第 3 回「研究セキュリティと研究インテグリティの確保に関する有識者会議　議事録概要

1. **日時：**2025 年 6 月 11 日（水）：16:00-17:30
2. **場所：**野村総合研究所 東京本社 29F 会議室 13・14／Teams 会議（ハイブリッド開催）
3. **出席者：**

（**委員**）天谷委員、伊藤委員、上田委員、川原委員、桑田委員、佐々木委員、佐宗委員、佐藤委員、恒藤委員、橋本委員、宮園委員、山越委員、渡部委員

（**政府側**）濱野内閣府事務局長、塩崎内閣府事務局長補、白井内閣府参事官、吉田内閣府企画官、米山内閣府大臣官房審議官、垣見内閣府大臣官房参事官、上田内閣府大臣官房企画官

4. **主な議題：**

（１）座長挨拶

橋本座長より挨拶がなされた。

（２）重要技術の流出防止等のための枠組みについて：事務局説明

事務局から、資料についての説明があった。

（３）重要技術の流出防止等のための枠組みについて：討議

橋本座長から本日の会議の流れについて説明があり、事務局が紹介した資料について討議が行われた。

討議における、有識者委員からの主なコメント

- リスクマネジメントに関して、共同研究の相手先が大学・研究機関なら開始時のチェックで済むが、民間企業の場合は資本関係の変更等、開始時のみではとらえきれない部分もある。
- 企業は大学相手に秘密保持契約（NDA）や不正競争防止法に基づく営業秘密等に関する契約を結ぶことが多いため、今回の案では、その提出をもって代用できるとしている。また、開始時に一度確認するのみならず、研究が進行していく中で参画者が変わる場合などは随時対応していただくことを想定する。
- デュー・ディリジェンス（DD）については、大学と資金配分機関（FA）が調整し、FA が確認・評価し補完するような、大学と FA 間の協力的な対応の内容までを示していただけると大学としても安心できる。FA に相談窓口を設け、並走いただける体制を整備していただきたい。
- DD は実施者によって粒度が変わってくるだろう。基本的には、FA に対して「大学にただ依頼するだけでは大学現場が困る」としっかりと伝えていきたい。納得できるところまでは大学と FA で

の意見交換をしていただくプロセスを構築したい。

- 資料 p.12 において示した項目だけでは、各大学において粒度・深度がばらばらになりかねず、年度後半に、どこまでどのような内容を見るべきかという議論をさせていただきたい。モデル事業の取組を参考にしながら議論したい。
- 資料 p.13 の項目までリスク確認対象とする場合、大学側では準備期間が必要となるため、対象プログラムについては、準備期間を考慮した公募要領としていただきたい。場合によってはDD の締め切りと応募の締め切りといった 2 段階の締め切りを設けることも一案である。
- 公募期間は様々な要因で決定されているため、単に期間を延長するというよりは、FA と提案者の間で丁寧な会話がなされる仕組みを作り、現場が困らないような体制としたい。
- 資料 p.14 のリスク軽減措置の例示について、オフキャンパス整備やサイバー攻撃対策にはそれなりにリソース、金銭的資源がかかる。そのような対策が特に必要であると FA が判断した場合は、事業費内にその支援分を入れてほしい。
- リスク軽減策について金銭的資源が必要なのはその通りであり、予算措置がない場合にはそれに見合ったリスク低減策しかできない。その点は関係各所でも説明している。
- 研究参画者・研究分担者が海外の場合、寄付金や兼職等については公開情報から得ることは難しい。また、直接問い合わせた場合でも正直に答えていただけない可能性がある。
- 海外の研究分担者の情報については、当面はオープンソースの情報から始め、FA と相談していただく。一案として、先方から誓約書を出してもらうこともありうる。今後どのような方法とするかは検討したい。
- 研究機関が NDA を締結していること自体、FA に対して明かせないような場合は、手順書の内容に沿ってリスクマネジメントを進めていただく形が基本となると考える。
- NDA を締結したものの何か問題が発生した際に、研究代表者や研究機関が具体的にどのような責任を負うのかという点は論点となるのではないか。特に懸念されるのは、NDA の内容や対応が曖昧であるために責任の所在が不明確になるケースである。
- 相手側が虚偽の情報を提供した場合、その責任を研究機関や研究者に負わせることは不合理であり、現実的ではないと考える。最終的には NDA に基づき関係者に誓約書を提出してもらう形に落ち着く可能性が高いと考える。誓約書を提出することで、責任の所在を一定程度明確化することができる。
- DD 先として、サンプルの解析を外注する場合の委託先業者や、IT 調達（生成 AI、オンライン会議ツールアプリケーション、PC や携帯電話等の通信機器端末の調達）については、現状考慮していない。今後改めて提案し、議論いただきたい。
- 特定研究開発プログラムに従事する職員や FA の職員に対してもリスクマネジメントする必要がある。その点については次回相談したい。職員のみならず、選考にあたる PD・AD にも DD する必要がある。
- DD について、一定程度は相手先からの情報提供に基づく必要があり、すべてをオープンソースで行うのは限界がある。相手との信頼性の観点からも難しさがあると考える。

