経済安全保障分野におけるセキュリティ・クリアランス制度等に関する
有識者会議（第７回）　議事要旨

１　日時

令和５年 10 月 11 日（水）16 時 00 分から 18 時 00 分までの間

２　場所

中央合同庁舎４号館　1214 特別会議室

３　出席者

（委員）

梅津　英明	森・濱田松本法律事務所 パートナー弁護士
北村　　滋	北村エコノミックセキュリティ 代表
久貝　　卓	日本商工会議所 常務理事
境田　正樹	TMI 総合法律事務所 パートナー弁護士
鈴木　一人	東京大学公共政策大学院 教授
冨田　珠代	日本労働組合総連合会総合政策推進局総合局長
永野　秀雄	法政大学人間環境学部 教授
原　　一郎	一般社団法人 日本経済団体連合会 常務理事
細川　昌彦	明星大学経営学部 教授
渡部　俊也	東京大学未来ビジョン研究センター 教授【座長】

（政府側）

高市　早苗	経済安全保障担当大臣
平沼正二郎	内閣府大臣政務官
秋葉　剛男	国家安全保障局長
田和　　宏	内閣府事務次官
井上　裕之	内閣府審議官
鈴木　敦夫	内閣官房副長官補
飯田　陽一	内閣官房経済安全保障法制準備室長
彦谷　直克	内閣官房内閣審議官
高村　泰夫	内閣官房内閣審議官
品川　高浩	内閣官房内閣審議官
佐々木啓介	内閣官房内閣審議官
遠藤　顕史	内閣官房内閣審議官
田甫　秀臣	防衛省防衛政策局調査課情報保全企画室長
熊野　有文	防衛装備庁装備政策部装備保全管理課長
西川　和見	経済産業省大臣官房経済安全保障室参事官

４　議事概要

（１）高市経済安全保障担当大臣挨拶

○　この有識者会議では今年２月の設置以来、６月の中間論点整理まで計６回にわたり、精力的に御議論をいただき、目指すべき制度の方向性をまとめていただいた。今後はいよいよ制度の具体的な方向性を御議論いただきたいと考えている。

○　再開に際し、今後の検討に当たっての重要なポイントは、「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」を、国が保有する経済安全保障上重要な情報を保全する制度としてきちんと位置付けるとともに、それを主要国との関係でも通用する実効あるものとしていくこと、そして、それがビジネスチャンスの拡大につながり、産業界のニーズにも合致したものとしていくことであるとの思いを改めて強くしている。

○　本日の第７回は、経済安全保障上重要な情報の具体的な中身等について御議論いただく。政府としては、皆さまからいただく提言を踏まえて、次期通常国会における法案の提出に向けた準備を進めてまいりたいと考えており、これまで同様に活発な議論を賜れれば幸い。よろしくお願い申し上げる。

（２）事務局説明

事務局から、資料の内容について説明があった。

（３）意見交換

○　資料１ページの「政府からCI（Classified Information）の共有を受ける意思を示した民間事業者等について」とある点につき、意見が三つある。第一に、サイバー関連情報を利用する基幹インフラ事業者に対しては、当該事業者の意思表示によるのではなく、セキュリティ・クリアランスの対象となるよう義務として規制すべきではないか。第二に、おそらく、「政府からCIの共有を受ける意思を示した民間事業者等」という表現から、これまでこの有識者会議にも説明に来られた民間企業の方々のような事業者を想定される方が多いと思われるが、それ以外に、企業の会計監査を行う監査法人や、サイバーセキュリティ監査を行う法人、CIに触れることになる法律事務所、特許事務所、環境監査を行う法人なども含まれると思われるので、一度議題としていただければありがたい。第三に、アメリカでは、国防総省、エネルギー省等の政府資金や補助金を受領した研究者にもCIの規制がかかる制度があることから、この点についても議題として検討していただければありがたい。

○　資料１ページの「CI以外の重要な情報の取扱い」の中で、「必要に応じ、信頼性の確認のための調査も含め、CIほど厳格ではないが、一定の保全措置を講ずる必要性を検討」とあるが、これに関連して、アメリカが導入しようとしているサイバーセ

キュリティ成熟度モデル（CMMC）2.0は、現在の予定では、2025年1月から全面導入が予定されており、我が国に対しても適用があると思う。これに対応するためには、対象者の犯罪歴、財務情報等の簡易な人的スクリーニングを実施できなければならず、また、CMMCを監査する日本の法人の方はCIと同様のセキュリティ・クリアランスを取得することが必要となるので、この内容を日米行政協定で事前に確定するためにも、是非この会議でも議論していただければありがたい。

○　資料２ページの「防衛産業保全マニュアル」に関連して、以前この会議で防衛装備庁の方から防衛産業保全政策に関する説明を受けたときに、法人クリアランスにおいて取締役会議長とCEO（Chief Executive Officer）に相当する方に対する個人のセキュリティ・クリアランスが入っていなかった。この点について、制度を統一的に見る観点からも、議論していただければありがたい。

○　資料３ページに「政府が外部から受領した情報については、秘密指定の効果は原保有者に及ばない」とあるが、これは原則として正しいと思っている。ただし、アメリカの機密指定制度を定めた大統領令13526号の1.3条には例外的事例の規定があって、政府による指定だけでは機密指定すべき情報を網羅することができないことから、行政機関の被用者や請負者、ライセンス資格保持者、政府資金受領者で機密指定権を持たない者が、機密指定を必要とする情報を自ら創出し、その情報が本大統領令等において秘密保全対象情報であると判断した場合には、当該情報の管轄権及び機密指定権を持っている行政機関に速やかにその旨を通知する義務を課し、この通知を受けた行政機関は30日以内に当該情報を機密指定するか否かについて決定を行うと規定している。このような制度の必要性についても議論していただければありがたい。

