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２回）　議事要旨

１　日時

令和５年３月１４日（火）１３時００分から１５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
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
永野　秀雄	法政大学人間環境学部 教授
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
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）座長代理の指名

前回欠席であったため事務局において意向を確認していた鈴木一人委員が、改めて座長代理に指名された。

（２）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。

（３）企業からの説明（１社目）

電機メーカー・Ａ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、説明があった。

○　ある海外企業から当社の技術に関して協力依頼があったが、機微に触れるということで相手から十分な情報が得られず、当社から一方的に技術を供与するだけで満足できるビジネスとはならなかった。また、別のケースでは、同じように相手から十分な情報が得られなかったので、こちらから断った。

○　今から振り返ると、例えば、政府間の枠組みの下で、お互いにセキュリティ・クリアランスを保有している者同士で共同開発などができれば、もう少し踏み込んだものになったのではないかと思う。

○　セキュリティ・クリアランス制度の導入によって、将来的に例えば衛星・ＡＩ・量子、あるいはBeyond 5Gといった次世代技術について、国際共同研究に関する機会が拡充してくる。しかし、こうした技術は軍事目的にも使用されるデュアルユース技術であることから、安全保障上の厳格な管理がなされていないと国際連携の枠組みに日本企業が入れなくなることが考えられ、事業機会を失うかもしれないということを危惧している。

○　現在日本では特定秘密保護法が整備されているが、本法では、安全保障に関する科学技術情報がカバーされておらず、既存の枠組みの中での対応には限界があると感じている。

○　セキュリティ・クリアランス制度は日本政府の情報を保護する、あるいは、アメリカ政府からもらった情報を保護することではあるが、G to Gの枠組みの中で、民間企業も交えて共有されるシーンが今後増えていくのではないか。

○　また、先端技術開発の初期の段階では、防衛技術と非防衛技術に区別するのは、議論の性質上、なじまないと考えている。防衛も非防衛も、両者を包含する制度にしてくれればありがたい。

○　サイバーセキュリティの分野でもセキュリティ・クリアランスは重要。最近では日本でもアクティブサイバーディフェンスの検討が進んでいると承知。アメリカをはじめとした諸外国との脆弱性情報や攻撃情報の共有が加速されていくのではない

かと思っている。こうした機微な情報の一部が民間でも活用ができれば日本全体でのサイバーセキュリティ対策が強化され、ひいては安全保障の能力が向上する。

○　サイバーセキュリティでは、政府から民間だけでなく民間から政府への情報提供も重要である。ただし、機微な情報を含むため、民間としても情報提供には外部との関係もあり抵抗がある。セキュリティ・クリアランスが整備されれば、これまで以上に積極的な情報共有がなされると期待できる。

○　諸外国との国際共同研究開発の際、日本国内でセキュリティ・クリアランスの実績を積み上げていくことは大前提であるが、その先にアメリカをはじめとする同志国にも通じるものが期待される。諸外国ではＩＳＡ（Industrial Security Agreement）という仕組みがあり、２国間でＣＩ（Classified Information）を共有できるようにしている。アメリカとイギリスでは2000年にＩＳＡが締結され、セキュリティ・クリアランスの相互適用によって、研究開発、技術情報の共有、防衛装備品の連携促進等を含む包括的な連携が行われている。ＩＳＡはファイブ・アイズ加盟国のみでなくインドも結んでいることから、ファイブ・アイズ加盟国以外も締結可能と思われる。

○　その他の仕組みとして、国家産業技術基盤ＮＴＩＢ（National Technology Industrial Base）というものもある。ＮＴＩＢは、当初アメリカとカナダで始まったが、ここにイギリスとオーストラリアが加わり、現在アメリカ、カナダ、オーストラリア、イギリスの４か国が加入しており、アメリカの国家安全保障上の支援を得ることを目的として設立。通常は案件ごとにＣＩにアクセスする場合にＮＩＤ（National Interest Determination；国益決定プロセス）に関する承認手続きが必要とされ、この手続きに60日から360日の時間がかかるが、他方、ＮＴＩＢに加盟のアメリカ現地法人はこの手続きが免除されており、円滑にＣＩへのアクセスが可能。このように、各国はセキュリティ・クリアランス制度を整備した上で、プラスアルファの国際的枠組みももって、その効果を最大限に発揮できるための取組を行っているというのが、我々の調査した状況である。

