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８回）　議事要旨

１　日時

令和５年 11 月 20 日（月）10 時 00 分から 12 時 00 分までの間

２　場所

中央合同庁舎８号館　特別大会議室

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
小柴　満信	経済同友会 経済安全保障委員会 委員長
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
畠山　一成	日本商工会議所 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
堀井　学	内閣府副大臣
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

４　議事概要

（１）委員交代

事務局から、久貝卓委員の退任及び畠山一成委員の就任について案内があった。

（２）高市経済安全保障担当大臣挨拶

○　大変御多忙な中、有識者の皆様には御出席を賜り、誠にありがたい。

○　この有識者会議を再開してからも精力的に御議論いただいているが、臨時国会において、経済安全保障分野におけるクリアランス制度につき、野党の方々からも、早期の制度創設が必要であるという立場から御質問をいただき、岸田総理からも、私からも、次期通常国会における法案提出に向け準備を進めていきたいと力強く答弁させていただいている。改めて、クリアランス制度への注目度、期待度の高さを感じている。

○　本日は、経済安全保障上重要な情報の保護ルールとして、事業者に対する信頼性確認、個人に対する信頼性確認といった、いわゆる FCL、PCL のほか、罰則についても御議論いただきたいと思っている。よろしくお願いしたい。

（３）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。

（４）意見交換

○　制度として国際的に通用しなければならないということが今回の有識者会議の基本的なコンセンサスとしてあると考えている。そういった意味で、今回の新法において特定秘密保護法の手続その他を参照するのは、基本的に正しい方向性であると考える。

○　今回の法律ができることにより、我が国の Top Secret 、Secret 等の構成は、特別防衛秘密、特定秘密、それから今回の法律と、かなり分散的な傾向の強い制度になってくるであろう。

○　今回の法律の大きなポイントは、国際的な観点での研究開発をいかに過不足なく実施できるかであり、その一番のポイントは、アメリカにおいてどの程度理解いただけるかということだと考えている。アメリカだけでいいのかという問題はあるが、特別防衛秘密、特定秘密保護法、今回の法律について、統一的な形でアメリカの情報当局に説明した上で基本的な形で支持をもらうということが、日米同盟という観点でも重要であり、今後の制度の施行の円滑な進行という観点も重要である。

○　資料 14 ページの罰則の参考資料の中で不正競争防止法（不競法）が出てくるが、民間における秘密の保全という点で不競法は重要だと思う。この表の中の「取扱にかかる法律での PCL/FCL 規定の有無」の欄が不競法は「×」となっているが、営業秘密に関して経産大臣が定めている指針には、行政指導のような位置付けかもしれないが、FCL 的な組織的管理の指針も含まれていると承知しており、ここは「△」くらいではないかと思う。

○　全体の法体系ということになってくるかもしれないが、前回会議の資料で経済安保上重要な情報の候補として挙がっていたサイバー関連情報、規制制度関連情報、調査・分析・研究開発関連情報、国際協力関連情報が新法において規定される場合に、不競法との関係はどうなるのか。形式的なことを言うと、不競法は不競法、この法律はこの法律、というような答えが政府側から返ってくるであろうが、実態的には、罰則の適用を含め、多分これらは重なってくるであろう。

○　個別論点の検討に当たっては、６月の中間論点整理が基点になるべきと考える。中間論点整理では、「既存の諸制度等との整合性にも留意しつつ、あるべき制度を検討することが必要」とある。この点、例えば、経済安全保障分野のクリアランス制度の信頼性確認についても、特定秘密保護法における適性評価との整合性に留意する必要があると考える。

○　事業者に対する信頼性確認について、仮に、産業保全の観点から、特定秘密保護法の下では求められていない CEO（Chief Executive Officer）等への人的クリアランスが必要とされた場合、新たな制度の必要性の一つとして掲げられている「企業からのニーズ」を減退させ、また、実務上対応が困難な企業が出て来得ることを懸念する。

○　個人に対する信頼性確認について、労使間を含めて、丁寧な手順を踏んだ上で本人の同意を得て調査を行うことに全く異存はない。今後、丁寧な手順とはどのようなものであるべきなのか、企業の立場から意見を申し上げたいと思うが、それらを法定することに対しては十分慎重に議論すべきと考える。

○　クリアランスの対象は、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及びその従業者に限定すべきであり、事務局資料８・９ページにある秘密保持契約の締結はそうした意思に基づく行為になると理解する。したがって、秘密保持契約なくして民間事業者及びその従業者が、クリアランスの対象とならないようにすべきであると考える。

○　相手国から信頼されるに足る実効性のある制度を目指すべきとかねて主張してきており、この点は中間論点整理にも盛り込まれた。ここで言う「信頼されるに足る実効性のある制度」とは、アメリカと全く同じ制度を導入するという意味ではないと理解している。現に、特定秘密保護法は、アメリカの制度と完全に同じ制度ではないものの、アメリカから信頼され、認められていると承知している。相手国に信頼されるに足る制度となっているかは、政府が判断し、相手国政府と交渉すべき問題と考える。

○　資料２ページ（第７回会議の議論の整理）１（３）の「FCL、FOCI」について、今回のセキュリティ・クリアランス制度の導入につき、アメリカと完全に同じ制度にする必要はないものの、カウンター・インテリジェンスに関わる部分に関しては一定の共通性が必要であり、その中で最も重要なポイントの一つが FOCI（Foreign Ownership, Control, or Influence）であると考える。

