「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１回）議事要旨

１　日時

令和５年２月２２日（水）１１時４５分から１３時００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）

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
小柴　満信	経済同友会 副代表幹事
境田　正樹	TMI 総合法律事務所 パートナー弁護士
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
星野　剛士	内閣府副大臣
瀧澤　裕昭	内閣情報官
井上　裕之	内閣府審議官
岡野　正敬	内閣官房副長官補
髙橋　憲一	内閣官房副長官補
泉　　恒有	内閣官房経済安全保障法制準備室長
飯田　陽一	内閣官房内閣審議官
高村　泰夫	内閣官房内閣審議官
佐々木啓介	内閣官房内閣審議官
品川　高浩	内閣官房内閣審議官

４　議事概要

（１）高市経済安全保障担当大臣冒頭挨拶

・　第１回「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」を開催する運びとなった。御多忙の中、有識者の委員をお引き受けいただいたことに感謝申し上げる。
・　「セキュリティ・クリアランス」については、昨年末に閣議決定した「国家安全保障戦略」においても、「主要国の情報保全の在り方や産業界等のニーズも踏まえ、セキュリティ・クリアランスを含む我が国の情報保全の強化に向けた検討を進める」とされており、重要な課題と認識している。
・　こうした中で、２月１４日に開催された経済安全保障推進会議において、岸田総理から、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法整備等に向けた検討を進めるための有識者会議を立ち上げ、今後一年程度を目途に可能な限り速やかに検討作業を進めるよう、私に対して指示があった。
・　先進諸国では、「一定の経済に関する事項を含む重要情報を取り扱う者」に、「セキュリティ・クリアランス」を付与する制度があるが、日本では同様の制度となっていないこともあり、海外における政府調達や民間企業間の取引においても、日本企業が不利な状況に直面するケースもあると承知している。
・　例えば、日本企業の従業員にセキュリティ・クリアランスがないために、ビジネスに必要な重要情報を得られないなどの例もうかがっている。今後、日本企業がビジネスチャンスを失ったり、共同研究から外されるようなことがあってはならない。
・　皆様におかれては、我が国にとって望ましい制度の実現に向け、忌憚のないご意見を賜りたく、よろしくお願い申し上げる。

（２）座長の互選・座長代理の指名

委員の互選により、東京大学未来ビジョン研究センター教授の渡部俊也委員が座長に選出された。また、会議に座長代理を置くこととし、座長により鈴木一人委員が指名されたが、鈴木委員は欠席であったため、事務局において鈴木委員の意向を確認することとなった。

（３）会議の運営

会議の運営について、以下のとおり決定された。

・　会議は、非公開とする。
・　会議の議事要旨は、原則として、会議終了後、発言者名を付さない形で、速やかに公開する。
・　会議における配布資料は、原則として、会議終了後、速やかに公開する。
・　会議の内容については、会議終了後、事務局が記者ブリーフを実施する。

（４）事務局説明

事務局から、資料３の内容について説明があった。

（５）自由討議

○　肝は「相手国から信頼されるに足る実効性のある制度」という点であり、日本だけの内輪の議論で制度を決めても、米国を始めとする諸外国に信頼されるものでないと意味がないのではないか、という問題意識を持っている。

○　国家安全保障戦略においても、産業界のニーズのみでなく、「主要国の情報保全の在り方」を踏まえるという言葉が入っているところが非常に重要だと考えている。本日の資料１にあるこの有識者会議の開催趣旨にも国家安全保障戦略とほぼ同様の内容が盛り込まれているので、この観点で皆様と議論をしていきたいと思っている。

○　産業界のニーズについて悉皆的な調査をしたわけではないが、明らかにニーズはある。ただし、発言する方によって制度のイメージが少しずつずれているという印象を持っている。

○　そういうこともあって、資料３の３ページにあるとおり、「いわゆるセキュリティ・クリアランス」という言い方になるのだと思うが、いずれにしても、やはり、諸外国から信頼に足りるものだとみなされなければ実効性のあるものにならないと思っている。そうした前提に立って、ニーズと制度をどのようにリンクさせていくのか、ここがまさに大きな論点だと思っている。