- 資料中の「リスクマネジメントの手順」のステップに含まれる「④実施状況確認」については、次回提示してご議論いただく予定である。
- 特定研究開発プログラムへの対応が数年に 1 回程度となるような中小規模大学については、その時のために体制を持っておくのはかなり厳しいと感じる。そのため、中小大学への支援等について手順書に明示的に記載される必要がある。
- 中小大学において、平時からの情報収集・管理はある程度できるものと考えるが、特定研究開発プログラムに関するリスクマネジメントにかかる情報収集は、確かになじみがない大学では困難である。FA との相談という形になるかと思うが、ある程度の支援を進めたい。
- DD 関連のツールを提供する民間の調査会社について、固有名詞は出さずとも手順書内に何らかの言及は必要だと考える。
- 外部ツールの活用については、最初から手順書に記載するとハードルを上げてしまう可能性がある。必要に応じて、あるいは FA との相談に応じて、外部のツールを使うこともある、といったことを記載することを検討したい。
- 各 FA は調査会社と契約するはずである。調査会社による DD 結果が必要な時は、FA が持つリソースとしての調査会社サービスを、大学側が利用できる、という形にしていただけるとありがたい。
- 今のところ FA に予算が付く話は具体的にはないが、当面、予算措置がなされるまでは無料のもので行い、予算が付くなら FA が対応すべきであると考える。
- 資料 p.7 の B 大学が海外の大学である場合の対応については、現状具体的な事例が存在しないため、運用していく中で検討していきたい。
- 大学間の情報共有の考え方についても手順書の中で示す必要があるのではないか。
- 自己申告や兼業届等は個人情報として大学が受領している情報であり、目的外利用が難しく、他機関への共有は不可能である。実際の運用上どのようなことができるのかを現場実態と合わせて確認する必要がある。
- 個人情報の扱いについては検討中であり、考え方をあらためて示す。
- 今回の提案では、「特定研究開発プログラムとして」という表現であったが、RS/RI の定義の明確化、再定義が必要である。
- 資料 p .13 のリスクマネジメントの実施事項に関して、大学自身が営業秘密として情報管理を行うのかはどこにも書かれていないため、整理が必要である。
- 可能であれば、内閣府等で、日本の研究機関が共通で使えるようなデータベースや検索ツールを用意していただけると効率的である。
- 検索ツールを国で設けることはなかなか難しい。オープンソースをベースに、一部大学では有料ツールも使いつつ、できるだけ負担がない方法を示したい。
- 資料 p .13 の「管理対象データ」等の管理に関して、「管理方針」と記載されているが、機微性の高い研究開発成果であることを踏まえると、方針だけでなく、本当に管理できるのかを確認する必要がある。

- 機微分野の研究開発では NDA だけでは不十分で、懸念人物が相手方チームにいる可能性もある。技術流出防止には NDA では代替できず、手順書の書き方に不安がある。
- 資料 p.13 の「管理対象データ」について、大学のサイバーセキュリティ対策はそこまで高くないと感じており、管理方針を示すだけでは保護になっていない。特に、特定研究開発プログラムにおいては通常のサイバーセキュリティ対策でよいのかという問題が出てくると思われる。とはいえ、各大学・研究機関にハイレベルのサイバーセキュリティ対策を一律で求めるのも無理がある。どこで線引きすべきか、誰が責任を持つのか。
- 機微性の高いデータは独立システムで管理することとし、その対応ができていれば、何か問題が起こっても責任は問わない、対応できていなければ責任を問う、という仕組みとすることが一案である。
- 情報セキュリティシステムはある特定のプロジェクトのみにかけているのではなく、大学全体にかけているものである。その上で、特定研究開発プログラムについては特にどのレベルが求められるのかを確認するという 2 段階程度になるのではと考えている。
- 特定研究開発プログラムは知名度も高くなり、攻撃側にとって格好の攻撃対象となる。国の信用にかかわるため十分注意する必要がある。
- これまで RS/RI の内容・概念が混乱していた。G7 の SIGRE で議論された国際基準に合わせて日本も修正するのがよいと思っている。
- 資料 p.10 の DD ツールについて、種類や費用についても政府や FA にて把握・整理してほしいという声をいただいている。
- 国内の誰かが DD ツールを開発しないといけないのではないかと考えられる。

以上