「経済安全保障法制に関する有識者会議」（第９回）議事要旨

１　日時

令和６年１月29日（月）13時00分から14時30分までの間

２　場所

中央合同庁舎４号館　共用第４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【座長】
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
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
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
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

（政府側）

高市　早苗	経済安全保障担当大臣・内閣府特命担当大臣（経済安全保障）
古賀　　篤	内閣府副大臣
田和　　宏	内閣府事務次官
井上　裕之	内閣府審議官
飯田　陽一	内閣官房経済安全保障法制準備室長・内閣府政策統括官（経済安全保障担当）
高村　泰夫	内閣審議官
佐々木啓介	内閣審議官
彦谷　直克	内閣審議官
品川　高浩	内閣審議官

4　議事概要

（１）高市大臣冒頭挨拶

・　委員の皆様におかれては、今回もご多用の中、ご出席を賜り心から感謝申し上げる。

・　前回の会議でご議論いただいたサプライチェーンの強靱化については、パブリックコメントも終了をしており、特定重要物資を追加する政令の閣議決定に向けて最終的な準備を行っている。

・　K Programについては、一次、二次研究開発ビジョンに基づく事業を進めているほか、新たな課題への対応の検討にも着手した。

・　本日は、基幹インフラに関する制度については、対象分野の追加の検討状況、そして、特許出願の非公開制度については、運用開始に向けた準備状況をご説明させていただくほか、経済安全保障分野におけるセキュリティ・クリアランス制度の検討状況についてもご報告をさせていただく。

（２）基幹インフラに関する分野別検討会合（令和５年12月20日実施）の結果について

○　検討会合では、事務局から、施行の状況と法案成立後のサイバー攻撃事案を受けた対応について説明があった。具体的には、国土交通省と厚生労働省からそれぞれ説明があり、その説明を踏まえて、港湾については、一般港湾運送事業を基幹インフラ制度の対象に追加することについてどう考えるか、医療については、個々の医療機関は基幹インフラ制度の対象とはせず、医療DXに関するシステムは引き続き検討していくことについてどう考えるかという点について論点提示があり、その説明を踏まえて、議論をさせていただいた。

○　港湾については、提案に異論はないということで、案に対して賛同する意見が多かった。

○　医療に関して、提案に異論はないという意見が多くあった。ただし、もう少し詳細に検討を必要とするのではないか、引き続き精査することをもって賛成という意見があった。また地域医療の中核となる病院は指定をすべきではないかといった意見もあった。サイバーセキュリティ対策がこれまで以上に求められる、医療施設の事業継続計画を実効的なものにする必要がある、障害時の地域連携の仕組みについて検討していただきたい、医療DXの追加については慎重に検討いただきたいという意見があった。

○　その他の意見として、今回の事業追加に関して、事案が発生してから特定社会基盤事業に追加されるという形は望ましくないのではないか。インシデントが発生し

たことを受けて追加するというようなボトムアップのアプローチだけでなく、トップダウンのアプローチも求められるのではないか。障害時のレジリエンスがより重要ではないかという意見があった。

（３）特許出願の非公開に関する分野別検討会合（令和５年12月４日実施）の結果について

○　検討会合では、事務局より、適正管理措置ガイドライン案や損失補償に関するQ&A案について説明があり、その後、説明のあったガイドライン案、Q&A案について議論を行った。

○　適正管理措置ガイドライン案については、情報保全に関して４つに分けて整理することは分かりやすい、「Need to know」の記載があったため官民両方に理解しやすく、これが浸透していけばよいと思う、全体的に見ると常識にのっとった内容であり、特に営業秘密にすることを規定することは民間事業者にとって大変分かりやすいなど、案に対して賛同する意見が多くあった。

○　そのほか、昨今は、クラウドサービスを利用したほうがセキュリティに優れている場合もあり、物理的管理措置の特定区域に関する考え方については、時代に即して適宜見直しの検討をしていただきたい、他の施策における情報管理はそれぞれ目的が異なるため内容が違うことについては構わないが、違う部分が合理的に違うのかどうかということも含めて整理をしたほうがいいなどの意見があった。

○　損失補償に関するQ&A案については、製品の販売または実施許諾による利益を補償の対象にすることは理にかなっている、かなり厳密な整理をしてもらったと理解したなど、案に対して賛同する意見が多くあった。

○　そのほか、他の出願人が保全対象発明と同じ発明を海外へ出願して特許権を取得した場合、海外でその発明を実施しようとすると差止請求を受けてしまうケースが考えられる。その場合、海外で取得された特許権の存続中、損失が生じることがあり得るため、その旨を明確にしていただきたいなどの意見があった。

