資料２

「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２回）議事要旨

１　日時

令和６年３月26日（火）9時00分から11時00分までの間

２　場所

中央合同庁舎４号館1214会議室

３　出席者

（委員）

上山　隆大	総合科学技術・イノベーション会議　常勤議員
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
畠山　一成	日本商工会議所 常務理事
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
渡部　俊也	東京大学未来ビジョン研究センター 教授

（政府側）

高村　康夫	内閣審議官
彦谷　直克	内閣審議官
早田　　豪	内閣参事官
田中　伸彦	内閣参事官

４　議事概要

（１）事務局説明

事務局から、資料１の内容について説明があった。

（２）自由討議

（委員のコメント）

○経済安全保障分野における重要技術について、研究セキュリティの方向で物事を進めることは非常によろしいと考える。日米同盟を中心として、今後約10年間を見据えて、軍事的なオペレーションやインテリジェンスの分野での平等性が高まってきた。また、経済安

全保障分野においても輸出規制や大学等の規制について足並みが揃ってきた。今後の同盟国・同志国との協調を考えていく上では、安全保障に関する重要技術の面での協調が極めて重要と考えている。先般、政府で閣議決定され、現在国会で議論されているセキュリティ・クリアランス法案はこうした方向性を強めるものと考えている。さらに裾野を広げていくということになれば､アカデミア全体がこういったことに取り組んでいく必要がある。その前提としてこうした仕組みは必要。

〇経済安全保障分野における重要技術は、2017年３月24日に学術会議で決定された軍事的安全保障研究に関する声明の軍事的安全保障研究との関係はどうなっているのか。基本的に経済安全保障分野における重要技術は、軍事的安全保障研究に含まれないと政府から名言していただくと非常にありがたいが、多分そうではないと思っている。ただ、2017年の声明は、1950年と1967年の状況とほぼ同じものを踏襲しているという実態がある。1967年に武器輸出三原則が決まったが、このトリガーの一つになったのは、東京大学で開発したペンシルロケットがユーゴスラビアで発見されたということ。当時の政府は極めて厳しい武器輸出三原則といったものを設けた。実際問題として、それまで我が国は武器をずっと輸出し続けていた。今、防衛装備移転三原則の問題が出ているが、朝鮮戦争の際には我が国がつくったタンクが朝鮮で使われていた。紛争地域において輸出されていた。もちろん占領下ということもあるかもしれないが。武器輸出三原則のトリガーとなったのはまさにアカデミアにおける無神経ということは認識しておく必要がある。

〇つい最近も、産総研において情報漏えいの事案があった。我々として冷戦時代の思考形態をそのまま引きずっていてはならない。新しい安全保障環境に対応するための技術面での協力を進めていくための措置は可及的速やかに取る必要がある。こうした国内的な状況も踏まえた上で、我が国に合致した措置をぜひ決定していただきたい。

〇資料の経産省の事例について、ぱっと見て１つの共通点がある。それは、次世代コンピューティングを使って何ができるか、次世代クリーンテックを使って何ができるかという非常にボトムアップ的な、帰納法的な視点になっているというところ。経済安全保障において自給率は重要であり、食料自給率の他にエネルギー自給率もあり、最近はデジタル自給率等の視点から見ると、やはり違う見方ができるのではないかなという話をよくさせていただいている。今回、経済安全保障となると、経済の安全保障やテクノロジーは切っても切れないものであるが、エネルギー自給率の12％をどうやったら引き上げることができるのか。また、今、デジタル赤字と言うと、この間、報道で5.4兆円と出ていたが、多分パブリッククラウドとデジタル広告を合わせると5.7兆円ぐらいになるが、報道に出ていないのは､増えるスピードである｡ムーアの法則で20～40％ずつぐらい毎年増えていくので、そこの危機感をもうちょっと考えるというところが必要。それをどうやって補っていくか

となったときに、今、既に議論が始まっていると思うが、技術インテリジェンスというところだと思われ、アカデミアの視点からだけで見るのではなく、経済安全保障の経済というところから、もうちょっとリスクを違う見方ができるのではないかなと思う。それによって特定する分野が変わってくるかと思う。

○2019年に当時のアメリカのOSTPのディレクターが研究インテグリティという概念を国際会議の場で持ってきたことがあった。その当時は研究セキュリティという言葉は明示的には使われなかったが、インテグリティという言葉の中にセキュリティの概念は含まれており、各国への対応を求めて以来、アメリカでのCHIPS科学法やガイドラインのようなものにつながった。資料で記載されていることについては、まず研究の分野特定について、非常に大きな第７期の科学技術基本計画のイシューになると考えている。第６期のときも重要研究開発領域を特定しようとしたが、非常に困難を極め、いろいろな研究のシーズの展開をエビデンスベースで測ることはとても難しかった。したがって、第６期ではそれを全てやり切ることは諦めた。それから数年経ち、今のデータベースでは、全ての研究領域において、その中のかなり細かいサブセクターごとの我が国における研究者、アカデミアの研究開発の競争力を各国と比較して見ることができるようになってきた。特許についても同じである。また、我々はそれぞれの研究者に投下されている研究費を一人一人追いかけることもできるようになっている。そういったシーズ開発においての安全保障的な視点が、恐おそらくは第７期の基本計画の一つの柱になると思っている。そうすると、リスクにさらされている研究領域という考え方が出てくるわけだが、対外的なリスク、対外的な共同研究における不正のみならず、どのような研究領域を伸ばしていくことによって、我が国の国際競争力を高めていくか、それが結局としてリスクの軽減につながっていくという二面性を考える必要がある。要するに、守ることと、成長させること、この２つの視点から、インテリジェンス的に見て、どこに資金を投入すべきかという議論につながっていくと思っている。同盟国・同志国の中で、我が国においてはこのような研究の状況であり、こういった研究者もいて、この分野において競争力を伸ばしていく可能性があるといった国際的な情報共有も考える必要がある。

○我が国における研究開発資金の限界性を考えたときに、どの分野で各国と協調していくかという情報共有の視点がそこからも出てくるだろう。そのため、そのような各国に対する情報提供こそが、同盟国・同志国の中における意識共有と国際協調の視点につながっていくので、強みのある研究開発の情報を提供しなければ、ほとんど対話にはならないだろうと考えている。そのような議論をしようと思うと、従来のCSTIがやってきたような研究開発に関する計画の範囲をかなり超えていき、安全保障的なものを入れないといけない。その議論をすることは、CSTIの中では現状としては簡単なことではない。NSSの方々とも議論をしていきながら、インテリジェンス機能を高めていくという方向性を柱として、第７

期基本計画のどこかで議論していく必要があると考えている。

○国際共同研究の相手であるG7各国が研究セキュリティに取り組んでいるのであれば、日本としても同じレベルで進めなければいけないという必要性は理解した。

○リスクにさらされている研究領域の特定と情報共有について、国によって限定しているところとそうでないところと両方あるという紹介があったが、リスクにさらされているという点では、我が国が技術優位性を持つ領域という観点に加えて、こういう国がこういう技術を取りに来ているのではないかという観点もあるのではないか。それがたまたま一致している場合があるかもしれないし、一部ずれているかもしれない。その辺りはどう考えるのか、他の委員あるいは事務局で考えがあれば教えていただきたい。

○デューデリジェンスについて、競争的研究費に関するガイドラインの改定等々について紹介いただいたが、同ガイドラインの改定に当たって、経済界との間で議論になったと承知しているのは秘密保持契約との関係である。契約上開示できるもの開示できないものがあるということで、経済界の現場の意見と政府側の要請との間で調整を行った。その結果、改定ガイドラインにおいては、既に締結済みの秘密保持契約があるため、提出が困難な場合は、金額とか相手機関名を記入せずに提出しても良いということになっていて、今後は秘密保持契約等を締結する際には、必要な情報に限り提出することがあることを前提とした内容にするように政府側から働きかけるということになっている。ガイドライン改定から２年半ほど経つが、政府として、どのような働きかけをされて、現在はどういう状況にあるのか教えていただきたい。

○経産省を含めていろいろなところで同種の議論が行われていると承知している。資料15ページに記載されている以外にも、同じ経産省において、外為法の中で取り得る措置ということで、あくまでも軍事転用可能性ということを前提にした上ではあるが、技術管理という観点から同じような議論をしている。そういったことが各所で行われている状況では、全体像がなかなかつかみにくいという感じもするので、特に関係省庁含めて全体で整合性の取れた形で議論をしていただく、あるいはNSS中心に調整をやっていただくことは非常に重要と考えている。

（事務局からの回答）
○青色の15ページの部分の考え方の話と、特にリスクにさらされているものとの関係ということと理解。これ自身は経産省の有識者会議の議論のために提供したものであるので、この紙上どうなるかということを考えるよりも、例えば研究セキュリティの取組との関係でどのように考えるべきかが重要。我が国が技術優位性を持っている領域を考えると、そ

の分野に公的な資金を提供してやっていこうというときに、自分たちで強いと思っている、これから更なる強みを確立していこうとする分野であるため、成果の公開を前提とする研究であっても、技術流出対策として、必要な責務相反・利益相反の管理はやっていくことが基本となる考えだと思う。したがって、自分たちがまさに強みを守った上で育てていこうと、そうした強み守っていこうという活動自身が重要ではないかということで「青の分野」をまず念頭に置いた形で提案をしている。また、「赤い分野」についても、これから育てていこう、政府の資金を戦略的に投入し強みにしていこうという分野においても必要な取組をやっていくことが同様に重要だと思い、この「赤」と「青」がまずは、国際共同研究を行う際、または将来の国際共同研究を念頭においた際に、対象となるものを検討する際の出発的になる考え方の一つになるのではないかと事務局として提案をさせていただいている。

○現行のインテグリティの取組と企業の関係で、特に企業の営業秘密との関係でお尋ねがあった。現状において、研究インテグリティは関係省庁それぞれで実施をしているということもあり、つぶさには承知しかねるが、他方、今回、アメリカの研究セキュリティの例を見るといわゆるアカデミアによる公開を前提とする研究を念頭におきつつ、政府資金によるこうした公開前提の研究が悪用されることがないようにするにはどうすればいいかという観点で、議論されていると個人的には理解している。したがって、成果公開前提の研究と、成果が営業秘密になりえる研究をどのようにやっていくかについて、また少し別な考え方や導入が必要なのではないかと思っている。したがって、今回はアカデミアを中心とした政府に研究セキュリティの主たる対象だと認識している。