○　資料２ページに「特定秘密保護法等との関係に留意し」とあり、続けて「経済・技術分野の主要な活動主体があくまで民間事業者であることに留意」とされている。今回のセキュリティ・クリアランスの制度は、民間企業による経済政策を目的の一つとしているので、国防を目的とする特定秘密保護法には馴染まないのではないかという考えを示しておきたい。

○　資料３ページに「政府が外部から受領した情報については、秘密指定の効果は原保有者に及ばない」とあるので、民間事業者が保有する情報に広げないということを制度設計の際に改めて明記していただきたい。

○　公共の安全に関する情報は、情報公開法の不開示情報として公開請求の除外の対象

となっているので、本制度の対象とする情報については、国民の知る権利や事後的な検証についても検討が必要ではないかと考える。

○　産業保全の観点について、民間事業者がセキュリティ・クリアランスの指定を受けるには、施設クリアランスの確保、秘密保持管理の強化、プライバシーに関わる信頼性確保のための調査など、労働者にも大きな影響が及ぶので、セキュリティ・クリアランスを受けることに対する事前の労使協議と、セキュリティ・クリアランスの運用や対象業務などの労使協定締結を法で義務付けておく必要があると考える。この点は、基本的な骨格にも追加いただきたい。

○　外国に通用する制度を前提とするならば、FOCI（Foreign Ownership, Control, or Influence）の適用等についても検討すべきではないかと考える。

○　信頼性調査への同意拒否や調査結果を理由とする不合理な配置転換など、労働者への不利益取扱いの禁止については、罰則を含めあらかじめ法で規定をしておくべきと考える。

○　罰則を法令で規定するのであれば、既存の制度との整合性に留意が必要。新たな制度のみを過重な罰則とすべきではないし、新たな制度に合わせて既存の制度の規定を変更することにも、慎重であるべきではないかと考える。

○　経済安保上の重要な情報という点では、例えば、特定秘密保護法にも、別表２号ロで貨物の輸出入の禁止等が挙げられているが、外為法を所管している財務省や経産省において、特定秘密保護法に基づく指定は何件ぐらいあるのか伺いたい。特定秘密保護法の運用基準による指定対象と今回の法律による指定対象が、オーバーラップしそうなところがある。今申し上げた外為法のようなところがまず十分に指定されていかないと、本当に民間にまでウイングを広げられるのかということがある。経産省や財務省などが年間どのぐらい特定秘密を指定しているのか、また、どういった案件で指定がされているかということについて質問したい。

内閣官房より回答

○　事実関係として、特定秘密保護法の別表第２号ロに関する運用基準のａ(b)(c)については、これまでのところ、指定件数はゼロである。

○　お聞きしてびっくりしたのだが、実際問題として、こういった情報が特定秘密保護法で全く指定されていないというのは、逆に言うと、これまで全く指定していないにもかかわらず、新たに制度ができた場合には指定されるというのは、規制をされ

る側としては間尺に合わないということになるのではないか。経済官庁がそういったものについて本当に守らなければいけない情報として指定をしていかないと、とても民間まで意識が高まっていかないし、さらに言えば、制度自身にも魂が入らないのではないかという気がするが、政府としてはどのようなお考えなのか。

事務局より回答

○　非常にもっともな指摘であると思う。その上で、今まで指定の実績がないということについてどう捉えるのかというのはいろいろ考えなければならない。少なくとも、我々がこの有識者会議を始めた一番の大きな理由は、安全保障の中で、経済に関する情報の重要性が増しているということ。これは逆に捉えれば、日本政府が保有する経済安全保障関係の重要な情報がターゲットになる可能性が、10 年前の特定秘密保護法制定時に比べはるかに高くなっているというのが現状だと思っている。したがって、過去に指定されていなかったから今指定しなくていいのかといえば、そういう状況判断ではなく、その上で、特定秘密保護法においても、その対象分野の中で経済安全保障上重要な情報をしっかりと守っていくことが必要であると考え、この議論をさせていただいている。

○　昨年５月に経済安全保障推進法が制定され、経済分野が安全保障と密接に関連するということが明らかになっている。さらに今回、経済安全保障分野で新しいセキュリティ・クリアランス制度を作っていくということになれば、その中核を担う担当官庁において、実際にどれが特定秘密であるのかを考えていくべきだと思う。また今後、そういった分野についても指定をしていくに当たり、今、積極的な取組みをしていただかないと、新しい制度を作ったらなぜか指定が増える、ということにもならざるを得ないと思っている。

○　先ほど他の委員から、特定秘密保護法は国防を目的としているというお話があったが、そんなことはない。外交、防衛、防諜、対テロという分野の中で、運用基準を読めば、実際かなり経済的な分野についても規定がある。この中で、経済官庁において全く指定がされていないということは、由々しき問題だと思うし、今後新しい仕組みを作っていくという過程においても、やはりこの点は、特定秘密保護法の運用として改善すべきではないか。新しい仕組みを作った時に、特定秘密保護法の射程についてどうやって整理をするかという点において、指定がゼロでは整理のしようもないということになると思っており、この点についても同様の考えなのか、お聞きしたい。

内閣官房より回答

○　特定秘密保護法上は、防衛・外交・対特定有害活動・対テロという部分について、別表該当性、非公知性、特段の秘匿の必要性という３要件を満たすのかどうかの判

断を各行政機関の長が行うことになっている。運用基準においてその統一的な運用を規範レベルで定め、特定秘密に該当する情報が出た場合には漏れなく指定をするようにというふうになっているので、経済官庁など関係省庁においては、そういったものに該当する情報が出た場合には、きちんと特定秘密に指定することになっている。委員御指摘の細目について指定件数がゼロというのは、結果的に、それぞれの情報を持っている各省庁がそういうものと判断した結果だと考えている。