○　その他、特許出願の非公開の制度全般に対する意見として、イノベーションを阻害するものであってはいけないという重要な施策の一つの柱になるため、経済安全保障制度の全体の中での位置づけや全体とのバランスを取りながら進めていただきたい、本制度の周知については継続して尽力をお願いしたいなどの意見があった。

（４）事務局説明

事務局から、資料１から資料１０の内容について説明があった。

（５）自由討議（欠席委員からの事前提出意見も含む。）

○　本日説明いただいた基幹インフラに関する対象事業の追加、それから特許出願の非公開に関する運用の準備状況について、いずれも事務局から説明いただいた方針を支持したいと思う。

○　基幹インフラに関し、医療については、分野別検討会合においても申し上げたことであるが、多くの医療機関が経済安全保障推進法上の基幹インフラに該当するかどうかは別として、医療が重要なインフラであることは異論がないところかと思う。そのため、個々の医療機関に対するサイバー攻撃への対処については、我が国として重要な課題だと思うので、政府においても万全の対策等を講じていただきたい。

○　今回の基幹インフラに関するところは、基本的にこの方向で私は結構だと思う。

○　セキュリティ・クリアランスについては、CSTIは、例えばAIホスピタルとか、あるいは医療データの集約とかをずっとやってきており、つくづく感じることは、現場で、この制度を受け止めることは難しいだろうという現状があると考える。とりわけ、それはセキュリティ・クリアランスに関わるような具体的なエンジニア、人材育成に相当後れがあるということを感じているからである。

○　アメリカなどのケースと比べていくと明確な違いがあり、我々のほうでもセキュリティ・クリアランスに係るような人材の日本全体の人材のデータベースをつくってやっているが、相当難しいと思われる。なので、私はこういう形のクリアランス制度をずっとやっていくことに基本的に賛成なのだが、これを現場が受け取れるようなインセンティブをどういうふうに構築できるかに関して、もう少し知恵を働かせないといけないのではないかと思っている。

○　特にサイバーセキュリティは様々な領域、例えばブロックチェーン、あるいは攻撃、あるいは防衛、いろいろな領域についての人材の状況を見たが、残念ながら非常に少ないと言わざるを得ない。それはすなわちここ20年の間、そのようなことに係る人材育成を我が国は怠ってきたということである。このことは今、内閣府で行っているｅ-CSTIの中でも明確に出てきているので、従来の文部科学省あるいは経産省の枠組みを超えたような人材の育成についてのフレームワークを考えないとい

けないということだけは申し上げておく。実際にAIホスピタルの中でやっている、あるいはいろいろなところでやっている医療データの問題について、現場に対するクリアランスというのは極めて重要だが、同時にそれをどうサポートできるのかということが、隔靴掻痒（かっかそうよう）の感があると思っていることだけお伝えする。

○　今回の基幹インフラに関し、異論はない。

○　DXが今後進展する中において、基幹インフラにおいてどの部分が対象事業範囲になるのかというのは当然変わってくるものだと思っている。これは港湾についても同様である。今回の基幹インフラの範囲において、現在は医療を含めないことについて同意はするが、今後、DXで横に広がっていけば、当然そこの部分の対象も広がっていく可能性があり、また、現状、医療もいろいろDX上問題があるのかもしれないが、今後もう少し医療機関でデータがつながり、レセプトも含めて様々な形でデータが使われる取組が広がっていくということになれば、当然医療についてもしっかり考えていかなければいけないということであるので、不断に見直されることは重要だと思う。

○　特許について、異論はない。

○　損失に関しては、特許というものの個別性をしっかり見ていく必要があると考える。１つの特許でその利益が生み出されるわけではなく、様々な特許を組み合わせて、ある意味、企業の防御手段として特許を使うケースもあり、特許の使い方にはいろいろあるので、そうしたものの実態をしっかり見ることが必要と考える。

○　資料１に記載の「異論あり」と申し上げた委員とは、私のことである。地域中核病院、それから地域支援病院、特定機能病院、これらを地域中核病院等と申し上げるが、これらの医療機関がどういった役割を担っているかというと、高度医療の提供、地域医療等の連携、総合的な医療サービスの提供、教育と研修の場、公衆衛生の予防医療、そして災害時の医療支援である。災害時なので、当然有事も入ってくるのだろうと思うし、公衆衛生、予防医療といった面においても、こういった医療機関は非常に重要な役割を果たしていると考える。この地域中核病院等がサイバー攻撃を受けた場合の影響であるが、１つ目は患者情報の漏えい、２つ目は医療サービスの中断、３つ目は医療機器の機能不全、４つ目は経済的損失といったことが予想される。私は、そういった意味で、少なくともこういった機関の上部の部分については、特定社会基盤事業として指定されるべきであろうと考えている。事務局か

らの説明を聞いたところ、経済安全保障推進法上の特定社会基盤事業には医療は該当しないという解釈ではないということであるが、それならば、今回指定しない、必要性がない理由は何なのかということを１つお聞きしたい。