○　組織又は法人に対するセキュリティ・クリアランスについては、特定秘密保護法において直接的な規定がなく、アメリカの FOCI では法人の幹部が個人クリアランスの対象となることから、導入すれば影響が大きいと思われる。しかし、これを導入しないと、ヒアリングでアメリカと機密情報を共有して入札や共同研究に参加することを希望していた企業の希望を叶えることができないと思う。アメリカ自身が自国の企業等にこの要件を課していることに鑑みれば、この要件を外してアメリカと日本の民間企業等との間で秘密指定された情報のやり取りはできないものと考えられる。

○　特定秘密保護法の場合、防衛産業には積み重ねられた運用があり、FOCI 要件が満たされていなくても適切に運用できている関係から、アメリカから認められたという経緯があると思う。この運用を他の産業全般に適用するのは不可能であることから、FOCI に関する法令等における規定は必要であると思われ、本来であれば、特定秘密保護法における制度にも必要となる改正をして FOCI を規定したほうがよいと思う。次回は、事務局から FOCI に関する概要を御説明いただき、各委員から十分な意見を出せる時間をとっていただくようお願いしたい。

○　資料３ページ（第７回会議の議論の整理）１（４）の「セキュリティ・クリアランスの対象範囲」について、前回会議で、サイバー関連情報を利用する基幹インフラ事業者には、セキュリティ・クリアランスを取得する義務を課すべきではないかという趣旨の発言をしたが、私の意見をより正確に申し上げれば、経済安全保障推進

法の特定社会基盤役務の安定的な提供の確保に関する制度における特定社会基盤事業者には、不正なアクセスを回避する仕組みの実装等につき充実した制度担保がなされているが、アメリカ等から秘密指定されたサイバーセキュリティに関する防御策等を共有し、特定妨害行為を防ぐための仕組みも必要であり、その場合には関係者のセキュリティ・クリアランスが必要になることから、この件に関する検討をする必要があると思う。アメリカが 2023 年３月２日に公表した国家サイバーセキュリティ戦略においても、戦略目標 2.3 として、インテリジェンスの共有と、被害者による通知に関するスピードと規模を拡大することが掲げられており、連邦政府は、重要インフラの所有者及び運営者に即座に利用可能なインテリジェンスを提供するため、秘密解除指針を見直すとともに、秘密情報へのアクセス範囲を広げ、かつ、セキュリティ・クリアランスの対象を拡大するための条件を決定する手続を見直すというふうに書かれているので、我が国でも同様の検討が必要であると考える。

○　資料５ページ（第７回会議の議論の整理）２（２）の「CUI、民間事業者が保有している情報」の４つ目の発言にある「少なくとも犯罪情報と財務情報をチェックしなければならず」という点について補足すると、アメリカにおける CUI（Controlled Unclassified Information）では当然のことではあるが、我が国でアメリカの CUI を共有する場合には、ここに記載のある犯罪情報と財務情報の他に日本国籍を有することも要件とされると考えられるため、その点でも必ず法定する必要が生じると思う。

○　資料４ページ（第７回会議の議論の整理）の２（１）「経済安保上重要な情報」について、前回、経済安全保障上の重要な情報の候補について議論したが、もう少し深掘りが必要かと思う。直接的に安全保障を目的にする法律は当然のことだと思うが、それ以外の法律でも安全保障に関わる情報はあり得る。今ここで、こんな法律も対象ではないかという議論をするつもりはないが、今後の仕組みとして、各省が率先して重要な情報の候補を出してくるとは思えないので、NSS（国家安全保障局）から検討を要請するなど、何か仕組みをきっちりと作っていくことが重要。そのような仕組みがないと、各省は、情報の候補を出してこないというネガティブな反応しかしないことが予想される。各省の政策の統一性をしっかり見た上で、各省に物申すことができるような仕組みを工夫していただけないかと思う。中身については、その中で議論していただければよいと思う。

○　前回会議で出てきた経済安保上重要な情報の候補も、NSS が各省庁に要請して候補を出してもらった上で作成したものだと思うので、今の御発言は、こうしたことを制度的な形にするということと理解した。

○　CEO に対するクリアランス取得の義務付けの議論については、議論の前提として、防衛省が防衛産業保全政策の中でどのように運用していて、これがアメリカとの関係でどうなっているかという実態が共有されないといけないと思う。防衛省から聞くのが一番よいと思う。

○　労使協定の締結を法律で義務付けるというのは、違和感を持って受けとめた。もちろん、労使間の円滑な関係はとても大事だということを前提に申し上げるが、それを法律で義務付けるということが適切なのかどうか。むしろ、これは法的義務というより、セキュリティ・クリアランスを取得する人が具体的なケースにおいてどれぐらいいるのかという程度の問題もあると思う。その企業の経営の中で、どれぐらいの位置付けを占める話なのかによって、経営判断においても相当違ってくるかと思う。そういうフレキシビリティを持つためにも、運用指針的なもので、こういうことを尊重するとか志向するといったことを書くのはいいと思うが、法律で義務付けるとなると意味合いが違ってくると思う。

○　労使協定の締結の義務化について、これは明らかに経営判断に属するものであり、法律で義務付けるというのは絶対にやるべきではない。これは本当に強く言いたい。

○　企業の活性化という観点では、もう少し企業へのインセンティブが明確になってほしいと思う。クリアランスを持っている会社について、これが例えば企業の格付けになるとか、政府が認証するとか、もう一歩踏み込んだインセンティブをつけていただければ、もっと企業も協力する気がする。当然、その中に、クリアランス対象者に対するクリアランスのポータビリティや経済的インセンティブを与えることも含まれ、その辺りの議論をもう少し強めにしていただけるとよいかと思う。