○　運用基準に該当すれば指定されるはずであるということだが、当該基準についても、各行政機関の長がそれなりの裁量性というものを持っている。指定がないのは由々しき問題。要するに、この分野に関わる部分を新たに法律で規定していこうというときに、現時点で行政機関の長が１件も指定していないと、じゃあなぜやるのだ、ということになる。やはり運用という意味で、今後経済官庁の各大臣が主体となっていく部分が多くなってくるわけだから、この問題について、どういった形で指定をしていくのか、どういったものが指定対象なのかということについて、十分な認識とビジョンを持ってもらわなければ、新しい法律を作っても運用上うまく回っていかないのではないかという懸念があり、申し上げている次第。

○　今の意見と全く同感。例えば、資料３ページに、新しい制度の基本的骨格だけ書かれているが、基本方針というものが必要だと思う。そのポイントは、なぜ特定秘密保護法が極めて抑制的に運用されたかということ。それは、必要最小限の情報を必要最低限の機関に限って特定秘密でやるということを特定秘密保護法の運用基準、閣議決定で縛っているから。こういう抑制的な方針の下で運用されている特定秘密保護法とは一線を画するべきではないかと思う。それが、中間論点整理の中にもあるように、「情報の機微度に応じて、柔軟かつ機動的に」ということであり、ここがキーワードだと思う。指定も柔軟かつ機動的にやっていくということで、抑制的とは一線を画した方針でやっていくということ。それは、３ページの基本的骨格にあるような、秘密の指定・解除、信頼性の確認、罰則という３つの項目とも関わる話である。柔軟性というのは、機微度に応じてやっていくということであり、Top Secret、Secret、Confidential の区分に応じて各項目の基準を変えていかなければいけないと思う。

○　柔軟かつ弾力的にやっていくという方針は、おそらく特定秘密保護法の単純な延長では出てこないと思う。そこと一線を画した上で、これは別な法律によるのかどうかわからないが、単純に特定秘密保護法の延長という頭ではなくて、切り換えてやっていくためにも、基本的な骨格だけではなく、中間論点整理で示した基本的な方針を書いていくということが大事な要素だと思う。そうすることによって初めて、

これまでの特定秘密保護法の運用とは違った形で提示するという姿勢が示されるのではないかと思う。

○　今の御発言について反対をするわけではないが、サンクション、つまり罰則がどのぐらいのものになるのかということは、非常に重要なポイントだろう。仮に、特定秘密保護法と同じ程度のものだとなれば、なぜその指定の運用が、片や柔軟で片や謙抑的でと違ってくるのか。これはある意味、構成要件を決定する重要な要素になってくる。今回のものについても、柔軟性という問題はあるのかもしれないが、やはり政府内の情報において、運用面での斉一性が図られるべきではないかというのが私の問題意識。

○　誤解があってはいけないので補足をするが、Top Secret、Secret については今の御発言と同じような感覚でいるが、Confidential まで同じような罰則であるべきかどうかは議論の余地があると思うので、そこは区分に応じて仕組みを考えていく余地も残しておいた方がいい、ということで申し上げた次第。

○　それは、新制度で守るべき情報は柔軟にすべきということで対象が増えるとした場合、特定秘密保護法と新制度の罰則が同じという状態が矛盾するのかどうかを、３階層にすることで解決できるかもしれないという感覚でよいか。

○　それは異論ない。

○　資料１ページの中間論点整理の概要を改めて見ると、非常に重要なことが書いてある。今後、論点をだんだん深掘りしていくと、ここに書かれている全体像や基本的な考え方を忘れがちになってしまうおそれがある。何か迷ったらこの中間論点整理に立ち返って考えることが重要である。

○　先ほど他の委員から、中間論点整理の「政府から CI の共有を受ける意思を示した民間事業者等」という記述に関して、基幹インフラ事業者の場合は別途義務化の手当てが必要ではないかという御意見があったが、私は、少なくとも中間論点整理の段階で、基幹インフラ事業者を別扱いで、例えば業法で何らかの手当てをするということは想定していなかった。したがって、もしそういう議論が今後行われるとすれば、改めて意見を申し上げたいが、基本的には慎重であるべきだと考えている。まさに「政府から CI の共有を受ける意思を示した民間事業者等」に限られるべきであり、この表現は非常に重要だと考えている。

○　資料３ページの「秘密指定の効果は原保有者には及ばない」という記述も非常に重要であり、中間論点整理にはなかった点である。もっとも、２ページの「特定秘密保護法等との関係に留意し」をどう読むかだが、特定秘密保護法では、改めて確認した限り、「秘密指定の効果が原保有者に及ばない」という明示的な規定はない。おそらく、そのような規定がないが故に、秘密指定の効果は原保有者に及んでいないのだろうと理解するが、そういう理解でよいか、確認させていただきたい。アメリカでは例外事項があるという指摘が他の委員からあったので、改めて確認させていただきたい。

○　資料３ページの「秘密指定の効果は原保有者に及ばない」について、民間の事業者と話をしていると、この点があまり理解されておらず、自分たちが保有する情報が急に指定されて自由に使えなくなるのではないか、といった不安をお伺いすることが相当程度あり、誤解に基づくところも相当あると思っている。他方で、重要な情報の候補ということで、民間の情報が上がっていって政府がそれを保有することになって、何らかの付加価値がついたような場合には、これは該当し得るというような形になっていくと理解している。

