第５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 7 月 18 日（金）10:00-12:00
2. **場所：**内閣府　中央合同庁舎第 8 号館 6 階 623 会議室／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、佐々木委員、川原委員、佐藤委員、椹木委員、徳増委員、中尾委員、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、福永内閣府統括官、原内閣府審議官、白井内閣府参事官、立松内閣府参事官、吉田内閣府企画官、米山内閣府大臣官房審議官、大川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

橋本座長から挨拶がなされた。

（２）新任委員、事務局の紹介

事務局から、産業技術総合研究所の徳増委員、内閣府事務局の福永統括官、原審議官、立松参事官、内閣官房国家安全保障局の大川参事官の紹介が行われた。

（３）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。

（４）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、事務局が説明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（●有識者委員、⇒座長又は事務局）

《雛形について》

- 手順書を最も必要とし確認するのは各大学・研究機関の担当者であるため、「3-3 研究者に求められる事項」にセキュリティに関するチェックリスト雛形が含まれているとよい。セキュリティに関する体制を整備する上では規程を策定する必要があるため、大学は手順書の先に規程の雛形を求めている。規程の雛形を手順書に含めてほしい。

  ⇒雛形の策定については、基本的には資金配分機関（FA）との対話の中で行われる。FA の公募要領の雛形がそのまま使われる場合もあり、変更される場合もある。現場が混乱しない現実的な雛形を作成する必要がある。

- 特定研究開発プログラムへの対応体制として、研究セキュリティの取組に関する内規の制定が求められているが、国で雛形を用意することを期待する。

《民間企業について》

- 企業の取扱いは注釈にあり、年度後半の議論となると理解している。大学や研究機関の研究はオープンであることが前提だが、企業研究は原則クローズであり、実態に応じた見直しが必要である。研究者が法律違反等でペナルティを負うのは当然だが、企業の従業員の場合、研究者としての独立性よりも従業員としての立場が優先され、会社としての処分が行われる。

  ⇒国費を使った研究が対象であり、企業研究は対象外となることもある。
- 産学連携の場合にも手順書で求める対応をお願いすることがあり得る。これは国との研究開発に限らず、第三者との研究においても起こり得ることである。

  ⇒産学連携は本件とは別途産業界と大学の間の契約で決定するものだが、手順書を参考にすること自体は構わない。
- 企業が確認した際、各省庁から提出される内容が一致しているよう配慮してほしい。
- スタートアップ企業のリスク管理は手順書にあまり記載がない。仮に B 大学がスタートアップになる場合、DD 等のガバナンスが難しい。
- スタートアップ企業は、安全管理保障担当部局とは管轄が異なる。投資先としてのリスクの検討が必要である。大学発スタートアップの責任は子会社にあるのか、親会社である大学にあるのか確認したい。
- 民間企業と海外企業については、年度後半の議論となると承知した。

《サイバーセキュリティについて》

- サイバーセキュリティに関わる対応として、P.25 において研究機関に「サイバー攻撃対策の強化」や「政府の定めるレベルの遵守」を求めている。サイバー攻撃は最も懸念され、政府は研究機関・大学が自らのサイバー対策が悪意ある攻撃に十分対応できるかどうか相談できる窓口を設けるべきである。ケーススタディ共有等の対応も必要である。手順書にサイバーに関する言及が少なく、踏み込んで検討すべきだ。

  ⇒国立研究開発法人にはサイバー攻撃への対策に関するガイドラインや予算措置があるが、大学は予算も支援組織もない。現実的な方法として、技術の度合いに応じてインターネット接続の遮断や流出のリスクを想定した情報管理等の対策を講じる。実態が判明するのに従い、国としての対応を検討する。
- ケーススタディの共有や相談窓口等は、そこまで費用をかけずに実施することが可能である。現状の大学のレベルでは進化するサイバー攻撃に対応できない状況だが、最重要科学技術を扱う場合、流出しても仕方なく事後に対応を考えるということでは不十分である。

  ⇒政府機関と相談しながら対応したい。絶対に取られてはいけないデータはインターネットから分離することで対応する。
- P.18・19 の DD 実施はうまく運用できるだろうが、情報セキュリティについては懸念が残る。情報セキュリティに対する認識には個人差があるため、基準を設けたり、グッドプラクティスを共有したりすることが必要である。また、包括的な組織管理も重要である。例としては、鍵での物理的管理には消防法上の理由でマスターキーを誰でも入手できるような抜け穴が存在するケースもあるだろう。他には AI 使用等のインターネット接続前提の業務も多いため、インターネット接続の遮断が現実的ではないこともあるだろう。）

  ⇒何も対策していない現状から改善していくプロセスを議論していることをご理解いただきたい。悪意を持って

見せしめ攻撃をされる危険性があるが、その際も慌てず、皆で共有しながら前に進めることが大切である。
⇒サイバーセキュリティは日々変化する。産学官の仕組みや政府サポート体制の整備が重要である。官民協議会のような仕組みを NSS 中心に考えている。まずは 0 から 1 にし、1 から先を日々努力していく。