○他方で、企業の技術流出防止という、次の会議で議論いただく予定だが、重要な技術情報について営業秘密技術管理・知財管理と一体的に、企業活動においてどのような取扱いをされることが望ましいか、どうした取扱をしていただくことが、経済安全保障上も政府が資金を投入する際には適切となるか、という議論である。今回、研究セキュリティはいわゆる成果公開を前提とした研究領域、これがまさに研究のオープン性ということで、基礎研究を含めたそうしたオープンな研究の成果がまさに経済成長にも資するものとして、これまで日本だけでなく、同志国においても同じような考え方に立って推進されてきたものであり、そうしたオープンな研究についてこの研究セキュリティの取組を整理していただこうということであり、研究インテグリティで議論された企業との関係を変更するものではない、逆に、企業活動と技術流出防止との関係は次回の分科会会議で議論をしていただくことを予定している。

○技術流出について、経産省の安保小委等、様々な場で議論されていることをNSSで調整していただけないかということ、ないしは調整するべきではないかという御指摘については、

経済安保上の政策の政府内の総合調整をするのはNSSの機能の一つであり、その御指摘がでないように必要な対応をしてまいりたい。

（委員のコメント）
○今、セキュリティ・クリアランスに関する法案審議が行われているが、そこで研究するとクラシファイドリサーチつまり政府機密研究となる。クラシファイドインフォメーションを使わないが、大学も含めて、民間の研究の中で機密が必要なものは、プロプライエタリリサーチ、日本語では民間あるいは企業機密研究ということにある。その外側にあるのが、大学等で行っている研究で、基礎研究で、所謂ファンダメンタルリサーチでありクラシファイドではない。この３つの領域を考えたときに、ここで議論している話は、クラシファイドではなく、機密がないところの研究についての規範で、先ほどG7のWGにわたくしは出ていたので少し付け加えると、先ほどの研究セキュリティ・インテグリティの定義というのも、基本的に学問の自由、透明性を確保し、国際的な共同研究をやるためにセキュリティが必要だという文脈になっている。

○もともとインテグリティの概念は、自分が不正などを行わないようちゃんとすればインテグリティが保てるというところだったが、資料にあるようにBad Faith Actorがいて、不正に知財を盗んでいくなどがあるので、その対策をしないとインテグリティが保てないでしょうという文脈になっている。そのため、そういう意味でのセキュリティをファンダメンタルリサーチに当てはめないといけない、G7で合意したということは、こういうことをちゃんとやっていないと付き合いませんよということ。

○アメリカにもともとこういう考え方があり、2018年とか2017年ぐらいから、相手機関が本当に信用できるかどうか、デューデリジェンスをちゃんとやっているかを見て、できていないと思うと、そこもハイリスクだとみなすという考え方がある。それをG7のところである意味合意したと考えていいと思う。

○G7のWGは、2021年から始まっているが、第１回は各国とも全部政府関係者とアカデミアの代表者がセットで出てきていたが、日本は代表者がだせなかった。いくつかの機関に要請をしたけれども出せず、学問の自由があるからそういう会議には出られないというのが背景になったと聞いているが、そもそも論理が全然違う話。今申し上げたようなことがちゃんと敷衍されることがすごく重要。今でもまだインテグリティはやるけれども、セキュリティはやらないみたいな傾向がある。そこの基本的な概念の共有化ができていない。そのために、求められているデューデリジェンスみたいなことは今の状態だと非常に弱い。

○各国とも、大学が自主的に取り組むことだから何もやらないということではなく、少な

くとも政府が合意しているので、そこは施策として情報提供は当然するし、人的な支援もする。カナダの場合は財政的支援もしている。なので、これは支援が必要ということと、認識をちゃんと共有することは非常に重要。

○リスクにさらされている研究領域の特定と技術情報について、研究領域の特定というのは恐らくどこでもやると思う。ただ、カナダは実はそれを指定研究機関リストとセットで出しているというところが特徴で、ほとんど輸出管理みたいな考え方。リスト規制とキャッチオール規制みたいな考え方で、これを本当にやるという話を聞いたのは実は比較的最近で、本当にうまくアカデミアの中で機能するのかは、ウオッチしたほうがいい。ただし、今言ったようにG7で合意しているということは、そこで懸念されている技術領域があったとすると、そのセキュリティ面での管理は尊重しないと一緒にできないということ。逆に言うと、自分が領域を決めるか決めないかではなくて、すでに半導体や量子等の分野は事実上米国等G7各国と共同研究を実施する際はデューデリジェンスをはじめとした管理をしないと信用してくれない。なので、自主的に決めるかどうかということと、そのフレームワークの中でやるためには、この分野はもうこういうふうにしないといけないという部分と両方あるということは認識しないといけない。

○私の所属している大学は、どちらかというとそれほど機微情報に関わるような研究を担っているわけではないが、こうした考え方は十分に理解できていないし、認識は全体的に不足していると思う。ただ、これから日本政府として研究力をどのように強化していくかという非常に大きな柱を立てていく必要がある。そして、その柱を立てていく中でどの分野については絶対に日本としては外せないのだということをしっかりとした方針として提示される必要があるし、優秀な研究者、特に若手の研究者をしっかりと育成することについてぜひお願いしたい。そういう流れがないと、幾らガイドラインやチェックリストを作っても、多くの大学組織においては手いっぱいという状況であり、形式的にやることだけで済んでしまう可能性がある。チェックリストを作れば作るほど、逆に言えば形式的にチェックしていくしかないという状況もあるわけで、まずは国全体としてどのように研究力を上げていくのかという重点化、その方向性をしっかり出していただくことが非常に重要だと思う。

○また、できるだけ日本の研究者が、特に若手の段階でどんどん海外に出て行くとか、海外の国際的な共同研究に参加していくような、そういった自由な場をもう少しつくっていくことが必要である。そういう流れがなければ、大学の研究力は、ごく一部除けばということであるが、なかなか高まっていかないのではないかと思う。ただ、G7で決まったことをどうするかという話もあるし、これは日本政府としては基本的に進めなければいけないということであると思うが、戦略的な１つの考え方として、経済産業省が出している重点

分野とか重点技術の整理はとても分かりやすい。さすがにこの２年、３年の政府のいろいろな取組や支援によって、まさにサプライチェーンの強靭化、この問題が非常に深刻だということはよく理解されてきた。経産省の整理はいい整理だと思うが、さらに食料、農業分野、医療、医薬品分野、医療機器などがあればよい。そうした中で、当然、先ほどデジタル赤字は基本的に貿易赤字ということだが、確実にこれらの分野も貿易赤字を生んでいくということでるため、そういうことを含めた上で、各省庁においても同じような考え方で整理していただくことが重要。

〇政府、アカデミアの先生方、あるいは研究者の方でも、そういったような政府の会議に出ている先生方を通しても、相当理解していただけるのではないかと思う。入り口としては、これまでやってきた経済安全保障の我々の施策との連動性とか総合性の中で進められるとまずは良いのかなと考える。

〇アカデミアの議論が中心ということであるとすると、むしろそういう整理をもうちょっとクリアにして議論していただけるとありがたいと感じる。その上で、他の委員からも発言があったが、どの技術領域をどう伸ばすのかといった議論で、企業をどのように取り入れていくのかという議論と、つまり、国がお金を出す研究開発の中でどう位置づけていくのか、こういったものをどこまでどう適用していくのかが、多くの方々に分かるようにしていくことが重要かと思う。そういう前提がないと、なかなかスタートアップしかり、中小企業しかり、どのように関わっていったらいいのか分かりにくいような気がする。ぜひよろしくお願いしたい。

〇情報の流動性が非常に重要な問題で､結局そういう情報は人にくっついて動いてしまう。そのため、そういった人材の流動性をどう担保・保障していくかが、今後の日本の国際競争力なりアカデミアの国際競争力という観点から極めて重要。直接リスクにさらされている研究領域の特定は、何も日本の中だけで決めることではないので、世界中でどういう技術がどういうふうに動いているかというのをどれだけ把握できるかが実は大きな問題ではないかと思う。そういう意味では、そういった技術の動向なりをどのように常にキャッチアップしていくかが重要だと思う。また、最近多くの紛争があるが、そこでどういう技術がどのように使われているのかということだけでもすごい量の情報が入ってくる。その情報収集能力をどう高めるかというところが最大の問題。

〇つまるところはデューデリジェンスをどこでどういう形で行うのかということだが、今のところ大学の現場あるいは研究開発機関でのデューデリジェンスをガイドラインとして求めているが、現状の情報管理は甘いと思う。アメリカの場合は、基本的に入り口で閉めており､FBIが入国の段階から全部バックグラウンドチェックしている。何か不正が起こっ

たときには、そこの研究機関に対しての当然ながら査察が入る。これは実は民間も同じなのだと思うが、デューデリジェンスは我が国ではなかなか難しい。現状、ガイドラインを作って、各機関がそれに応じてチェックしてくださいということによって、形式としては国際的な協調関係の中でそろえることはできていて、それをやるべきだというのは確かにそのとおりだが、どこまでそれが実行できるのかという問題は必ず残ると思う。これをあまりあからさまに言うと、大きなハレーションが起こることは間違いない。そこは恐らく関係省庁の方々も考えておられるとは思うが、実態には大きな違いがあるということをまず認識した上でこの問題は進めないといけないと思っている。

○今日の資料の中で、視点がサプライチェーンから入っているが、アカデミアを引き込まなければいけないため、アカデミアにとっても非常に大きな研究開発上のチャンスがやってくるのだという論理も同時になければ、なかなか難しい。

○もう一つは、アメリカにおいてほとんどの研究開発は完全にアンクラシファイド。九十数パーセントが、例えばDoDであってもアンクラシファイド。ただ、アンクラシファイドであるけども、コントロールされているということはある。Controlled Unclassified Informationと呼ばれるように、どこかで緩やかな管理をかけている。NSFの資金に関しては、完全にファンダメンタルリサーチであるため、アンクラシファイドであり、それのチェックも非常にリスクの高いところだけで実施している。日本においてはアカデミアに対するファンディングのシステムが非常に限定されており、現状ではJSTかNEDOを中心として幾つかしかない。アメリカの場合は実に多様なファンディングのシステムをつくっており、アンクラシファイドだけれどもコントロールしなければいけないのは、それに合うようなファンディングでやっていくという形になっている。これが入り口にある。

○これは別にアカデミアだけではない。出口のところで、経産省が例えばGX基金みたいなところで産業界に補助金を出して、研究開発を推進していくということに関しても、実は大きなリスク管理というものの視点が当然ながら入って来る。ひとえにアカデミアの問題ではなくて、産業界における研究開発ということにも波及をしていくということなのだと思う。それを全部束ねる意味でのデューデリジェンスの仕組みは非常に現状難しいだろうなと思う。例えば何か起こったときに、アメリカだったらすぐに研究室にFBIが入ってくる。そのことを常に認識しながら、危機感を持って研究開発を現場ではやっているということだと思うが、現状日本では難しいなとは思っている

○先ほどターゲットになっている技術とかはどういうことかという議論があったが、例えば中国製造2025では、かなり詳細な形で彼らがターゲットにしている技術を明確にしている。先ほど他の委員からもあったが、公開情報をどうやって分析していくのかということ