○　先ほど私が申しあげたとおり、資料２「分野別検討会合の議事要旨」も政府の文書なので、こういう表現が本当に妥当なのかどうかということもお聞きしたいと思うが、地域医療の中核となる病院であっても、その提供する医療の代替可能性に差異があるものではないと書いてあるが、しからば、高度な医療技術を提供する三次医療機関の病院も、災害医療、島しょ医療に強い病院も、私の行きつけのクリニックも、本当に差異がないと思わせるような表現である。こういった文書が国民の目に触れることがあっていいのかという問題もあって、結論は大勢に従おうと私は思ってはいるが、少なくとも今の点について、今なぜ必要ないのかということについて、明示的に説明いただきたい。また、このミスリーディングな表現が国民の目に触れるのはよろしくないのではないかとも考える。

○　何度も有識者会議に出させていただき、定性的には非常によく分かった。しかし、具体的な例がないとなかなか動けないという日本の経営者の悪いところであると思うが、もう少し具体的なケースを示していただいたほうが、自分に関係あることだと理解しやすいと感じる。

○　基幹インフラに関してずっと気になっていることは、これからDXも含めてインターネットをどうやって守るのかということである。新しい技術、QKDだとか量子インターネットだとかあるのだが、既存のインターネットをどうやって数年以内に守るか。現在、耐量子計算機暗号については、政府の中で議論がされていないが、ここだけはぜひ基幹インフラにとどまらず、今後、本当にシリアスにディスカッションしていただきたいと思う。

○　特許に関しては、国によっていろいろ法制度が変わるので、いろいろ分かりづらい例が出てくるのだろうなという感じがするので、ここは専門家の方に議論をお任せするが、今後制度の運用が開始していろいろな例が出てきたときに、フレキシブルに対応できるようなことを法整備の中でどうやって担保していくかというところは気を配っていただけるとありがたいなと思う。

○　基幹インフラの港湾について、しっかりと国交省も交えて議論していただいたということで、感謝する。

○　コンテナターミナルのターミナルオペレーションシステムということで、かなり広範囲にこのインフラの議論ができているのだろうなと思うが、これから例えば清水港では水素ステーションを構築していく、あるいは今、箱舟というか、データセンターを港湾のところに整備していくような実証実験も木更津のほうで行われていると思うが、そういった新しい港湾のスマート化の中で出てきているシステムについても、今後議論を展開していただき、適宜対象に加えていくというというような対応をお願いしたいと思う。

○　サイバーセキュリティの観点で、基幹インフラ関係に絞ってコメントさせていただく。まず、サイバー攻撃を予知するということはほとんど不可能である。これは何か特別なものを持っていれば確実に守れるというものではなく、相手側は私たちが持っているシステムの脆弱性を突いて､それを悪用する形で攻撃をしてくるので、いつ、どこから来るか分からないということで、事前に予測することは非常に難しい。そういう意味で、サイバーセキュリティ対策という観点で今回の対応を取るというのは重要なことではないかと思う。その面で、港湾、医療について、制度を適用するのは適切ではないかと思う。サイバーセキュリティはチームスポーツであるということをよく言われる。１つの組織ではできないということだと思う。今回、こういうことをやりなさいということで事業者の皆さんにお願いをすることによって、事業者だけに責任を押しつけるということになってしまうと全く本末転倒だと思うので、民間、役所の皆さん、それから大学も合わせて、力を合わせて対処しなければいけないだろうと考える。そういう意味では、これは今日の議題とはずれるが、今、政府で検討してくださっているアクティブ・サイバー・ディフェンスの法案が見送りになってしまったというのは非常に残念である。こちらも、これも併せてしっかり進めていただきたいと思う。

○　東京2020オリンピックの際、何かあったときには対応せよということで、いくつかの病院が指定を受けていた。幸か不幸か新型コロナウイルス感染症の影響で無観客開催となってしまったためそういう面では大事故が起こるということはなかったが、そういった緊張感のある病院に対するサイバー攻撃は非常に心配である。

○　私は所属先で情報セキュリティに責任ある立場に就いているので、サイバー攻撃がいつ来てもおかしくないという覚悟ではやっているわけだが、例えば電子カルテというのはベンダーが非常に少なく、導入するには高額のお金を払わなくてはいけない。使っているユーザーもそれほど多くないので、脆弱性がどこにあるのか、よく分からない。そういう面では、攻撃されたときの被害は甚大だろうと思う。経済安全保障推進法の枠組みの中で対処するかどうかは分からないが、ほかの委員が指