○　世の中が変わり、経済安全保障は非常に重要なイシューと捉えており、政府で経済安全保障推進法やセキュリティ・クリアランスについてディスカッションされることは、非常に良いことだと考えている。我々としてもこうした議論を進めていきたいと考えている。

○　国家の安全を考えたとき、テクノロジーは今までと違う位置付けを持っており、これを「政治がテクノロジーと出会う時」と表現している。

○　テクノロジーは大きな転換期を迎えている。量子コンピューティングのような次世代計算基盤が大きな意味を持ってきており、これがなければ、ＧＸやカーボンニュートラルなど色々なことが達成できない。したがって、ここがまず一つの切り口になると考えている。より具体的に言えば、その根底にある半導体と量子技術が重要。

これは日本一国ではできないので、日米、さらにはライク・マインデッド・カントリーとの連携で巨額のＲ＆Ｄ費用や社会実装費用を分担しながらやっていくことになる。その上で、当然ながら情報を守るというところがポイントになってくる。

○　具体的な直近の問題を挙げると、最先端半導体や量子分野における日米協力が、おそらくまず一つの成功例になっていく。そうした研究をする所のＩＴインフラ、サイバーセキュリティに関しては、今までとは違うレベルのセキュリティが必要となってくる。また、これらに関わる研究機関、特に国研や大学における留学生を含む人たちのバックグラウンドチェックや継続的なモニタリングといったものが新たに求められるようになってくる。

○　おそらく実際のケースを想定して国の制度を検討していく方が、全体的・抽象的なディスカッションをするより速いと思う。

○　重要な課題だから１年をかけて議論をするという話であるが、そんなに悠長に構えていられる話なのかというと、必ずしもそうでもない。

○　量子技術と先端半導体、特に２ｎｍ以下の先端半導体の用途は、安全保障分野が大宗を占めるのではないかと推定される。

○　日米の半導体の共同開発といったものを実効的に実施していくためにも、まさにセキュリティ・クリアランスの仕組みが重要。

○　現在、我が国にセキュリティ・クリアランス制度が定められていないかというとそうでもない。特定秘密保護法という法律によりセキュリティ・クリアランスが定められている。ただ、分野が外交、防衛、防諜、テロの４分野に限られている。この４分野を拡張的に解釈するということも一つの考え方かと思うが、国際共同開発の分野で、どういった形で法的な手当てをしていくのかというのが一つの喫緊の課題だと思う。

○　今回は、特に経済界からの要望ということでもあるので、民間における技術をどういう形で守るのかということが非常に大きなテーマになってくる。

○　現在の我が国の法制度を考えたとき、民間の安全保障に関わる情報・技術の保全は、特定秘密保護法では非常に分野が限られているが、不正競争防止法もある。いずれの法律も上限１０年の拘禁刑が定められている。

○　諸外国とのレシプロシティという意味では、米国として関心を持つのは、サンクションがどの程度なのかと、審査がどのような形でなされるのかという辺りが肝になってくると思う。

○　今後の検討に当たっては、今我が国にある制度との連続性も問題になってくるわけで、特定秘密保護法や不正競争防止法との関係をどう整理するのかも大きな論点だと考える。

○　先般あった経済安全保障関係のシンポジウムで、米国高官が、どういったところを経済安全保障で守っていくのかという議論の中で、「Small yard, high fence」だと言っていた。経済が相互依存を強めている中で、真に守るべき分野は何なのかを限定し、そこについては厳重な鍵をかけるということが一つの指針ではないかと思う。セキュリティ・クリアランスの法制度においてもこういったことが極めて肝心と考える。

○　経済安全保障推進法は誠に時宜を得た法律で、今着実に施行されているが、セキュリティ・クリアランスについても、産業界のニーズ等も紹介されており、政府の意向もあり、大変なニーズがあるということは分かった。

○　ただ、周辺に聞くと、このセキュリティ・クリアランスは、一部の人を除きなじみがない制度であり、知らない人がほとんどである。それを踏まえると、制度の検討・導入を進める上で、必要性や制度がどういうものであるかについて、国民や一般的な企業にとって分かりやすい説明をしていくことが大変重要である。