が非常に重要。ビッグデータということになると思うが、公開情報の中からリスクは一定程度出てくると思う。各研究機関が行うのか、それともそれを所管する省庁が行うのかというのは別だが、そういった形での公開情報を集積することによってリスクをあぶり出していくという一つの手法というのはあるし、実際にそれは一定限度有効だろうと思っている。

○我が国はやはり学問の自由が強くて、すぐ研究室に警察が入るということはなかなかできない。非常に我が国は民主的な国であるし、実際の運用としては極めて大学の自治、それから学問の自由が守られているということは付言しておきたい。

○デューデリジェンスについて、少なくともG7あるいはアメリカでこのファンダメンタルリサーチの領域で言っているのはほぼ自己申告に基づく情報とオープンソースである。オープンソースデューデリジェンスという言い方をするが、決してバックグラウンドチェックとは言わないというのが特徴。そこは人権等いろいろな問題が生じてしまうし、かつオープンソースデューデリジェンスであったとしても、バイアスがかかったりするので、それが人権の問題につながり得るということで、アメリカではそこの注意もしている。いずれにしてもこれはオープンソースデューデリジェンス、あるいは自己申告で、申告された記録だけ見てもコンシステンシーがない場合があり、そういうことに気をつけろということ。例えばハーバード大学だとそれを自分でやっている。カナダはコンソーシアムを組んで、オープンソースデューデリジェンスの業者と契約して実施し、それを共有するという形を取っている。アメリカの大学でも、公開されてはいないが幾つかはそういうやり方をしている。幾つかの大学がアソシエーションになって、その中核機関が代わりにデューデリジェンスをやるという構造で、これも基本オープンソースである。産総研の事案も、ちゃんと公開情報を分析していれば防げただろうというような話であって、アメリカでも同じようにそういう事例がたくさんあるかと思うので、これは実行可能であると思う。しかし、それなりに体制とか、カナダみたいにコンソーシアムを政府が支援するとか、そこはちゃんと体制づくりを支援することは必要ではないかと思う。

○リスク軽減策について、企業として、次回、営業秘密をどうやって守るかという話になると思うが、特に研究に関して、企業としてやることは、当然よく言われているDX。DXの研究現場における重要なことは、手持ちの秘伝のエクセルシートを持たないということ。要はかなりのところが研究現場において今は個人管理となっている。これが一番危ない。完全にそこはペーパーレス、全部データを共通にする。また、リスク軽減策にしてみると、情報インフラはすごく重要だと思うが、アカデミアの実態はどうなっているか。もうできているのか、それともあまり注目されていないのか。

（事務局からの回答）
〇我々が承知している範囲だと、研究データ管理の話は多分幾つかの御議論があって、まさに研究の公正性を守るために研究データをきちんと記録をして、ちゃんと後でトレースできるようにしないといけないといった話や、研究のオープン性を広げていくために、そうしたデータを公開も含めてやっていかないといけないといった話。先ほど言ったようにセキュリティの観点も含めて、出せるような状態になるまではきちんと管理をした形で進めていかないといけないが、セキュリティの部分の議論はこれまで十分だったかと言われると、もちろんサイバーセキュリティ等の問題とも絡んでくると思うが、その部分の議論は、今回こうした形で研究セキュリティという議論の中で一つ扱っていくことは今後あり得るのかもしれない。

（委員のコメント）
〇例えばデューデリジェンスを大学の現場に委ねる。これは恐らくオープンソースの情報だけでやれるところはある程度網をかけることはできるが、それだけでは現実は難しいと思う。これを言えば言うほど大学側は、どんなリソースで、どんな人員で、どうやってチェックするのだという反応が来るし、大学のみならず、恐らく日本のファンディングエージェンシーにおいても、運営費交付金がほとんど変わらない中でやるのは難しいと思う。私が考えるのは、ファンディングのルートを特定の目的性のあるものに分類をして、そこから出てくるものに関しては相当コントロールをかける。そういった対象になる可能性があるというアグリーメントの下で研究開発を行うという形のルートが日本にはないと思う。恐らく別のファンディングのシステムを構築することにも踏み込まないと、現場だけにやれと言っても実際のところはできない。聞いた話だと、とある国立大学でもh-Indexも物すごく高い若い研究者がいて、そこのラボの人はほとんどが特定国からの人。なんでこんなにh-Indexが高いかといえば、そういう優秀な研究者が特定国から来ているから。この人たちがアメリカの研究現場でアクセプトされるかどうかは正直分からないが、そんなところまで大学の現場にチェックしろと言っても、現実問題としては難しいと思う。そうすると、どこかでコントロールの在り方をファンディングのシステムと絡めて、そこのアグリーメントの中でやらないと、ここのチェックは難しいだろうと個人的に思っている。

〇実際に回すとなると本当に難しいと思うし、同志国の研究所でも特定国出身者はたくさんいる。それぞれの頭の中までチェックするというのはなかなか難しい。かなり自己申告的な、不正はやらないでくださいというレベルならできると思うが、そこは今後アカデミアとファンディングエージェンシーが十分議論できるような場をつくっていくことが重要ではないかと思っている。

〇対話・情報共有の場についても、とても難しい話。他の委員の御意見を伺っている限り

においては、これもすごく時間をかけて少しずつということだが、その理解と認識を共有していく体制づくりは恐らく可能。ただ、全体に関してやるということが非常に難しくて、学問の自由があり、しかも今、先ほど大学にデューデリジェンスを実施してもらうのが難しいのではないかとおっしゃったとおりで、ほとんどそういった余力がないという状況の中で起こっている。研究者自身が研究の時間をある意味で奪われてしまうという状況すらある。そのため、持っていき方がとても大事で、先ほど他の委員がおっしゃったように、明るい未来を見せながら、もっと国と一緒に積極的に取り組んでいきませんかというような働きかけが必要である。ただ、先ほどの例えばオープンソースを使って、あるいは自己申告を通しても、ある程度形式的ではあるが、今の研究者データベースを使ってもある程度可能であるし、もし何かプロジェクトとか採用するときは必ず業績と経歴は確認する。そうすると、80％ぐらい分かるが、そのようなことをしなければいけないという考え方を理解していただくことが一番大事。だから、これを全面的に打ち出すことによって、まだ大変な作業があるとか、組織的に大変な人員を確保しなければいけないのかというような話にならないように、うまく持っていっていただくのが本当に大事かと思う。

○ベースにはやはり単に同盟国・同志国だけに縛るわけではないけれども、国際的にどうしていて、だから、その中に日本の研究者が入り込んでいこうと思うと、こういうことをやらないといけないというのはデファクトスタンダードですよということで、いかに人材を回していけるかが一番重要ではないかなと思う。日本だけでは進めていけない部分もあるので、どういうふうに共同研究をやっていくか、そこに原点を置くことが重要かと思う。

○必要な情報共有とか対話をする場というのは必然性があるので、自主的に結構やっている。対話、情報共有の仕組みというのはインフォーマル、自主的にやっているところに対して、情報提供ができる機能がどれだけあるかというところが政府側では重要。さっきのオープンソースDDだって、政府でどこかで契約して、そういう情報提供をするとなればそこに集まってくる。情報共有の場には政府がいないほうがいい場合もあるし、そういうのは現実にいろいろある。

○今の御意見に全く賛成。シンクタンクの設立について議論しているが、政府の中に置いておいてはなかなかできない。外部に出して情報共有ができ、インテリジェンス機能を持ち、今まで少しずつCSTIなどでやってきた分析も含めて、これをどこかで共有し合える場をつくらないといけない。民間の方々にとってもそういう情報が非常に有効な経営基盤になる。ぜひ色々な方々に御支援いただき、そういう場を一緒につくっていただきたい。

○私も、政府が何でもやるというのはあまりよろしくないのではないかと思っている。特に情報の話の場合、偽情報等もそうであるが、今回も学問の自由とか、偽情報の場合は表

現の自由とかが関わってくるということになり、大学とか研究機関が個々にやるのは大変だということになると、受皿のようなものを、官民で協力して作り、そこに情報を入れていくというのが非常に重要だと思う。調査とかそんなことを言うと暗いイメージがあるが、基本的には今回のものは多分、公開情報中心の分析ということになってくるので、そこは別に政府が何らかの権限を持って対応する必要は全くないのかなと思う。

○一定のインテグリティでは足りない部分をセキュリティで補っていくということでG7で合意したということだが、リスクにさらされている研究領域も含めて、アカデミアがそれをどのように受け止めるか、また、実際にそれを実施できるかどうかという点が問題の焦点だとすると、無用なハレーションを避けるという意味でも、G7の合意、デファクトスタンダードを前面に押し立てて、アカデミアの理解を求めていくしかないのではないか。また、体制としてアカデミアだけではできないということであれば、官が前面に立つのではなく、自主的なものを促しながら、それをサポートしていくような手だてを考えるのが、ファンダメンタルリサーチに関する研究セキュリティ確保のポイントではないか。

（事務局からの回答）
○まさに我々が今、内部でいろいろ議論しているが、我々の悩みが正しい悩みだったのだなということが非常によく分かった。当方の担当でも今年アメリカに出張して、いろいろと研究機関とも話してきたが、外国人の研究者がたくさんいる研究所も多く、そういう研究所がまさにアメリカにおける科学技術を支えているという実態もある。

○一方で、今、G7等で議論されている研究インテグリティだけでなくてセキュリティもどう高めていくのかということで、議論して一番思っているのは、NSSが旗を振っているだけでは進まないということ。まさにCSTIをはじめとして関係省庁、アカデミア、それから経済界も含めて、まさに全体として同じような頭のつくりをしていかないと物事が全く進まないという非常に難しい領域だろうと思っている。

○国際的にはかなりのスピードで動いてきているので、今までのような考え方だけでは難しく、国際研究という切り口の中でこういうことをしっかりと進めていくということで、関係者も巻き込んでいく必要があると考えている。

○国が全てチェックする、国が主体となって権力的に実施するようなイメージ、誤解を持たれると、恐らくこの話はうまくいかなくなってしまう話であるので、その辺も我々としても理解しながら、皆さんの御協力を得ながら取り組んでいきたい。

以上

「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）議事要旨

１　日時

令和６年４月12日（金）15時00分から16時30分までの間

２　場所

中央合同庁舎４号館1214会議室

３　出席者

（委員）

青木　節子	慶應義塾大学大学院法務研究科 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
北村　　滋	北村エコノミックセキュリティ 代表
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

（政府側）

飯田　陽一	内閣官房経済安全保障法制準備室長
彦谷　直克	内閣審議官
品川　高浩	内閣審議官
早田　　豪	内閣参事官
田村　亮平	内閣参事官
田中　伸彦	内閣参事官