摘するように、何らかの形で病院というのは守っていかなくてはいけない対象だと思う。

○　規制がかけられることに対して、「困るな」という考えは病院側の本音ではあると思う。病院は、日々多くの患者さんが来るため非常に多忙である。サイバーセキュリティ対策のため新たな措置を取らなければならず、マンパワーを割かなければいけないということになれば、それは非常に困るというのも本音としてはある。そういう意味で、厚生労働省とよく相談をしながら、病院をいかに守っていくかということを考えていきたい。

○　基幹インフラについて、検討会に参加し、基本的に港湾の中の一般港湾運送事業の追加というのには賛成するが、もう少し粒度が上がるといいと産業界としては思う。例えばターミナルオペレーションシステムが機能しないと大変な混乱になってしまうがターミナルオペレーションシステムにリンクしているシステムについてはどこまで投資をすればいいのか、もしくは置き換えればいいのかというのは、産業界としては迷うところ。その辺はぜひ相談に乗っていただきたいと思う。

○　今回のような基幹インフラの対象事業の追加があまり頻繁にあると、ビジネスの予見性が下がる。特に、急な追加はサプライヤーの変更や新たなシステムの導入等、かなりの負担になる。対象範囲が明瞭であり、しかもあらかじめ相談が出来るということであれば、対象事業の追加は国益のためにも行った方がよいと考える。

○　特許出願の非公開については、外国の法律という管轄外の部分も考慮して検討いただいたということで、難しい問題によく対応していただいていると思う。

○　適正管理措置に関して、大企業では特許システムはほぼクラウドシステムを使っている。その中で、非公開特許についての扱いだけは特別扱いをする方向で、産業界全体の合意を取ろうとしているが、人的な管理措置とか物理的な管理措置の定義が古い用語を使われているので、かなり迷う面も多いと思う。この点は内容が理解可能な人とそうでない人というように、人的管理措置の対象を明確に伝えていきたいと考えているし、事務局の方にもその辺の協力をお願いしたいと思う。

○　損失補償の範囲の定義については、損失補償の規模が小さいと思われて、さらに提出書類があまりにも多いということになると、特許出願をせずに営業秘密としておく、もしくは、他の方法を模索するというような、本来の立法趣旨と違う方向に行きかねない。是非、この点は慎重に検討していただきたいと思うし、我々のほう

でも協力したいと考える。

○　事務局の説明については支持する。

○　周知についてはいろいろなレベルでいろいろな形で尽力いただき、大変感謝している。改めて、説明の際には、個々の制度だけではなくて、こういう経済安保制度全般の背景とか趣旨、制度、それから今の制度の整備の進捗状況、こういったところを踏まえて、個々の制度の趣旨を説明いただきたい。

○　基幹インフラ分野について言うと、先ほどの説明にあったとおり210の事業者が指定されたということで、具体的なところが見えてきていると思う。特に、中小を含めてある程度見えている方々に対してはさらに具体的な説明とか、もし工夫できる部分があれば、ぜひよろしくお願いしたい。また、これまで申し上げてきたとおり、個々の企業のポテンシャルに合わせた実効的な対応をしていただきたい。

○　経済安全保障推進法とセキュリティ・クリアランスとは違う制度なので内容は変わってくると思うが、一定程度事業者側に負担がかかってくるので、結果的に同じような規制も出てくると思うので、重なる部分については、うまく調整して効率的に簡素化していただきたい。

○　基幹インフラと特許出願非公開制度についての報告、それぞれ準備を着実に進めてくださっていることについて、事務局の皆様の尽力と対応にまず感謝を申し上げたい。

○　特許出願の非公開制度については、ガイドラインと損失補償のQ&A案を整理していただき、手続面や実務面の課題と対応を明らかにしていただいて、経済界・産業界の疑問にも応えていただいていると思う。今後の運用開始に向けて具体的な詳細が定まっていくにつれて、経済界・産業界の個別具体的な疑問もまた生じてくることとなるので、この点について、先ほども事務局の説明で、地方も含め、関係機関も含め、周知の機会を続けていただいているということであり、引き続き制度に関する周知の徹底をよろしくお願いしたい。

○　基幹インフラについては、２つのお願いを申し上げたい。

一つは、医療機関と医療情報システムについて、先ほどもご出席の委員の方から発言があったとおり、医療機関におけるサイバーセキュリティ対策の観点からのデータ保護は重要な課題と考える。私に誤解と認識不足があるかもしれないが、検討

の対象が「医療情報システム」ということで立論されていたのが、いつの間にかと言っては大変失礼であるが、「医療DXに関するシステム」というふうに置き換わって、今後のシステム開発の内容によって、ということでの将来の課題とされていると理解している。しかし、地域における医療の体制整備についての重要性、特に災害対応や医療データ保護という観点から、対象事業としての検討について再考していただく必要があるのではないのかと思う。