○　この制度は、日本の経済安全保障、日本の安保を守るために必要であるということをぜひ言っていただきたいし、そういう検討を進めていただきたい。また、それを示すための立法事実も必要であると思う。

○　近年日本の企業の先端技術の管理体制が不十分で、海外に流出する事例は大変多いと認識しているし、不正競争防止法については、法改正はあったものの、刑事罰はまだ不十分だとの指摘もあるので、海外流出のリスクのある技術を持つ企業への対応が重要と考えている。

○　米国にあるセキュリティ・クリアランスを日本が持っていないため、共同プロジェクトに参加できないという議論も大変重要だとは思うが、日本の安全保障にとってこういう制度が要るのだという議論も十分に尽くしていただきたい。

○　他国の制度がどうなっているかということについては他の委員からも発言があったが、まず米国でどうなっているのか、その制度概要や運用は大変参考になると思うので、ぜひそのうち紹介してほしい。米国に加え、やはり欧州、特に高い技術力を持つ中小企業も多いドイツなどの制度も、日本と産業構造が似ていることから参考になると思うので、できればそういうデータ等もこれから紹介いただければ大変参考になると思う。

○　日本の中で先行的な制度になるのは、特定秘密保護法だと思う。外交、テロ、防衛の対策に関わる重要な秘密が漏洩した場合、これが懸念国に出たら大変なのは当然だと思うので、そういう情報を取り扱う従業員、特に公務員に対して適性評価を実施しているが、その運用状況や政策の効果も大変参考になると思う。難しい面もあるとは思うが、いつか紹介していただければありがたい。

○　繰り返しになるが、日本企業のニーズに応えることも大変ありがたいことではあるが、あわせて、日本の安全保障のためにこの制度が必要だということを掘り下げて検討していただければと思う。例えば、経済安保の中で官民重要技術のプロジェクトでデュアルユース技術がこれからいっぱい生まれてくると思う。量子技術などもそうだが、そういうものが、日本の暗号、世界の暗号技術に大きな影響を与えるとなると大変なことなので、これを取り扱う方々に対しセキュリティ・クリアランスが必要ということ、あるいは、特許の非公開制度も今回導入されたが、これも安保の観点から、限定的ではあるものの、大量破壊兵器関連の発明は非公開になり得る。こうした技術を取り扱う人について一定の信頼性、適性というものを確認することはやはり必要だと思う。そういう観点からの検討もしていただくことによって、国民の理解も得られる制度ができてくるのではないかと期待している。

○　日本の大学のランキングがどんどん下がっていく中、日本の社会の課題に対して大学は何をできるか、何をすべきか、という観点から考えてきた。そして、今後は知識集約型社会、データを解析してそれを次の産業につなげていく、もしくは、軍事力などの国力の評価につなげていくというところで役に立てるのではないかということで、例えば大学と外国企業とのゲートウェーを作ったり、量子コンピュータのパートナーシップを作ったり、そうした様々な試みをしてきた。その中で気づいたのは、相対的になぜ日本はここまで弱くなったのかということ。中国のＧＤＰは今や日本の３倍以上になり、博士人材も圧倒的に中国の方が多い。インパクトファクター、引用される論文の数でも大きな差がついている。今でさえ差がついているのだから、おそらく１０年経ったらもっと差がつくのだろう、ということである。

○　ご案内のとおり、外国の中には軍民融合という考え方の国もある。民間の技術も全て国力のため、産業、イノベーション、軍事という全てのところで一体となって国力を上げる。他方で日本はどうかと言うと、そこは基本的に圧倒的に弱い。産業界、アカデミア、政府のコラボレーションが非常に弱いと思う。

○　特に先端分野の話があったが、デジタルの世界は、データを集めれば根こそぎ産業を持っていける、他国の経済領域をどんどん侵食できるという特性がある。ここの備えも実は日本はまだまだ弱いと思う。そういう意味で今回の高市大臣が主導されているセキュリティ・クリアランス制度は、こうした日本の弱みを解決する第一歩ではないかと思っている。

○　大学には基本的に軍事研究禁止という思想があり、そういった分野には協力しづらいという環境もある。また、基本的にプロジェクトベースというより、個々の研究者が予算を取って自分の研究をやるので、国のために何が必要かという形での研究を組成していくのは非常に苦手であり、こういったところも変えていかなくてはならないのではないかと考えていた。