○　資料８・９ページの図で説明されている民間提供情報を特定秘密に指定した場合における効果について、ここに書かれていること自体は非常にクリアに理解できたのだが、自分の問題意識として、例えば８ページの図において、A 社が情報を政府に提供し、政府で他の情報と混ぜて何らかの付加価値がついて特定秘密になったという時に、この情報を再び A 社に戻した場合はどうなるのか、ということも知りたい。また、この情報を政府が D 社に提供した場合には、A 社にとっては自社が提供した情報が含まれるが、どういう扱いになるのか。D 社としては、A 社から既にもらっていて、セキュリティ・クリアランスが不要だと思っていた情報が、重ねて政府から提供された時には特定秘密になってしまうのかどうか。罰則付きになってしまうため、どうしてもこれを明確にしておかないといけないし、自分が政府に提供した

情報が戻ってきたら特定秘密になってしまうとなると、むしろ情報提供することへのディスインセンティブになってしまい、これはこれで、経済安全保障上重要な情報について民間も含めて厳格な鍵をかけた上でスムーズな情報交換をするという制度趣旨にも反することになりかねない。

○　秘密保持契約を締結して提供されるというプロセスになるということは、逆に言えば、秘密保持契約を締結するまではどんな情報をもらえるかが分からない。そのため、秘密保持契約を結んだ上で情報をもらったら、実は自分が提供した情報がほとんどであったとか、少し付加価値がついた程度のものだったというような場合が想定される。このような場合、政府はそもそも秘密指定をしないということなのかもしれないが、秘密指定がされた場合、おそらく、自分が政府に提供した情報と政府によって秘密指定された情報とを分けて管理し、自分が提供した情報については秘密指定の効果は及ばないという形で明確にするのではないかと思う。こういう情報をきちんと政府が集めて、インテリジェンスとして民間に提供していくことで経済安全保障に資するということがこの制度を作る成果だと思う。罰則付きの義務でもあり、こういうところを明確にしておいた方が、民間からも情報が提供しやすくなり、政府としても集めやすくなると思う。その辺りについても、今後整理をいただくということであれば、御検討いただきたい。

○　資料８ページの図の「政府」の枠に「分析等付加価値を付加した場合」と書いてあるが、仮に全く同一の情報が秘密指定されて政府から提供元のA社に提供された場合には、たとえ　秘密保持契約を結んでも、A社が以前から保有していた情報である以上、秘密指定の効果はA社に及ばないという理解でよろしいか。

内閣官房より回答

○　今の御質問について、資料８ページは、分かりやすさの観点で「分析等付加価値を付加した場合」と記載しているが、一例として申し上げると、民間の商用衛星をA社が持っているとして、民間の商用衛星の画像であれば別に特定秘密にはならないのだが、それを政府が購入・入手した場合に、その画像を分析して付加価値を付けた場合には、特定秘密として法的義務の対象になり得るだろうということで書いたものである。御質問はA社から受け取った情報を政府がそのまま秘密指定してA社に戻す場合にどうなるかということだが、そもそも、特定秘密に指定すべき情報であると政府が判断した場合に、特定秘密保護法は政府統一で厳格に保護することが目的であるため、そういった特定秘密として保護しなければいけないような情報をA社に戻すのかといった話がまずはあろう。政府側としては、保護すべき情報を渡すことについて相当慎重に判断すると思われる。現に、特定秘密保護法でも、適合事業者として認定する制度はあるが、その前提として、政府が事業者に渡さなけれ

ば行政の業務を遂行できないような、いわゆる非代替性がある場合に情報を渡すことになっており、もらったり戻したりということをやるような形にはならないのではないか。制度の観点から申し上げれば、当然、特定秘密を渡す場合には、適合事業者として認定し、また、それを前提とした上で、取り扱う人間に適性評価を付与して情報を渡すことになるので、その特定秘密を渡す以上は、それは特定秘密保護法の規律に服することになるということである。いずれにしても、その情報を守りたいのか、またどう守るかということであり、実態面としては、その過程で政府と会社との間でいろいろ議論をすることになると考える。

事務局より回答

○　補足すると、今の説明は、実務の話なのか理論の話なのかが若干整理しにくいところがある。おそらく委員の御指摘としては、理論上本当にあり得ないのかという御質問かと受け止めている。その辺りは一度整理をさせていただいて、次回お示しさせていただく。

○　資料８ページの「分析等付加価値を付加した場合」という記載に少し違和感を抱いたのが、分析という形での付加価値をつけなければ特定秘密にならないかのように受け止められてしまうというところである。付加価値を付さない情報だけで特定秘密になるというケースは論理的にあり得るのではないか。これまで実例がなくとも、今後これが制約要因にならないだろうかと懸念する。このように資料に記載することで、付加価値をつけた場合でないと特定秘密として指定できないといった形で、あたかもこれが必要条件かのように受け止められることは好ましくない。

○　逆に、それが必要条件ではないとすると、政府からA社に同一の情報が戻るということになるので、あくまで特定秘密の話ではあるが、この場合の法的効果を整理していただきたい。

○　今の点について、政府がA社から提供された情報に付加価値を付けることなしに特定秘密にすることができるということは、おそらくCUIの問題とも関わってくると思う。つまりCUIであったものがCIになる。逆に言うと、政府が提供を受けた場合についてであるが、例えば、先ほどの衛星画像の例で言うと、これを購入し加工されない状態で特定秘密になるとすれば、それはA社が使用しているプロダクトそのものが特定秘密に該当するということになる。この場合、A社とD社との取引が、要するにCIレベルの情報をコントロールするということになるという解釈にもなり得るため、次回、事務局の方からこの点の整理をしていただく際には、CUIとの関連においてどのように考えるべきであるかについても議論する必要がある。