○　もう一つは、基幹インフラの対象事業を営む経済界・産業界の中には地方に事業活動の拠点を置いている各社もあり、新たな制度に関する届出など、実務上・手続上の疑問や照会など伺いたいことが生じる場合､主務官庁で対応いただくとしても、その主務官庁の窓口へのアクセスやコミュニケーションのしやすさということを考えていくと、速やかにお答えをいただくことができるのかどうかといった不安がある。例えば、主務官庁の地方機関での体制の整備も含め、対応を円滑にしていただけるようにぜひご配慮をお願いしたい。

○　特許出願の非公開、セキュリティ・クリアランスについては、特にこの場で申し上げることはない。

○　基幹インフラについて、資料１「基幹インフラに関する検討会合　議事のポイント」の「その他」で、私の発言を「インシデントが発生したことを受けて事後的に特定社会基盤事業を追加するようなボトムアップのアプローチだけではなく、トップダウンのアプローチが求められているのではないか｣とまとめていただいている。この発言を受けて、資料４の３ページ目には「サイバーセキュリティ事案が発生した事業を事後的に特定社会基盤事業に追加するのではなく、重要なインフラ事業については、あらかじめトップダウンで予防的に特定社会基盤事業として指定しておくことが必要ではないか」と掲載されている。事後的に対応するのではなく、あらかじめここは危ないということが分かっていれば、予防的に特定社会基盤事業者を指定しておくこともあり得るとは思っている。

○　一方、私の発言の本意は、資料２「議事要旨」の４枚目の最初の○（マル）にある｢トップダウンでリスクの高い製品を示すような仕組みを併せて構築しなければ、いたちごっこになりかねない。今のままでは事業者のみの負担が重くなり、効果が上がらないのではないかと懸念する」という点にある。

○　先ほどチームスポーツであるとか、もう少し粒度を細かくというご指摘がほかの委員からあった。将来DX化がさらに進んで、いろいろなものがネットワークで結ば

れた場合に、特定社会基盤事業者になっていないところを経由して、特定社会基盤事業者が思わぬ形でいろいろなアタックを受けることも十分考え得る。その場合に指定にこだわっていては、対応が不十分になりかねないと危惧している。むしろチームスポーツとして、行政の側からリスクの高い製品を示すような仕組みも考えた方が良いのではないかという趣旨で申し上げた。資料等を変えていただく必要はないが、意見として申し上げておきたい。

○　特許出願非公開制度について、大変よく論点は整理されており、また、残された課題についても今後丁寧に検討されると伺っており、全く異論はない。

○　基幹インフラについて、新しく一般港湾運送事業を基幹インフラとして指定することについては賛成する。

○　医療分野、医療機関について、ほかの委員からも様々なご意見があった。今回は経済安全保障法制の定義からしたときに、病院や医療機関がそのまま該当するわけではないということかもしれない、つまり、整合性がないというご判断の中でこういう結論が出されたということについては了解した。

○　ただ、先ほど何人かの委員の方が意見されたことだが、医療法上の措置からすると、医療安全とか医療の質をいかにして守るかということが非常に重要な課題になってくるし、それに対して、病院、医療機関に対していろいろな形でチェックが入っているということもある。したがって、現状を少し考慮してということも判断上あったのかと感じた。

○　先ほど広域地域においてある意味での司令塔の役割をする医療機関があるのではないかというお話があった。緊急時における広域地域連携、あるいは広域の医療機関連携の中において、司令塔を果たす医療機関として例えば災害拠点病院であるとか基幹災害医療センターといったような制度が用意されている。これは各都道府県の医療計画の中で指定されている。そして、そこにおける施設要件としては、耐震設備であるとか備蓄であるとかという話があるので、当然そこにはサイバーセキュリティが入ってもいいと感じる。今回は経済安全保障法制上の措置として対応されなくても、いろいろな災害とか震災が起こっている現状の中で、こういう制度を強化していく。特別の役割を果たす病院に対してはきちんとした基盤整備を国と厚労省、そして都道府県とが協力して進めていくということをお願いしたい。

○　医療DXとの関係であるが、先ほどもほかの委員から意見があったように、単に医

療DXとの関係というよりも、例えば、これもご指摘があったとおり、医療ビッグデータあるいはリアルワールドデータを使って、これから新しい創薬あるいは新しい医療機器を開発していくということもあり、大変重要である。既にこれについての試みは進められているが、まだ完成していないと感じる。これは、経済安全保障法制にも関係することである。そして、特定の施設を指定するというよりも、情報ネットワークとして構築されたものをどのようにその基盤を強化していくかという形の中で、ぜひ政策を推進していただければと思う。国、厚労省、製薬企業、その他との間でいろいろ協力しながら、ぜひ進めていただきたい。これには重要な基幹病院とか大学病院が参加していくといった仕組みが期待されているようなので、それとの関係でもこれから検討いただければと思う。

