Research Organizations)」を公表。また、同年初頭より、主要研究助成機関に申請のあった機微技術分野の研究に関連する助成金申請について、「当該資金で支援される活動に関与する研究者が指定研究機関リストにある機関に所属する、またはそこから資金等の支援を受けている場合は資金が提供されなくなる」と発表した。この他、オープンソース・デュー・ディリジェンス[9]のガイダンスを公表する等、研究セキュリティを確保するための各種取組が進められている。
- EU では、「欧州経済安全保障戦略」の実施の一環としての、2024 年１月の経済安全保障政策パッケージの発表を経て、同年５月に研究セキュリティに関する理事会勧告を採択[10]。当該勧告では、関連する取組についてのガイドラインやリストの策定、研究の国際協力に関連するリスクへの対処を支援するサポートサービスの創設や強化、政府内の分野横断的な協力の強化や、研究資金配分機関や研究実施機関に関するものを含め、加盟国に対して 14 の勧告がなされている。加えて、欧州委員会に対しても、「欧州研究セキュリティ専門知識センター（European Centre of Expertise on Research Security)」の設置を含む、より構造的な支援のオプションを検討し評価する旨の、11 の勧告がなされている。

  また、EU 加盟国でも関連の取組が進められており、例えばオランダでは、研究セキュリティと類似の概念として「知識の安全保障（knowledge security)」を掲げている。2022 年、国際共同研究において機会と安全上のリスクを検討することが求められる、大学・研究機関の管理者に向けて「知識の安全保障に関する国家ガイドライン」を公表し、オランダ研究科学機構（NWO）に資金支援の申請書を提出する際は、同ガイドラインを遵守することが要件とされる等、研究セキュリティを確保するための各種取組が確認できる。
- 英国では、政府が自国の研究・イノベーション部門の継続的な成功に不可欠な国際研究協力の完全性を確保することを目的に、2019 年より「Trusted Research」キャンペーンを開始した。同キャンペーンは、英国の研究者、大学、産業界が国際協力に自信を持ち、潜在的なリスクに関して十分な情報に基づいた意思決定を行えるよう支援し、研究

---

[9] カナダのガイダンス（https://science.gc.ca/site/science/sites/default/files/documents/2022-10/ISED-Research-Portal-Guide-EN-FINAL.pdf）では、「意思決定を支援するために公開情報を収集し、分析するインテリジェンス分野（仮訳)」(an intelligence discipline that collects and analyses public information to support decision-making）とされている。本提言では、以降、様々な形での公開情報に基づいたデュー・ディリジェンスをオープンソース・デュー・ディリジェンスとする。

[10] https://www.consilium.europa.eu/en/press/press-releases/2024/05/23/council-adopts-a-recommendation-to-enhance-research-security/

者や職員を潜在的な盗用、悪用、窃取から保護するための取組であり、アカデミアや産業界に対してそれぞれガイダンスを発出している。また、大学向けの公的な相談窓口である「研究協力アドバイスチーム（Research Collaboration Advice Team）」を設置し、国際共同研究における国家安全保障上のリスクについての相談や質問への個別対応も行っている。さらに政府は、開放性と独立性を維持しつつ、大学内の研究セキュリティ能力を開発するための資金オプションも含め、英国の大学を外国による国家安全保障上の脅威から守るための方策に関する協議を今夏から開始する意向を表明している。