○　資料 12 ページの海外の施設クリアランス制度概要資料に、諸外国では「経営陣、出資元の外国資本等の保全上の影響を考慮」といったことが記載されているが、外為法との関係性について関心がある。外為法には、外国からの出資が１％以上ある場合には審査を受ける投資スクリーニングの制度がある。外為法において不適当とされればおそらく FCL も通らないだろうが、外為法上の審査を通過したものについて FCL を通過する基準は何か。また、FCL を通過したことが逆に外為法上の審査にどの程度影響し得るかということで、２つの法律の整合性が問われるのではないか。このため、FOCI の適用を検討するには外為法も含めた議論が必要である。

○　資料３ページ（第７回会議の議論の整理）１（４）の「セキュリティ・クリアランスの対象範囲」にある「CI に触れることになる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、法律事務所、特許事務所、環境監査を行う法人などもクリアランスの対象となると思われる。」という指摘については、今後もう少し詳細に検討した方が良いと考えている。大企業に対する監査には、会計監査と業務監査があり、会計監査はおそらく CI には関係ないが、業務監査はケースバイケースで CI に触れる可能性もあると思う。法律事務所については、例えば、CI に関連する罪を犯して留置された者に弁護士が接見する場合、セキュリティ・クリアランスを保有していないため弁護活動ができないというのはナンセンスである。このため、法律事務所といっても配慮が必要になる部分はあると考えられ、この点をもう少し詳細に検討する必要がある。

○　代表取締役や CEO などにどの範囲までセキュリティ・クリアランスの取得を義務付けるかという点について、最近は、会社法改正の関係で取締役と執行役を分け、取締役にはほとんど社外の者をあてるケースも増加しているところ、こういった社外取締役にまでクリアランスの取得を義務付けることは困難と考えられる。CEO、CTO(Chief Technology Officer)、CIO(Chief Information Officer)等、どの範囲までクリアランスが必要になるかは企業によって異なるだろうから、どういうケースがあるかを会社法の規定等に照らして詳細に検討する必要があるのではないか。

○　一連の議論は、自ら CI を取り扱う者が個人のセキュリティ・クリアランスを求められるのは当然であるが、CEO 等については、CI を自ら取り扱わない場合であっても、企業の FOCI の観点から個人のセキュリティ・クリアランスを取得させておく必要があるのではないか、という議論だと理解している。この二種類を分けて整理する必要がある。

○　資料６ページの「論点」について、特定秘密が対象としているのは、Top Secret 級

と Secret 級の情報であり、Confidential 級の情報は対象としていないので、「Confidential 級の情報においても、特定秘密保護法に準じた取扱いとすることで良いか」という質問の意味するところがよく分からない。

事務局より回答

○ Confidential 級の情報は、御指摘のとおり現行の特定秘密保護法では保護の対象になっていない。今回、中間論点整理に沿って Confidential 級も含めて経済安全保障上の重要な情報を保護することとした場合、Confidential の部分をどのような制度にするのかということを考えたときに、特定秘密保護法と同様とする考え方もあるし、それと少し異なる扱い、例えば法定刑を少し低くするといったこともあり得ると思われ、そうしたことについて御議論を賜りたいということで問題提起をさせていただいた趣旨である。

○ 資料７ページの図の「Ｃ事業者」について、おそらくほとんどの方が、ファシリティ・セキュリティ・クリアランスを受ける事業者は１社だけという理解だと思うが、アメリカでは、組織クリアランスにおける FOCI の規則により、親会社や子会社、関連会社も組織クリアランスの対象になる場合がある。この点については、事務局から是非とも次回の会合で説明していただければありがたい。

○ 経済安全保障推進法の基幹インフラ制度では、特定社会基盤事業者の指定を受けたのが全て日本の事業者であり、外国の事業者が含まれていないことが気になったが、クリアランスの議論は、外国企業の日本法人や、日本企業に勤める日本国籍を持たない社員などにどのように及んでいくのか。

事務局より回答

○ いわゆる外国企業の日本法人については、日本国で法令上、日本の法人として登記されている場合には、対象になり得ると考えている。これは、例えば、日本企業も、アメリカの現地法人であれば、アメリカのクリアランスを取ることができるのと同じと考えている。個人に対しては、原則として、自国の国籍を持った人間に付与すると承知している。

○ 資料 11 ページで、特定秘密保護法における適合事業者の基準として「特定秘密取扱場所への立入り及び機器持ち込みの制限」という項目があるが、立入りが制限される場所における安全確保が実態としてどのように行われているのかをお尋ねしたい。すなわち、事業者には、労働契約法第５条で「労働者の安全への配慮」が義務付けられており、立入制限区域においても労使や産業医などが職場巡回するなどの必要があるが、実態はどうなっているのか。

内閣官房より回答

○　特定秘密保護法の制度で定めているのは、特定秘密を明確に保護しなければならないということなので、企業の組織が業務として特定秘密を扱う場合には、行政機関と同じレベルで扱う必要があるだろうという観点で、場所の制限や必要な施設設備の設置、機器の持ち込み制限、必要な施設整備の内容を定めておく必要があるということで、こう書いている。そもそも特定秘密保護法上、実際にそれができていることを前提として契約を結ぶことになるので、それぞれの会社が、特定秘密も含めて労働者と経営者とどういうふうに安全管理をしているかということではないかというふうに考えている。

○　今の御説明は、法律では適合事業者として準備しなければならない条件を規定しているにとどまり、実際の運用は労使の取り決めに委ねられるという話であると理解。今回のクリアランス制度も、クリアランス取得に対して相当に厳格な基準が設けられ、特定秘密に準ずる形となると考えられるが、結果として、クリアランスを持っている人間しかそこに入れないとなった場合には、そこにいる従業員の安全を一体誰が担保するのかということが大変重要な課題だと思っている。この基準を置いたときに労働者の安全をどうやって担保していくのかということについても、既存の法律と照らし合わせて是非議論していただきたい。安全は何よりも優先されるものだと思っている。