○　最後に、我々がセキュリティ・クリアランス制度に期待することは、他国からも同等性が認められることが重要である。まずは外国の制度を精査し、取り込むこと。その上で、将来的な取組としては、ＩＳＡのような、国際的な情報連携を促進するような取組を期待する。こうした取組みが民間の需要拡大のみならず、サイバーセキュリティ分野で説明したように、我が国の安全保障レベルの強化にもつながる。

○　また、日本において、防衛分野を中心として機密情報をしっかりと管理されているが、今後、セキュリティ・クリアランス制度を整備していくなかで、防衛分野を対象外としないでいただきたい。今回検討している制度が防衛分野を切り離した制度とされると、省庁ごとにセキュリティ・クリアランスを取得する必要が生じ、運用コストや管理コストが増す。また、将来の先端技術の研究開発においては、その技

術が防衛分野なのか非防衛分野なのかを初期段階において議論するのは実態としてなじまないことから、ぜひ、防衛も含めて、政府一体となって検討していただきたい。

（４）意見交換

○　資料３の３頁には、「経済安全保障推進法やＮＩＳＣにおける重要インフラにおいても宇宙／防衛領域は含まれておらず」との記載があるが、現在検討中の制度では、宇宙・防衛領域を除外して法制度化することが考えられているのか。

事務局より回答

○　現状、経済安全保障推進法には、例えば、基幹インフラ分野があるが、そこには、必ずしも宇宙は入っていない。今後、もちろん議論・検討していく必要はある。

○　資料３の３頁に、「米国等の諸外国からも認められるレベルの制度創設」とあるが、基本的な検討対象はアメリカの制度でよいと思われる。これは、ＮＡＴＯに関するセキュリティ・クリアランスは、アメリカの制度と類似したものであるためである。また、イギリス・ドイツ・フランスにおけるセキュリティ・クリアランスに関するリーガルリサーチは困難であると言われていることから、事務局は、これらについて過去に書かれた論文を参照すれば十分であると考える。

○　当然のことながらセキュリティ・クリアランス制度をやると、本人にとっても企業にとっても負荷がかかる側面があると思うが、そういった点についてはどのような議論をしているのか。

企業より回答

○　もし制度が導入されたら、それなりの負担があることはよく承知をしている。人物チェックだけではなくて、組織の情報管理の在り方も含めてのクリアランスがあるということもよく承知している。

○　セキュリティ・クリアランスの制度そのものが大事という話と、これに加え、国際的枠組みがないといけないということを示していただき、大変よかった。防衛と非防衛を分けるべきでないという指摘も全く同感。重要な二点を示していただいた。

○　セキュリティ・クリアランスを実施するに当たり、社内的に、人事管理なり労務対策上、問題ないようにしていくために関係者の同意がある状態が重要。セキュリティ・クリアランスを広げていくと企業が直面することになる人事や労務といった問題についてはどう考えるか。

企業より回答

○　確かにバックグラウンドチェックの面で本人には負担があるが、秘密情報に関わるけれども意義のある仕事として、今と同じような気持ちでその分野で働くことについての誇りとやりがいを持って取り組んでくれるのではないかと思っている。

○　将来の期待として、サイバーの話で、民間から政府への情報を提供することが重要というお話があったが、ここは、おそらくセキュリティ・クリアランスがなくても可能な話なのではないか。

企業より回答

○　サイバーについて、企業が政府にボランタリーに情報提供すればできるとは思う。ただ、正直なところ、民間企業の立場としては、政府に情報共有するのを一般的に嫌がる傾向はある。よって、政府と企業の相互の連携の枠組みができれば円滑に情報共有できるのではないかと考えている。

○　ＩＳＡは民間同士の枠組みで、実はこれに類するものは他にも色々なレベルでたくさんある。例えば、ＴＳＡ（Technology Safeguard Agreement）はミサイル、衛星の打上げ関連で出てくるが、これも、日本はアメリカと結べていない。こうした国際的枠組みの締結についても将来的な課題として事務局には検討いただきたい。

○　事務局に聞きたい。特定秘密保護法では現在４分野があるが、特に技術分野で切っていくと、デュアルユースの部分がなかなか切りづらいのかなと思う。企業の話として落ちていった場合に、人的な観点でうまくガバナンスが利くのかなという疑問はある。今後の方向性として、国際共同開発以外の局面でセキュリティ・クリアランスが必要になるという場面としてどのようなものを政府は想定しているのか。