○　「原保有者には及ばない」という記載により、元々情報を持っていた方には及ばないということが明確になっているとは思う。政府に一回上がって、再び政府から民間に降りてきた場合には、その情報は新しいセキュリティ・クリアランス制度の対象になり得るが、当該情報の原保有者には情報指定の効果が及ばないので、原保有者から直接誰か第三者に渡すときには法律上の制約は及ばないという形になるだろう。ただ、この際、どういう場合に機密指定の効果が及び、どういう場合に及ばないのかということについて、混乱が起きる可能性があるのではないかと思っており、ある種の萎縮効果が起きてしまうこともあると思う。私もこの「原保有者には及ばない」という考え方に異論はないのだが、情報の指定内容に加えて、どういう形で民間に提供された場合には秘密指定の効果が及ぶのかといった、情報の提供のされ方も含めてきちんと説明をしていかないと、民間事業者の中に誤解が生じてしまうおそれがあるようにも思えるので、そのあたりを今後、議論の中で明確にしていただければと思う。

内閣官房より回答

○　特定秘密保護法が保護する対象は、基本的に行政機関が保有する情報であり、民間が保有する情報は原則として対象とならない。

事務局より回答

○　例えば、現行の特定秘密保護法では、漏えい罪の罰則の対象になる者は、「特定秘密の取扱いの業務に従事する者」とされている。公開されている特定秘密保護法の

逐条解説においては、この罰則の対象になる「特定秘密の取扱いの業務に従事する者」というのは、行政機関の職員を除けば、「第５条第４項に基づき特定秘密を保有し、又は第８条第１項に基づき特定秘密の提供を受けた適合事業者の従業者」となっている。そして、この第５条第４項、第８条第１項のいずれの条文においても、「契約に基づき保有」あるいは「契約に基づき提供」と規定されている。したがって、元の情報保有者はこの罰則の対象にはならないし、嫌がる事業者に政府が無理やり情報を押し付けて、「新たに情報提供しましたから、あなたは今日から制度対象です」ということもない。あくまで契約、ここでいう契約は秘密保持契約だが、秘密保持契約を締結して、相手が同意した場合に政府から提供する、あるいは保有していただく、という制度となっているので、そういう前提で提供を受けた方には規制が及ぶし、そうではない形で元々持っていた方には規制が及ばない、そういった整理になっている。

○　資料５ページの「重要な情報の候補」の中で、規制制度関連の審査等に係る情報が挙がっているが、これを本当にここでいう重要情報として扱うべきものなのかどうかという感じがしており、より具体的にどんな情報なのかを示していただくとありがたい。重要情報であることの基準の一つとして、外に敵がいるということがあると思う。それはプロの諜報員や工作員を動員して不正をしてでも取得したいという情報ということだと思うが、同じく５ページに「厳重な鍵」などと書いているとおり、要は、国家公務員法の守秘義務では足りないので、更に情報を指定してアクセスを止めるほどの重要な情報だという印象が、いただいた資料ではあまり感じられないことから、そういう点を申し上げておきたい。

○　資料５ページについて、事務局の方からざっと簡単にでも御説明いただけないか。

事務局より回答

○　５ページに挙げた情報の例は、事務局で、各省庁から提出をいただいたもの。各省庁には、幅広く、何らかの経済性を帯びるような情報であって、保全が必要と考えられるような情報について提出いただきたいとお願いをした。その上で、集まってきたものを事務局がある程度類型化して、サイバー関連情報、規制制度関連情報、調査分析研究開発関連情報、国際協力関連情報という４つに整理したもの。

○　他方で、ここに挙げられているものが全て我々が考える経済安全保障上重要な情報に当たるかどうかは、議論の余地があると思っており、一定のメルクマールが必要ではないかと考えている。中間論点整理においても、我が国として真に守るべき情報に限定することとされており、その限定のためのメルクマールが何らか必要であろうということで、５ページの下の枠内にある「国家及び国民の安全を支える我が国の経済的な基盤の保護に関する情報」というものを、もちろん漏えいすれば国家・

国民の安全に一定の支障を与えるおそれがあるものであることが前提であるが、我々が保全すべき経済安全保障上重要な情報の領域と考えてはいかがであろうかという御提案として記載させていただいたもの。

○　規制制度関連情報については、経済安全保障推進法のように経済安全保障自体を目的にしているような法律は当然入ってくるかと思うが、それ以外でも例えば、個別の業法は、法目的は必ずしも国の安全ではなく公の秩序などだが、それに基づく規制権限の中で出てきた情報の一部が安全保障に関わることも当然あると思う。そういうものをどう拾っていくかという丹念な作業が必要ではないか。

事務局より回答

○　御指摘のとおり。先ほど申し上げた考え方であれば、我が国の経済的な基盤の保護に関するものであるかどうかや、漏えいした場合に安全保障に影響があるかということを考えていくことになる。こういうものをあぶり出す姿勢という意味では、単純に法目的だけを見て判断していくという作業ではないのではないかという意見だけ申し上げておく。

○　若干議論が外れるかもしれないが、国が保有する情報については、厳格に守って罰則等で縛っていくのだと思うが、「経済的な基盤の保護」という、いわゆるindustrial securityに近い概念をこの法律の中で提起していくということであれば、国が保有するものだけではなく、民間に生起する我が国の経済的な基盤に関する情報であって、CUI（Controlled Unclassified Information）に近いような、漏えいすれば国家国民の安全に一定の支障を与えるおそれがある情報についても、規制の指針になるようなものを盛り込んでいくべきではないかと考える。すなわち、経済的な基盤の保護という、かなり広めの視点をこの法律で提起するのであれば、ただ単に国由来の情報だけではなく、民間が保有するデュアルユースの中でこれに該当するものについての民間に対する指針を与えるような規定といったものもぜひ盛り込んでいただくのが、多分民間企業にとっても親切ではないかというふうに思う。