○　海外企業と日本の研究機関との間の共同研究契約などでは、不平等な内容の契約になっていないのかを精査する必要があると考えている。つまり、実は日本のセキュリティ・クリアランスの体制が甘いから、もしくは無いから、不平等な形の研究契約になっているのかもしれない。

○　国立研究開発法人は、元々国にあった研究機関を外出ししたことと、国がそもそもマネジメント人材を十分に育ててこなかったという経緯もあるので、今でもいくつかの国立研究開発法人においてマネジメント人材が十分に足りていないのではないかと危惧している。具体的には、法務分野、知財分野、研究倫理分野、経済安全保障分野、外為法分野等に精通した人材である。そういった中で、これから国研が次世代の量子や半導体の重要部分を担うときに、そこのマネジメントがしっかりしていないと国益を損ねるということになるため、ここは非常に注意していかなければならない分野なのではないかと思う。

○　今回は画期的な取組だと思うので、貢献していきたい。

○　経済安全保障推進法の法制化に際しては、民間事業者の自由な経済活動を極力阻害

しない範囲にとどめることや、新たな規制と既存の規制の役割を明確にし、労働者も含め現状と比して過度な負担とならない配慮が必要であると考える。

○　その観点からすると、セキュリティ・クリアランス制度は、資料３にあるとおり、政府が、民間企業の労働者も含めた個人に、信頼性を確認した上で情報へのアクセス権を付与し、当該情報が漏えいした場合には厳罰を科すことが通例とされており、これまで法制化された事項と異なり、対象となる労働者の範囲や労働者に与える負担の大きさが相当程度大きなものになると感じている。

○　今後の検討に当たっては、特に労働者に与える影響について、相当に慎重に検討を重ねていく必要があり、その事を要望として申し上げておく。

○　第一に、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を検討するに当たっては、米国における同様の制度を参考にして検討すべきであると考えている。なぜならば、我が国の企業が米国政府の機微な情報を扱う調達案件の入札に参加しようとする場合、米国のセキュリティ・クリアランス制度を遵守しなければならないし、量子暗号のような国家安全保障に関わる機微技術に関して米国との国際共同研究を推進する場合も同様であると思う。

○　したがって、今回、ある分野におけるセキュリティ・クリアランス制度の構築について、米国の制度より緩いものを検討したとしても、米国との情報共有ができないことになり、現実に機能しない結果を招くと考えている。

○　第二に、今回の法制度検討に当たり、米国の機密情報に対応したセキュリティ・クリアランスのみならず、機密情報には該当しないものの一般市民への情報開示が制限されるＣＵＩ（Controlled Unclassified Information)、すなわち管理された格付け情報と呼ばれる米国の情報保全制度に対応した制度を構築する必要があると考えている。特に日本企業による米国政府調達の入札要件として必要になる。なお、このＣＵＩに関する情報保全制度は、米国では一般に「セキュリティ・クリアランス」とは呼ばれていない。

○　また、米国国防総省は、ＣＭＭＣと呼ばれるサイバーセキュリティ成熟度モデル認証を２０２５年１０月から全ての入札の要件とすることを予定していることも考慮する必要がある。

○　セキュリティ・クリアランスは、情報保全の仕組みとしてとても大事だと思う。そ

の上で、私はスピード感がいると思う。今回、１年を目途ということで話があったが、やはりスピード感を持つのであれば、例えば毎年６月には政府から骨太の方針が示されるが、その中で、ある程度の方向性を盛り込むぐらいのスピード感が必要である。

○　これまでこの会議以外で色々な方の議論を聞いてきたが、セキュリティ・クリアランスについてはいくつかの目的が混在しているため、まずは目的を明確にすべきである。その意味で、事務局資料３の３・４頁は大変大事な整理をしていただいていると思う。他の委員も指摘しているとおり、基本は日本の安全保障のためにやる仕組みであり、日本国として守らなければならない情報にアクセスする必要がある者に対して与える資格であるという基本は、しっかり押さえておかなければならない。