事務局より回答

○　正にこの有識者会議で今後議論していただくことになるが、諸外国との実質的同等性や企業のビジネスチャンスにつなげていくということを考えれば、政府内の情報保全体制がしっかりしている枠組みを諸外国に示す必要があると考えている。諸外国で、情報保全の対象となっている分野がどういう分野なのかと考えると、国際共同開発だけに限られない。

○　いま国際共同開発が立法ニーズとして強調されている。企業が関わってくると、何らかの形で限界を決めなければならない。そうした中で国際共同開発は切りやすい。技術で切ると、デュアルユースや宇宙、サイバーなど、そんなところも含まれるのかという話にもなると思う。今後ここで議論していくと思うが、他にどういう対象があるのかということを明確にしていくことが企業サイドにとっても重要だと思う。

○　日本の安全保障にどうつながってくるかということについて、ロジカルな議論がないといけない。入札や国際会議に参加するという、ビジネスチャンスにつなげるだけということではだめ。整理学や仕分けが必要だが、やはりその際のキーワードは日本の安全保障なのではないか。

○　サイバーに関して、民間企業が持っている情報にもセンシティブな情報があり、政府側あるいは外に出していくときに、セキュリティ・クリアランスがあった方が共有しやすいという話だったかと思うが、政府に出していく際にというより、大学など、政府以外に出していくときのことを念頭に置いているのか。

企業より回答

○　大学が入っている、入っていないということが重要なのではなく、要は、アメリカでは、セキュリティ・クリアランスを持った民間が政府と情報共有する場・ネットワークがあると聞いており、こうした場が日本にも必要なのではないかということ。それにより情報共有が円滑に進むのではないかと考えている。もちろん、その中にアカデミアの先生が入ることは全然問題がないと思う。

（５）企業からの説明（２社目）

電機メーカー・Ｂ社から、資料４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、説明があった。

○　資料４に基づいて弊社の状況を話す。弊社は機械、機器に強い会社であるため、説明はサイバーセキュリティを割愛し機器の説明に限らせていただく。その方が、より企業の特徴が出ると考えている。

○　「１.基本的な立場」のうち、国の保有する防衛関連の機密情報（いわゆるＣＩ）の民間開示を拡大する制度見直しを要望と記載しており、これについては、現時点では日本政府との関係で、防衛関連の個別のプロジェクトごとにＣＩの開示を受けているが、この手続は契約ごとに行っているのが現状である。このため、長い目で見た際、クリアランス・ホルダーの育成という観点からはマイナスである。

○　外国政府も参画した国際共同開発プロジェクトにおいて、相手国政府のＣＩへのアクセスを得ようとすると、さらに手続きがが必要となり多大の時間を要している。

○　防衛装備品の国際共同生産の例では、相手国政府のＣＩを得られるまでに数年以上を要した。仮に、セキュリティ・クリアランスを一定期間保有でき、かつ、その制度が相手国から信頼されていれば、この期間は短縮された可能性もある。

○　ただし、先般の事例は防衛省の装備計画と結びついたものであり、日本の装備品に関する契約がある。

○　自衛隊の装備品とは関係ない国際共同開発案件において、先方が保有するＣＵＩ

（Controlled Unclassified Information）の開示を受けるに当たり、弊社社員に日本政府からのセキュリティ・クリアランス保有者がいなかったこともあり、調整に長い時間を要したにもかかわらず契約に至らなかったことや、最終的に開示を受けることができたが、周辺情報だけに留まったこともあった。

○　自社の開発した製品に、海外からの機微な技術が搭載されており、同じく弊社社員に日本政府からのセキュリティ・クリアランス保有者がいなかったため、自社製品であるにもかかわらず、双方で十分な意思の疎通ができず、お互いに不便を感じていたケースもある。