《手順書全般について》

- 手順書はマニュアルとして正確性を期すものであるとし、これまでに①企業秘密の取扱いの手続、②個人情報同意プロセス、③複数機関間契約、④学生や職員の取扱い、の 4 点を指摘した。具体的には、①不正競争防止法上の営業秘密管理を明確に求めているか否かが手順書上では不明である、②プロセスについての記載がない、③どのような契約を結ぶ必要があるかの記載がない、④学生・職員の取扱いの記載がない。これらは年度後半に追記するのか、確認したい。
  ⇒指摘は承知している。原案は大枠であり、年度後半に議論する。
- オープンソースデュー・ディリジェンス（DD）のエンティティリスト確認について、どのリストを選定するのか、その定義付けが必要である。頻繁に更新されるリストをすべての大学が自己費用で購入するのではなく、国からの提供も必要である。
  ⇒実際にどこまでできるか不明確であり、そのような問題を念頭に置いて議論を進める。
- 現場からは、手順書の実行可能性に不安がある。特定研究開発プログラムへの関与者の指定について、平時から全構成員を情報収集の対象とするのは現実的でなく、濃淡管理が必要である。その際、専門分野と指定された特定研究開発プログラムとの関係性、過去の海外機関との研究時の知財ライセンス契約、海外機関との共同研究実績を考慮する認識でよいか。
  ⇒対象者は限定される。まずはリテラシー向上を目指し、その上で委員御指摘の対応を行うという二段階の体制を考えている。各大学ができる範囲で実施するのが現実的である。
- 職員の所属や雇用形態も多様であるが、どのように対応するのか。
  ⇒プログラムごとに対応を指示することになるだろう。例えば半導体関連のプロジェクトでは関わる職員も指定される場合があるが、一般的なプロジェクトにおいてそこまでの指定は不可能である。FA が国と相談しながら範囲を明確にし、大学に伝える。並行して大学内のリテラシー向上の意識を醸成する。
- 特定のプログラムから開始し、やがて運営費交付金・国の予算のプロジェクトに適用が拡大されるとのことであるが、どのくらいの期間をかけて対象を拡大するのか。
  ⇒現段階では何年と明記できない。現実的な対応が必要である。
- 本会議が想定する海外からの脅威や不審なアプローチについての認識合わせをすることが重要である。手順書内に定義や例示があると現場としては研究者に説明しやすい。
  ⇒日本のみならず、海外各国事例も検討したいが、海外は情報開示に応じない場合がある。
- 大学職員向けのアンケートで、プライベートでの不審なアプローチや若手研究者のヘッドハンティングによる技術流出事例が報告された。手順書で対処できるリスクとできないリスクを年度後半で議論・整理いただきたい。
  ⇒退職者の再就職問題などもあるが範囲が広がりすぎるため、手順書記載事項の範囲で実施し、必要に応じて手順書を改訂するのではないか。リスク軽減（ミティゲーション）を主旨とし、ゼロリスクを目指すものではない。
- P.18（1）「特定研究開発プログラムに関与できる職員」の定義が曖昧である。一般的な業務上の関与が、手順書上の「関与」の範囲に含まれてしまう可能性があり、「特定研究開発プログラムにおける機微情報

取扱いの可能性のある職員」等のより絞った記載とすべきである。

- DD を各研究機関で実施するのは負担が大きい。大学間や FA から大学への過去事例・グッドプラクティス・出身機関情報等の知識の蓄積と共有の仕組みがあれば負担軽減につながる。
  ⇒知識の蓄積は重要であるため、政府の責任で行い、共有できるようにする。どこまで行うかは今後の議論となるが、大学に全てを任せても難しく、政府への提言も行っている。運用しながら作り上げるものであり、基本方針や公募要領に入れていくことになる。大学に丸投げすることはしない。
- 悪意ある第三者が情報を得ようとしたとき、個人レベルでの防御は不可能である。国や FA が情報漏洩を許容できないプロジェクトと判断した場合は特別なサポートが必要であり、体制を早急に立ち上げるべきである。
- 共同研究のカウンターパートのリスクアセスメントを研究代表者（PI）に求めるのは危険である。国や FA が必要と判断したプロジェクトの背景調査等は専門部隊が実施し、疑念があれば PI から必要な情報を得るという一貫体制の確立が必要である
- トライアンドエラーにより、小さなことからでも体制を確立すべきである。
  ⇒最初から完璧なものはできず、できることから実施する。絶対に取られてはいけないデータはインターネットから分離するのが現実的な方法である。
- 経済安全保障に関わる対応はコストを度外視して行わなければ、防御態勢がザルのようになる。
  ⇒御指摘は理解できるが、まず現実的に可能な対応としては先ほど述べた通りである。
- P.18「３-３　研究機関に求められる事項」においてリスクマネジメント（RM）の主体は研究機関であるが、その旨の記載がない。
  ⇒RM の主体について、実際には契約の中で記述される。

以上