- 豪州では、政府と大学や資金配分機関が共同で設置したタスクフォースが、「大学セクターに対する外国干渉に対抗するためのガイドライン」を発出し、外国干渉を受けるおそれのある職員に対し、外国の所属等の情報開示の要求や意思決定者に外国干渉リスクを知らせるためのデュー・ディリジェンスの実施を推奨している。また、同ガイドラインに基づいて、各大学で自主的な取組が進められるとともに、資金配分機関である豪州研究評議会（ARC）において、競争的資金の申請が重要技術に該当する場合はそのリスクを検討する等、研究セキュリティを確保するための取組が確認できる。
- 日本では、2021 年 4 月、統合イノベーション戦略推進会議において「研究活動の国際化、オープン化に伴う新たなリスクに対する研究インテグリティの確保に係る対応方針について[11]」を決定し、この政府方針に基づいて競争的研究費に関するガイドラインの改定[12]、研究者、所属機関向けのチェックリスト雛型を作成[13]するなどし、これらの研究インテグリティの取組のフォローアップ調査、大学等関係機関へのアウトリーチを実施してきた。2024 年 3 月には、国立研究開発法人改革の中で研究セキュリティ・インテグリティの確保・徹底を含めた関係省庁申し合わせを公表[14]した。これによりＧ７の取組を紹介する形以外で、初めて研究セキュリティについて政府文書の中に記載された。

（３）オープンで自由な研究環境を確保し、同志国等と対等な立場で国際共同研究を実施するために必要な研究セキュリティ対策（相手国から求められ得る研究セキュリティの対策）について

- 米国をはじめとした各国の政策文書でも、研究におけるオープン性や協力の重要性が謳われている一方、米国 NSPM-33 に記載されているように、一部の国は、このオープンな研究環境を利用して、研究実施のコストとリスクを回避しつつ、不当に自国の競争力を増大させようとしている。これらを踏まえて、研究成果の公開の原則等を維持し、オ

---

[11] https://www8.cao.go.jp/cstp/kokusaiteki/integrity/integrity_housin.pdf

[12] https://www8.cao.go.jp/cstp/kokusaiteki/integrity/shishin.pdf

[13] https://www8.cao.go.jp/cstp/kokusaiteki/integrity/checklist1.pdf（研究者向け）
https://www8.cao.go.jp/cstp/kokusaiteki/integrity/checklist2r.pdf（大学・研究機関向け）

[14] https://www8.cao.go.jp/cstp/stsonota/kinoukyouka/kinoukyouka.html

ープンで自由な研究環境を確保したうえで国際協力を推進していくために、研究セキュリティについての施策を検討すべきである。

- 同志国等の制度やその実態を踏まえ、我が国が経済安全保障上の重要技術の育成に関して、相手国と対等な立場を維持し、国際協力を深化、拡大させていくためにどのような対策が必要であるか。以下、前述のＧ７での整理に沿って記載する。

① リスクにさらされている研究領域の特定と情報共有

- 各国では、研究インテグリティの取組を基礎としつつも、リスクの高い研究領域を特定し、研究コミュニティを対象として研究セキュリティ・インテグリティの取組を実施している。我が国においても、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である。その上で、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を推進していく上で、相手国から求められる場合や、同志国等と対等な立場で実施することを念頭に、競争的研究費を投入する研究開発プログラムの性質に応じ、特定の研究領域[15]における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を行っていくことが必要であり、当該研究開発プログラムの資金支援を行う各府省において当該研究セキュリティの取組の検討を行うことが必要ではないか。
- なお、リスクの高い研究領域の特定にあたっては研究者・研究機関、資金配分機関、関係省庁等が十分に検討・議論することが重要である。

② デュー・ディリジェンスを実施し、透明性及び関連情報の開示を確保することにより、リスクのある活動の領域を特定。標準的な組織慣行として、個々の研究プロジェクトについてリスク軽減策を実施

- 諸外国では、デュー・ディリジェンスの実施にあたり、研究者や研究機関が参照するチェックリストやガイドラインを公表している。我が国においても、国が支援を行う研究開発プログラムに関して、実効的なデュー・ディリジェンスの実施に資するようなガイドライン、チェックリスト等の検討が必要ではないか。
- その際、リスクマネジメントの観点からリスクに応じた段階的な対応が可能となるよう検討を行うことが必要と考えられる。