○　資料には「防衛以外の官民の国際共同開発案件においても日本企業が円滑に当該プロジェクトに参加するにはＳＣ制度が必要」であり、「デュアルユース分野における国際会議・学会等ではＳＣ保有者のみが参加する発表の場があるが、こうした場に参加できないなど、デュアルユース品の国際共同開発に支障が出る可能性を危惧」と記載している。これは、学会に参加する際Clearance Holder Onlyであるセミナー・コミュニティに参加・聴講ができないということである。純粋に防衛用途の技術に関する学会に参加できないことは現状仕方がないと思うが、防衛と民生が一緒になったデュアルユース技術に関する学会もあり、これらに参加できず最新のデュアルユース技術に触れることができない。

○　例えば宇宙分野で、今後軍民の境目が一層あやふやになる中、民間企業間の情報交換を進める必要もあると想定されるが、こうした際に情報共有が難しくなることもあるだろう。宇宙や軍事の分野で海外企業のＩＴサービスの技術を使うという話が生じた際は、弊社のアクセスが制限されてしまう可能性がある。

○　「防衛以外の分野におけるＳＣ制度については先行各国の情報保全・ＳＣ制度運用を精査し、防衛以外の戦略分野に関するＳＣ制度が具体化することを期待」と資料に記載しているが、ＣＩの範囲の中に安保関係の科学技術や経済、基幹インフラという分野を含むかどうかということである。アメリカのＣＩの範囲にはこれらが含まれると承知。他方、これが日本だとどの情報に該当するのか、アメリカではどう民間企業と情報共有や保全を行っているかについていまだ理解が及んでいないため、運用や制度を明らかにする必要がある。

○　次のページに「２.クリアランス制度に期待すること」としている。ＣＩの範囲をどこまでにするかという論点は残るが、基本的に国が保有するＣＩの情報交換は黄色の矢印を経由する。つまり、アメリカＣＩが日本政府経由で日本政府からクリアランスを付与された企業及びその従業員に提供され、また、日本のＣＩがアメリカ政府経由でアメリカ政府からクリアランスを付与された企業及びその従業員に提供されるルートは堅持されると理解している。しかし、国際共同開発はＣＩだけではできず、ＣＵＩレベルのクリアランスを付与された者同士で専門的な又は技術的な会話ができるような運用がなされることにも期待したい。これが薄いグレーの矢

印に該当するが、契約又は案件ごとに当該作業を行うことは企業・政府双方の負担となろう。仮に同じ企業で同じ技術者が別案件に参加する場合、案件ごとに最初から体制を築くことは非現実的であり、一定期間クリアランスを保有することは必要な選択肢である。

○　なお、ＣＩの範囲については、資料２でいうところのＡ区分に該当する。一方でＢ区分に該当する国の技術情報を共有いただくことになるであろう特定重要技術情報、基幹インフラの部分に拡大することは、官民共同での次世代の技術開発、官民共同での海外との技術開発にとっては有効になる。資料左黒枠の⑤安保関係科学技術、⑦基幹インフラなどについてどのような運用がなされているのか、まだまだ勉強する必要がある。範囲拡大に当たっては、諸外国の制度も踏まえ、官民での検討を期待する。

○　最後のページは、「３.制度設計にあたっての要望」。繰り返しになるが、セキュリティ・クリアランス付与の審査基準の明確化（人と施設に関する情報保全義務の内容明確化）、セキュリティ・クリアランス対象となる人物のバックグラウンド調査は国が実施していただきたい。企業は労働法制等の関係で、民間がバックグラウンドチェックを行うことは難しいため、ＣＩについては国に調査をお願いしたい。政府の一元的窓口の設置が欲しいとしており、これは現状も調査を装備品については防衛省に依頼し、宇宙になると内閣府に依頼しているところ、今度範囲が拡大した場合、複数の機関でそれぞれ調査に数年以上を要するとなると負担が大きいため、政府の一元的窓口をお願いしたいということである。契約単位の適合事業者・従業者指定から、資格要件に基づいた有期の指定に変更、セキュリティ・クリアランスの有効期間、失効要件、違反時の罰則の明確化は先ほどから要望しているとおりである。制度の周知徹底を通じた官民双方の「情報保全」能力の向上が一丁目一番地である。

