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３回）　議事要旨

１　日時

令和５年３月２７日（月）１６時００分から１８時００分までの間

２　場所

中央合同庁舎８号館　共用会議室Ｃ

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
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
星野　剛士	内閣府副大臣
中野　英幸	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
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）事務局説明

事務局から、資料１・２の内容について説明があった。

（２）企業からの説明

電機メーカー・Ｃ社から、資料３の内容に基づき、経済安全保障分野におけるセキュリティ・クリアランスをめぐるニーズや具体的事例、課題等について、以下の説明があった。

○　２ページについて、当社の基本認識としては、このような大きな政策的な動きが出るということが、日本が置かれた経済安全保障環境が厳しいものであると認識。
○　３ページについて、防衛及び経済安全保障に関連する領域が拡大してきており、その技術が急速に進展・高度化している中で、特にＡＩ、量子、半導体、コンピューティング、デジタル技術といった分野など、当社も注力する技術分野が、防衛及び経済安全保障分野において重要性を増していると認識している。
○　一方、こうした環境の中で、同盟国・同志国との連携がより重要になってくるということで、各国政府間での取組みも進んできている。そうした中で、民間企業の立場からも、外国政府が保有している情報を共有・開示していただくことで、様々な役割を果たしていけるのではないかと考えている。
○　セキュリティ・クリアランス制度は、政府が保有する情報を、どのような条件でどのような制度で開示していくかというものだと認識しているので、こうした制度が検討されていること自体は歓迎しているが、どのような中身とするかは、政府において考えていただくことだと考える。
○　４ページの課題認識について、現状の日本における秘密の保持は、個々の契約ごと、あるいはプロジェクトごとに、契約により担保されている形になっている。資格要件となるベーシックな制度にはなっていないということが、１つの問題認識。
○　外国政府の安全保障に関連する情報について、アクセスが制限されており、その点についてのビジネス上の障壁も大きい。
○　また、今後、共同開発・共同研究が増えていくであろうことから、当社としても、これらに対して円滑に参画できるような制度的な枠組みが求められていくことになると考えている。
○　期待として、外国の政府との間での合意の下ではあるが、企業間での相互の情報共有が円滑になることがある。実際、外国政府が保有する機微な情報についてのアクセスが得られず、日本から効果的な提案ができなかったことや、外国の企業が保有

している機微な技術が得られないために、日本側で効果的な活用ができないなどの課題があった。

○　ファイブ・アイズの中の国では、一定程度の情報共有がなされていると聞いているが、具体的にどのようにされているかについては承知していない。

○　セキュリティ・クリアランス制度により、そうした情報へのアクセスの質が向上することで、日本企業としてグローバルに経済安全保障分野に貢献することができ、成果物にかかるＱＣＤ（クオリティ、コスト、デリバリー）が向上するのではないかと考える。

○　また、様々なサイバーセキュリティ・インシデントが起きている中で、政府側が保有している様々な情報を開示していただければ、会社のセキュリティレベルの向上につながるだけではなく、新たなセキュリティ・テクノロジーの提案をすることもできると考えている。

○　最後に、５ページの要望について、これまでの議論のキーワードともなっている諸外国との実質的同等性を確保するとともに、経済活動への阻害にならないよう、また、日本においての労働法制との調和という関係も課題としてあがってくるのではないかと考えている。

（３）意見交換

○　ファイブ・アイズに属する国家間において、どのような情報が共有されているかは明らかではないが、サイバーセキュリティに関する情報は広く共有されていると思われる。その上で、本日の資料１（第２回会議の議論の整理）でも言及されているＩＳＡ（Industrial Security Agreement；産業保全協定）が、二国間で相互にセキュリティ・クリアランスを認め、機密指定された情報を共有するための協定となる。また、ＮＴＩＢ（National Technology Industrial Base；国家産業技術基盤）に加入しているアメリカ、カナダ、オーストラリア及びイギリスは、ファイブ・アイズからニュージーランドを除いた構成になっている。ニュージーランドが加入していないのは、同国に、それほど大きな先端技術産業がないためではないかと推測される。資料１の２ページでは、「加入したアメリカ現地法人は、ＣＩ（Classified Information）にアクセスするためのＮＩＤ（National Interest Determination；国益決定プロセス）に関する承認手続が免除されており、円滑にＣＩへのアクセスが可能」とあるが、少し説明を補足する必要がある。例えば、日本とアメリカが一般的なＩＳＡを締結しても、ＩＳＡでアクセスできるのは、アメリカの制度上、通常は極秘（Secret）までとなっていることから、これ以上のレベルの機密（Top Secret）等にはアクセスすることができない。アメリカ政府が、機密（Top Secret）や機微区画情報（Sensitive Compartmented Information）等の高い機微性をもつ規制対象情報（Proscribed Information）まで、外国に親会社が存在するアメリカ