---

[15] 例えば、2024 年 4 月の日米首脳会談における日米首脳共同声明「未来のためのグローバル・パートナー」において例示された分野（We are committed to strengthening our shared role as global leaders in the development and protection of next-generation critical and emerging technologies such as AI, quantum technology, semiconductors, and biotechnology through research exchange and private investment and capital finance, including with other like-minded partners.）の他、経済産業省の有識者会議の資料（経済安全保障に関する産業・技術基盤強化アクションプラン改訂版 令和 6 年 5 月）のように、研究セキュリティの更なる取組を要する経済安全保障上の重要技術として、経済安全保障の観点から技術優位性のある分野（これから技術優位性を確保しようとする戦略分野も含むもの）とすることが一案。

具体的には、

１）競争的研究費を投入する研究開発プログラムについては、研究成果の公開を前提とする研究であることが想定されるが、政府方針に基づく研究インテグリティの取組が実効性を持った実施に繋がるよう、ガイドライン、チェックリスト等を作成・周知し、資金配分機関や研究機関等において所要の確認を徹底するといった実態的に有効な手法についての検討が必要ではないか。

２）競争的研究費を投入する研究開発プログラムのうち、リスクの高い研究領域を含む特定の領域において、ⅰ．国際共同研究の実施に関して、相手国から求められる場合や、ⅱ．同志国等と対等な立場で研究を実施するために必要な場合は、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が必要となると考えられる。

また、上記の他、パイロット、トップランナーとして、諸外国の先進的な取組と同等の取組が必要な場合は、先行的に研究セキュリティの取組を実施することも想定される。

- こうした２）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の一例として、例えば、外部の公開情報に基づいたデータリソースの利用や、複数の研究機関でコンソーシアムを形成してデュー・ディリジェンスを行う仕組みを創設するなどしてオープンソース・デュー・ディリジェンス等の充実によるリスクマネジメントを実施していくことも考えられるのではないか。
- 実際にこのような取組を行っていくにあたり、まずは、オープンソース・デュー・ディリジェンスの具体的な事例を蓄積し、研究現場の規模や実情に応じたより効果的な実施方法を検証し、蓄積した好事例を横展開していくことが一つのやり方ではないか。

③　研究関係者間で研究セキュリティ・インテグリティに関する対話・情報共有を行うための場及び認識を増進させるリソースの確立

- 我が国においても、研究資金を提供する省庁・機関のみの活動だけでなく、水際対策なども含め、捜査・公安当局、法執行機関等も含めた政府内の関係機関の連携を促進していくべきではないか。
- 研究資金を提供する省庁・機関等を中心に、研究機関等からの相談等の窓口設置や政府と研究コミュニティとの双方向の情報交換の場の創設やその機能の強化について検討が必要ではないか。

（４）今後の課題・留意点等

- 米国では、NSPM-33 において、研究セキュリティ・インテグリティ確保のための連邦省庁、特に国土安全保障省（DHS）に対し、国務省（DOS）と連携して留学生・外国人研究

者の審査をすることを要求[16]。我が国においても、入国時における審査を徹底するなど、関係省庁が緊密に連携して水際対策を更に強化するべきではないか。

- 経済安全保障をめぐる国際的な動きに応じた対応をするため、研究セキュリティ・インテグリティに関するリスクの特定等に関する調査分析機能を強化する必要があるのではないか。
- 各関係機関の現場において、規模や実情に応じた研究セキュリティ・インテグリティの取組を徹底するために必要な体制や、先行的な取組の実施等についても検討していく必要があるのではないか。
- 研究セキュリティ・インテグリティの取組はオープンな環境を確保し、国際協力をよりいっそう推進するためのものであり、取組の推進により特定国や特定の研究者の差別助長につながらないよう十分な配慮が必要ではないか。
- 研究セキュリティ・インテグリティの取組は、多くの関係機関が一体となって推進する必要があるため、本提言の内容や総合科学技術・イノベーション会議での検討も踏まえ、必要に応じ政府関係機関の共通の方針の策定や実施にあたっての工程表を作成するなどして着実に取組を実施していく必要があるのではないか。