４　議事概要

（１）事務局説明

事務局から、資料１の内容について説明があった。

（２）自由討議

（委員のコメント）

○今回のテーマでは技術流出防止対策をどのような形で整理をしながらターゲットとの関係で議論を詰めていくかということと理解。資料15ページの③、④において、左側の「経済安全保障上の重要技術の研究開発」ではリスクに応じたデューデリジェンスやモニタリングというものを「右記に加え」とあるが、サプライチェーンの強靭化でも、こうしたリスクに応じたデューデリジェンスやモニタリングがおそらく必要であり、経済安全保障上の重要技術でサプライチェーン強靭化を除いた研究開発において、何故ここが強調されるのかについて理解が進まない。資料９ページで、サプライチェーンの強靭化が②に該当し、①が今回のテーマであるということであるが、領域に着目するよりも、その技術優位性が揺らぐのかどうか、あるいは確保するためにどうするのかということであり、それは例えば不可欠性の維持という②のケースにおいても、実際にこれらが技術優位性について何らかの形でキャッチアップされたりする場合においては、おそらくこのリスクに応じたデューデリジェンスやモニタリングが必要なのではないかと思う。ミスリードとまで言わないが、15ページのような整理をすると、なぜこれから技術優位性をつくり上げていこう、確保していこう、というときだけに、社内・従業員における管理や取引先における管理でアディショナルにリスクに応じたデューデリジェンスやモニタリングを捉えるのか、理解ができなかったので教えていただきたい。

（事務局からの回答）
○御指摘のとおり、15ページ内右側の部分でリスクに応じたデューデリジェンス、モニタリングについて、サプライチェーン支援ではやっていない、必要ではないということを示唆しているものではない。サプライチェーンの強靭化の支援について技術優位性を軸に技術流出対策の措置を取ることとしており、これを技術の研究開発一般に横展開していこうとの議論を進めているということ。また、前回検討会合の議論で、事実上、成果公開を前提とする研究を担うアカデミアにおいてさえ、米国と共同研究を行うときに半導体、量子等の分野でデューデリジェンス、モニタリングの措置を取らないと、大学の場合でも相手にされなくなりつつあると委員から御発言があったかと思うが、まして重要な技術情報について営業秘密として管理を行う産業界においてもということもあり、営業秘密の部分について、技術一般の研究開発、特に半導体、量子のような分野で、国際的な協力連携が必要な場合、その技術情報の営業秘密管理や情報管理において、追加的な要素があり得るかという議論をしたいということ。今後、重要技術の支援の文脈のみならず、サプライチェーン強靭化においても同様に必要だということが結論になれば、技術でアップデートされた内容を今後どのようにサプライチェーン側に反映させていくかについて、本日の議論を踏まえてきちんと対応していきたい。

（委員のコメント）
○前回の委員の御指摘との関係についてはそのとおり。つまり、国の資金による委託など

で行われる研究開発であって、特に国際共同研究開発のようなケースにおいては、こうしたリスクに応じたデューデリジェンスやモニタリングがより求められる。そうでないと相手にされない、と言うと表現が適切でないかもしれないが、そういうケースにおける研究開発の特性として必要なものは何かという議論あるいは論旨を整理していただければと思う。

○産業界でどういう対策をしているかについて紹介させていただく。資料１ページについて、誤操作・誤認等での漏えいが 21.2%、ルール不徹底が 19.5%であるが、これはかなりの部分が社内での対応する仕組みで防げると思う。例えば、弊社では USB や外部メモリに一切ダウンロードできないようにしている。それは特に情報を限っているわけではなく、全てのサーバーに入っている情報が対象。また、メールに添付書類がある場合は全て暗号がかかるようになっている。なぜかそういうことをしているかというと、例えば Excel ファイルにおいて、最初のシートには一般情報しかないが、別に幾つかシートがついており、請求書をある会社に送って、別に設計図がついている、さらに送った先が別の人を CC に加えて、送ってきたものに対してさらに全員返信で返してしまう等、それで漏えいが起こり得るので、添付書類をもう一度チェックして、送り先はこれで大丈夫か確認させるようにするだけでかなりの部分が防げるのではないかと思う。また、これは資料にも出ているが、やはり従業員の中で会社の屋台骨、明らかに機微な情報にアクセスできる技術者、もしくはその技術を活かせる技術者はごく限られているため、モニタリングをかけている企業がほとんどではないかと思っている。また、ほかの国の関係会社のマネジャーや管理職クラスに就いた者が情報を持ち出すケースはそれなりに多いと思うので、注意していただきたい。

○ここまでが実態の話で、やはり一番問題なのは従業員が退職時に持ち出すケース。これの一部は先ほど言ったモニタリング、機微な技術を扱っている人が急にメールのやり取りが増え、数か月後に退職し、退職した先は別の国の会社であるという事例が起こっていると聞いている。これもきっとそういう努力をすることによってある程度は防げると思う。こうした技術情報なので、その技術がサプライチェーンに問題があるから等は関係ない。データのやり取りを見ていると大体分かるので、あまりにも大量のデータを自宅に送っている場合はかなり注意が必要であろうと思う。

○営業秘密管理の法制度は徐々に改善されて、令和５年には外国で搾取があっても日本でビジネスがあれば日本の法制度で裁けるようにしていただいたが、それにしても営業秘密の侵害や搾取については原告に立証責任がまだ残っており、訴訟を他国で実施できるのかは非常にハードルが高い。資料でも紹介されているパナソニックの事件もそうであるが、昨今起きている特許侵害訴訟の一部も、もともとは営業秘密を搾取問題だったのではない

かと想像できる。そういう意味では営業秘密は使いにくい法制度で、原告としては証拠集めに手間もかかるし、必ず勝訴できるという確信もないような状況であるので、まずは基本的なところを整備することだと思う。ただ、法制度にするといきなりハードルが上がり、スタートアップ等これまでそういうことをしたことがない方々に法制度で義務を課すのはどうかと思うので、こういったことを皆さんで周知して、簡単にできるところからまず手を打っていくことが現実的には一番の早道ではないかと思っている。その後にガイドラインなり法制度なりベストプラクティスなり、政府からリコメンデーションを出していくのが法制度をいじらない範囲での一番の早道ではないか。

（事務局からの回答）
〇関係省庁とも協力して各社、どのような形で対策を講じているのか、まさにベストプラクティスのような事例を示して、その事例がそもそも支援の体系とどのように結びつくかというのは当然あるが、ガイドラインにするまでもなくやれることもたくさんあるという御示唆だったと思う。さらに、そうした事例を含めてどのような形で御紹介をし、営業秘密の管理をどのように我が国全体で高度化していくかについて、法の範囲外でやれることはたくさんあるという御指摘だったと思う。ご指摘を踏まえ、そうした事例を明らかにする作業の一環として、ベストプラクティスを明らかにする今回の作業を継続させていただき何らかの形でまとめさせていただきたいと思う。

（委員のコメント）
〇不正競争防止法違反に関連して簡単に申し上げる。これまでの報道にあったような違反の事例を見ると、きっかけは知人の依頼であったり外国からのソーシャルネットワーキングサービスを通じての勧誘であったりということのようであるが、流出から発覚までに１年であるとか、場合によっては数年を経過していた例が見受けられる。技術も情報も一旦外へ出れば取り返しがつかないだけに、流出の予防に加えて、仮に流出が起きてしまった場合には、それをいかに発見するかという視点が求められているのではないかと思う。社内・従業員の管理については、既に監視カメラやデータログなどの物理的な管理が積極的に進められていることに加え、セキュリティークリアランス制度が動き出すことや、警察などからのアウトリーチ活動もあって、状況は改善されていくものと思う。これまでの事例の事実関係を見る限り、従業員にとって功を焦らないで済むような環境、特に研究開発環境が必要ではないかという印象を持った。

〇資料１ページのIPAのアンケートのようなものは昔から繰り返しやっており、2014年に実施して発見したこととしては、流出しても気がついてない場合の方がはるかに多いということ。何故それが分かったかというと、そもそも企業が様々な検知活動をやっているかどうかを横軸に取って、実際流出したかどうかを聞きと見事に上に凸になる。なので、モ

ニターも何もやってないと、何も起きてませんと言うが、少しずつ何か検知活動をやっているとどんどん増えていくということであり、これは明らかに気がついてないということ。どれぐらい気がついてないのかというのは、その当時のデータから、２倍、３倍のレベルではないと思った。

○最近の報道でも転職が盛んになったので流出が増えたという報道ぶりは多いが、不競法の改正等があって、事件になるものが増えていて、現在でもまだまだ氷山が全部出ているわけではないなというのがその当時の推計からの印象である。その主な流出ルートはやはり人だと思う。

○デジタルでできることは大分対策ができるということだが、問題は基本やはり人。このIPAの調査もそうだが、当時からも流出ルートはほとんど重要なものは人であった。退職者と現職については、やはり先ほどのモニタリングが重要。それから、そもそも重要なチームにその人を入れるのかということをしっかり判断する必要がある。これは国の情報の場合はセキュリティークリアランスをやるが、民間の場合はそれはやらないため、それに相当するデューデリジェンスをどうやってやるのか、そういう問題をやはり検討しておかないと、海外との関係、例えば米国との関係で、日本の中でそれをやらないのはまずい。特に国プロで重要な技術あるいは経済安全保障上の支援を行ったものについては、やはりそういう仕組みが必要だろうと思う。国際的には防御が弱い国が狙われるのも分析で明らかであり、例えば日中韓でいうと、日本が強化すると中韓でも強化するし、一番弱いところが狙われるという構造。最近では、中韓では技術窃盗には３倍から５倍の懲罰賠償を乗せてくるので、そういう競争の中で考える必要があり、そこにどれぐらいの手当てをするかということは重要な観点かと思う。

○バイ・ドールの話も、知財の移転であれば基本、公開情報なので影響は限定的とも言えるかもしれないが、生産技術などであれば国境を越えるというときに通常ノウハウの移転も伴うため、基本は輸出管理上の対策もしないといけないことになる。特許で例えば子会社だからといって海外に行ってしまうとか、管理されてないという状態はやはりまずいと思うので、そういう観点からも管理をすべきだろう。

○資料９ページのいわゆるサプライチェーンの強靭化の②、③についてはよくできており、防止措置も例えば外為法を使うとか不正競争防止法をより強化する中でかなり対策が可能なのだろうと思う。まだいろいろ問題があるということは踏まえた上で申し上げる。今回、①について、15 ページに大変重要なまとめ方をされているが、コア技術をどのように定義するかという形で提起されていることは特に重要だと考える。いわゆるサプライチェーン強靭化については、もともと物資あるいは素材といった物理的なものを前提とし

ているので、基本的に外為法が有効である。それに併せて、技術ももちろん今も革新が続いていることを前提にしながらも、ある程度出来上がったものを前提としているため、営業の秘密情報管理の規定が相当有効であると感じる。ただし、①については、破壊的イノベーションという表現が示すように、いわゆるサプライチェーン強靭化の延長にあるというよりも、むしろ別次元の技術として捉えるべきということだとすると、恐らく不正競争防止法等をどのように強化してもなかなか対応が難しいのではないか。そのことを前提とされているという感じがした。