○　本日の議論は政府保有のＣＩにどのような形で資格を付与いただくかというものだと認識しているが、企業は原子炉等規制法や経済安全保障推進法上の基幹インフラや特定重要技術に当たるＣＵＩも扱っている。会社の中で、誰がどのような権限で又はどのようなバックグラウンドでこれらにアクセスすることができるのかをチェックするのは難しい。昨年５月に運用が始まった外為法のみなし輸出制度、これも結局従業員の善意に依拠する制度運用になっている。実際、その従業員がどういった人物であるかについて国籍も含め差別的に扱うことができない。営業秘密は不競法の範囲だが、社内の情報管理については労働法制との関係もあるが、セキュリティ・クリアランスをＣＵＩまで含めていくと、従業員をどういった形で管理するかは難しい課題である。労働法制と情報保全の整合性を図っていただき、考え方を示していただきたい。

（６）意見交換

○　誤解を招かないように申し上げると、資料４の３頁左端の「米国の状況」のところで、セキュリティ・クリアランス・ホルダーが「民間：103 万人」「不明：32 万人」となっているところは、原典によると「民間」とあるのは「Contractor」つまり「請負人」であり、「不明」とあるのは正確には「Other」つまり「その他」であり、技術開発契約や委任契約などがこれに当たる。

○　資料４の３頁の下欄に、矢印で示すとおり「直接日米が専門的会話をできる運用環境の確立を望む」とあるが、誤解を招く恐れのある表現である。なぜならば、機密指定されている情報を政府が全く関与することなしに、日米の民間企業同士で自由に会話することは恐らくあり得ないためである。これは、インターネット上のやりとりでも同様であり、アメリカ内においても、機密情報をやりとりするための情報システムには国家安全保障システムにおける基準を満たすことが求められるが、これは日本でもよく知られている NIST SP800-171 とは比較にならないほど厳格な基準である。

○　軍民両用分野で官民が協力していく事例は今後増えていくと思う。ついては、民生目的で建設された製品であってもクリアランスを受けた者でないと扱えない、いびつな状況は続くのであろう。その点で、デュアルユース品目のクリアランスについて、ＣＩかＣＵＩかといった射程の議論はあるが、これまでの国際共同開発については防衛と防衛の共同開発が一般的であったが、そうでないものがこれから次第に増えてくるのだという観点から我々の検討も進めていかなければならない。

○　最近話題になっている宇宙空間におけるデータセンターを作るといった話の中で、外国製のクラウドサービスなどのサービスを使うことも増えると思われ、そうなるとハードウェアのクリアランスだけではなく、ソフトウェア、とりわけクラウドサービスに対するアクセスにもクリアランスの問題が出てくるという意識を整えることが必要である。

○　ビジネスオポチュニティに対する管理コストはどんな形で考えているのか。また、企業の組織のことを考えると、輸出管理や研究開発、事業部門、経済安全保障の担当部門の組織の中の位置付けをどうすれば上手に企業の中で運用していくことができるのか。

企業より回答

○　ビジネス上のコストについて、数年以上かかるのは非常なコストであると考えている。そういう意味でも、一定期間クリアランス・ホルダーという形で認めてもらえ

る仕組みであれば、コストという意味で企業にとって、あるいは調査コスト削減という観点から政府にとっても良いことだと思うし、あるいは諸外国とも同一条件になるのではないか。輸出管理との関係については、例えばクリアランスを必要としないケースでは、本来、輸出管理部門だけで経済産業省との協議を進める。ただ、企業内の輸出管理部門というものは、どうしても抑制的に考えてしまうため、経済安全保障を担当する部署が輸出管理部門と協議をしながら、少し前向きに進めていくべく政府との調整を進めている。

○　資料の４頁に、制度設計に当たっての要望として「ＳＣ対象となる人物のバックグラウンド調査は国が実施」とあるが、これは基本的には、特定秘密保護法の枠組みをそのまま他の分野に拡大するイメージか。

企業より回答

○　御指摘のとおり。

○　資料の４頁に「政府の一元的窓口の設置」とあるが、これは、今も基準の斉一化は内閣官房でしているはずだが、所管大臣と行政機関の長の枠組みでやることになっている。適合事業者の認定も含め、省庁を超えてユニバーサルな資格要件とするのは難しいのではないかと考えているが、イメージとしてはどのようなものを考えているのか。特定技術や特定分野の資格という、今は特定事業者に契約単位で与える形になっており、そういったものがあれば便利だろうとは思うが、制度的にどんなものになるのか、イメージがあれば伺いたい。

○　仮に情報分野を４分野から広げていったときに、情報の指定の在り方が硬直的という問題、例えば、指定することに慎重である一方、一旦指定されるとなかなか解除もされないということがあるのではないかと思われるが、企業から見たときに、使い勝手の良い制度にするため、指定と解除の在り方の機動性をどう考えるか。