２．経済安全保障上の重要技術の研究開発成果の社会実装と技術流出防止について

（１） 背景・現状

- 2023 年６月、産業技術総合研究所の職員が不正競争防止法違反の容疑で逮捕される事案が発生するなど、企業等が持つ「営業秘密」の漏洩を巡る摘発が後を絶たない状況である。
- 一方、米国では 2022 年８月、「CHIPS・科学法」を制定し、半導体関連の設備投資等の支援が可能な基金を含め、５年間で計 527 億ドル（約 7.6 兆円）の支援提供を決定した。加えて、助成対象者から安全保障上の懸念国への技術ライセンスや製造能力拡大等を禁じるガードレール条項を公表した。
- 技術流出の経路は様々であるが、大きく「モノ」による技術流出、「カネ」による技術流出、「ヒト」による技術流出の３つに分類できる。このうち、「モノ」及び「カネ」による技術流出については外為法における輸出管理及び投資管理の対象であり、現在、別途、技術流出防止策のための検討が進められているところである。
- 「ヒト」による技術流出については、営業秘密を不正な方法により取得、開示する行為について、適切な営業秘密管理を行っている前提で不正競争防止法の対象となる。営業

[16] 未来工学研究所「研究インテグリティ（Research Integrity）に係る調査・分析」（令和 5 年 3 月）
国土安全保障長官は、国土安全保障省（DHS）が国務省と連携し、米国の研究開発事業に 参加・参画しようとする非移民学生及び交換訪問者の外国人個人を国家安全保障上のリスクについて確かに審査する責任がある。国土安全保障長官は、教育及び文化交流プログラムのために米国に来る外国人の合法的な入国と滞在を支援しながら、国家の安全を守るために、留学生及び研究者に関する情報を DHS が保持することを、適用法に沿って確実に行う責任がある。

秘密管理の一環として、転職時に秘密管理や競業避止などの誓約書を求めるケースもあるが、実効性が不明という課題も指摘されているところである。また、安全保障の裾野が経済分野に急速に拡大する中、国として重要な技術を適切に管理することが喫緊の課題である。

- そこで、経済安全保障推進法に基づくサプライチェーン支援においては、2024 年３月、我が国が優位性を有する特定重要物資やその部素材について、その中核的な技術がひとたび流出すれば、将来における当該物資の外部依存につながり得ることに鑑み、以下の技術流出防止措置を実施することを計画の認定要件として追加したところである（詳細は参考参照）。
  （ア） コア技術等へのアクセス管理
  （イ） コア技術等にアクセス可能な従業員の管理
  （ウ） 取引先における管理
  （エ） 技術移転等
- また、日本企業 770 社が回答した質問調査によって、営業秘密の漏洩を検知する活動を行っていない企業は、自社では営業秘密漏洩が起きていないと回答しているのに対して、検知活動を行っている企業は営業秘密漏洩を経験したとする回答が有意に増加することが示されている。実際に多くの営業秘密漏洩が起きているにもかかわらず、自社の営業秘密の漏洩に気づいていない企業が多く、実際の漏洩は公表されている数値よりはるかに多いことが示唆されている[17]との情報がある。

（２） 国が支援を行う研究開発プログラムに関する入口から出口までの段階に応じた技術流出防止策の検討

- 経済安全保障推進法に基づくサプライチェーン支援においても、我が国が優位性を有する特定重要物資やその部素材について、国から資金支援を行う場合、一定の技術流出防止措置を求めているところである。そこで、国が支援を行う研究開発プログラムに関しても、我が国の技術優位性の強化を目指す技術領域及び将来の我が国の技術優位性の創出を目指す技術領域における社会実装を見据えた研究開発成果の技術流出防止のため、入口から出口までの段階に応じた対策が必要である[18]。
- 具体的には、主に、
  ・破壊的技術革新が進む技術をはじめ、将来の技術優位性の創出を目指す技術領域
  ・我が国が技術優位性を持つ技術領域のうち、既に一定の技術流出防止措置を求めている特定重要物資を除く領域