○　基幹インフラと特許の両方について、提案に賛成する。

○　地域医療の中核となる病院を制度の対象としない理由としては、地域の医療機関が連携することによって、医療提供体制が確保されているという代替可能性の点が挙げられていた。首都圏であれば、確かにこの連携は可能であるかもしれないが、地方においても同様と言い切れるのかどうかということについては、疑問もあるのではないかと思う。代替可能性については、引き続き地域の実情や地域間の格差を見極めた上で検討を進めていく必要があるのではないかと考える。

○　基幹インフラと特許の非公開制度、双方について事務局の準備状況を支持し、提案にも賛成する。

○　一般港湾運送事業を基幹インフラの対象事業に追加することを支持するし、名古屋のコンテナターミナルのシステム障害が発生してから、一連の行動、措置がかなり迅速、適切であったということを評価したい。

○　経済安全保障推進法や基本指針との整合性という観点から、一般港湾運送事業を対象にし、それ以外に対して今は対象にしないということも理解するし、港湾の問題だけではなく、その事業ごとの事業法関係の法令、サイバーセキュリティ関係の法令、そして経済安全保障法制の全体的・総合的な法制度によってサイバーセキュリティを強化していくという方向性についても支持し、理解する。

○　目的は、サイバー攻撃に対して堅牢かつ回復力のある体制を構築するということなので、その方針でよいと思うが、経済安全保障推進法を使ってもっとできることがあるのではないかというご意見については、何人かの委員からもご指摘いただい

ているところであり、医療関連のサイバー攻撃は世界でも重要な問題として指摘され、様々な事案が報告されている。もう少し現状がどのようになっているのかということの検討と、各法律間の整合や相互の運用によって効果を出す方法というところを所管庁間で検討することが必要ではないかと考える。

○　ほかの委員より、能動的・サイバー・ディフェンス（ACD）の法制の見送りについてのご発言があったが、新しい国家安全保障戦略の中で、日本が能動的・サイバー・ディフェンスを行うということは既に規定されているので、ますますサイバーセキュリティ方面は大事になっていくため、迅速な対応が求められていると思う。

○　特許出願の非公開制度における損失補償の金額の審査については、非公開にされた特許の価値を正当に判断できる第三者による検証が本制度への理解と定着に重要と思う。特許出願者が納得できる複数の専門家による検証と、その根拠の開示がされるよう、仕組みの構築が必要と考える。

○　本日の３つのテーマについて、主体が産業界ということからいくと、上手に（産業界に政府から）広報しておかないと、ほとんどの経営者が自分のところは関係ないと思ってパスしてしまう。そこは何とか我々としても避けたいと思っているので、こういうものが出てきたときに、経済同友会として意見書を提出すると同時に会員への周知及び注意喚起を行う。また、政府の事務局の方に当会に来ていただき、広報の機会を設けたいなと思う。

事務局より回答（基幹インフラについて）

○　医療も、特定社会基盤事業に追加すべきというご指摘については、経済安全保障推進法を担当する立場から言うと、ご指摘いただいた点は重要だと思っている。一般論としては、経済安全保障推進法そのもの、あるいは基幹インフラの制度そのものは、いわゆる重要設備の調達規制という形を取っているわけであるが、他方で、事業法では安定提供の観点からのサイバーセキュリティ対策、それから、サイバーセキュリティ基本法では行動計画の中でより具体的にどういった対策を取っていくのかということになる。その上で、医療の分野では委員からご指摘のあったような、医療法あるいは薬機法などのサイバー対策と並行して、推進法として基幹インフラ規制をどのように考えていくのかというのがまず整理すべきことだと思う。その上で、今のままの推進法で十分なのかということにつき、その運用面も含めて、例えば、リスクが高いながらも対象事業に指定されていない事業者の取組を推進するために、何らかの対応ができないのかというようなご指摘もいただいている。トップダウンのアプローチが必要だという考えもある一方、委員からの不断の見直しは重

要なのだけれども、頻度が高いことよりも、事業者が対応できるような十分な情報の発信など、準備作業を官民あるいは大学等も含めてどう連携して進めていくのかとの指摘もあった。そういう意味で、基幹インフラの取組、サイバー攻撃をはじめとする外部からの妨害行為の内容もどんどん進化しているということだと思うし、民間におけるそれに対する対応もどんどん進化していく性格のものであると思うので、とりわけ国民の生活あるいは事業活動、そして国の運営そのものを支えるインフラについて、非常に言い古された言葉であるが、緻密な不断の見直しを適切なタイミング、予防的な対応も含めてしっかり進めていくことが重要であると思う。また、それを支える人材という観点からの取組も重要だと考える。あるいは、先端的な技術への取組も重要だというお話が各位委員からもあったので、そういった指摘を踏まえながら、引き続き基幹インフラに対する取組を先ほど指摘のあったACDの取組も含めて、全体像を持って関係部局と連携しながら進めていく。