○　今のお話はまさにおっしゃるとおりで、要は「我が国の経済的な基盤の保護」に関わるものが、政府が保有する情報とは限らないということだと思う。よって、国が保有していない情報であっても、一定の保護ないしは一定の管理をする必要があるだろう。ただし、その場合に問題になるのはおそらく、例えば身辺調査など、情報にアクセスする者に対する制限をどのようにかけていくかということと、それが果たして法に基づく強制的なものであるかどうかということだと思う。CUIに関するガイドラインを出すにしても、それをどうやって守っていくのか。政府が保有する

ものに関しては、このセキュリティ・クリアランス制度に基づいて、アクセスできる権限を与えることが可能だが、民間のCUIについては、守るべき情報であるということをガイドラインで示すことはある程度可能だとしても、ではそれをどうやって守るのか。つまり、セキュリティ・クリアランスの対象情報を特定するという側面と、それをどうやって守るのかという側面をどのようにして担保していくのかが重要な問題になってくるであろう。その際に、不正競争防止法等の既存の枠組みでやるのか、それとも全く違う考え方を出すのかという観点で、コメントさせていただいた。

○　先ほど、「CIの共有を受ける意志を示した民間事業者等」に関する説明の中で、アメリカの大統領令13526号に、民間企業等がこれは特定秘密のようなものに該当するのではないかといった場合に官庁にそれを申し出て、主務官庁は30日以内にそれを指定する仕組みがあると申し上げたが、例えば、経済安全保障推進法で創設された特許出願非公開の審査に関して頭の体操をしてみると、いい発明ができたということで、ひょっとしたら防衛関係に影響を与えるような重要な発明が、セキュリティ・クリアランスを全く得ていない民間事業者及び弁理士の先生方から出願されたという場合には、これまでの説明は通用するのだろうか。

事務局より回答

○　資料５ページの規制制度関連情報のところに挙げている審査情報とは、特許出願非公開制度でいえば、おそらく、特許出願の内容そのもののようなものより、出願されている発明が、例えば軍事転用できるとか、一定の危険性のある技術であるとか、そういう非公開にすべきかどうかの判断に関する情報であると思う。もちろん、この制度はまだ運用が始まっていないので、実際に始めたら、我々が想定していないような秘密にもしかしたら触れるかもしれないが。

○　今の説明は理解したが、特許関連技術については非常にデュアルユース性が高く、軍事的有効性が高いものがあり、これに関しては、従前の事務局からの説明にあったような、政府が秘密指定したものを民間に下ろしていく、という説明は通用しないのではないかという点を問うた次第。

○　委員の指摘は、審査関連情報の話ではなく、非公開にするとされた発明の取扱いを指すと思われるが、特許非公開制度には人的要素の保護の要素は今はない。CUIについて今回の制度で検討するのであれば、この点についても、ガイドラインなど何か工夫ができないか。例えば、不競法においても、人的要素の保護という点は書いていないので、ちゃんとしたデュー・デリジェンスをやらないといけないといったことが入るかもしれない。

○　経済官庁が特定秘密に指定した情報はなかったということについて、一国民として気になるのは、本来指定されるべき情報が指定されてこなかったということであれば、由々しき事態であると思う。その原因は、情報指定は必要最小限にすべきであるという考えのためなのか、又は担当官が勝手に判断したためなのか。今後、セキュリティ・クリアランス制度を経済安全保障分野にまで広げるという際には、10年前の特定秘密保護法制定当時と比べて、技術革新が激しく、地政学的リスクも日々変化し、生成技術やデジタル技術といった様々な技術が日々革新されていることを踏まえると、これらの情報が重要情報か否かを審査する者が専門家でなければ困るだろう。専門家を名乗る各省の担当官が、これらの情報を重要情報ではないと判断してそのまま指定されないのは非常に困るため、技術に関するリテラシーが必要である。これらの情報がどれだけ経済的な影響力があるかということを、審査担当官がきちんと審査できるということを担保する必要がある。

○　どこまでがいわゆるセキュリティ・クリアランス制度の対象になってくるCI情報であり、どこからがいわゆるCUIとしてカバーされていくのか。民間事業者がもやもやしているのは、そこではないかと考えている。すなわち、民間事業者が保有している情報は、確かに国家安全保障には重要かもしれないものの、従前は特段規制がかかっていなかった情報であり、それについて、どこまで規制が及び、それが今後の研究開発やビジネスにどう影響が生じるのかという点。今すぐどうすべきという案があるわけではないが、先ほどの説明にあったとおり、政府に提供された情報で、かつ、秘密保持契約の締結等の形式要件を満たしたものがセキュリティ・クリアランスの適用となり、そうでないものはガイドラインの適用になるといったように分けて説明をすべき。国に提供すると想定外に情報指定がされてしまい、民間事業者が当該情報を利用しにくくなる、様々な共同開発がしにくくなる、といったように誤解を生んでしまうといけない。国際共同研究開発をやりやすくするためにこのセキュリティ・クリアランス制度を構築するはずだったのに、提供してしまうと様々な要件が生じて情報が自由に使えなくなる、といった印象を与えると逆効果となる可能性もある。どこまでが今回の制度の対象であるのか、CUIを含めるのであればセキュリティ・クリアランス以外の制度かもしれないが、それにどう対応するのかについては慎重な説明が必要。

○　資料５ページの重要な情報の候補に関して、「経済的な基盤の保護に関する情報」という案については、「基盤」という用語が何を指すのかが少し不明瞭だと思った。これをもし法律の要件にするのであれば、「経済的な基盤の保護に関する情報」とは何かを問われると思うので、ここで言う「基盤」というものがどういう意味で使