---

17 https://www.semanticscholar.org/paper/Empirical-study-regarding-the-leakage-of-know-how-Hirai-Watanabe/525532821be1b0af5baa574f3f00455f430eaa9c

18 一方、外為法における安全保障貿易管理は、国際社会の平和・安全の維持を目的とし、国からの資金支援の有無によらず、軍事転用可能な貨物・技術の輸出について法的規制を課すものである。

として各府省が支援し、決定する社会実装を見据えた研究開発プログラム（特に、国際共同研究にあたり相手国から求められる場合や、同志国等と対等な立場で実施するために必要な場合に、各府省が支援し、決定する研究開発プログラムも含む）を対象領域とするべきではないか[19]。

① 該当する研究開発プログラムにおいて求められる技術流出防止措置要件

- 経済安全保障推進法に基づくサプライチェーン支援において、先行して技術流出防止措置要件（詳細は参考参照）を定めていることから、上述の研究開発プログラムに関しても、当該技術流出防止措置要件を踏まえつつ、対策を講じることが有効といえる。
- 対象技術は、社会実装を見据えた研究開発を行うものであることに鑑み、国の支援を受けて行う研究開発の成果及びその活用の際に必要となる技術の設計・生産・利用の各段階において有用かつ中核的な技術（ソフトウェアを含む）（以下「コア重要技術」という。）及びコア重要技術の実現に直接寄与する技術（以下「コア重要技術等」という。）のうち非公知のものとすることが考えられる。
- 技術流出防止措置要件としては、コア重要技術等に関して、経済安全保障推進法に基づくサプライチェーン支援における措置を踏まえ、当該対策における（ア）から（ウ）までにあたる事項に相当する事項を充足するにあたり、リスクに応じ、オープンソース・デュー・ディリジェンス等の技術流出防止措置を行うことが有効といえる。その際、企業ヒアリングの結果から得られた以下に挙げるような、事業や研究開発の国際化を前提にした上での企業等での独自の取組による営業秘密管理強化の好事例も参考にすることも考えられるのではないか。

  <u>（ア）技術へのアクセス管理</u>

  ・物理環境のセキュリティ整備として、社内のワーキングエリアにおける段階的なセキュリティゾーンを区分けし、それぞれのゾーン内で取扱可能な文書等の情報区分を規定する。

  ・研究開発段階のもの、実際に生産・製造を視野に入れた開発段階のもの等、それぞれの研究内容に合わせて、技術へアクセス可能な従業員の範囲を適切に設計する。特に、例えば生産・製造技術の場合、生産・製造を視野に入れた開発段階においては、生産・製造プロセスの全工程にまたがって技術の全体像を知る従業員をできる限り限定するとともに、当該従業員に対しては所要の処遇を行う。

---

[19] 例えば、2024 年 4 月の日米首脳会談における日米首脳共同声明「未来のためのグローバル・パートナー」において例示された分野（We are committed to strengthening our shared role as global leaders in the development and protection of next-generation critical and emerging technologies such as AI, quantum technology, semiconductors, and biotechnology through research exchange and private investment and capital finance, including with other like-minded partners.）の他、経済産業省の有識者会議の資料（経済安全保障に関する産業・技術基盤強化アクションプラン改訂版 令和 6 年 5 月）のように、研究セキュリティの更なる取組を要する経済安全保障上の重要技術として、経済安全保障の観点から技術優位性のある分野（これから技術優位性を確保しようとする戦略分野も含むもの）とすることが一案。

（イ）技術にアクセス可能な従業員の管理

・重要な技術をもつ従業員を把握し、当該従業員への外部からの接触の有無を確認するなど、リスクの管理を行う。

・退職後の競業避止義務の誓約について、重要な技術をもつ従業員に同意を得、一定期間有効なものとするための取組として、ストックオプションの行使や割増退職金支給の条件として、競合他社に転職しないことを定める。