子会社と共有することを認める決定がＮＩＤである。ＮＴＩＢに加盟している４か国については、2019 会計年度国防授権法第 842 条により、2020 年 10 月１日から、国家産業保全プログラム（National Industrial Security Program）の下で特別保全合意（Special Security Agreement）を締結している加盟４か国に親会社があるアメリカ子会社に対して、規制対象情報にアクセスするために必要なＮＩＤプロセスが免除されることになった。

○　契約単位でない仕組みということを要望されているが、企業が保有している技術分野を包括的に指定するような仕組みをイメージしているのか。

企業より回答

○　資料２にもあるとおり、例えば、他国では、セキュリティ・クリアランスは一定年数有効な有期のもの。関係ないプロジェクトの情報に関係ない人が参加するということではないが、Need to know の原則の下で、プロジェクトに必要な単位の人間で情報共有できるような仕組みとしてほしいということ。

○　また、制度ができることの一番の効果は、お互いの情報共有をして、新しい提案をしていくということかと考えている。

○　セキュリティ・クリアランス制度ができた場合、どのくらいのレベル・職種の方が、どのくらいの規模でセキュリティ・クリアランスを取れば、海外でのビジネスがうまくいくと想定しているか。

企業より回答

○　想定を重ねることになるので試算はできないが、おそらく、日本のセキュリティ・クリアランス保有者を増やしていく方向になるのであろうと思う。海外と比べると、日本の方が、事業規模に比して、特定秘密保護法等のセキュリティ・クリアランス保有者が少ない印象があり、お互いの技術を交流させて様々な提案をするということになると、日本のセキュリティ・クリアランス保持者を増やしていく方向になると考える。

○　出口論になるが、要望事項として、個人のバックグラウンドは政府の責任で調査をとのことだが、例えばガイドラインのようなものではなくて、法律に基づいて政府が主体となって調査してほしいという趣旨で良いか。

企業より回答

○　御指摘のとおり、企業側でバックグラウンドを調べるのは難しいという印象を受けており、どういう項目をどう調べるかは政府側で決めていただきたいというのが希望である。

○　イメージが具体的になったと思う。審査基準の明確化という要望をしているが、事務局から諸外国の制度の説明があったが、例えば、どのような点が他国とは異なっているとお考えか。

企業より回答

○　従業員等がセキュリティ・クリアランスの審査を受ける際に、どういう事項を申請書に書けばいいのかということを、ある程度細かく規定してもらうというのが一番大きいのではないか。もちろん、どのような基準で許可するかは政府側で決めることだが、例えば、犯罪歴の有無ということは民間企業では把握できないので、そういったところは政府側でどのように手続されるのかといったことが明確になればいいかと思う。

○　セキュリティ・クリアランスを取得すればこうしたことができるといった話はこれまでもあったが、セキュリティ・クリアランス保有者に対する制限や制約などはあるのか。

企業より回答

○　例えば、イギリス法務省が昨年８月に出したガイダンスで、セキュリティ・クリアランスを保有している者は、北米、西ヨーロッパ、オーストラリア、ニュージーランド以外に旅行する場合には申請して承認を求めなければならないと承知している。

（４）永野委員からの説明

永野委員から、資料４の内容に基づき、米国におけるセキュリティ・クリアランス制度の基本情報や最新の動向について、説明があった。

なお、同資料の記載に加え、口頭で以下の補足があった。

○　（６ページの最下部に関し、）日本企業が共有できるとしても、一般的には極秘（Secret）以下の情報にとどまる。ただし、先端技術の共同開発等であれば、機密（Top Secret）の共有も想定し得る。