防衛装備庁より回答

○　立入りが制限された区域内の安全確認をどのように実施するのかということについて、実際の運用を企業につぶさに確認したものではないが、クリアランスは秘密に触れるために必要になるものであることから、通常想定される方法としては、労働環境の安全確認をするときはその場所で秘密を取り扱っていない状態にした上で立入制限区域内を見ていただくというようなやり方があるのではないかと思う。すなわち、秘密指定された文書がテーブルの上に載っていない状態や、もう少し大きなものであるとすると、覆い隠すような形にするなどして、クリアランスを持っていない人が立ち入った時に秘密に触れることがない状況を創出した上で、勤務環境が適切かどうかを確認できるのではないか。そういうやり方になるのではないかと思う。

○　資料 13 ページに特定秘密保護法の適性評価における調査の方法が示されているが、この手続において、行政機関と事業者と適性評価を受ける個人とが実際にどのように情報のやりとりをしているのか教えていただきたい。また、留意事項で、調査の過程で取得された個人情報については目的外での利用や提供が禁止されているとあるが、この禁止は誰に及ぶのか、罰則があるかについても確認したい。

内閣官房より回答

○　適性評価を行うのは行政機関なので、適合事業者の側から特定秘密を扱うだろうと考えられる従業員の名簿を提供いただいた後に、行政機関から対象となる従業員に対して書類を送ることになる。告知書では、適性評価の実施に同意する場合には同意書と質問票に記入して封筒に入れ、封をして提出してくださいということになっているので、基本的に従業員は封をして行政機関に提出するし、場合によっては会社の保全責任者を経由して提出する場合もあるけれども、その場合には中身を見ないようにということで、そこは閣議決定された運用基準にも書かれているし、「封をして」と告知書に明記されているので、基本的に個人情報は、提出する個人と行政機関の間で取り扱われるということになる。

○　目的外での利用及び提供禁止は、法律で書かれているので、当然行政機関の側もそうだが、いわゆる適合事業者についても、この義務が係ってくることになる。ただ、これに違反した場合の罰則というのは、特に法律上は規定されていない。

○　個人のプライバシーは守られているという趣旨の回答であるが、実際には、民間事業者には人事の担当者がいるので、本当にこれを厳格に運用することができるかどうか、やってみないと分からないところもあるが、これまでの様々な事例などを考えると、個人の調査票は、紙で書いて封をするということではなく、例えば、一元化の問題もあるが、セキュリティのかかった電子データで行政機関に直接渡すなど、事業者が見たくても見られないような仕組みなどを講じておくことも必要ではないかと思う。

○　評価対象者の結果の通知に関して、これまで通知されなかった例はあるか。また、苦情申立ての事例もあれば教えていただきたい。

内閣官房より回答

○　結果通知については、法律上結果を通知すると明記されているので、結果が通知されないということは制度上は予定されていない。

○　苦情の申立てについては、これまで適性評価に関係する苦情申立てはなかったと把握している。

○　調査結果が本人に通知されないことはないという回答であるが、我々が事前にヒアリングした限り、通知されないケースもあると伺っている。本人のキャリアパスにも直結するものなので、あらかじめ通知されるまでの期間を示した上で、必ず通知をする仕組みにしていただきたいと思う。

○　調査結果に対する苦情申立てもなかったということであるが、これも苦情申立ての機会なども担保いただくとともに、行政不服審査法の対象とすることも併せて御検討いただきたい。

○　先ほど労使協定の義務付けに関して、慎重であるべきとか、認めるべきではないとか、いくつか厳しい御意見をいただいたが、これまで挙がっている中だけでも相当程度労使で確認しなければならない事項があると思う。義務付けを法律に書くか書かないかを論ずる前に、制度を導入するに当たって、個人の信頼性確認はもとより、事業者の確認をするに当たっても、秘密の区画を新たに作り、秘密の取扱いを規定して、それを誰に適用するのかなど、相当程度働く人たちに影響があることだと思うので、事業者がこれに手を挙げるなら事前に何をしておかなければならないのかということについて、この場でも議論いただいて、あらかじめ何らかの形で示すなど方法を検討いただけるとありがたい。

防衛装備庁より回答

○　アメリカにおける FOCI の運用は、取締役や株主の構成、実際にその企業がどういう市場で売上を上げているかといったことを確認する。例えば売上の基盤が懸念国であったとすると、その国に相当依存しているということでリスクと評価されることになる。取締役会・株主の構成メンバーについての何らかの助言が入ったり、企業が国内外のあちらこちらに研究拠点なり生産拠点があったとするならば、そういった施設、工場、研究拠点の設置の仕方や他の関係企業との業務提携の状況について、どういう方針であるかの計画を示させるというような形でリスク評価を実施していると承知している。

○　防衛装備庁では、そのような幅広い視点ではなく、もう少しポイントを絞った形で実施している。実際に秘密を取り扱う契約を締結する際にこのプロセスを取り込んでいる。すなわち、入札に参加する前に、企業から、実際に契約を履行することになったら、どういう人が秘密の取扱いに関与することになるかという業務従事者のリストを出していただいており、その中に懸念されるような国の国籍保有者がいれば、そこは懸念があるな、というふうに判断をさせていただくということである。入札に参加したいという企業が社内で取扱者ではない者が秘密情報にアクセスできない社内体制になっているかということもチェックさせていただいている。