（ウ）取引先（共同研究パートナー等のサードパーティを含む）における管理

・取引先を経由した技術流出防止のため、取引先のリスクを評価するチェックリストを作成するとともに、取引先から提出された情報を元にリスク評価を行い、公開・非公開部分の適切な線引きを行った上で戦略的に連携を行う。

（ア）から（ウ）まで共通　リスクマネジメントの観点からのデュー・ディリジェンス、モニタリング等の仕組み

・リスクに応じ、デュー・ディリジェンスを実施する。例えば、Need to know の原則に基づき、特定のプロジェクトに関してはプロジェクト毎に本人の同意を得たうえで、個別に、秘密保持契約の締結、本人からの情報提供、本人による情報管理等に関する誓約の取得、オープンソース・デュー・ディリジェンスなど、アクセス可能な従業員の選定にあたり、そのプロジェクトの参加の段階から、プロジェクト毎の性質に応じた段階的なリスクマネジメントとして所要のデュー・ディリジェンスを実施する。

・リスクマネジメントの観点から、重要な情報が適切に管理されているか、情報を大量に持ち出す等不自然な動きが無いか等について業務の IT 化とあわせてモニタリングを実施する。さらに、怪しい挙動が確認された際、メールを含む電子コミュニケーションやデータストレージについて監査できる体制を構築する。

・全社員が遵守すべき情報管理規律を整備するとともに、当該規律遵守の署名やフォローアップを実施する。

・内閣府（科学技術・イノベーション推進事務局）が公表している研究インテグリティのチェックリスト等を参照し、社内や取引先のリスク等に関する取組について、社内での啓発活動等を行う。

・経済安全保障担当の部署横断的な組織を設置し、関係部局からの情報を集約し、総合的な相談窓口業務や組織横断的なリスクマネジメントを実施する。

- なお、技術流出防止策を講じるにあたっては、プロジェクトに参画する研究者からの過度な敬遠を防ぐため、それぞれの研究の特性やリスクにあわせたメリハリのある必要十分な対策を講じるべきである。例えば、研究者の記憶にとどまる残留情報の管理などは、研究者からの過度な敬遠につながる場合があるため、研究者の記憶にとどまる残留情報は開示や使用の制限の対象外とするなど留意が必要である。

② 日本版バイ・ドール制度の特定条項の論点（特に経済安全保障上の重要技術に係る社会実装を目的とする政府等からの研究開発委託の際における特許権等の海外移転の整理）

- 国が企業、大学、研究機関等に委託した研究開発において得られた特許権等の知的財産権は、産業技術力強化法第１７条により、研究開発を受託した者に帰属させることが可能とされている（いわゆる「日本版バイ・ドール制度」）。
- このため、国が実施するほぼ全ての委託研究開発プログラムで、研究開発の受託者に知的財産権を帰属させることも可能となるような委託契約がなされている。
  （なお、一部の委託研究開発については、成果の保全等が必要なことから、本制度を適用せずに、当該成果に係る知的財産権を国の所有とする場合がある。）
- ただし、当該知的財産権の移転等にあたっては、子会社又は親会社への移転等を除き、あらかじめ国の承諾を受けることを条件としている。
- 日本版バイ・ドール制度では、国の委託研究開発から生じた知的財産権を受託者（民間企業等）に帰属することを可能としているが、受託者の子会社又は親会社が国外企業である場合等、国による委託研究の成果が国外流出することを防止できない可能性がある。
- 想定され得るケースとしては例えば、①国外企業の日本法人が親会社に知財を移転する場合②国内企業の子会社がM&A等により新たに国外企業の子会社となり、当該国外企業に事業売却・譲渡を行う場合③国内企業の本社が国外に移転し、国外企業となる場合が考えられる。
- 一方、経済産業省は「委託研究開発における知的財産マネジメントに関する運用ガイドライン」を作成し、国外企業たる親会社又は子会社への知財の移転にあたっては、「研究開発の委託者に事前連絡の上、必要に応じて契約者間の調整を行うことについて、委託契約書において定めておくことが重要」としている。
- しかし、ガイドラインの適用対象は経済産業省又は経済産業省所管の独立行政法人[20]が