○　（７ページの「機微区画情報」に関し、）この区分は、機微性があまりにも高いため究極の Need to know が制度化されたものと考えてよい。

○　（８ページの「ＣＵＩ（Controlled Unclassified Information）に関し、）このＣＵＩとは、日本でいうと、省庁内限りの取扱厳重注意とされる情報に類似するものである。アメリカでは、かつてこのレベルの情報はＳＢＵ（Sensitive But Unclassified）と呼ばれ、省庁ごとにばらばらな類型の設定・指定・管理がなされてきた。しかし、そのせいで連邦政府内部における情報共有が滞り、アメリカ同時多発テロに関する事前の情報共有がなされなかった一つの要因にもなったとの指摘があり、連邦議会で改革の必要性が論じられたという経緯がある。

○　（13 ページの「第４段階」に関し、）この第４段階の記述は、原則に関する記述である。30 ページで「参考」とさせていただいた論文（下）の 243 ページにも記述しているが、民間企業（請負人）の被用者等の場合には、調査依頼を行った連邦行政機関の保全決定担当官ではなく、ほとんどの行政機関は、その判断を国防総省聴聞・不服申立部（Defense Office of Hearings and Appeals）に委託しており、専門性を有する保全専門決定者（security specialist adjudicators）が、セキュリティ・クリアランスの付与の適否について決定している。

○　（15 ページの「ＤＣＳＡ（Defense Counterintelligence and Security Agency；国防カウンターインテリジェンス・保全庁）が全連邦行政機関の約 95％の身上調査を実施している」との記載に関し、）ＤＣＳＡは、連邦行政機関の被用者の約 95％と、民間企業の被用者等のほぼ全てに対する調査を実施している。なお、残り５％は、別のセキュリティ・クリアランス制度によるわずかなものを除くと、自らセキュリティ・クリアランスを実施することが認められているインテリジェンス機関の被用者等であり、これは誰がそのインテリジェンス機関に所属しているかを他の行政機関からも秘匿することが必要なために認められている特例である。

○　（17 ページの「保全行政責任者指令第４号」に関し、）保全行政責任者というのは、インテリジェンス部門のトップである国家情報長官（Director of National Intelligence）のことである。

○　（19 ページの「定期的再調査手続」に関連し、）最新情報としては、昨年８月にＤＣＳＡの部局が事業者向けに発出した文書の中で、2023 会計年度限りを目標に、国家産業保全プログラムの適用を受けている民間の請負者等に対する定期的再調査手続を廃止するとともに、機密（Top Secret）から秘（Confidential）までの情報区分にかかわらず、全てのレベルのセキュリティ・クリアランスの自己申告書において機密（Top Secret）レベルで用いられている標準書式第 86 号（SF-86）を用いることとし、これを５年ごとに提出することを求めるとともに、継続的身元審査（Continuous Vetting）の要件に服することになるとされている。これは、アメリカにおいて、これまでの３段階の情報区分自体は文書管理等で維持されるものの、セキュリティ・クリアランスに関する限り、機微区画情報を除き、情報区分に対応した差異がなくなり厳格な機密（Top Secret）レベルにおける手続に統一することで、カウンターインテリジェンスが強化されること意味している。

○　（27 ページの「ＣＵＩ）に関し、）アメリカが全ての機微な技術をＣＵＩとして指定することができないのは、自国でこれらの技術を用いた製品を全て製造することはできず、日本の精密技術なども利用する必要があるためである。したがって、このような技術の多くはＣＵＩに指定されている。現在、アメリカでは、ＣＵＩに関する統一的な身上調査規定は存在していないものと思われ、その人的スクリーニング（バックグラウンド・チェック）は、個別の制度ごとに設定されているものと考え

られる。このため、今後、我が国の企業に対してアメリカのＣＵＩへのアクセスに必要となる制度等が導入されるような場合には、日本とアメリカの政府間でその内容に関する一定の交渉を行うことは可能であると思われる。

（５）質疑応答

○　ここでアメリカの制度を押さえておく意味は、アメリカから実質的に同等レベルの保護がなされているとみなされる制度を作ろうというのが共通認識であるからだと思っており、いずれの企業からもそのような話をいただいた。アメリカから実質的に同等レベルの保護だと見られるためには、日本とアメリカの違いはあるものの、どこが重要な点か。日本はアメリカのここを参考にして補強すべきだという点はあるか。