○　その上でもう一つの目的として、産業界の方々から要望がある、日本企業が海外でビジネスを広げていくこと、これも大事なポイントだとは思う。例えば、先ほど調達の話も出ていたが、米国防総省の調達に参加するために必要だという話もある。ただ、気をつけなければならないのは、このセキュリティ・クリアランスの制度で即こういうことに参加できると思ったらそれは間違いだということ。セキュリティ・クリアランスというのはそのための必要条件であって、十分条件ではない。

○　ではどうすればいいかと言うと、そこをブリッジするには、軍事の分野にはＧＳＯＭＩＡというものがあるように、経済安保の世界でもそういう国際協定がもう一つなければ海外ビジネスの展開にはつながっていかないということを頭に置いた上で、そこも含めて考えていかなければならない。

○　経済界からも指摘があるように、主要国、特に米国との実質的同等性をどう確保するかというのが最大のポイントだと思う。そのとき、先ほど他の委員から特定秘密保護法の話もあったが、これまでの４分野に加えて経済安全保障という部分にどう広げていくかというのは最大の課題、焦点だと思う。そのとき、これまでの特定秘密保護法を防衛省は大変着実に実施してきたと思うが、これを経済安保に広げたときの課題として二つ見えてくる。一つは、罰則が最大１０年というそこそこ重い罰則であることから情報指定が極めて抑制的になっている。そうすると、経済安全保障の世界になったときに、情報の機密性の程度に応じた区分がなされていない結果、１０年という重い罰則だけになってしまう。この点、米国では、Top Secret, Secret, Confidential と区分されている。今後、機動的に経済安保でも使っていく上で、このままでいいのかということも考えなければならないと思う。

○　また、経済官庁が大事だと思うが、バックグラウンド、信頼性の確認というものが各省バラバラではいけないと思っている。経済官庁も役所側として色々と関わる。一応の統一基準というものは作られているが、正直申し上げて、これが役に立っていないのではないか。経済界のニーズも聴取すべきだが、経済官庁からも具体的にどのようにこれに取り組んでいくのかを、自分のこととして、内閣官房にお願いしておけばよいということではないと思うので、ちゃんとそういうところの関わり、心意気を見せてほしいということで、そういうヒアリングも必要であると感じている。

○　今回、セキュリティ・クリアランスというものについてニーズを踏まえて制度設計を考えていくときに、それぞれの立場からそれぞれの考えていることが少しずつ違っており、色々な変数があるのだろうということで、今、私自身も悩んでいるところである。例えば、他の委員からも指摘があったが、そもそも目的がどこにあるのかというところで、いわゆる安全保障に重きを置いた目的で、一定の安全保障上機微な情報にアクセスするときの資格という風にみるのか、もしくは、国際的な研究のような場面での研究目的で、機微情報を扱う資格と見ていくのかによって、これまでの日本の既存の法律との整合性という点でも、見るところが大きく変わってくると個人的には思っている。

○　日本の重要な技術情報、それから安全保障に関連する情報を海外に出していく場面に重きを置いて話す場合もあれば、海外の重要な情報に日本の民間企業がアクセスするときの「入場チケット」という観点で見る場合もあり、これも考慮要素が異なり、どういう既存の法律との整合性を考慮するかが変わってくるのだと思う。外に出していく部分では、例えば外為法のみなし輸出における技術情報輸出の考え方や、民間事業者の情報であれば不正競争防止法上の営業秘密とも関連してくる。他方、海外の情報にアクセスする部分では、おそらくこれまで日本の法制上あまり直面していなかったところであり、私なりに悩んでいる。

○　また、目的と関連して、国家安全保障戦略や経済安全保障推進法の考え方に出てくる優位性、不可欠性の確保の概念を意識することも重要だし、むしろ自律性の確保の話も出てくるのではないかとも思う。

○　さらに、より直近の議論をみると、いわゆるクリアランスの認証制度に重きを置いた議論になるのか、そうではなく情報の中身が問題になるのか、こういったところを、色々と言われているニーズも踏まえながら、変数は多いけれども議論を重ねて整理し、望ましい制度設計を考えていくことが必要ではないかと考えている。