われているのか、どの辺りまで広い概念を持った言葉として使われるのかについて整理が必要ではないか。

事務局より回答

○　事務局でもまだ検討途上なので、引き続き検討していきたい。

○　対象情報の検討の中には、例えば、原子力、先端半導体、AI といった技術も含まれることになるのか

事務局より回答

○　御指摘のとおり。一点だけ誤解を招かないように申し上げると、ここに書いてあるのは、新しい制度の対象になるかもしれない重要な情報の候補であり、ここに書いてあるものが全て「経済的な基盤の保護に関する情報」に当たると決まっているわけでないことは御理解いただきたい。

○　「国家及び国民の安全を支える我が国の経済的な基盤の保護に関する情報」であって、これが漏えいすれば国家・国民の安全に一定の支障を与えるおそれがあるというものということであれば、例えば、AI 技術や半導体技術の中でも、それが何らかの形で漏えいすると国家及び国民の安全に支障があると考えられる場合には、おそらく定義には含まれるのであろう。

○　経済安全保障推進法は、国家及び国民の安全に関わる経済的な基盤の話であるところ、例えば、エネルギー安全保障や食料安全保障については、既存の別法で手当てされているので、同法のサプライチェーン支援の対象に入っていない。しかし、素直に読めば、「国家及び国民の安全を支える経済的な基盤」の中には、食料安全保障やエネルギー安全保障も含まれるであろうという意味では、経済安全保障推進法よりももう少し広い概念にならざるを得ないのではないかと思う。どこまでのスコープで考えるのかについて検討が必要であろう。

○　重要情報の候補について、例えば、規制制度の審査関連情報などは、政府の求めに応じて民間事業者が情報提供するという流れになると理解しているが、これにセキュリティ・クリアランスが関係してくるということになると、今後こうした情報を民間事業者が社内で取り扱う場合には、セキュリティ・クリアランスが必要ということになるのか。

事務局より回答

○　民間からの申請書に書かれた情報は、当然元々民間が保有している情報であって、そのものを指定しようということではない。ただし、様々な事業者から出された情報を集約して我が国全体を見た結果、これは政府しか知らない情報というものも出

てくる。我々が情報保全の対象として守りたいのはまさにそういうものであり、審査情報については、民間から出てきた情報が元であっても、それを役所が見て分析することにより新たな情報が生まれ、その新しい情報が漏れたら安全保障上支障があるという場合には、そうした情報を指定の対象とするということを考えている。

経済産業省より回答

○　先ほどの委員の質問も含めて補足すると、規制制度の審査関連情報については、おそらくこのTop Secret、Secret、Confidentialのうち、Confidentialのものがほとんどであると思う。また、Confidentialの中でもセキュリティ・クリアランスをかけて扱う必要があるものとそうでないものに分かれると思う。例えば、これから開発していかなければならない重要な技術を新しく外為法の規制対象にしなければならないと考えたときに、どこかの国に言われてするのではなくて日本の中で考えて提案すべきとしたときに、その検討のために、企業に対して、法的な義務をかけながら情報を共有するということが現状ではなかなか難しいため、そういったものを産業界と対話をしながら作っていく際に、この新たな制度が活用できるのではないかと考えている。

○　また、研究開発を行う時に、サプライチェーン上これから重要なのは何かという分析は、懸念国がどういうところを狙って来ようとしているのかという情報をまとめて作っていくことになるが、こういった分析情報も、政府の中では国家公務員法の守秘義務でカバーできるかもしれないが、これを民間企業にも義務を及ぼして共有するといったことを考えた際に、この新たな制度を活用できるのではないかと考えている。

○　今の説明を聞いてもよく分からなかったので、経済安全保障上の規制が及ぶところと、セキュリティ・クリアランスの規制が及ぶところの範囲を明らかにしないと、民間企業としても判断が難しいかなと思う。こちらでも持ち帰って考えてみたいと思う。

○　資料５ページにあるのは、あくまでも重要情報の候補であるので、これを具体的に秘密指定するということは別の議論だと思う。

○　途中からCUIの話になっている印象だが、一連の議論の中で改めて整理しておきたいのは、中間論点整理にもあるように、今回作ろうとしている制度があくまでもCIを念頭にしていること。一方、CUIの管理が必要ないということではなく、これについては本日の本題ではないが、別途、明確なガイドラインを作るべきと考える。ただし、別途といっても、新たに法律を作る際、法律の中に、CUIを保護していくというプログラム規定のようなものを設けた上で、それに向けて政府の努力義務規

定のようなものを設け、それを根拠にして、政府がガイドラインを作っていくというような手法もあり得るかもしれない。経済安保推進法でやるならば、そういう仕掛けを設けることもあり得るだろう。その際には、官民で一緒に作っていくというプロセスも必要であろうと思うので、どういった場で議論することが適切かということも、併せて別の機会に改めて検討が必要であろう。

○　今の御発言は私案ということだと思うが、賛同できるものだと考えている。その際、「経済的な基盤の保護」という概念を是非どこかに入れていただきたいと思う。industrial security というときには、アメリカでいう CI に加えて CUI、さらに research security といったところまで視野に入れていただきたい。これだけのものを視野に入れた法律にするというのが我が国のためにもなるだろうし、今後の国際的な情報交換、政府由来のものに限らず、アカデミアなども含めた国際的な情報交換のきっかけになる法律となってほしい。

○　CUI については、ガイドラインでは無理だと考える。アメリカでは、CUI も、セキュリティ・クリアランスほど厳しいものではないが、人的スクリーニングということで、少なくとも犯罪情報と財務情報をチェックしなければいけないということになっている。これがアメリカで問題となっていないのは、使用者責任において採用時にチェックすることが労働法上認められているからであり、我が国ではこれは難しいので、法定しなければならないという問題がある。この問題を解決しないと、2025 年に迫っている CMMC の導入ができないこととなり、アメリカの一般的な公共入札に我が国の企業が参加できなくなるという大きな問題があるため、この場で法的事項として検討いただきたい。