〇ただ、もちろん今御説明いただいたように、企業がやるべきことはまだたくさんあるため、基本的に 10 ページにあるように技術流出対策をより高度化し実施していくのは非常に大事であるが、①については経済安全保障上非常に重要な分野であるため、従来の枠組みの上に乗せるだけでいいのか、むしろ、入り口から出口までの全体的管理が必要という言葉があるように、技術開発の中間段階まで含めたいろいろなリスクマネジメントを仕組みとして整備するという考え方が重要かと思う。今回、そういう意味では非常にいい整理をされているが、技術の定義のところはまだ少し議論が必要なのという感じがした。

〇実際に起きている現象、実際はどうなっているのかがよく分からない中で、検討せざるを得ない状況になっている事情もあるとは思うが、その観察すべき現象がどうなっているのかを気にして見ているかどうか、観察しているかどうかでその現象がぐっと変わることもあると思う。そういう環境を日本で作るのはそう一朝一夕にはいかないのかなと思いながら議論をしているところだと思う。

〇この重要技術についての技術流出対策の中で不正競争防止法を紹介していただいた。基本的に外事警察で技術流出対策になると、不競法は一つのツールとなる。それを考えると、基本的に不正競争防止法というのは経済安全保障上の一つの大きな手段であるという位置づけが事実上あると言えると思う。営業秘密の中にいろいろなものがあり、全てそうではないだろうが、やはり経済安全保障上重要な営業秘密を不競法に位置づけるとなると御議論があるかもしれないが、基本的にそういった観点で所管の大臣なりが指導できるような経済安全保障的な観点の頭出しが要望できないかと思っている。

〇法律の目的が違うと言われそうだが、今の不正競争防止法の少なくとも罰則の適用としての使われ方は経済安全保障的な観点での執行が圧倒的に多い。出口から言うのも非常にアバウトな議論であるが、抑制的な観点での行政的な措置も経済安全保障上の観点からの規制等を不競法の中に書き込めないかと思う。不競法のことをよく知らないと言われるかもしれないが、不正競争防止法は、検挙された場合、大体スパイ類似のことで使われている。そういったものはある程度受け止めてもいいのかなという気がして、やはり一定程度

の特殊な扱いをすることが可能になるような仕組みができればいいと思う。

○今日の話は主に企業に焦点を当てていることを念頭に置きながらも、資料９ページはいかにも、経産省的なフレームワークの中でのサプライチェーンだと思う。つまり、例えばコンピューティング、グリーンテック、バイオテック、防衛等の分野の将来的な優位性を見据えた研究開発投資については、CSTI における研究開発投資の方向性でもこういう分野が一番重要な分野で、国はどこにどういう形で投資をすべきかを科学技術基本計画の中で書いていることになるが、資料に書いているように、それぞれの分野で特に重要なサプライチェーンに注目し、これらのいわゆるクリティカルテクノロジーがどういう現実の企業におけるサプライチェーンと明示的につながっているのかが重要。そしてそれがどのような形で国家としての競争力につながるのかという議論は実はそんなに簡単な話ではない。

○CSTIは今までずっと主に文科省系の中で大きくこの類の研究投資の促進をやってきたが、一番議論として欠けているのは、そこが最終的に企業のサプライチェーンにどう食い込んでいくのかということ。これは実はつくり上げることが非常に難しい。もしそれが明確になっていれば、国の研究、さらに言うと、それを委託として受けているような企業との間で共通のリスク管理のようなフレームワークを実施すべきだということにはなるが、必ずしもその明示化にはまだ至っていないということがとても重要。そのため、企業の側でまず人を通しての共通的なリスクの在り方、これは概念としてはその通りで、同じようなフレームワークをつくっていくべきだと思うが、それが果たして重要なサプライチェーンになるのかという議論が一方である。基本的にはそんな競争力のあるような企業体の中の基本技術として評価していくかどうかは相当分析をしてみないと分からないと思う。その意味で、資料９ページは、非常に経産省的なフレームワークの中で見ている研究開発とサプライチェーンの関係と感じる。これは重要であるが、国の研究開発投資とサプライチェーンの関係を例えば文科省的なフレームワークで見ると実はよく分からない。これは経産省の知見も借りながら、どこでどうつながっているのかを明確に特定した上で共通のリスク管理の在り方のガイドラインをつくっていくという形になるべきだと思う。

○まずそういうようなフロントラインの研究開発と、サプライチェーンの問題がある。同時に、この②のところにおける不確実性。つまり、破壊的なイノベーションが起こって技術の優位性が生まれて、やがては明確に技術優位性を持つ領域が生まれるという形。例えば次世代コンピューティングであれグリーンテックであれ、誰が見ても我が国における技術優位性のあるような領域がもう明確に生まれていれば、それなりに網のかけ方はあると思う。ここの少し細かい洗い出しが必要ではないかと思う。それはCSTIの分析も含めて一緒に考えていかないとリスクマネジメントのやり方に濃淡がつけにくいと思う。経産省の

方もよくそのことを御理解しているとは思うが、改めてかなり綿密なコミュニケーションを取っておく必要があると思った。

（事務局からの回答）
〇企業に寄っている議論として、将来技術の研究とはいえ、実用化、事業化を念頭にする限り、サプライチェーン、エンジニアリングチェーンにつながっている、つながりうることが予見されるのであれば、企業において営業秘密管理がしっかりと実施されていることをある種、前提にしていると言える。この前提を経産省的だということであれば御指摘のとおりであり、①の将来技術の領域でどのようにやっていくのか、それだけで十分なのかについてはより詳細に検討しないといけないではないかとの指摘と考えている。。

（委員のコメント）
〇付言すると、経産省的だというのはそれが問題だと言っているわけではない。各国のイノベーション政策に関わる人たちと議論すると、結局20ぐらいのクリティカルテクノロジーを挙げ、そこに国家投資をし、そこが一体どのサプライチェーンにつながっているかということを盛んに図ろうとしており、その中でこのリスク管理の問題を捉えようとしているので、協力が必要だという話。

〇実態が分からない中でどこを捉えて考えればいいのかがよく分からないが、重要な点は外国の団体・企業との関係なのかもしれない。様々な団体との研究開発も含めた取引の中で、その国の法制、法令の強制を受けて日本人が不利な目に遭う、日本人が日本の法律に違反をしてしまう、また、違反ではないにしても、非常に妥当ではない結果を招くというようなことから自国民を守るというのは、日本国の義務なのだと考え方を変えていくことが必要なように思う。

〇国民が違法行為を犯さないように、または違法ではないにしても、不当な結果をもたらすような行為を行うことがないようにどうするのか。すぐにできることと法整備をしていかなければいけないことなどあると思うが、法整備を待っていてはまた違う状況になってしまうため、まず事前に何ができるかを考えてみると、ある取引などに入る前に基準が示されていることが大事で、経済安全保障上重要な技術は何なのかという定義をし、基準を出していただいて、何らかのガイダンスがあれば、企業はどのように行動すべきなのかが分かりやすくなる。また、それについて相談をする窓口があることが大事だろうと思う。、注意基準があったとしても取引が進んでしまうときもあり、途中で企業がこれは危ないのではないかと思うときに、安心して相談できる場所や手続も必要だろうと思う。また、違法な行為に対する処罰を厳しいものにすることも違法取引の抑止として重要だろうと思う。

○外国政府による強制が不当だが違法ではない場合にどうするのかがむしろ難しいのかもしれないが、これも様々なガイダンス、ガイドラインなどの作成・履行により、文化を変えていくことも必要ではないかと思う。安全保障貿易管理に関するガイダンスが出て以降、時間をかけて大学も文科系の学部の教員、職員の意識も大きく変わった。そういう地道な努力が必要で、様々なものの組合せが必要。今、できるところからすぐに進めていくことが大事ではないかと思う。

○なかなか難しいところがあって、オープンサイエンスですよねと言いながら、ある部分はちゃんと理解して縛っていかないといけない。今、特に産学連携をもっと深化させようと言っているときになかなか難しい状況はあると思う。そこのリテラシーを我々がどう獲得していけるのかになると思うが、先ほどのお話にもあったように、何が相談事項なのかも理解しないとなかなか動けないというところを、どのように周知していくかだと思っている。

○どういう外縁なのか、どういう資金のどういうものが対象なのかについては、議論が必要であるため、ここに例示することはできないのかもしれないが、かなり具体的に示された上での議論になってくるのかなと感じている。ある程度外縁がはっきりしてきたときには、どういうプレーヤーが関わっているのか、ないしは関わり得るのかが想定されると思うので、広く中小企業等に広くお知らせする。こういう趣旨のこういう規制が世の中で行われているという状況自体をお知らせするのも非常に重要で、関わりが深くなりそうな中小企業等にどうリーチしてどう知らせていくのかというプッシュ型のアプローチも考える必要があると思う。

○本日の議論は専門家の中でも難しい議論。いろいろな法体系を含む内容が重なり合う議論になり、ある一定の知見や関わりのレベルに合わせてどううまく伝えていくかも重要になると思うので、ぜひよろしくお願いしたい。

（事務局からの回答）
○今回の議論は、規制という文脈ではなく、政府がある種インセンティブを与える場合に、経済安全保障上の重要な技術情報の管理について、その保有企業等に、どのような行為、行動が望ましいのかを明らかにした上で、そうした行動を企業等に求めていくことと併せて支援をしていこうということ。まさに規制の議論とは異なるものではないかなとは思うものの、いわゆる一定の営業秘密管理を求めるということで、管理のためにコストが何らか発生することは当然あり得る。スタートアップ等に対する周知については、どのようなことが求められているか、先ほど委員からもあったとおり、簡単に始められる対策もあるという言葉と併せて伝えていくことが考えられるし、リスクに応じたということで、どう

いうリスクがあるのかという定量的な特定はなかなか難しい部分があるが、どのようなリスクと対応があるかということについての企業自身の判断と、国がどのようにそれを評価し、受け止めるかということとの関係でもあるので、重要な御指摘をいただいたというように理解し、適切に中小企業、スタートアップに周知し、広く参加を求めていくうえでの一つの材料にさせていただきたい。

（委員のコメント）
〇今の不競法は使い勝手が悪く、その結果として、本来営業秘密として守られるべきものが守られず、さらにモニタリングも不十分で流出してしまっているとすれば、そうした使い勝手の悪さは改善しなければならない。他方、企業が営業秘密として守るものと日本の経済安全保障上重要な技術は異なると思う。そこを合わせていくためには、やはり官民の対話が一層必要になるが、対話の基盤となる共通のリテラシーがないのが現状である。