企業より回答

○　指定が機動的に行われるようになり、資料２のＤ・Ｅ区分などの、企業保有情報が指定されていくようになると、企業内でこれまで当該技術に携わっていたエンジニアが関われなくなる可能性がある。そういう意味では、Ｄ区分やＥ区分に突然国の指定が入ってくるというのは、我々としては慎重に対処していかなければならず、時間をかけたやり取りが必要と考える。また、解除するときも、確かに硬直的になってしまうことによる使い勝手の悪さはあるとは思うが、他方で、制度の安定性も重要な要素である。したがって、指定を外すときには、そこに関与している技術者たちとも、なぜ外すのかを十分議論することが重要である。

○　外交の世界では、指定されるとその後ずっと指定され続けることとなりがちであるが、経済安保、デュアルユースの世界では外交の世界の運用の硬直性が支障にならないか。

企業より回答

○　ケースによるが、資料３頁に記載したアメリカのＣＩにおける⑤安保関係科学技術や⑦インフラのような情報を指定するのであれば、指定時の十分な検証が必要になり、また、定期的に技術が陳腐化していないのかということの検証も必要になってくるだろう。

○　画期的な技術が一つ生まれると、民生技術がいきなり安全保障において最高の技術になる可能性もある。この技術はＣＩとかＣＵＩに指定した方が良いのではないかという状況もあり得るがそこはどう考えるか。

企業より回答

○　あると思う。ある場合には資料２でいうところのＤ・Ｅ領域になると思っているが、その情報を指定するかどうかは企業側とよく相談してほしい。

○　ある機関が情報をＣＩに指定したり、もしくはＵＩ（Unclassified Information）に指定すれば、以降は一切変更しないというのではなく、民間の意見や学術的な判断を経た上で、状況に応じ、機動的にＵＩからＣＩに変更したり、反対にＣＩからＵＩに変えるのがよいということか。

企業より回答

○　そのとおり。

○　民間企業にセキュリティ・クリアランスを導入した場合、経営者の方々が、実際にセキュリティ・クリアランスを受ける従業員の方に報酬で報いることを考えても、政府入札の事案が多いことから、なかなか思い切った手当を出しづらいのではないか。また、複数の企業間においては、賃金体系が異なることから、セキュリティ・クリアランスを受ける従業員の方々への評価や手当に差が生じることも考えられる。このため、政府がセキュリティ・クリアランスを申請する民間企業の従業員の方に対して、直接に 10 万円を給付するとか、毎月一定のセキュリティ・クリアランス手当を支払う制度を設けた方がよいと考えている。

○　アメリカでは、機密レベルのセキュリティ・クリアランスをもつ方に対しては 1300 万円以上の報酬が支払われているが、我が国では、アメリカのようなセキュリティ・クリアランス所持者の労働市場が存在していない。このため、セキュリティ・クリアランス制度を導入する際に、政府が民間企業の被用者に直接に一定の手当を支給

する制度を導入した方がよいと思うが、貴社はこのような制度の導入をどのように考えるか。

企業より回答

○　仮にそういうのがあればいいなとは思う。いずれにせよ、確かに、それなりに負担であるというのは本人たちからも聞いている。観光目的であってもクリアランスに関係している業務に従事している間は、懸念のある国に行くことができないという話も上がった。国が持つか会社が負担するかは別として、何らかの形で負担に報いることは考えなければならない。誇りを持っているだけでは済まされないと思う。

○　スライドの最後のところで、ＣＩに留まらない情報についても気を付けながら対応していると思うが、そことの比較で、セキュリティ・クリアランスの特別な難しさや、差別や従業員の取扱いについて気を付けている点があれば教えてほしい。

企業より回答

○　クリアランスにおいては、ＣＩを扱う者については国に調査いただけることとなっているが、ＣＵＩや安全保障上の情報については現状完璧な管理ができているとは言えない。ここは労働法制との矛盾を抱えているところであり、かつ法律が複数に分かれているため、一本筋が通るような何らかの考え方が示されると動きやすくなると考えている。