○　資料４ページの図について、例えば、新制度の罰則が特定秘密保護法と同様の 10 年、もしくは５年となったときに、特定秘密は Confidential 級に罰則がなく国家公務員法の１年の罰則しかないということになってしまって均衡がとれない。これは本会議の管轄事項ではないが、特定秘密保護法の改正を行った方がいいと思う。

○　先ほど労働協定の話があったが、アメリカの原子力事業者は、労働組合の代表による労働安全衛生チェックが労働協約の中に含まれている関係で、労働組合の代表の人も、秘密管理区画の中に入るためにセキュリティ・クリアランスが必要とされ、そのことについて組合も合意している。日本にも、こうした労働安全衛生チェックが必要かは分からないが、労働組合の方々もそういうふうに現実の秘密にアクセスしようとするときはセキュリティ・クリアランスを受けており、従前は事業場の安全チェックをすることができていても、秘密管理区画に関してはセキュリティ・ク

リアランスを受けることに合意しない限り、それができなくなる可能性については留意したほうが良い。

○　CI 以外の重要な情報について議論しないということではないが、中間論点整理では、新たな制度の方向性として「CI を念頭に置いた制度」と記載されている。CI について、どの情報が対象になって、それに対してどういう保全をかけるのかがまだ決まっていない段階で、CUI の議論を行うのは混乱を来たすことにつながるので、まずは CI について議論し、その後 CUI についての手当てを考えるという順番にしていただきたい。

○　その関連で CUI を議論する前に、CI に当たる４ページの図の左下の Confidential の空白部分は、現状、特定秘密保護法でカバーされてないが、現状のままでいいのかどうかについても議論すべきである。

○　資料５ページの経済安保上重要な情報の候補について、本当に重要という印象がまだ持てておらず、もう少し具体的な説明が必要だと感じた。単なる民間からの情報ではなく、それを活用して政府が付加価値をつけた情報が対象になるという事務局からの説明はよく分かったが、そうした情報は４ページの４象限のどこに該当するのかということも分かるようになると、もう少し分かりやすくなるのかなと感じた。こうした情報に関して、悪意ある人や国からの不正なアクセスが増えて来ているといったある種の立法事実のような情報も併せてあると、確かにこうした制度は必要だということが積極的に理解できるようになると思う。

○　外為法の議論があったが、アメリカではどうなのか。日本ではその関連の指定がゼロだということだが、アメリカでの実績などが分かると、アメリカを念頭に置いて作ろうとしていることもあり、意味があるのではないかと思う。

○　サイバーの関係では、脅威情報や被害情報はむしろどんどん公開して対策に努めてもらったほうが効果的だという指摘もある中で、これを情報指定の対象にするということと、どういう整理していくのか。

○　先ほど、CI について議論を重点的に行うべきだとの指摘があったが、全くそのとおりだと思っており、これを明確化していくのは非常に重要な作業だろうと思う。ただ一つだけ申し上げたいのが、法律の目的がどういったものなのかというのが結構重要だろうということ。特定秘密保護法の改正ではないとすれば、なぜこういった形の新しい制度であるかという点で、それを引っ張るのはまさに法律の目的という

ことになってくるわけで、その法律がどこまでのものを射程にするのかという法律のストラクチャーといったものも考えないといけないと思う。要するに、従前の仕組みとの整合性はもちろんだが、なぜ新規の法律にするのか、という部分が出てこないこともあり、そういった意味で、「経済的基盤の保護」という言葉に新規性があるのではないかと考えている。要件ばかり詰めていくと、法的な整合性の観点から、特定秘密保護法の改正でやればいいじゃないかということになる。そのため、「経済的基盤の保護」ということが、新規立法の立法事実、推進力になってくると思う。そういった意味で、新規の制度にするという観点でも、法律の目的が特定秘密保護法とは違う、というように視野を広げることが一つの支えになってくるし、諸外国との制度の整合性といった意味でも意義付けができるのではないかと思っている。

○　先ほど、事前の労使協議や、セキュリティ・クリアランスの対象業務について労使協定の締結を義務づけるべきといった指摘があったが、いろいろ組合絡みの仕事をしていると、使用者側と良好な関係にある組合は良いが、かなり敵対している労使関係もあって、そういう企業・組織においては、前向きな議論ができるのかどうか。現実問題として、これが全部義務付けとなると、そこで止まるのではないかと思う。どこまで義務付けを入れるべきなのか、ちょっとここは妥協をして欲しいとか、そういう議論も必要になってくるのかなと思う。

○　情報をなるべく広く指定をしようとする方向で発想を持っていくのか、ある程度抑制的に考えてやっていこうとするのかということで、ある程度法律の思想が変わってくるところはあると思う。中間論点整理の前にお聞きしたようないろんなニーズを捉えると、国際共同開発を活発にして、ある程度海外に入っていこうというところを前提として、こういう議論になってきているという面がある一方で、今後出てくる議論としては、知る権利とか特定秘密保護法のところで問題になったように抑制的にするべきではないかといった点がある。広く指定することによって、海外との協力という意味では活性化されるかもしれないが、国内では抑制効果が出ないかなど、法律の向かう方向性を左右するような気がする。大きな方向性としてどういう発想でこれを考えていくのか。既に事務局の方でお考えのところなのか、これから議論すべき話なのかわからないが、説明いただけると今後の議論の参考になると思う。

事務局より回答

○　非常に難しい部分だが、私どもとしては、この制度を持つことによって、民間ベースのビジネスはもちろん、同志国・同盟国との情報共有を強化していくということになるので、その意味において、必要な範囲は情報を秘密として指定して保全して