○　防衛産業であると、通常は、秘密情報を取り扱う部署の関係者以外がこれらの情報にアクセスすることはないと思っている。本当にその事業に携わる人がどういった形で秘密を取り扱うのかどうかということ、それから、親会社にせよ、事業提携先にせよ、その会社に影響力を及ぼしそうな企業について情報提供していただき、実際にその親会社等に情報を提供しなければならない状態にあるのかどうか、という

ことについての確認をとる。懸念がある企業については、入札に参加していただけない、という形でやっている。このように、防衛省・防衛装備庁から提供する秘密情報が企業の特定の関係者のみで取り扱われること、その情報が外国から影響を受けることがないような形になることを確認するというやり方を取っている。

○　FOCI にはいろいろな要件があり、例えば資料 12 ページにあるように、諸外国では、外国人の株式保有割合や役員の国籍などを確認することとなっている。これ自体は FOCI の考え方からすると理解可能だが、既存制度との整合性を踏まえると、かなり難しい要件が出てくる可能性があり、既存制度との整合性をきちんと確認していくことが重要だと考える。例えば、５％以上を保有している株主というのは、経済安全保障推進法の基幹インフラ制度でも同趣旨の基準が設けられたが、そもそも外国株主が５％以上保有しているどうかは、上場会社からすると、基準日以外では分かりようがない。金融商品取引法上の大量保有報告書が提出されるのは５％を超えた場合であって５％以上ではない上、その計算方法についても、金商法では共同保有の概念なども含まれており、金商法と今回の制度での考え方が一致していないと、５％という形で出してほしいと言われても、制度として機能しなくなってしまう。国籍情報についても、個人情報保護法上の個人情報に該当するのでどう集めるか、海外の個人情報保護法との関係で、外国籍や外国所在の人の個人情報をどう集めるのかといったことが非常に重要になってくる。また、別の委員からも話があったが、外為法との整合性も重要。外為法では１％の保有で投資審査がかかるようになっているが、そこで審査する内容と今回のセキュリティ・クリアランスとして審査する内容は、目的はやや違うところがあるとは思うものの、重なってくるところもあると思う。例えば、経済安全保障推進法の特定重要物資の関係事業者については、外為法における対内直接投資の審査対象に追加する形で整合性がとられたが、セキュリティ・クリアランスについても、他の法律との整合性を取っていくことが重要なのではないか。こうした作業が、うまく制度を機能させるという意味でも非常に重要になってくると思うので、横断的な検討が必要である。

○　アメリカとの整合性を考えて国際的に信頼に足る制度にしなくてはならないというところは極力担保しつつということになると思うが、やはり、CEO や全ての役員が常に個人クリアランスを取らないとファシリティ・セキュリティ・クリアランスが取れないということになってしまうと、少なくとも今の日本においては、現場に相当混乱が生じる可能性があると思っている。そもそも国籍の関係で日本のクリアランスを取れない方や、自身ではなく家族の関係でクリアランスを取れない方などが役員になれないということになると、相当大きな問題となってくるような気がする。その意味では、企業の信頼性確認のために役員の調査をするということと、フ

ァシリティ・セキュリティ・クリアランスの要件として個人クリアランスを要求するということを分けて考え、CEO や全ての役員の国籍情報やバックグラウンドをある程度調査はするが、個人クリアランスはあくまで秘密情報に接する人にのみ要求するというような形でうまく整合させて、役員全員が個人クリアランスを持たなくても良いという形にできないだろうか。

○　資料 13 ページにある適性評価情報の目的外利用禁止について、解釈を確認させていただきたい。特定秘密の保護以外の目的に使ってはならないということは、会社で人事配置の参考にするとか、セキュリティ・クリアランスが取れなかったから手当に影響が出るといったことが、今の特定秘密制度でもできないことになっているということだと理解したが、現行の制度設計はそういう意識を持って作られているのかということを確認したい。また、私は、制度である程度信頼性を担保できるのであれば、担保していったほうが良いのではないかと思っている。例えば、少し場面が違うが、経済安全保障推進法の基幹インフラ制度では、設備を供給するシステム会社は自社の役員の国籍情報などを、届出義務者である特定社会基盤事業者を通さず直接行政機関に提出できるような仕組みを作っている。こちらの制度でも、例えば従業員個人が会社を通じずに直接行政機関に対して、オンラインでも何かしら管理番号を付けていれば提出できるような形にするとか、何かそういう形で明らかに制度上プライバシーが担保される仕組みを用意することで懸念が軽減できるのであれば、そういうことを試行する手もあるのではないかと思う。

内閣官房より回答

○　特定秘密保護法上の目的外利用の禁止については、適合事業者との関係で申し上げれば、適性評価のためにしか使わないという理解で間違いない。運用基準にも、人事評価のために適性評価の結果を利用等してはならないと明記されている。

○　基本的にこの制度は、大企業が関わることが多いのではないかと思っているが、技術分野によっては中小企業やスタートアップも関わってくる可能性があると思う。イノベーションの促進という視点からも、こうした分野にそうした企業が今後関わっていくという視点も重要かと思う。一方で、今回のように、企業に負荷がかかるというようなことになると、企業の規模やキャパシティによっては、負荷にどう耐えるのかという観点は重要。やらなければならないことはやらないといけない、ということかと思うので、そうした企業向けの環境整備というのはしっかりやっていただく必要があると思っている。

○　資料６ページの「Confidential 級の情報においても、特定秘密保護法に準じた取扱

いとすることで良いか」という記載につき、事務局から、罰則については特定秘密保護法と同等とするか、場合によっては劣るとすることも考えられる、という説明があった。この点を検討する上で、第５回会議の防衛装備庁の資料の中で、Confidential の情報は、我が国では「秘／特別防衛秘密（秘）」に当たると整理されている。そうすると、Confidential 情報に対する罰則は、特別防衛秘密に適用される 10 年の刑と、秘密保全に関する訓令が根拠になっている秘情報に適用される１年の刑とが混在しているという理解でよろしいか。前提となるファクトなので明確に共通認識を持っておきたい。