永野委員より回答

○　セキュリティ・クリアランスには、人、施設及びサイバーセキュリティの３種類があるが、施設とサイバーセキュリティに関するセキュリティ・クリアランスの導入に反対する日本人は多くないと思われる。やはり、我が国で議論となるのは、人的セキュリティ・クリアランスであろう。我が国でこの点が問題となる一つの要因には、法的問題のほかに、日本と西洋の社会における人間観の違いがあると考えている。アメリカを始め西洋社会では、キリスト教的な背景により人間の本質は悪や弱さにあるとする性悪説に基づく人間理解に立脚していることから、人的セキュリティ・クリアランスで着目する個人の弱さや脆弱性にストレートに結びつき、理解されやすい。これに対して、我が国の社会は一般的に性善説に立っていることから、ある人の人格等を悪あるいは弱さから把握しようとするセキュリティ・クリアランスは、その人の人格を全否定するような恐ろしい制度のように誤解される場合が多いのではないかと考えている。この点については、原子力関連施設をテロ攻撃等から守るための核セキュリティ対策に関する教育用ビデオを見たときに、施設への入構手続の厳格化は社内における個人への疑念ではなく、事業者としての姿勢が問われることから協力が求められるといったような性善説に立脚した言い換えが常になされていることで気がついた。

○　人的セキュリティ・クリアランスを実施する場合、当然のことながら法的な差別は禁止される。この点につき、日本とアメリカにおける法的な差別禁止事項は、ほぼ同一であるが、社会的な違いが出るのが国籍である。アメリカではアメリカ市民であることが多くのアメリカ人にとってプライドとなっていることから、セキュリティ・クリアランスでアメリカ国籍が要件とされ、また、二重国籍の場合に審査が厳しくなっても全くと言っていいほど問題にならない。これに対して、我が国においては、戦前来の経緯もあって様々な国籍をお持ちの方がいらっしゃることから、たとえ国家安全保障に関わる職についてであっても、日本国籍を要件としたり、二重

国籍であることで別の扱いを受けることになると、国籍差別として論じられる場合が想定し得る。

○　なお、アメリカで、アメリカ生まれのアメリカ市民であっても、大家族制が根付いている国からの移民の方で、現在も出身国の親族との深いつながりがある場合、セキュリティ・クリアランスの審査において懸念事項の一つになる。特に、その出身国の政府が自国民の人権を十分に尊重しておらず、そのインテリジェンス機関が、国内にいる親族に圧力をかけてでもアメリカ市民から機密情報を取得しようとするおそれがあるとアメリカ政府が判断している国家の場合には、セキュリティ・クリアランスの取得が困難になる場合がある。具体的には、出身国に残った高齢の親に対して年金等を止めるぞといった圧力がかかることが想定されている。このことは、公民権法第７編において明示的に雇用における出身国差別を禁止しているアメリカにおいても、国家安全保障上の懸念から、そのようなアメリカ市民にセキュリティ・クリアランスを与えないことは、そもそもその取得が権利ではなく、国家の裁量に基づくものであることから差別には該当しないとする判断が判例法理として確立している。また、30 ページに「参考」として挙げた論文にも示しているが、我が国の周辺国の中には、レベルの違いこそあれ、アメリカから、そのような圧力をかける可能性のある国家であると判断されている国が多いことは事実である。

○　このような懸念は、日本生まれで日本国籍を持っている方であっても、このような周辺国における親族との間で緊密な関係が続いている方には妥当すると思われる。しかしながら、我が国で、このような方にセキュリティ・クリアランスを付与した場合、その後、親族がいる外国政府のインテリジェンス機関につけ込まれてしまえば、その方の家族関係が破壊され、高齢の親の生命や健康が阻害されることすら起こりかねない。これまで、我が国の政府は、こういった説明を公にはしてこなかったと思われるが、セキュリティ・クリアランス制度の導入に当たっては、国民への丁寧な説明がなされるべきであると考える。