〇共通のリテラシーをどのようにしてつくるか。国内外の情勢や研究開発動向等の調査・分析等を担うシンクタンクを立ち上げるという話があったが、これがなかなか見えてこない中で様々な審議会等で技術管理の議論をしている。結果的に出てきたものが大幅にずれていることはないにしても、微妙にずれていたりすると、企業としては、何をベースに管理していったら良いのかわからないという結果になりかねない。管理の対象を広くとれば、安全保障上は良いかもしれないが、経済力、技術力が低下し、国力としてマイナスになってしまう。やはり、共通のリテラシーが一番重要であり、それがないところで議論するのは難しいと思う。前回会合においても、政府の様々なところで議論が行われているので、NSSで調整していただきたいと申し上げたが、それをかみ砕いて言うと、今申し上げたようなことになる。

〇共通のリテラシーの外縁がある程度はっきりしてきたときに議論すべきなのが、よく言われる「スモールヤード・ハイフェンス」の中身である。「スモールヤード・ハイフェンス」については、もう少し具体的な言葉をもって語る必要がある。最近、在中国EU商工会議所が出した提言を見ていると、管理を行う場合、その対象は、リスクを起点にproportionate、targeted、preciseでなければならないと言っているが、これなどは具体的で分かりやすい。共通のリテラシーの下で、そうした原則に基づいて、対象を絞り込んでいかなければならない。そうした作業なくして、企業の営業秘密管理が不十分だと批判されても、企業としては路頭に迷うだけである。

〇国の委託研究開発が対象だとすれば、ある程度国の資金が投じられている以上、アメリカのCHIPS法と同じようにガードレールがあってしかるべきと思う。他方、セキュリティークリアランス法案の審議を見ていて、一番気になるのはCUIの管理のあり方をめぐる議論

がどう発展していくかである。セキュリティークリアランスの有識者会議でも、この問題は宿題になっており、今後議論するのであれば、ゼロから議論してもらいたいと考えている。今回は、技術管理をめぐる議論のうち、国の委託部分からスタートするということだが、結局は共通のリテラシーという全体の話に戻ってくるのではないか。

○あまり難しいことを言うとソリューションがないが、法目的が違うということは本質的。だから、営業秘密というのは民間が民事に対して秘密ということをどう捉えて、それが制度的に刑法に落ちているわけであるが、経済安全保障は管理の話で、やはりそこはどうしても原理的にはずれは生じる。それを別の体系でつくろうとすると、韓国だと法令が営業秘密、不競法と同じく別にあって、この技術は国家革新技術だからといって、不競法に対する重加という話になってしまう。これは結構ハードルが高いので、リテラシーのところでうまく阿吽の呼吸で何かできないかといった話になると思うが、本質的にはやはり分類にはずれが生じるとは思う。

○経済安保に特化したものというのはなかなか難しそうだと思っている。例えば資料６ページにあるように自然人の罰金は2000万円で、海外使用は3000万円だが、民間企業でも重要な技術を持ち出して訴訟になっても、3000万円程度は搾取した側が喜んで情報提供者に支払ってくれる金額だと思うので、経済安保問題とは整合性は低い。もちろん刑事罰も同じである。今から検討を始めておかないと、急に何か起こってからでは間に合わないので、検討を法務省なり経産省なりと内閣府で今からでも進めていただきたい。

○リテラシーという話は非常に説得力もあるし、現実的かなと思うが、リテラシーをつくるに当たっても一定の根拠は必要だろう。法律、設置法にするのかは分からないが、結局、やはりそこの問題には多分行き着くのだろうというように思う。

以上

「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４回）議事要旨

１　日時

令和６年５月20日（月）14時00分から15時30分までの間

２　場所

中央合同庁舎４号館共用第２特別会議室

３　出席者

（委員）

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
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
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
渡部　俊也	東京大学未来ビジョン研究センター 教授

（政府側）

飯田　陽一	内閣官房経済安全保障法制準備室長
高村　康夫	内閣審議官
彦谷　直克	内閣審議官
品川　高浩	内閣審議官
早田　　豪	内閣参事官
田村　亮平	内閣参事官
田中　伸彦	内閣参事官
白井　　俊	科学技術・イノベーション推進事務局参事官（研究環境）
宮澤　武志	科学技術・イノベーション推進事務局企画官
西川　和見	経済産業省大臣官房経済安全保障室長
大隈　一聡	経済産業省産業技術環境局研究開発課長

４　議事概要

（１） 事務局説明

事務局から、資料１～３の内容について説明があった。

（２） 自由討議

（委員のコメント）

○この度の報告案について基本的に賛同する。その上で2つほどのコメントを申し上げる。研究インテグリティのガイドラインの策定に主体的に関与してきた総合科学技術イノベーション会議では、大学関係者や国立研究開発法人など幅広いアカデミアからの意見聴取を行なって、国の研究開発に伴う研究の正当性、公正性を担保する必要性から、ベストプラクティスも含めた議論を積み上げてきた。一方で、国家安全保障への潜在的なリスクを念頭におくべき研究セキュリティの問題は、大学における研究の自由や大学の独立性を念頭に置きつつ、今後の検討すべき重要な課題となると思われる。現在は、国家的なミッション性が高い国立研究開発法人を中心に研究セキュリティのベストプラクティスを議論することから始めようとしている。ただ、この報告案にも記されているように、各国では行政当局と大学との間での緊密なディスカッションを通して研究インテグリティの方向性を打ち出そうとしていることを鑑みるに、今後は多くの留学生を引き受けている大学との共通の議論の場を設ける必要も出てくるのではないかと考えている。言い換えれば、この報告書の参考資料の概念図の中で「研究インテグリティの取組の徹底による研究セキュリティ」と記されている部分についてはまだ厳密な定義が示されていない。この点は、総合科学イノベーション会議においても今後の検討の対象となると考えている。

○また、研究セキュリティを論じる際には、我が国の現状におけるコア重要技術、将来の技術的優位性を生み出す可能性のある領域と、それらと産業界のサプライチェーンとのつながりなどを明示的かつエビデンスを持って示すことができなければ、具体的な研究セキュリティの議論を深めることは難しいであろう。総合科学技術イノベーション会議では、次期科学技術イノベーション計画において、今後の我が国おける重要科学技術領域とそこから生まれてくるクリティカルテクノロジーを特定するための議論を深めたい。また、それらの課題に適切に政策提言を行うことができ、専門知識を持つエキスパートを結集したシンクタンクの構築を急ぎたいとも考えている。

○報告案について、全体のタイトルがあって１、２とあったほうが、まず何を論じているのか、何を目指しているのかが分かりやすいように思う。１の中でも、最初に研究インテグリティ・研究セキュリティの定義があり、各国を含めた現在の状況などに進んでいくが、例えばデューデリジェンスについて、３ページ４行目の「オープンソースデューデリジェンス」では何も説明がないが、６ページで「様々な形で公開情報に基づいたデューデリジ

ェンス（以下「オープンソースデューデリジェンス」という）」とあり、最初にある種の専門用語として使っているものをどういう順序で出していくのかは重要だと思う。また、ある一定のサークルでは分かっている言葉かもしれないが、定義を記すことも明確化につながるのではないか。デューデリジェンスの定義のようなものは資料３にはあるが、本文中にはない。まずは共通理解を深めなければならないので、１の位置づけやその意味の明確化があれば、もう少し分かりやすいのではないか。脚注は非常に役に立ち、非常に便利であった。

〇今の御意見は実はごもっともで、１と２が結構違って見えるが、実はフレームワークとしては同じことを言っている。２に対応する資料３において、ここで対象領域が何であるか、それに対してどういう行為が問題になるのか、それについての具体的な対策として、ヒトの管理と取引先における管理と技術移転等の管理というフレームワークになっている。これは実は１でも全く同じで、もっと言えばCUIと言われているものについての対策をしていると見ていいかと思う。なので、１と２は同じフレームワークの中で言っているものだということを少し明確にしていただくほうがよいのではないか思う。ただ、それが見かけ上違うように見えるのは、１については、経緯が国際的な議論の中で進展してきたものであるということ。さらに言うと、今回のG7のコンセンサスも、もともとアメリカで2019年にNDAAで指摘されてきたことについて、今まで大学で行ってきた管理の方法を一つのソリューションとしてコンセンサスを取ってきたものだと思うが、そこで使われてきた言葉などがそのまま使われているので、見かけ上違うように見えるが、基本は同じことを言っている。ただ、大学の場合は、成果公開がデフォルトになっているので、そこでちょっと違う面があるぐらいだと思う。先ほど申し上げた2018年、19年ぐらいのアメリカの考え方は、実はその後日本で、例えば東京大学とIBMなど、量子コンピューターや半導体などで国際共同研究をするとなると、基本その時点で遵守しないといけないような管理の考え方になっていた。特段の管理の方法、これは結局、人のデューデリジェンスと相手先の管理と、それから、技術移転は決めればいいだけの話だが、資料３の③と④をちゃんと管理していないと、相手が信用してくれない。なので、日本としてどの分野で何が大事なのかは、それは決めればいいと思うが、ここ半年間でも日米で一緒に研究を行うプロジェクトの発表はたくさん出ている。AI、半導体、量子などの分野での対策は待ったなしであり、資料３の参考イメージの一番上の諸外国の先進的な取組と同等の研究セキュリティはやらないと、少なくともこれは日米だけではなくてG7で合意しているので、一緒にできませんということにならないように、ここはマストである。別途国としてどういう分野で実施するかというところもあると思うが、そうは言っても国際共同研究をやらないと伸びないので、結局はかなり広くなるのだろうと思う。

〇報告案にもある手順書というのがガイドラインに相当するのだと思うが、アメリカはNSF

などいろいろなところでも注意事項が出ている中、そういうものがやはりまだない。なので、それはマストである。どうそれを実行していくかということで、体制や予算も必要という順番だと思う。

（事務局からの回答）
○まず、本報告案における、オープンソースデューデリジェンスなどの定義の位置であったり、それらの説明をきちんと入れるということ、また、全体のタイトルもきちんと位置づけたほうがいいということで、他の委員からも１と２が同じフレームワークであることが分かるような記述が必要ではないかという意見もいただいたので、内容を変えずにその部分が上手に説明できるように工夫をしたい。

（委員のコメント）
○大学関係と企業ではニュアンスが違うように受け取られることもあろうかと思う。大学の研究の自由やオープン性、それから、イノベーティブな研究はやはり広くいろいろな形での参加をもって進めるべきだということを丁寧に強調し、そして、日本の研究開発力の基盤強化をこれから進めていかなくてはいけないという大きな国家戦略がある中で、これがどういう意味合いを持つかが、もう少し分かりやすくなっていればよいと思う。