防衛装備庁より回答

○　特別防衛秘密というカテゴリーの中には、Top Secret, Secret, Confidential が含まれるが、特別防衛秘密は米側から日本側に高度な装備品が供与されるに当たり、米国政府から特に保全が求められたことを前提とする秘密であり、基本的に特定秘密と同等以上の保全を求められているというカテゴリーである。これとは別に、特定秘密というカテゴリーがあり、また、防衛省においては省秘と言われている Confidential 級のカテゴリーがあるということ。

○　特別防衛秘密の中に Confidential 級のものもあるということか。

防衛装備庁より回答

○　カテゴリーとしてはおっしゃるとおり。そのときには罰則は 10 年以下となる。

○　別の委員が指摘していたとおり、FOCI には会社法等に伴う色々な論点がある。米国でも、必ずしも役員全員が個人クリアランスを取る必要はなく、株式会社においては通常必ず取らなければならないのは取締役会議長と CEO のみ。理由は、この２人が CI 関連の業務を理解していなければ、企業の決算や経営が成り立たないから。この点に関しては是非とも議論していただきたい。そうしないと企業のガバナンスが成立しない。ちなみに、海外の防衛企業では、全ての役員がセキュリティ・クリアランスを取っており、役員の指名候補にはセキュリティ・クリアランスを過去に取得できなかった事実の開示が要件として掲げられているところもある。ここまでやるのは防衛産業であるが故だが、一般産業においても、少なくとも取締役会議長と CEO の２人がクリアランスを取得していないと、誰が経営の責任を負っているのかという話になる。加えて、大企業だけではなく、関連会社や秘密指定された情報を共有する下請企業などのサプライチェーンまで対象に入ってくる。FOCI については、まだ色々な誤解があるので、次回時間をとっていただき、いろいろな立場から意見をいただいた方が良いと思う。

○　日本の企業でも、取締役やCEOが日本人ではないケースが増えてきており、そのあたりの実態も踏まえて議論を進める必要がある。

○　罰則の法定刑について、現行制度は罰金額が低いように思う。防衛産業にとどまるうちはそれでもいいが、これからは半導体や量子などもっと大きな市場を相手にするわけで、やはりマーケットとして圧倒的に大きい。そうした市場価値の大きい分野にまでCIという概念を広げていくのであれば、やはり罰金額の上限が低いと思う。

○　日本の特定秘密保護法に関しては、アメリカの法制度と同一の制度ではない、つまりアメリカが求める厳しいレベルをすべて充足している訳ではないが、法律を補完する政令や省令、ガイドライン、そして個別契約の締結などにより、いわば「合わせ技一本」で、アメリカの法制度と同レベルの制度になっていると理解している。すなわち、日本の制度の一つ一つは、「一本」ではないが、「技あり」の積み重ねで、全体としてアメリカと同等性が認められているということかと思う。これを前提とすると、今回のセキュリティ・クリアランスの法律を作るに当たっても、法律だけで「一本」を取らなくてもいいはず。「合わせ技一本」を目指し、ある程度のところまでを法律で規定した上で、残りは、今後規定する政令や省令、ガイドラインや個別契約の蓄積などで、全体として、アメリカのセキュリティ・クリアランスの法制度と同様の制度とするようにすればいいのではないか。そういった考えの下で、どこまで落とせるかという検討も必要だと思う。議論されている代表取締役や理事長などにクリアランスを求めるかについても、実は先ほどの「合わせ技一本」の理屈によれば、法律自体からは落とせる可能性もあり、今回どこまで詰めて議論する必要があるのかという検討が必要だろう。

○　罰則に関して、事務局資料６ページに「Confidential級の情報においても、特定秘密保護法に準じた取扱いとすることで良いか」とあるが、「準じた取扱い」の中身が非常に大事。同等の水準とするのか、あるいは劣った水準で担保するのか。既存の制度下ではTop Secret級とSecret級に対する罰則が10年以下、Confidential級に対する罰則が１年以下となっている中で、経済安全保障の世界でのConfidentialというものをどのように区分していくのか。罰則が劣る場合には、それは保護法益の違いから来るのか、また、その程度によって適性評価の調査の程度が違ってくるのか、それにより罰則がどの程度変わるのか。こうした点の整理を事務局がきちんと詰めていくべきだと思う。

○　資料12ページ※２において「公開されている申告フォーム（SF328）」に基づく記

述がなされているが、NISPOM の改正により、５％要件が消えていたような気がする。その理由は判然としないが、4.9%を狙ってきた懸念国企業がいたのではないかとも考えている。他の委員からもあったように、株式公開会社にとって株主を確定できるのは大体年に１回ぐらいしかないという実務上の問題もあると思うが、そもそもこの５％という数字が NISPOM の改正で消されたと考えているので、確認をお願いしたい。