厚生労働省より回答（基幹インフラについて）

○　先ほど委員の皆様から、医療について、基幹インフラ制度の対象としない方向で検討という点についてご意見をいただいた。この対象事業の追加に当たっては、代替が困難であるかどうかが対象分野に加えるかどうかの考え方の一つとして掲げられているところ、特定機能病院や地域医療支援病院については、高度な医療を提供するといった重要な機能を担ってはいるが、これらの病院に何かあったときに、他の病院などでカバー、代替できないものとして承認しているわけではない。

○　災害等の有事ということも想定されるが、委員の先生方からもご意見があったように、医療計画に基づいて、有事においても地域において医療に著しい影響が生じないように連携体制を担保するように努めている。

○　規制として今回対象事業に追加するかどうかという点でいうと、現時点では対象にする必要はないと考えている。いずれにせよ、サイバーセキュリティ対策は重要であるので、その取組は進めていく必要はある。

○　加えて、医療のサイバーセキュリティ対策として予算などの面でも充実を図っている。令和５年度補正あるいは令和６年度の当初予算などでも、これまでの取組をさらに加速するような予算内容を盛り込んでおり、その充実をさらに図っていきたいと考える。

委員から追加の発言

○　別の機会でもお聞きした話をもう一回お聞かせいただき、誠に感謝する。一言だ

け申し上げたい。それは、今回、基幹インフラは経済安全保障推進法ということで、安全保障の名がついた法律である。釈迦に説法みたいな話であるが、現代戦においては基本的にサイバー攻撃から戦争が始まると言っていいと思うが、他国にとって我が国がこういった基幹インフラについては厳重な守りを固めているのだというメッセージが一方で安全保障上はあると考える。ガザ地区における紛争においても、病院における攻防といったものがあれだけ注目されるというのは、病院、特に総合病院の安全保障上の重要性ということなのだろうと思う。したがって、他国が我が国を見た場合、どのように考えるかということであるが、有事の場合において、我が国は病院施設について重視していないというメッセージを伝えているということにほかならない。繰り言を言うつもりはないが、過去の機会でも、病院施設は基幹インフラに入れるべきであるということを私は主張しながらも、今日に至っている。私が申し上げているのは、ただ単に医療法上の枠組みの中だけの問題ではなくて、我が国が、基幹インフラについて何を守っていくのかという気概を他国に対してどのように示すかということである。

○　内閣府のCSTIにおいて研究開発ということを中心に議論をずっと進めて、同時にそこに関わるイノベーション政策が我々にとっての政策の核になると思うが、そのような考察と今回のセキュリティ・クリアランスの法制度のところでは、まだまだ隔靴掻痒の感があると考える。我々がやらなければいけないと考えていることは、今後の５年間における国益に資する技術、研究開発の問題であるが、安全保障の概念が経済や技術の分野に大きく拡大しているという認識でこのセキュリティ・クリアランスの議論が進んできている一方で、技術開発、研究開発に関する視点がどこまでここの中で議論されているのだろうかという問題意識を持っている。

○　国益に資する研究開発、クリティカル・テクノロジーということを、どの分野が我が国の利益につながるがということを今後恐らくCSTIは第７期の科学技術基本計画の中で示していかなければいけない。そのときに、研究開発に関わるセキュリティ・クリアランスのガイドラインがどのような形で明確化されていくのだろうかということに強い関心を持っている。具体的に研究開発の分野でも、例えば欧米、アメリカ、イギリスを中心とするところで共同の研究開発をしていくときに、例えばアメリカで言えば、具体的にはカーネギーメロンやジョージアテックのようなところとも議論したときに、同じような問題が研究開発についても起こってきているということである。今後、我が国が研究開発において全ての分野において国際的なコンペティティブネスを維持していけるかどうかということは正直分からない。そうすると、自分たちの弱点を補うような形での国際共同研究開発がとても重要になってくる。そのことを進めていくときに、当然、そこに関わる研究者のセキュリティ・