○　米国を含めた海外との相互の認証は大前提になると思われるので、その意味では、海外当局との議論も踏まえながら考えていくことが必要となるのではないか。この点、直近では、例えば、一般データ保護規則（ＧＤＰＲ）という欧州のデータプライバシーに関する強い規制が導入された際、日本政府はいわゆる十分性認定において、同程度の保護が得られる個人情報保護法がありますということを言って、ＥＵと日本との間で個人情報のやり取りがスムーズにできるようになった。こうした相手国との相互認証を取りに行く前提での交渉が行われており、こういった事例は今回のテーマとも親和性があるのではないかと思う。

○　プライバシーの問題や労働法の問題については他の委員からも話があったが、やはり慎重に考えなければならないところはあると感じる。他方で、今回の制度の必要性や合理性、もしくはプラスとなる部分も多くあると認識しており、既存の労働法制、プライバシー法制の中でも、もちろん一線を越えてはならない部分はあるにせよ、何らかの形で制度設計をしていくことが出来るのではないかと直感的には思っており、今後議論させていただければと思っている。

○　経済安全保障の観点からセキュリティ・クリアランス制度をもって保護すべき重要な情報・モノとしては、政府が定める２０の重要技術分野に関わる情報や技術ということになるかと思う。セキュリティ・クリアランスの基本は戦略的不可欠性を高めるための措置であると同時に、他国に流出することで、我が国の安全保障を脅かすことになる技術が対象となるべきだと考える。

○　日本企業が外国でセキュリティ・クリアランスを求められるのは、外国における高度な技術を含む共同研究を実施する場合や、安全保障に関連する装備の共同開発といった場面になると思う。また、防衛に限らず、重要インフラの保護なども含む外国の安全保障に関わる調達における入札をする際にも、セキュリティ・クリアランスの整備が求められることになるかと思う。この場合、共有すべき情報に他国における防衛機密や安全保障装備に関する機密が含まれる場合が対象になると考えられる。さらに日本における情報保全の在り方、例えばサイバーセキュリティのレベルなどが問われることになるかと思う。

○　セキュリティ・クリアランスは、あくまでも日本政府が日本国内の技術者・研究者に対して行うものであるため、国際的な共同開発や外国における調達への入札に参入することは、日本企業による国際ビジネスに不可欠なことと考える。そのためには、外国におけるセキュリティ・クリアランスと同等のものを実施し、その同等性を確保することによって、外国でのビジネス活動を可能にするような制度であるべ

きと考える。

○　セキュリティ・クリアランスは外国での機微な情報を含むプロジェクトに参加するための「入場券」であり、その入場券として適切だと考えられるレベルの制度にならなければ、産業界に対する負担ばかりが大きくなる結果になると思われる。セキュリティ・クリアランスに関しては、個人のプライバシーへの配慮とのバランスが重要と思われるが、あくまでも、これは外国での活動に参加するための「入場券」であるため、その「入場券」を必要とする人が受けるものであり、それを必要としない人に広げるものではない、ということになるかと思う。

○　事務局資料３の３頁に「いわゆるセキュリティ・クリアランス」ということで「いわゆる」が付いているが、この部分について各委員からかなり多様な意見が出ていると認識している。基本的には、ここに書かれている枠組みであれば、政府の保有する重要な情報を指定して、それに民間含めアクセスしようとする者に対して行う措置、アクセス権を付与するための資格ということであり、その際、客体というか、どういう情報をどういう理由で国が提供する必要があるのかというところだけはっきりさせれば、おそらくそれほど制度設計は難しくないはずだと思う。

○　しかしながら、一方で、民間のニーズと言われているものがかなり多様であり、日米英等のプロジェクトで必要になるという話とか、あるいは、セキュリティ・クリアランスをもってアクセスできる情報自体にアクセスする必要があるということ以上に、セキュリティ・クリアランスというものが他でも役に立つということ、いわば運転免許証を持っていることが運転以外の場面でも役に立つというのと同様のニーズも含まれていると思うし、また、ＣＵＩの話があったが、これは一般的には「セキュリティ・クリアランス」とは米国では言われていないと思うが、確かにここも米国と連携していく上でかなり重要な論点となり得ると思う。