○　企業のガバナンスの問題と秘密情報へのアクセスの問題は別の話ではないかと感じる。決算情報、事業計画などでどのような数値が出るか、どれくらいうまくいっているのかということは、ガバナンス上把握しなければいけないが、そうした情報が CI になるとは考え難く、前回提示された経済安全保障上重要な情報の候補にも当然入っていない。ガバナンスを効かせるために CEO らが秘密情報にアクセスすることが必須であるかは、別の問題として議論する必要があるのではないか。現状でも、日本企業が他国でクリアランスが要求される事業を行っている場合、日本人の役員では当該国のクリアランスが取れないはずなので、海外子会社の事業とし、当該子会社に所属する現地人のクリアランス保有者が事業の内容を見て、日本の本社は、数字やアクセス可能な範囲の情報で事業実績を判断しているということだと思う。また、単なるアイデアだが、代表権を一人に限る必要はないので、専務などに代表権を与えてクリアランスを取得させ、ボードメンバーの中で CI を扱う部門を担っていただくなどすれば、常に CEO ないし社長にクリアランスが必要という設計にする必要はないのではないか。今、日本企業には外国籍の CEO や社長も多いと認識しており、その方たちに誤ったメッセージを与えてしまうと良くない一方、国際的な制度との整合性も必要という観点で悩ましい問題だと思う。

○　アメリカでは、取締役会議長や CEO は、CI であっても自分に共有しろと言える権限がある。もちろん、アメリカの会社の中にも、カウンター・インテリジェンス部門の人間がいるが、見ていないところでやられたら、それを発見できない恐れがある。CEO として情報を触れる必要があるのかないのかという話ではなくて、そういう権限がないならば CEO の意味がないというのがアメリカ人の理解であろう。だから、最低限、CEO と取締役会議長には、クリアランスがないと、なんの仕事もできないということになる。軍事情報であれば、具体的な数字を見ることで機微なことを類推できる場合があり、そうした情報を、セキュリティ・クリアランスを持っていない人間に見せられるわけがない。単なる数字や決算情報といった話とは違う。この点も次回共有できるようにしていただきたい。

○　アメリカでの運用を確認することが重要。現実的なクリアランス制度が議論しづら

い状態になってしまうと、制度が機能しなくなってしまうので、よく検討する必要がある。

○　事務局資料 12 ページの「海外の制度概要」に経営陣への言及があるが、「経営陣」の範囲などについて、各国別にもう少し詳細なものを見せていただきたい。罰則の各国比較も簡単でいいので示していただきたい。

○　セキュリティ・クリアランスを取れなかったことが企業の経営にどう影響するのかを知るため、アメリカの連邦証券取引委員会のデータベースで検索したところ、ファシリティ・セキュリティ・クリアランスを取得できなかったことから運営ができなくなったことが、重大な経営上の問題になり得ると記載されていた。

○　こうした点は、防衛産業は慣れていて積み重ねがあるが、今度のファシリティ・セキュリティ・クリアランスにおいては、十分に説明を尽くしていかないとなかなか理解が広がるものではない。経営にも直結するので、施行準備期間を長くとって、経済団体や産業界に説明していく必要がある。

○　現在の特定秘密保護法における施設クリアランスについても、窓を作ってはならない等の要件があったのではないか。

防衛装備庁より回答

○　施設クリアランスとして防衛省で見ているのは、秘密の取扱い施設の構造だけではなく、保全責任者としてどのような者が指定されるか、取扱者のリストが用意されるか、企業としての保全体制をどのような規則に基づいて作っていくのか、教育をしているのか、といった点がある。その上で、実際に秘密を取り扱う施設をどのように作っていくかというと、御指摘のように基本的に窓がないことを念頭に置いているものの、やむを得ない場合には、曇りガラスにするなり、窓から出入りができないように鉄格子を設置するなりすることになる。また、出入口を原則１か所にすることといった基準が作られている。

○　先ほど他の委員から「合わせ技」で信頼を得ればよいのではないかという話があった点に関し、おそらくアメリカに対してはそれなりの相互のやり取りがあるため、ある種の相場観があると思うが、今後の経済安全保障上の重要機微情報に関しては、アメリカだけではいけないのではないか。例えば、防衛の特定秘密保護法の話になるかとは思うが、GCAP のようなイギリス・イタリアといった国々との関係や、将来的には AUKUS でのいわゆる新興技術を含めた技術協力だとか、そういったことに広がりが出てくることを考えると、日米間特有の理解が他国に共有されるかどうかと

いうことは考えておくべきだと思う。

○　現行制度が、防衛省に関する秘密や特定秘密保護法など色々な仕組みが重なっていて分かりにくい構造になっているがゆえに、細心の注意を払っていかなければいけないというところはあると思う。そういう意味で、罰則の問題についても、例えばConfidential の扱いについて、可能な限り一貫性を持った説明が可能になるように、注意しながら立法を進めていただきたい。

○　資料 14 ページについて、先ほど他の委員から罰金額が低いのではという指摘があったが、不正競争防止法には第 22 条に両罰規定があり、法人に 10 億円以下の罰金が科される場合がある。こうした両罰規定の存在についても合わせてまとめていただけるとありがたい。

○　実質的同等性の確保という観点から海外との比較が大事だと考えており、その一つの重要な要素が罰則の程度だと思う。その意味で、罰則の諸外国との比較は、必要条件だと思う。ただし、国によって法体系が異なり、軽重の付け方はそれぞれの国の思想に拠るところもあるので、単純に同じ年数でなければならないと言うつもりはない。

○　不競法の罰則は徐々に上がってきており、比較するタイミングで異なってくる。セキュリティ・クリアランスについても同じようなことが言えるのかもしれない。

（４）堀井副大臣挨拶

○　本日は、御多忙の中、第８回有識者会議に御出席いただき、感謝申し上げる。
○　皆様の活発な御議論を伺って難しい論点も様々あるが、政府として制度の実現に向けて最大限努力してまいりたいとの思いを新たにした。
○　本日いただいた御意見を参考にしながら、引き続き法案提出の準備を進めるべく更に検討を深めてまいりたいと考えているので、今後とも皆様方の活発な御議論をお願い申し上げる。