いくということである。あらかじめ広くとるとか、狭くとるということを判断の切り口としては持っていない。

○　非常にお答えされにくい質問をしたが、理解した。

○　諸外国がセキュリティ・クリアランスの対象としている情報の範囲と、お示しいただいている重要な情報の候補のギャップをどう見るか。余りにもギャップがあると思う。外為法のように、各国ともにやっているものなどが一番わかりやすいと思うし、他にも幾つかそういう共通項があると思う。全部網羅的にやる必要はないが、代表的な項目を各国がどういうふうにやっているのかが調査可能かどうか。非常に機微にわたるから無理ですよということなのかもしれないが、実質的な同等性というところを重視するならば、この対象範囲だけでは判断しようがないと思っている。調査の可能性はどうか。

事務局より回答

○　例えば、アメリカのセキュリティ・クリアランスの対象情報は、大統領令には「国家安全保障に関連する科学的・技術的・経済的事項」としか書かれていない。一方、アメリカ政府でも、それぞれの機関において、具体的に何を指定すべきなのかということについて、職員に対してガイダンスを与えなければいけないので、こういったものが Top Secret/Secret/Confidential という classified information に当たるのだというガイドが作成されているのではないかと伺い知ることはできる。具体的には、アメリカのある省庁について、情報公開請求が行われた関係で公開されているものがあり、それを見ると、我々が思うよりもはるかに広範に秘密指定ができるような項目になっている。ただ、公開されているのがごく一部の省庁のみであり、一般的にはこうした項目自体が秘密指定されているがゆえに、それだけを参考に議論するのが難しいというのが現状。

○　今の点だが、同等性ということを考えると、法的に特定秘密制度と新しいセキュリティ・クリアランス制度の二つになるという状態が、諸外国では CI は一つの制度で管理されていることとの関係で、果たして同等であるとみなされるかどうか分からない。特定秘密保護法と今我々が議論している CI の話はワンセットにしているというふうに見せないといけないと考えてよいか。

○　特定秘密保護法の方も工夫して、そう見せていくのではないかと思う。

○　アメリカは大統領令の下に細かい規定があるが、各省庁レベルに関しては、省令自体が機密指定されていて、各省の機密指定マニュアルは、探しても出てこない。か

つて、比較憲法学会の先生がドイツとフランスの制度について調べていたが、特に規則レベルまで行くと、その規則自体が機密指定されていて出てこなかったという。したがって、これ以上調べるといっても、若干困難と思う。

○　企業を外部で監査する法人に関して調べてみたが、アメリカの公認会計士の例で、例えばナイジェリア出身の公認会計士で親族がナイジェリアに残っている方は、アメリカとうまくいっている国であり、親族に母国政府の関係者もいないので、セキュリティ・クリアランスが認められたが、同じような境遇の方で、パキスタンの方は認められなかった。また、アメリカ人で、会社をやっていたが、一時期不況になって収入が減り、州の税金を払えなくなって不動産に担保を設定された人がいて、一度セキュリティ・クリアランスを申請したら認められなかったが、お金を全部返して、あの時はお母さんが緊急入院して巨額の医療費がかかったのだということで不服申立てをしたところ、今は信用できるということで、セキュリティ・クリアランスが認められたということがある。

○　日本の防衛産業では、おそらく公認会計士の方と守秘義務契約を結んでいるにとどまっていて、その方がセキュリティ・クリアランスを取っているかということまでは調べていない。しかし、これをアメリカがちゃんとやっているということは、我々もちゃんとしないとならず、当然、外国のインテリジェンス機関はそこを突いてくるので、しなくてよいわけはない。また、NATO の環境監査をやっていた知人は、セキュリティ・クリアランスをとっていた。なぜ必要なのかと聞いたら、戦闘機のエンジンの排出量を計測するからということで、かなり上のレベルのセキュリティ・クリアランスを取っていた。日本においても、少なくとも、公認会計士、あるいは弁護士で特定秘密なり今度の秘密が関係する法律相談をされる方、そして弁理士に関しては、必要性があるのではないかと思っているので、御議論いただくべきだと思う。

○　公認会計士にせよ弁護士にせよ、CI に本当にアクセスする必要があるのであればセキュリティ・クリアランスの対象にならないとおかしいというだけのことであり、職務上本当に CI にアクセスする必要があるかどうかの話であって、常にセキュリティ・クリアランスを求められるとか、例外的に除外するといった考え方ではないと思う。

○　法人にセキュリティ・クリアランスをかけるという制度を作るなら、公認会計士や弁護士も対象になり得るということをあらかじめ説明しておいて、驚かないようにすべきだと思う。

○　弁護士がどこまで本当に CI にアクセスする必要があるのか現時点ではよくわからない。会社の CI にアクセスすることは、民間の弁護士の立場では、おそらく通常は生じないように思う。弁護士は、法律の要件とか、こういう法律を守らないといけないとか、違反したら罰則があるといったアドバイスはするが、そこで CI の中身に触れることまでが必要となる場面は通常はないように思われるので、今後精査が必要であるとは思うが、正直、弁護士がクリアランスを取らなければいけない場面がすぐにはピンと来ない。監査法人についても、CI に本当にどこまでアクセスする必要があるかを整理して考える必要があると思う。

（４）平沼内閣府政務官挨拶

○　本日は御多忙の中、第７回有識者会議に御出席いただき感謝する。

○　本日私はこの有識者会議に初めて参加させていただいたが、皆様に活発な御議論をいただいて、政府としてしっかりと取り組まなければならない大変重要な課題であるとの思いを改めて強くした。

○　本日いただいた御意見を参考にしながら、我が国にとって望ましい経済安全保障上のセキュリティ・クリアランス制度の設計に向けて、更に検討を深めてまいりたい。

○　今後とも委員の皆様の活発な御議論のほど、何卒よろしくお願い申し上げる。