（７）自由討議

○　資料２で「情報の区分イメージ」をお示しいただいたが、企業には既に情報保全も含めた様々なレベルでの規制があり、今回の制度が重複した規制になることは避けるべき。この点で言えば、事務局にはご尽力いただくことになるが、第１回目の資料にあった「我が国の情報保全の枠組み」が「情報の区分イメージ」のどこをカバーしているのか、経済安全保障推進法との関係も含め、お示しいただけるとありがたい。

○　今後の検討に当たっては、労働者も含め対象となる範囲を絞り込んでいく必要があるのではないか。

○　「信頼性の確認とプライバシー」で言えば、労働関係法令との関係や懸念点なども明らかにしていく必要がある。

○　国家安全保障戦略及び本有識者会議の趣旨にもあるとおり、セキュリティ・クリアランスを含む情報保全の強化に向けた検討を進めるに当たっては、産業界のニーズをくみ上げるのと同時に、主要国の情報保全制度の実態を把握し、それらとの同等

性をいかにして確保するかが重要。その意味で、諸外国の情報保全制度の概要およびその運用についても、できる限り早く委員間で共有することがバランスのとれた議論に不可欠である。

○　資料１「（２）情報保全の必要性」にあるとおり、前回の有識者会議では、産業界のニーズも重要だが、我が国の安全保障の観点から議論を尽くすべきとの至極もっともなご指摘があったところ。そこで、改めて国家安全保障戦略を見ると、国力の一要素である「情報力」に関して、新たなセキュリティ・クライアランス制度の創設の検討に関する議論も踏まえて、情報保全のための体制の更なる強化を図る旨が盛り込まれている。したがって、産業界のニーズと並行して、我が国の情報力をいかにして高めていくか、そのためには、どのようなセキュリティ・クリアランス制度が必要かという議論も不可欠である。

○　諸外国を調べる話について委員の方々から重要なご指摘があったと思う。フランスもドイツも、素人目には調べて整理できたらいいと思うが、実際は大変複雑ということで労多くして益なしということかと理解した。他方で、上記のような観点で整理をする場合に論理が必要。日本の立場として日米安保が一番重要だということ、ドイツ、フランスと違って、アメリカがこういう立ち位置なのでアメリカを見るべきなのだ、という整理学が必要だと思う。そういう整理をした上で実体論としては、効率的な対応が必要と思う。

○　少なくともアメリカは調べるということかと思う。

○　アメリカのセキュリティ・クリアランス制度は、連邦憲法上の人権保護と適正手続が尊重されており、かつ、制度に関する情報のかなりの部分が情報開示されていることから、調べやすく、かつ、参考になる。

○　ＣＩに関するセキュリティ・クリアランスの検討に加え、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に関する情報保全制度は、我が国の企業にとっても必要になることから、早期の検討課題とすべきである。

○　アメリカのセキュリティ・クリアランス制度の中には、民間企業等の法人に関するＦＯＣＩ（外国による所有権・管理・影響）と呼ばれている制度が、施設クリアランスの中に組み込まれている。これは、民間企業等が外国関係の株主に支配されていたり、外国籍の役員等が、国が機密指定した情報にアクセスしないようにすることなどを確保するための制度である。現在、我が国にはＦＯＣＩに関する制度がな

い。このため、防衛産業のみならず、基幹インフラ役務を提供する事業者にも適用することが求められる同制度に関する検討を早期に開始するべきである。

○　国家安全保障に関わる重要な技術にアクセスしたことのある研究者・技師について、その退職後の情報保全をいかに確保するかという問題は、アメリカでも解決が難しい問題とされ、2021 会計年度国防授権法でも検討の対象になっている。我が国においても、これらの研究者・技師を継続して雇用する等の方策を検討する必要がある。また、セキュリティ・クリアランスを得て機密情報に接する研究者については、関係する論文発表も制限されることから、どのように報いるかを十分に考慮しなければならない。

○　民間企業の被用者に適用されるセキュリティ・クリアランス制度の構築に当たっては、これらの被用者に報いるために、政府が直接に被用者に一定の手当を支給する制度の導入を検討するべきである。

○　防衛関連以外で本当にクリアランスが必要と思っている企業がどのぐらいあるだろうか。制度化していくに当たっても、立法事実としてまずはここから考えていくことが、制度の運用の面でも重要。今分かっているのは、現在の４分野では足りないということだが、制度の改変をどう行うか。