○　資料４の 18 ページの「連邦行政機関による判断基準」と、特定秘密保護法に基づく適性評価における調査内容７項目を見比べた際、日本とアメリカの大きな違いとしては、指針のＢ.外国の影響、Ｃ.外国の利益を優先する傾向、また外国政府や外国法人との接触といった、Ｌ.業務外活動のような項目が重視されていると感じる。これに比べ、特定秘密保護法は、スパイ活動及びテロリズムとの関係にとどまっており、非常に限定的である。例えば某国との関係の影響度を見る上で、スパイ活動やテロリズムに該当しなければ、こういった国と密接な関係を有していてもいいのかということになる。そういう点は、アメリカから実質的同等性を認めてもらう上でクリティカルか。

永野委員より回答

○　必ずしもそうとは言えない。法令上の表現は異なっていても、基本的に各国とも、外国のインテリジェンス機関からつけ込まれ得る人の弱さに関わる点に着目して同様の判断を行っているものと考えられる。

○　アメリカの大統領令で定められているセキュリティ・クリアランス対象情報の範囲はかなりざっくりとしたものであり、実際には各連邦行政機関で定めている指定マニュアルで運用が決まっており、それは公開されていないと承知しているが、これと同様の運用ができるという確証があればそうした方が良いということになるのか。

永野委員より回答

○　特定秘密保護法のときは、対象情報を明確にするために、詳細な別表が策定されたと考えている。

○　今回検討されている法制においてセキュリティ・クリアランスが必要となる情報に関しても、国民に明確な説明を行う必要があることから、今回は細かなところは省令等で定めればいいとは考えるが、法令において別表等の形式により、可能な限り明確に対象となる情報類型を列挙するべきであると思う。

○　研究機関のセキュリティ・クリアランスについて、アメリカの大学では、政府と連携するリサーチセンターのような機関を設けることで制度をうまく回しているようだが、アメリカでも大学そのものでは民間向けのセキュリティ・クリアランスを取得していないのか。

永野委員より回答

○　アメリカでは、大学や研究機関が国家の機密情報を扱う場合、連邦政府が所有・運営している組織の場合には連邦行政機関と同じセキュリティ・クリアランス制度が適用され、民間が運営する組織の場合には、民間の請負人に適用される国家産業保全プログラムにおけるセキュリティ・クリアランスが必要になる。また、大学においては施設管理担当理事などに対してもセキュリティ・クリアランスが求められ、かつ、関連施設における施設クリアランスも必要となる。

○　セキュリティ・クリアランスが取得できない場合に、何となく、当人が過去に何か悪いことや犯罪を行った人であるかのように捉えられがちであることを懸念している。ただ、資料４のアメリカにおけるセキュリティ・クリアランスの判断基準を見ると、それはひとつの事象として見られているに過ぎず、むしろ外国の影響力がどのくらいあるのかといった点や、何か弱みがあってコントロールされてしまうのではないかだとか、そういった観点で見られているという理解でよいか。例えば、性行動の項目も、必ずしも犯罪だけではなく、何か秘密にしていることがあった場

合に、それを公表するなどと圧力を掛けられてしまうおそれがあるといったものであり、また、外国に家族がいたり資産を持っていた場合でも、すぐに自国に逃げ帰ったり資産を持ち帰ったり売却することができれば問題ないといったものであって、何か悪いことをしているということではなく、純粋に影響力・圧力をかけられてしまう可能性がある人かどうかを見ていると理解してよいのか。つまり、資格を得られなかったからといって直ちに当人に問題があるように見られてしまうのは、適切ではないという理解でよいか。

永野委員より回答

○　アメリカのセキュリティ・クリアランスの判断基準に関する考え方については、おっしゃるとおりである。また、アメリカにおいても、日本の特定秘密保護法においても、セキュリティ・クリアランスで得た情報は、公務員の懲戒事由に該当する場合を除き、人事評価等で他目的使用をしてはならないとされている。

なお、セキュリティ・クリアランスの取得が求められる国家安全保障に直結する職務は、世の中の仕事のうち、ほんのわずかに過ぎないので、当該職に就けなくても生活に困ることは稀であろう。また、アメリカのインテリジェンス機関や防衛産業で機微な情報を扱う仕事に従事する場合には、セキュリティ・クリアランスの保有と維持が雇用条件になっていることからセキュリティ・クリアランスを失うと解雇されることが多いのに対して、日本では労働者の解雇に対して非常に厳格なルールが存在していることから、セキュリティ・クリアランスが必要となる特定のプロジェクトの職務に就くことが予定されていた者が、セキュリティ・クリアランスを取得できなかった場合、そのこと自体は解雇事由にはならず、別のプロジェクト等に配転してもらうことが可能であると思われる。