○先ほど他の委員から紹介いただきましたように、東大とIBMとの共同プロジェクトなど、どういう状況で、どの技術分野でこのような対応が必要なのかを示していただくことで、理解は深まると思う。事例等で明確に示すことによって、誤解や混乱が起こることだけは絶対に避けるべき。そのためには、導入部を丁寧に作っていただくことが必要。現状でもすでに配慮されていると思うが､それについてもう一度見直していただくのがいいと思う。例えば、大学の研究体制の在り方など現状の問題については、配慮するとされているのでよい。最初の立てつけや構成の仕方の工夫だと思う。

○G7の作業部会からの話について、うまくまとめていただいている。基本的に競争的研究費に関する様々な問題については不十分なままで終わっていると思っているが、特にG7のフレームワークの中でも恥ずかしくない仕組みにしていただきたいと思う。

○資料１の６ページの今後の課題・留意点で、特に関係省庁が緊密に連携して水際対策をさらに強化すべきではないかということで、留学生・外国人研究者等に関する問題について論じられている。また、経済安全保障をめぐる国際的な動きに対応するために、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、と２点指摘があり、これは誠にもっともだと思うが、どうやるのかがやはり気になる。やはり審査の徹底や調査分析機能の強化は、この問題はかなり専門的な局面が多

いのではないかと思うので､やはり統一的な形でのエンティティが必要なのだろうと思う。NSSは基本的に総合調整の機関なので、こういった恒常的な事務を行う組織が少なくとも将来的には、具体的な形でG7とともにやっていくためには必要かと思う。

○セキュリティクリアランスについては、今回統一的な形での調査機関を設けると法律上なっているが、そのようなインプリメンテーションを行うための組織を特定するのが、具体的な形での政策を実現するためにも重要なのではないか。

○今後の課題・留意点という形で御指摘いただいたが、政策をどういった形で実施していくのかについては、CSTIという考えもあるのかもしれないが、各省に分散しても多分この事務はできないのだろうと思っているので、総合調整を担う場所以外のどこかを考えていくということ。これは、内閣官房と内閣府の事務分掌でおのずと切り分けられていくと思っている。

○企業からすると、何が今までと違うことをしなくてはいけないのかが非常に分かりづらい。国際協力の研究なども、多分ここで言われているものとほぼ同等のことは既にできており、企業によって変わるとは思うが、要するに本当に企業のオペレーションや文書管理から実施しているので､何が今までと違うのかが企業からすると少し分かりづらいと思う。あるとすれば、海外の従業員を日本に呼んできて研究をすることがあるが、国の競争資金をもらった研究に携わる人の確認ということか。これから誰でも簡単に連れてこられるようになるわけではないということか。それぐらいしかあまり関係がないと思うが、全体的に言わんとすることは非常によく分かるし、これは必要だと思う。ただ、ここで一番のポイントは大学と思われるので、企業からすると、今までやっていることと何が違うのかがちょっと分かりづらいなと思う。

○手順書を作っていただけるということで、そこはぜひ工程表も含めて出していただけると、どういうところを企業が変えていかなくてはいけないのかが分かりやすいと思う。

（事務局からの回答）
○研究セキュリティ・インテグリティの議論が、G7の議論も含めて、国際的には急速に進展している一方で、営業秘密管理を行う企業とは異なり、いわゆる「パブリッシャブル」な領域、つまり成果を論文等で公表するという前提での研究開発、その際のリスク管理をどうするかということ。同じ国からの支援を受ける研究開発であっても、こうした成果の公表を前提とする大学等アカデミア中心の研究セキュリティ上のリスク管理と、成果に対して所要の営業秘密管理を行う前提の企業のリスク管理とで、前提が大きく異なっている

という点もあると思う。その点が同じフレームワークでありながら、大きく違っている点だが、委員からも御指摘いただいたので、それが分かるような形で記載を工夫させていただきたい。

（委員のコメント）
○１に関して、特に企業に対してのメッセージは何なのか。

（事務局からの回答）
○企業も大学と連携することもあろうかと思うが、その際に、そういうリスク管理は当然知を共有すべき大学等においても、今回は政府資金が提供される、競争的研究費が関与する場合ではあるが、研究セキュリティ・インテグリティの取組として、リスク管理を行っていくことがある種国際的な常識になりつつあるということと、企業も大学等との付き合う際はそうした動きを踏まえる必要があるということが企業向けのメッセージになると思う。

（委員のコメント）
○やはり企業は、１については関係ないと政府に言ってほしいのが実態。基本的には２において一般企業は関係するという説明なのだと思うが、ただ、どこが対象かと書いていないと書いていないこともあって、やはり一般の人は見た瞬間それがよく分からず、ですから、そこはある程度切り分けや明示が必要かと思う。、心配する人は心配すると思うので。

○企業も海外と共同研究はやっているので若干関係してくることもないわけではないと思う。

○前回の発言と重複するが、他の委員からも指摘があったように、１、２の共通項を導入部分で書いたほうが分かりやすい。重要経済安保情報の保護及び活用に関する法律案の審議の過程では、CUIの中でも特に民間保有情報をどのように扱うべきかに関する議論が多くみられた。この議論がどのようになるか注視している。そういう観点からすると、１も２もCUIの民間保有情報の件であって、本来であれば、６ページの今後の課題にあるように、いわゆるシンクタンク機能により提供される「これはリスクが高いので、さすがに民間でも適切に管理しよう」という共通のリテラシーに基づいて対応していくのが理想である。しかしながら、シンクタンク機能も共通のリテラシーも今のところない中において、とりあえずできるところからやろう、G7でも議論があるので、というのが現状だと思う。その皮切りとして、国のお金が入るプロジェクトから管理しようということだと理解している。１の軸足は大学等にあり、２の軸足は企業にあるということだと思う。

○６ページの今後の課題の２番目に指摘されている、リスクの特定等に関する調査分析機能については、「研究セキュリティ・インテグリティに関する」という修飾を外せば、１と２の両方に言える課題ではないか。

○資料３の２ページにある参考のイメージ図について、報告案では、一番下の研究インテグリティが現在行われているものであり、政府方針に基づいて様々な確認等を徹底すると真ん中の水色のところになり、一番上にはオープンソースデューデリジェンスなどを充実することでたどり着く、という整理になっているが、文章だけでは、この階層構造を理解することは難しい。他の委員が強調されたように、一番上の部分はG7で決まっていることであり、一番下の部分は現在も実施されていることを踏まえれば、真ん中の部分だけが曖昧になっているというのが実態ではないか。下からだんだん上に積み上がっていくというよりは、上と下が決まっている中で真ん中をどうするのかという点がポイントだと思っている。

（事務局からの回答）
○１と２の共通的な事項を括り出すというのは各委員からも指摘いただいたので、工夫していきたい。また、１についてはいわゆる「パブリッシャブル」な領域であるので、単純にCUIというものではないと考えているが、技術情報自体も含め、御指摘のとおり、成果が公表されるのか、もしくはコントロールされたある種の秘密情報として企業において管理されるのかという違いだけで、そういう意味で言うと、そうした技術情報に関するリスクの特定、同定、そうしたリスクの調査分析については、１と２の間に、かなり相似的な内容があるのではないかと思います。そのあたりをどのように共通的に表せるかは、シンクタンクへの触れ方も含め、事務局のほうで工夫したい。

○資料３にある図がないとなかなか分かりにくいという御指摘について、関係各省とも議論をしていく中で、だんだんこれが理解は進んでいると思うが、もう少しこの図をどのように表現し、報告案の中でより理解をしてもらうためにどのように表記するかも検討していく。

（委員のコメント）
○全体をまとめるときの参考となるかわからないが、基本これは企業も大学もガバナンスの話。守るべきものが何なのかというところで、企業は当然営業秘密など企業の事業活動上で守るべきものをちゃんと守っていますかという話で、大学は社会から期待される透明性やインテグリティ、学問の自由に対して脅威があるから、その脅威に対してどう対応する必要があるかという意味では全く共通。そういう整理の仕方が一番いいかなと思うが、うまくまとめていただければと思う。

○２の方が特にCUIとの関係がもう少し明確になった方がいいと思う。あと、やはり外為法との相関。資料３は非常に分かりやすいが、要するに何にどこまで影響が及ぶのかが分かりづらくなっていて、先ほどの図でも同様であるが、何となくスモールヤード・ハイフェンスのようだが、最近は、やはりラージヤード・ローフェンスで、境界が分からなくなっている。ガードレールというコンセプトは、定性的にわかりやすく、そのようにしなければならないと思う。そのあたりは本当に企業が一番意識するところだが、経済界でこれを説明するときにはそこに苦労があると思う。

○最初にこの資料を読んだときに１と２が全く別物のように感じたので、ぜひ共通事項が何なのかを整理いただくのがいいと思う。２に関しては、一つ一つはごもっともだと思う。一方支援を受ける対象の企業の規模が明確ではないが、報告案を読んでいると、前提は大企業という印象である。というのは恐らくここに書かれている技術流出防止措置を実行するには、それなりの資金あるいは知識が必要で、例えば記載の好事例は非常に良いが、実際に実行するとなると、恐らく中小企業あるいは特殊な技術を持つスタートアップでは難しいと思う。どう実行するのかも念頭に置きながら提案をする必要があるだろうということと、想定される企業規模もある程度イメージできるような書きぶりであったほうがよいのではないか。もう一点は、他の委員からも御指摘があったが、外為法が適用できる部分と、外為法の適用外でこの措置が必要であるケースが明確になっていると理解しやすくなると思う。

○他の委員の御指摘ともほぼ同様のことになると思うが、結局、官民技術協力あるいは国の競争資金が入っているという下で、これまでも産業界や企業で講じてきている例えば技術流出の防止措置もそれなりにある中で、改めてどこが追加的にあるいは重点的に産業界において強化すべきところなのかというメッセージをクリアに出していただけるように、例えば今後の課題や留意点でも強調していただくといいのではないか。

○言い換えると、国の競争資金あるいは国際的な協力関係の中で、領域や時間軸で「ムービングターゲット」を内在する研究開発のプログラムを実施していく上で、例えばサプライチェーン支援における計画の認定要件の際に企業に求める技術流出の防止措置との関係において影響を与えることが生じてくることが考えられ、そうした影響も含めて、トータルで産業界に対して技術流出の防止について何を求めているのかを整理して示していただくと非常にありがたい。そのような整理のもとで、産業界の取組みを促していくことが大事なのではないか。

（事務局からの回答）

○まず、CUIや外為法との関係は、直接的には記載していないが、１は、いわゆる「パブリッシャブル」な領域である旨説明しており、また、２は国の研究開発プログラムに参加する民間企業が保有する営業秘密という、当該プログラムの管理される成果としての技術情報だと考えれば、まさにCUIの一部を対象にしているということ。さらに、外為法との関係については、いわゆる公知のものは外為法の対象にならない。また、外為法は、国の資金の有無に関わらず、所要の技術情報については、居住者と非居住者の間のやり取りが対象になっている。外為法とは独立して、今回の議論は、補助金などの支援を受ける企業との間でもある種の契約の中で合意をしていくということになると思っている。こうした外為法との関係は外為法の所管部局である経産省等とも相談の上、適切に記載させていただきたい。