---

[20] 経済産業省所管の独立行政法人・研究開発法人であるNEDOの業務委託契約標準契約書においては、ガイドラインの適用にあたり、以下のような条項を設け、子会社・親会社への知的財産権の移転等における国の承諾を不要とする規定を、国外企業への移転に限り適用除外している。

（知的財産権の所属）
第31条
3　乙は、次の各号に掲げる事項を遵守しなければならない。
一～三　（略）
四　当該知的財産権の移転（第３１条の６第１項に規定する持分の放棄を除く。以下この号において同じ。）、又は特許権、実用新案権若しくは意匠権についての専用実施権（仮専用実施権を含む。）又は回路配置利用権若しくは育成者権についての専用利用権（以下「専用実施権等」という。）の設定若しくは移転の承諾をしようとするときは、あらかじめ甲の承認を受けるものとすること。ただし、合併又は分割により移転する場合、及び次のいずれかに該当する場合は、この限りではない。
イ　乙が株式会社であって、その子会社（会社法第２条第三号に規定する子会社をいう。）又は親会社（会社法

委託する技術に関する研究開発にとどまっている。

- そこで、少なくとも、国による経済安全保障上重要な技術の委託研究開発の成果について国外企業等に知財を移転する場合は、受託者に事前連絡を求めるとともに、委託者は当該事前連絡を確認の上、契約者間の調整を行うよう徹底することが必要ではないか。

（３） 今後の検討課題・留意点等

- 経済安全保障上の重要技術の研究開発成果の社会実装を見据え、今後の研究開発プログラムの検討、実施にあたり、必要に応じ、官民対話などを実施しつつ、関係する各府省の間で共通の方針（基準や取組）を調整した上で、各府省において、技術流出防止策をとるべき研究開発プログラムを特定し、当該プログラムにおける技術流出防止策を新たに徹底する必要があるのではないか。
- また、技術流出防止策をとるべき研究開発プログラムの特定にあたり、経済安全保障をめぐる国際的な動きも考慮し、何が我が国にとってリスクとなるのか調査分析を行う機能を強化する必要があるのではないか。
- 事業や研究開発の国際化を前提にした上での企業等での独自の取組による営業秘密管理強化の好事例も参考にして、企業等の規模等も考慮しつつ、リスクに応じた適切な対応となるよう、必要な技術流出防止策を円滑に実施するための施策について検討する必要があるのではないか[21]。

第２条第四号に規定する親会社をいう。）に当該知的財産権の移転又は専用実施権等を設定若しくは移転の承諾をする場合（ただし、その子会社又は親会社が日本国外に存する場合を除く。）

[21] 例えば、K Program では、「適切な情報管理に必要な費用は、委託研究契約等における研究開発経費（直接経費）として支出することができるものとする。」との規定を設けている（令和４年９月 16 日 経済安全保障重要技術育成プログラムの運用・評価指針）。

【参考】 経済安保推進法に基づくサプライチェーン強靭化における対応（技術流出防止措置要件の追加）

我が国が**優位性を有する特定重要物資やその部素材**について、その**中核的な技術がひとたび流出すれば、将来における当該物資の外部依存につながり得る**ことに鑑み、以下の**技術流出防止措置を実施することを計画の認定要件として追加**（2024年３月）

※ 対象物資は、**工作機械・産業用ロボット**、**航空機の部品**、**半導体**、**蓄電池**、**先端電子部品**
（いずれも認定に係る特定重要物資・その原材料等に関するもの。）

＜安定供給確保取組方針＞（抜粋）

（ア）**コア技術**（生産に有用かつ中核的な技術及び当該取組の成果である技術）及び**コア技術の実現に直接寄与する技術**
（以下「**コア技術等**」という。非公知のものに限る。）へのアクセス管理
・コア技術等に**アクセス可能な従業員を必要最小限の範囲に制限し**、併せて**適切な管理を行うために必要な体制や規程を整備**する