クリアランスの問題が出てくることは間違いないと考えている。それをどのような形で明確化していくのかは、恐らくCSTIはNSSの皆さんと議論したいと考えていると思うし、同時に考えないといけないのは、このようなセキュリティ・クリアランスの中に入っていくことをよしとするような研究コミュニティーを拡大していく。その拡大をするためのインセンティブ構造をどうつくっていくのかということだと思う。研究者にとってのインセンティブというのは当然、研究のファンディングや、研究環境等である。そことほぼ一体化してセキュリティ・クリアランスのガイドラインあるいはルールづくりを進めていかなければ、幅広い研究者のコミュニティーをこのフレームワーク内に呼び込むことはなかなか難しいと思う。アメリカでは、例えばGAFAのようなところが明確にやっている。これはさらに言えばARPA-E（米国エネルギー高等研究計画局）のような形で極めて使い勝手のいい研究費を提供するとともに、ある部分的にはクラシファイドの研究開発を行っていく。その中においてのルール作りを明確にやってきているということだと思う。今回のセキュリティ・クリアランスに関する制度、法制には、もちろん事務局の方は完全にそのことはよく分かった上で進められると思うが、恐らくは次の段階として私たちが考えなければいけないと思っている研究開発におけるセキュリティ・クリアランスの問題ということをどこかで議論させていただきたい。そうでなければ、幅広い意味での人材育成も含めたセキュリティ・クリアランスの問題を研究開発と結びつけて行っていくことは難しいのではないかと思う。

○　私は、このセキュリティ・クリアランスの制度、ようやくできたかということで、本当にうれしく思っている。私の記憶が間違っていなければ、過去に別の機会で、サイバーセキュリティにセキュリティ・クリアランスは必要だと主張した。それがずっとできないな、できないなと思っていたので、これができるということは本当にうれしく思う。

○　セキュリティ・クリアランスは、今のところ経済安全保障分野に限ると伺っているので、その点は少し残念である。これは多くの安全保障あるいは外交の分野にも広げていっていただきたいと思う。例えば、私たちがこういう有識者会議に入るときに、私たちのバックグラウンドもチェックしていただくということを本来はやらなければいけないと思う。そうしたら私は入れないかもしれないが。それも含めて政府の議論を高めていくためには必要だと思う。

○　これは事務局の皆さんに申し上げることではないのかもしれず、高市大臣にだけ聞いていただければいいのかもしれないが、立法府の対応が欠けているような気がする。つまり、国会の中に行政がやっている秘密制度をしっかり監査するための委

員会をつくらなければならず、例えば、情報委員会というのがアメリカやイギリスにはちゃんとあるので、そこで秘密会をきちんとやって、行政が行き過ぎたことをやっていないかということを監査する制度とセットになって、このセキュリティ・クリアランスというのは本来動かすべきだと思うので、ぜひそこを今後検討していただければと思う。もしかしたら、すでに別の場でそういった議論があるのかもしれないが、一言申し上げさせていただく。

高市大臣より回答（セキュリティ・クリアランスについて）

○　情報監視審査会、これは衆参、国会でしっかり特秘法について行っている。私も委員の経験があるが、完全に密閉した空間で、議事録も残らない、公開されない形でヒアリングを行っている。

事務局より回答（セキュリティ・クリアランスについて）

○　１点、委員からご指摘のあった点、研究開発なり技術というものが、この経済安全保障分野がセキュリティ・クリアランスの制度のスコープに入っているかいないかといえば、当然入っているというのが１つ目の答えである。他方で、何度も強調させていただいたとおり、政府が保有する情報であるので、民間企業、あるいは大学、研究機関が自発的に始められた研究開発について、先ほど最後に説明したとおり、民間の保有情報は対象とならないので、クリアランスという言葉は誤解を招くので使わないほうがいいと考えている。時にデューデリジェンスとか、人的なチェックということで申し上げる部分なわけだが、そのルールとして政府の中でできているのは、研究セキュリティ、インテグリティーの文脈で、資金の流れに着目をして、きちんと議論を整理しようということ。今、委員がおっしゃったような観点からは、まだこれから研究開発ということになると、政府のファンディングなり政府から情報提供を受けて行う研究開発と、それ以外のものも含めた全体像の中でどのような制度設計をしていくのか、まだ追加の議論が必要な部分があるので、まさにご指摘のあった次の科学技術基本計画の議論の中で、経済安全保障上の管理の仕組みをどのように持ち込んで、同盟国なり関係国と円滑に共同研究ができるのか、あるいは日本としての研究開発の成果なりをどのようにしっかりと守っていくのかということについては、引き続きCSTI含めて関係府省と議論をさせていただきたい。

委員から追加の発言

○　セキュリティ･クリアランスの制度について､20年ぐらい前から必要だと言われ、今､大臣のお力で非常に進んでいるところなので､一日も早く日本がセキュリティ・クリアランス法を持ち、日本としての諸外国に対する責任を果たせるようになればと思う。

（６）古賀副大臣閉会挨拶

○　本日も活発なご議論をいただき、各委員の皆様方に対し、大変感謝している。

○　本日いただいたご意見を踏まえ、基幹インフラ制度については、一般港湾運送事業を基幹インフラの対象事業に追加する方向で検討していくということだと考える。

○　これまで委員の皆様方には有意義なご知見をいただき、改めて感謝を申し上げる。

○　今後とも、経済安全保障に対する法制を検討するに当たり、知見を賜りたい。引き続きのご協力をよろしくお願いしたい。