○中小企業、スタートアップの関係は、どのように実施していくのかという配慮事項の話かと思われるので、御指摘を受けたということで、適切に報告案の中でも記載させていただきたい。サプライチェーンについては、推進法に基づく支援の際にはこうした形で御議論いただいて､次の支援はどうするのかを検討していただくことになろうかと思う｡また、今後、現実の課題も変わっていくと考えれば、この報告案の後に出てくるサプライチェーンの措置については適切にアップデートされる形で御議論いただくのだろうと考えている。

○サプライチェーン強化に向けた特定重要物資に係る技術管理要件については、先般の取組方針改定で反映されたところであり、今後の計画認定から実際に要件が課されていくこととなっている。今回の技術に関する議論に係るヒアリング含め、様々な課題について勉強させていただいているところだが、サプライチェーン支援においても、今般の議論も踏まえながら、実際に運用していく中での企業の反応なども踏まえ、アップデート等検討していければと思っている。

（委員のコメント）
○企業ヒアリングについては、国家間のプロジェクトであるか、安保上重要であるか、とあまり区別せずにヒアリングを受けていた。この報告案では国家間のプロジェクトと我が国の安保の重要なもの別に書かれている。企業でも全部門が読むガイドラインは非常に作るのが難しい。読む側の使う言葉や理解の仕方も違い、、競業避止や、人や国による差別を書けない状況でガイドラインを作らなければならないので、苦労は非常によく分かる。その中で、例えば段落１の背景では各国が何をやっているかが中心に書かれていて、そこで各国が使っている言葉で説明されている。段落２は安保上重要なものや外為法に近いような内容も含まれ、やはり日本の法律で使われている言葉が使われていて、それらがどう対応しているのか、法曹の人間ではない者にとって非常に分かりにくいことは確かだと思うので､もし共通の定義みたいなもの､安易な定義ができれば分かりやすくなるかと思う。

○段落２のほうがどちらかというと産業界に関わるところかと思う。研究インテグリティという話が出ていたが、やはりneed to knowの研究当事者にいかに自由で闊達な研究開発をしてもらうかという観点で見なくてはいけない。これを妨げてしまうとやはり有益な研究開発はできないので、国益に反することになる。一方で、今度はneed to know以外の方に情報が漏れるのは徹底的に防ぐ必要があるという二面性があると思っており、企業などで実行していることは、例えば秘密保持契約などの契約で縛るものは技術分野の特定も細かく、狭く定義して、残留情報についてはある程度は許容するような書き方になる。一方、そういうneed to knowの方々の悪意もしくは事故や誤操作により情報がneed to know以外の人に漏れるのがもっとも大きな問題であるため、これについては厳しく徹底的に、技術分野や情報の種類等も絞らずに全ての情報についてウォッチングをする。その両面性が非常に大事で、その部分は９ページ、10ページに書いていただいたと思っている。その中で不競法は、営業秘密として認めてもらえるように徹底的に管理も行っているが、営業秘密を搾取されたときにそれを証明するのが非常に難しい。人と情報がペアで流出する状況が、一番ダメージが大きい。しかし、それに対する絶対的な対策は実はなくて、人に対して十分な名誉とか報酬を与えることと、それから、スパイ対策というのを啓蒙することぐらいが産業界で実際にできることではないかと思われる。

○今日の御議論をお聞きして少し解像度が高まった気がする。一つは、他の委員の御指摘にあったような、中小企業やベンチャー企業がどう理解できるのかということ。それから、こちらも他の委員が指摘されていたが、ほかの施策との関係性の構造等を分かりやすく御説明いただくということをぜひよろしくお願いしたい。

○一点質問だが、本件の具体化に向けて、具体的なアクションとしてはどういうスケジュール感でどういうふうに進んでいくのか、もしあれば教えていただきたい。

（事務局からの回答）
○他の関係の施策も含めてしっかりと記載をさせていただきたく、また、現実に難しい、できている点、できていない点も参考情報になるかと思うが、御指摘を踏まえて記載を試みたい。また、スケジュール感ついてはこれから政府内でしっかりと議論していくということに尽きるが、その点も御指摘を踏まえて記載したい。

（委員のコメント）
○今回ヒアリングされた企業はほぼ問題ないということだと思うが、依然ちゃんとできていないところが多いと思う。特に人を通じた流出、取引先を通じた流出、この２つが非常に多いので、やはりできていないことがかなりあるという前提で考えたときに、それは企

業の責任で自分の利益が失われるのは仕方がないということではなく、今回、特定重要物資など国の要請で守ってくださいと付け加えたわけなので、そこについてはこの水準まではきちんとやってくださいということだと思う。そのときに、どこまで人のアクセス管理をするのかになるが、国籍は聞いてはならないので聞いていない。他方、どこの国の人がいるか分かりませんということでは、民間だけの話であればよいのかもしれないが、この特定重要物資などについてはやはり何とかしないといけないので、そこをどうするかが一つあると思う。

○それから、正確なところを理解していただいたほうがいいと思うのだが、１に関して、あるいは大学に関して、公開がデフォルトだから基本CUIは関係ないというのは必ずしも正しくなく、研究活動の中でもCUIは使う。一番分かりやすいのは、例えば個人情報であり、研究開発の中で使うが、必ずレビューして外へ出ないようにしなければならず、それは今後の研究開発においては、Ｋプロなども一部そういうところはある。研究成果は公開してよいが、そこに使う材料については管理しないといけないというところは共通だと思う。

○気になっている点を二点だけ申し上げる。一つは、資料３の２に関する表の「主な対象領域」として、サプライチェーンの場合は政令で12分野が示されており、そのうちの６分野で技術流出防止策が求められているのに対し、今回の右側の２つはそういう枠がない中で技術優位性ということをキーワードに書かれている。他の委員からも御指摘があったとおりラージヤードにならないように、何か基準や大枠をはめる必要があると思う。

○もう一点は、この枠組みがスタートする段階で確認ができれば良いと思うが、デューデリジェンスについて、本人からの情報提供などについて、どういう情報を出してもらえば良いのか、労働関係法令との兼ね合いをどう考えれば良いのかなど、セキュリティクリアランスで議論されているようなことと同じことが気になる。今回の取組がスタートするまでにはある程度はっきりさせたほうが良いと思う。

（事務局からの回答）
○執行段階において適切な運用をどのように確保していくのかという御指摘だと思う。一つはスモールヤード・ハイフェンスでしっかりと必要な領域だけに対応措置を求めていくのかという話と、それから、実際にデューデリジェンスを求める中で、実際の法令の関係も含めて、どのようなやり方、手続、手順で具体的にやっていくかという話だと思う今後これを各省において検討、実施していただく中で、基本的にはサプライチェーンと同様に、支援の前提条件を明確にすることが最も重要かと思う。したがって、公募であれ何であれ、何らかの支援を行う際の方針の中で適切に記載するということだと思う。まさにそれをできるようにするのがこの場の議論の大きな趣旨だと思うので、御指摘いただいた点も含め

て、今後関係省庁と議論をしていく中でしっかりと明確化を図って、御懸念のないような形で運用に努めていきたい。

（委員のコメント）
〇支援の方針の中できっちり書いていくというお話について、要するに何がその元になるのかが知りたくて、先ほどいわゆるタイムスケジュールの話も出ていたが、政令もしくは閣議決定以下の何かが出てくるのか、それとも省令レベルなのか。今回有識者会議の基本的報告という形で出ていくことになると、法律ではないのかもしれないが、どういったもので定められていくのか。

（事務局からの回答）
〇今回のものは、基本的には予算措置に関係する話だと思っている。そうなると、一般的には補助金であれば補助金の要項を明らかにして、公募していくというのが通常なので、そうした要項の中で明確にしていくということになると思う研究開発の場合も公募を実施するのが一般的なので、例えばファンディングエージェンシーの公募要領に同記載するのか、これが例えば独法の場合と政府の場合とどのように異なるか、これは若干工夫が必要になると思うが、執行の段階において明確に文章も含めてきっちり示していくということに一般的にはなると思う。さらに、例えば、推進法に基づく指針その他の中でも何らかある程度のガイドラインもできないかということを含めて検討していきたい。

（委員からコメント）
〇予算の要綱は一つ考え方ではあると思うが、一方、行政の透明性という観点からも、統一的な方針がその背景にあって、要項が定められているということが示されてしかるべきかと思うので、御検討いただきたい。

（事務局からの回答）
〇今の御指摘はごもっともなので、政府全体の方針として、各補助金等の執行にあたって基準なりルールを定めてやってくださいという形を政府全体でとるのか、それが閣議決定という形になるのか、それとも実際の関係省庁の申合せになるのか、様々な形態があるのだと思うが、単純に有識者会議の御報告を受けて、それから各省庁が勝手に考えて勝手にやるということを想定して議論しているわけではない。そういった政府全体の統一的な方針となるようなものをベースとして、その上で、各省庁にその方針に沿って補助金なり委託研究開発費を執行していただくということで、今回御議論いただいていると御理解いただきたい。

（委員のコメント）

○先ほどの話と関連するが、基本的に内閣官房における総合調整の発動という形で今回の議論はされており、G7の作業部会での見解との接合性も考えているということであったので、個別の補助金においての要項はそれぞれのものだが、やはり統一的な方針のようなものが必要ではないかという意見があったことも明記していただきたい。

（事務局からの回答）
○今まで技術優位性の議論として、多分技術でピックアップできるものもあると思うが、技術でピックアップして、これを対象として考えるという構えを取るつもりはなく、すごく曖昧ではないかと言われるかもしれないが、やはり他国との関係において技術優位性を確保している、あるいは将来確保できるというのは何なのだろうかを考える中で、国の資金を投入するプログラムとしてその範囲が明確になっていく、限定されていくというのが基本的な考え方で、技術に対してはニュートラルに考えていかなければといけないと思っている。それから、企業の規模は何を想定するのかと委員からも御指摘いただいたが、大企業やスタートアップということをこの文脈では限定する必要は全くないと思っており、逆にこの支援のプログラムを考えたときに、当然スタートアップなり中小企業は組織としての資金や体力を含めて限界があるものの、イノベーションの担い手として重要なプログラムに参加してもらうためには、逆にどういった措置を講ずることが必要なのかということも併せて考える必要があると思う。これはKプロのとりわけアカデミアが参加するプログラムの中で、情報管理のための経費を例えばKプロの予算執行の中には組み込むといった議論をこの有識者会議あるいはプログラム会議でも御議論いただいたが、そういった形でしっかりとした担い手を取り込まなければいけないので、そこに配慮した制度設計あるいは補助金なりの設計をしていくのは当然のことであると考える。

以上