○　資料２のＤ・Ｅ分野に当たる企業のヒアリングを是非していただきたい。別の委員が指摘されたように、制度のみでは解決できない従業員の転職に伴う情報漏洩の問題もあると思う。ただ、アメリカの企業の中には、日本企業と好んで協業をするところがある。何故かというと、日本は人が辞めないから。だからこそ、日本企業は強く必要とされている。上手にやれば、競争力につながる。肌感覚から言うと、ＩＳＯのような形の、国際的に業務を行っている企業に対するある種の情報セキュリティーに関する資格のような、そういうものもあってもよいように思う。こうすれば、企業がついてくると思う。

○　本日の２社はコストを吸収できる事情があり、そこは意識しておく必要がある。また、特に宇宙分野では、いわゆる小規模なベンチャー企業がかなり入ってきており、アメリカの防衛もこうしたベンチャー企業に発注するようになってきている。これまで伝統的な防衛事業をやってきたことのない企業が防衛分野に参入することが進んできている。労務の問題などのコスト負担を、新規企業が受け入れられるかどうかは、よく考えておく必要がある。

○　安全保障のためにどの技術が重要なのかというのは、特定秘密保護法の４分野だけではなく、経済安全保障推進法でいうところの特定重要技術であればＣＵＩに該当するかと思うが、企業が自ら判断しているのが現状だと思う。安全保障をやっている組織なり人なりが、兵器転用可能な技術である、安全保障上重要な技術なのだという判断をしていく必要がある。

○　企業の負担という観点では、国家安全保障戦略でも書かれたことだが、防衛産業からの撤退が進んできている。セキュリティ・クリアランスが追加的なコストとなり、防衛産業の更なる撤退を促すことのないようにしないといけない。追加的なコストに関して、財政的支援も含め、何らかの形でディスインセンティブとならないような配慮・対応が必要。

○　前回会議以降、アカデミア方々との間で意見交換をさせていただいた。日本が隣国等からの脅威にさらされている中で、先端技術及びデュアルユース技術の開発、経済安全保障分野に貢献したいという研究者もかなりいるのではないかと思われる。ただ、実はアメリカでもいろいろな大学で多くの研究者が積極的にＣＩ、機微技術の研究に関わっているかというとそうではなく、少数の大学や少数の方々が、オフキャンパスの環境下や、特別にセキュリティの担保された環境下で研究を行っている。また、必要に応じて、大学が企業と連携し役割分担しながら研究に取り組むなどの工夫をしているケースもある。日本の大学においても、このようなアメリカの事例を参照しつつ、研究者がセキュアな環境で安心して研究に取り組めるような枠組みを考えるのも必要ではないか。本日の議論とは直接は関係ないかもしれないが、今後そういった視点も検討する必要があるのではないか。

○　防衛産業撤退の懸念がないかという指摘があったが、今後資格制度が出来て、この資格を企業が持てば、企業にとっては逆に参入障壁となって、新規参入が生まれないという側面も無くはない。海外とのビジネスにおいて、国内で制度が出来たときの効果も、今後事務局が多面的に分析すべきではないか。

○　最後は結局、防衛産業のエコシステムをどう設計するかという話にも及んだので、どういう風に議論するかはいったん整理させていただく。

（８）高市経済安全保障担当大臣挨拶

○　皆様、本日も大変ご多様な中、第２回の有識者会議にご臨席賜り、誠に感謝。

○　本日は企業の方々から、経済安全保障分野におけるセキュリティ・クリアランス制度に対する具体的なニーズ、課題などについて大変貴重なお話を伺うことができた。

○　衆議院本会議で答弁が求められていたので、私自身が最後の６分の１くらいしか聞けなかったことは非常に残念だったが、その後、有識者の皆様から様々な論点が、話せば話すほど膨れ上がり、増えてきているなということで、問題の所在、議論を深めていかなければならないと思った。

○　前回の会議で、1 年程度を目途になどと言っておらずに早く、というご意見もいただいている。日本企業が海外でビジネスチャンスを失うような状況の放置はできない。

○　そして、同盟国・同志国との信頼関係、これも非常に重要なことなので、話せば話すほど論点は増えてしまっているが、日本にとって望ましい制度を一刻も早く作ることを目指して、スピード感をもって議論を進めていただきたいと思っている。引き続きよろしくお願いしたい。