○　したがって、「いわゆるセキュリティ・クリアランス」の範囲をどこまで含めるのかということ、また、そこから漏れたものが必要ないというわけでもなく、民間のニーズにはかなり重要なものも含まれていると思うので、それはどうするのかということ、そこを整理する必要があるのではないかと思う。

○　セキュリティ・クリアランスには、先ほど言われたように、Top Secret, Secret, Confidential の３つのクラスがあるということも含め、諸外国の制度をしっかり精査する上で、バウンダリー（境界、射程）を整理することが必要。

○　既に指摘があったように、民間の方が対象になるものであるから、調査方法とプロセスについては、当然プライバシーとか点検場面とか様々な配慮点があると思うが、そこまでここで議論するのかどうかということについても整理する必要があると感じている。

○　今の段階ではまだ話すのが早いかもしれないが、スタート時点で何をやるのかという論点もある。例えば、特許非公開制度では、スタート時点ではここに絞ってしっかりやるという考え方が言われているが、今回ももしスピードが必要なのであれば、そのような考え方も必要かもしれない。

○　米国では、企業に対する外国関係者による所有、支配又は影響、いわゆるＦＯＣＩ（Foreign Ownership, Control or Influence）と言われている制度があることを考慮する必要がある。

○　セキュリティ・クリアランスを受ける労働者のプライバシーの保護を念頭に、複数レベルのセキュリティ・クリアランス制度を検討すべきである。特定秘密保護法には一種類しかない。米国では科学者・研究者に対するセキュリティ・クリアランスのレベルは、最高レベルの機密（Top Secret）情報に対するものではなく、極秘（Secret）・秘（Confidential）のレベルに対するものである場合が多いので、我が国もプライバシー保護の観点からこれを検討すべきである。

○　我が国の重要インフラを担っている企業の労働者等のうち、サイバーセキュリティに従事している方々のセキュリティ・クリアランスについては、インテリジェンス機関との情報共有やサイバー攻撃事案に対する緩和策を攻撃者等から秘匿するため、機密情報に対応した最高レベルのセキュリティ・クリアランスを要件とすることを検討すべきである。この対応により米国との情報共有が可能になる。

○　セキュリティ・クリアランス等を受ける労働者に特別手当を支払うことを検討すべきと考える。米国で機密（Top Secret）レベルのセキュリティ・クリアランスを持つ労働者の平均賃金は、日本円換算で１３００万円を超えている。負担ばかりを労働者に課すのは不適切であり、これに報いる在り方というものも考えるべきである。

○　設置が検討されているサイバーセキュリティ事故調査委員会の民間委員については、セキュリティ・クリアランスを要件とすべきである。米国でも同様の制度となっているとともに、我が国でも昨年、有識者会議において、産業界の委員から同じ見解が述べられている。

○　先ほど他の委員から、スタート時点で何をやるのかという話があったので、それに関連して申し上げると、今回どれぐらいの規模感をもってやるのか、米国のようにクリアランス保有者４００万人という規模感で臨むのか、あるいはこれぐらいのレベルからというように臨むのか、これによって全然違ってくると思う。というのも、専門的な背景調査ないしバックグラウンド調査には人と金が相当かかるわけで、国の限られたリソースの中でどういうふうにプライオリティを置いてこれに取り組んでいくのか、という視点で見て行かなければならないと思っている。そういう意味では、先ほど述べられたようなスタート時点でどうするのかを考える上で、限られたリソースの中でどうしていくかということも、今後の視点として必要ではないかと思う。

（６）星野内閣府副大臣挨拶

・　本日は、第１回「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」に参加をいただき、感謝申し上げる。
・　本日皆様からお寄せをいただいた様々な知見、すなわち諸外国でセキュリティ・クリアランスの保有を求められる事例や、経済安全保障の観点から保護すべき重要な情報などについて様々な観点から貴重なご意見・ご示唆を頂戴した。
・　本日の議論を踏まえ、政府としても、委員の皆さまのご知見をお借りしながら、我が国にとって望ましい制度の実現に向けて、しっかり検討してまいりたいと考えている。
・　今後とも活発なご議論のほどよろしくお願いする。