（イ） コア技術等にアクセス可能な従業員の管理
・上記従業員の**相応な待遇（賃金、役職等の向上）**を確保するなど、**退職等を通じたコア技術等の流出を防止**する措置を講じる
・上記従業員が**退職する際にはコア技術等の守秘義務の誓約**を得る
・関係法令に十分配慮しつつ、**退職後の競業避止義務の誓約**についても上記従業員に同意を得るための取組を行う

（ウ）取引先における管理
・取引先がコア技術等の全部又は一部を有する場合、保有の事実及びその詳細について、当該取引先と**秘密保持契約を締結**する
・（ア）、（イ）に相当する内容の措置を講じることを求め、関係法令に十分配慮しつつ、その**履行状況を定期的にレビューするなど取引先からのコア技術等の流出を防止するために必要な措置**を講じる

（エ）技術移転等
・コア技術等の技術移転により、**取組対象物資の外部依存・供給途絶に陥る蓋然性が高まることのないようにすること**
・申請者又はそのグループ会社が**次に掲げる＜他者又は他国に対する行為＞**のいずれか**を行おうとする場合**であって、
①又は②に該当するときは、当該行為を実施する前に十分な時間的余裕をもって**物資所管省庁（経産省）に相談**を行うこと

＜他者又は他国に対する行為＞
- 他者**（申請者の子会社を含む）**に対し、**コア技術等に係る知的財産権を移転**する、供給確保計画の認定の対象とする取組に係る**事業を譲渡する**等、**コア技術等そのものを移転**する場合
- 他者に対し、**コア技術等を提供**する場合
- 他者と**コア技術等に関する共同研究開発**を行う場合
- 他国において**コア技術等に係る研究開発**を行う場合
- 他国において供給確保計画の認定の対象とする品目のうち**コア技術等を用いたものを生産する拠点を建設**し、又は**既存の生産拠点における設備投資**を行い、結果として**当該生産拠点における当該品目の製造能力が10%を超える割合で増強**する場合
（ただし、当該生産拠点で生産する当該品目の85%以上が当該他国で消費される場合を除く。）

① コア技術等の**強制的な技術移転のおそれ**があること、又は**他者の属性**※**によりコア技術等の流出のおそれ**があることを**申請者が知った場合**
※「過去５年間において、国際連合の決議その他国際的な基準に違反した実績がある者」又は「外国政府等による影響を受けて事業を行う者」

② ①のおそれがあるとして物資所管省庁（経産省）から**事前相談をすべき旨の連絡を受けた場合**

引用：経済安全保障法制に関する有識者会議 官民技術協力に関する検討会合（第３回）資料１

経済安全保障法制に関する有識者会議 構成員

（五十音順）

青木　節子	慶應義塾大学大学院法務研究科 教授
阿部　克則	学習院大学法学部 教授
上山　隆大	総合科学技術・イノベーション会議 常勤議員
大橋　　弘	東京大学大学院経済学研究科 教授
兼原　信克	同志社大学 特別客員教授、公益財団法人笹川平和財団 理事
北村　　滋	北村エコノミックセキュリティ 代表
小柴　満信	経済同友会 経済安全保障委員会 委員長
小林いずみ	ANA ホールディングス株式会社 社外取締役
角南　　篤	公益財団法人笹川平和財団 理事長
土屋　大洋	慶應義塾大学大学院政策・メディア研究科 教授
長澤　健一	キヤノン株式会社 顧問
畠山　一成	日本商工会議所 常務理事
羽藤　秀雄	住友電気工業株式会社 代表取締役 副社長
原　　一郎	日本経済団体連合会 常務理事
松本洋一郎	東京大学 名誉教授
三村優美子	青山学院大学 名誉教授
渡井理佳子	慶應義塾大学大学院法務研究科 教授
渡部　俊也	東京大学未来ビジョン研究センター 教授