○　ＣＵＩについては、基準がだんだん変わりつつあり、半導体の世界での要件についても変わりつつある。これはアメリカの輸出管理と対比しているような感じを受けている。ＣＵＩの規制動向とその範囲が今後どのような形で広がっていくとお考えか。

永野委員より回答

○　御質問のとおり、特に半導体分野がそうであるが、アメリカが重要技術として指定した技術に対しては、今後も規制は強化されることが予想されることから、それに関連するＣＩやＣＵＩの範囲も拡大していくものと思われる。

○　セキュリティ・クリアランスの背景調査を担当するのが、アメリカの場合は国防総省のＤＣＳＡであるが、なぜＦＢＩ（Federal Bureau of Investigation；連邦捜査局）や他のインテリジェンス機関ではないのか。日本で誰がやるかと考えた際に、防衛省なのか警察庁なのかなど考えるが、なぜＤＣＳＡが担当することになったの

か根拠があれば教えてほしい。

永野委員より回答

○　アメリカでは、歴史的に戦時における軍事機密を保護する必要性から、軍がセキュリティ・クリアランスを担ってきた伝統があり、2005 年２月までは、国防総省国防調査局（Defense Security Service）が連邦政府における身上調査の多くを担当してきた。しかし、同局による身上調査は時間がかかり、機密（Top Secret）レベルに関しては１年を超えてしまう場合もあったことから、連邦議会から機密情報を扱う予定者がいつまでたっても赴任できない等の指摘を受け、2004 会計年度国防授権法により、機密情報を扱う連邦政府被用者等に対する身上調査業務は、その機能・人員ともに、連邦人事管理庁（Office of Personnel Management）に移管されることになった。その後、2015 年に同庁が中国からのものと思われるサイバー攻撃を受け、２千万人を超える個人情報が流出するというアメリカの歴史上最大の情報流出事件が発生した。この事件の発生原因は、同庁が個人情報を暗号化しておらず、これを扱うシステムが 20 年以上前にプログラミング言語の一種であるＣＯＢＯＬで書かれた古いもので大幅な更新が困難であったこと等であったが、これらのシステム上の問題に対処できる連邦行政機関は、国防総省しかなかった。このため、複数の制度改正を経た後に、2019 年 10 月から、国防総省に新設されたＤＣＳＡが、セキュリティ・クリアランスにおける身上調査等を担当している。

（６）自由討議

○　アメリカにあって日本にない制度として、日本には大臣、副大臣、大臣政務官等に対するセキュリティ・クリアランスがないことが挙げられる。アメリカでは、大統領が行政府の上位職で上院の助言と承認を要する閣僚等のＰＡＳ官職（ＰＡＳ（Presidential Appointment with Senate confirmation）positions）を指名するが、当該候補者のセキュリティ・クリアランスは、大統領法律顧問室（Office of Counsel to the President）が統括し、ＦＢＩ、内国歳入庁（Internal Revenue Service）、政府倫理局（Office of Government Ethics）及び候補者の就任が見込まれる行政機関の幹部職員が関与して行われている。

○　アメリカにおける大学へのセキュリティ・クリアランスと同様の制度を、日本の大学にそのまま適用することはできないと考えている。この点については、現行の特定秘密保護法の下では大きな困難が伴う。また、本有識者会議で議論の対象となっている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規定する法律においても、同様であると考えられる。このため、現在、一般の大学に所属し、将来的にセキュリティ・クリアランスが必要となる情報に接することに同意していただける研究者の方は、法人に対してセキュリティ・クリアランスを実施すること

ができる国立の研究機関や民間企業に移っていただくしかないと考えられる。

○　このような形で、セキュリティ・クリアランスを受けることに同意して、国立の研究機関や民間企業に移籍していただくことになる先端技術研究者の方には、その報酬、研究費、必要となる施設などの面で十分に処遇する必要がある。特に、研究論文を公表して世に問うことが大きな目標であった方々に、機密情報に関わる論文は公表できないという制約を課すことになることから、本制度の運用面で、十分な手当をしなければならないと考える。

○　我が国においてセキュリティ・クリアランスの背景調査を担当する行政機関は、アメリカと異なり、防衛省が担当する必要はないと考える。

○　そもそもなぜセキュリティ・クリアランスが必要なのか、というところで、資料４のアメリカにおける理由の最初に、現実に外国政府等の工作員が存在し、活動していることがあるということを挙げているのは分かりやすく、また、そうだろうなと思った。産業界のニーズもあると思うが、このことが制度を導入する上で日本においても重要になってくるのではないかという印象を持った。

○　民間事業者に対するセキュリティ・クリアランス制度というのが、政府関係とは別にあるということを筋道立てて分かりやすく説明いただいた。正にこれは、経済安全保障の世界の中でセキュリティ・クリアランスを位置づけられることを考えられるものであり、とても示唆に富んだ制度であると思うし、またアメリカの制度は中身もかなり充実したものであるとの印象を持った。

○　資料２で各国の説明を受けたが、特にアメリカについては、永野委員の話で大変理解でき、また企業の方からのお話で外国の運用についても理解できた。この制度がどこの国にもあるということは分かったが、これが実際に定着して実態的な運用が行われているということについても追加的な情報をいただければありがたい。アメリカがこの制度を活用しているのは分かったが、アメリカ以外の国においてセキュリティ・クリアランス保有者は何人いるのか、いつから始まったのかなどの実態的なことをお話いただけると、世界では非常に普及している制度であるが日本だけができていないということが分かると思うので、そういった点についても追加的な情報を事務局から提供いただきたい。

○　事務局が作成した資料２の諸外国の制度比較表について、今後セキュリティ・クリアランスの調査項目の比較も、各国制度との同等性の観点を検討する上で重要だと

思うので是非入れ込んでいただきたい。

○　アメリカの制度と我が国の特定秘密保護法とで、外国からの影響力の考慮の仕方に差異があるのではないかという指摘があったが、特定秘密保護法は、二国間で機密（Top Secret）の情報を交換することも想定して作られた制度であり、両制度間に実質的に大きな差異はないというべきである。国籍や配偶者、渡航歴といった我が国らしい帳票を捉えながら外国との関係を判断していく仕組みになっている。

○　今後どういった形でこれが進んでいくのか、特に特定秘密保護法とセキュリティ・クリアランスの関係について論じられていたが、思ったこととして、１つ目に、国際共同開発という面になってくると、特別防衛秘密との関係も整理が必要である。２つ目に、ＣＵＩに該当する部分について、特に民間企業においてどういった形で規律していくのかということについて、土俵となるのは不正競争防止法以外ないのではないか。３つ目に、研究機関については、アメリカにおいてもリサーチ・インテグリティをいかに保全していくかが大きな課題となっており、かつこの点が一番弱いと言ってもいい。この辺りを我が国でどのように対応していくかは大きな課題である。いずれにしても、我が国において国家安全保障という概念が発見されたのはつい最近であると言っても過言ではない。そのようなものは、行政法の中では外為法ぐらいしかなかったが、その中でセキュリティ・クリアランスを我が国の行政法の中でいかに築けるかということが重要だろう。

（７）高市経済安全保障担当大臣挨拶

○　今回も、有識者会議委員の先生方におかれては、長時間ご出席をいただき、また、闊達なご議論をいただき誠に感謝。

○　前回の会議では、企業の方から、セキュリティ・クリアランス制度のニーズに関わる具体的な事例や、国際共同開発やサイバーセキュリティ対策におけるセキュリティ・クリアランス制度の有用性のほか、諸外国と機能的に同等性を持った制度整備の必要性などについてお話を伺った。

○　本日の企業の方からのお話でも、具体的なニーズ、そして検討課題に関して大変貴重なお話を伺うことができた。また、本日は特に、永野委員から主にアメリカに関する制度についてお話を賜ることができ、我々も理解を深めることができた。また、昨年来、色々なリサーチに基づいて事務局でまとめた諸外国の制度の比較、こういったものも我々の理解を深めることになったと思う。

○　どのように法律を作っていけばいいのか、何を法令で定めていけばいいのか、この辺りは整理が出来てきた、イメージが出来てきたと思う。どうか今後とも、活発なご議論、よろしくお願い申し上げたい。