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４回）　議事要旨

１　日時

令和５年４月７日（金）１３時００分から１５時００分までの間

２　場所

中央合同庁舎４号館　1208 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
星野　剛士	内閣府副大臣
中野　英幸	内閣府大臣政務官
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
遠藤　顕史	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の内容について説明があった。また、諸外国におけるセキュリティ・クリアランスの保有者数について次の通り説明があった。

○　アメリカでは約 400 万人のセキュリティ・クリアランス保有者がおり、１年あたり 100 万人程度の者がセキュリティ・クリアランスを新規取得・更新等している。

○　アメリカ以外の主要国、例えば、イギリス、ドイツ、フランス、カナダ、オーストラリアでも、数十万人以上のセキュリティ・クリアランス保有者がおり、毎年その四分の一から六分の一程度の者がセキュリティ・クリアランスを新規取得・更新等していると考えられる。

○　日本では、令和３年末時点で特定秘密の取扱いの業務を行うことができる者の数は 13 万人程度。令和３年中に適性評価が実施された件数は３万件程度。

○　なお、官民のセキュリティ・クリアランス保有者の比率について、アメリカでは官対民で約７割対３割。諸外国では、官よりも民が多いところもあるようであるが、日本では官が約 97%、民が約３％となっている。

（２）企業からの説明（１社目）

重要インフラ事業者・Ａ社から、資料２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２の１ページ、セキュリティ・クリアランス制度の必要性について。重要インフラ役務の安定提供に必要なシステムをどのように守るのか。そのためには、インテリジェンス情報というのが非常に重要であると考えている。

○　どのように守るのかの基本は、まずは防御を強化すること。そして、いかに早く発見するか。そして、迅速な隔離・除去。これを３つの基本としている。現在、国家を背景とする高度な脅威の集団が現実として存在しており、この脅威に対してどのように対応するかが重要。最新の侵害手段は常にアップデートされており、これに対して、自分たちの設備・システムは健全なのか、そのリスク評価をいかに速く回すか、これにかかっている。そうした対策のためには、海外または他社の詳細な一次情報が、リスク評価において非常に重要であると認識している。

○　１つの事例として、当社では海外のサイバーインシデントについて民間で契約しているコンサルタント等から色々と情報を取っているが、あるインシデント事案の現場に直接赴いたことのある海外の方と面談する機会があり、そのときの情報と我々が得ていた情報とのギャップの大きさ、詳細さに非常に大きな差があった。

○　つまり、いかに詳細な一次情報にアクセスできるかが、重要インフラ事業者の設備・

システムを守るために非常に重要であるというのが当社の経験である。

○　次に、予防的応動について。サイバー空間には国境はなく、有名な事案として、アメリカのコロニアルパイプラインの事案、フロリダの水道局のような事案がある。このような事案がどういう風に起きたのか。マルウェアの新型・亜種が出た時に、その情報をいかに速く取るか。それに伴って、当社のセキュリティの監視チームの強化、インシデントレスポンスの対応の迅速化・被害の抑止に非常に有用と考える。そのためには、セキュリティに関する海外の国家機関や事業者との情報交換を行うに当たり、セキュリティ・クリアランスが必要になると考えている。

○　別の事例として、当社がセキュリティを強化し始めた頃、人脈を伝って海外の同業他社や政府機関を直接訪問して情報を集めていたが、海外当局の方と話をした際には、具体論に入った途端に、「あなたはプライベート（民間）だから」ということで詳細を聞くことができなかった。

○　また、別の海外当局の方と話した際には、物理攻撃とサイバー攻撃のハイブリッド型にしっかり対応せよとの助言をもらったが、両方の訪問で先方から言われたのが、「セキュリティ・クリアランスをすぐ取りなさい」ということであった。

○　一方、国内の政府機関にも相談したが、結局は民間独自で動かざるを得ず、そのために人脈を活用し、現在の体制を作った。

○　２ページ、セキュリティ・クリアランス制度の活用範囲について。セキュリティ・クリアランスは、サイバーセキュリティ部門をメインに、その他リスク担当組織が主に取得し、必要な範囲、制度上問題ない範囲でビジネス部門・システム部門に指示することを想定している。当社は、リスク管理担当役員を設置し、全社リスクを管理している。

○　３ページ、政府に対する要望について。政府間の枠組みの下で、ヨーロッパやアメリカの国家機関と日本の民間企業との情報交換が可能となるような関係性を構築していただきたい。インテリジェンス情報は、正確さ、詳細さ、そして鮮度（時間）が命。特にファイブ・アイズのヨーロッパやアメリカの政府機関との連携は切にお願いしたい。

○　また、政府の情報保全制度の明確化をお願いしたい。重要インフラ事業者のうち、競合関係にある企業とは信頼は成立しないが、個社間で信頼関係が成立する会社とは情報交換をしている。ただ、情報量とその多様性に限界があり、政府が保証する情報共有に期待するところはある。一方で、官民の情報共有の活性化には、秘密保持のルールをしっかり作っていただき、情報共有に伴うリスクへの懸念をぜひ払拭してもらいたい。当社のある被害案件を共有した場合、当社のインフラ事業者としての適格性に疑念が呈されるような情報が、社会的に流布される事態になることを懸念している。このようなことがないように保証をお願いしたい。

（３）意見交換

○　非常に重要なご指摘をいただいた。事務局による整理が必要かもしれないが、根源的な問としてサイバーセキュリティにおけるインシデント情報は国家機密なのかという問題がある。サイバー攻撃は政府も攻撃されるし民間も攻撃される。インシデント情報やこれを惹起するマルウェア情報について、国が攻撃された場合は国が持っていて、民間企業が攻撃された場合は国家機密では無いということになってくる。また、インシデント情報は、発生してすぐ共有するのが重要。

○　サイバーセキュリティについては、様々なプロトコルや防御についての情報があるところ、インシデント情報やマルウェアの特性がセキュリティ・クリアランスを付与しないとアクセスできない情報なのかどうかは整理する必要がある。

○　資料２の２ページで、社内のどの部門にセキュリティ・クリアランスを付与するかという論点だが、民間企業にセキュリティ・クリアランスを付与するときには法人に対するセキュリティ・クリアランスが必要なので、社長も対象になる。施設部門や管理部門の役員の方々にもセキュリティ・クリアランスが必要。

企業より回答

○　社長の下にセキュリティ担当役員がおり、サイバーセキュリティの最終部門長としてのセキュリティ担当役員はセキュリティ・クリアランスが必要だろうということで青色としている。社長はいろいろな部門を兼任していることもあり負担が大きいというのもある。

○　重要インフラに関するサイバー情報を共有するのにセキュリティ・クリアランスが必要となる場合がある。それは防御策である。実際、アメリカのコロニアルパイプライン事案が起こってから、国土安全保障省が、防御策についてはパイプライン事業者の間で秘密指定されて共有するという対応がされていた。インシデント情報の共有にセキュリティ・クリアランスを要するかについては確かに議論が必要だが、防御策は明らかになることで対策がなされてしまうと問題なので、機密（Top Secret）レベルのセキュリティ・クリアランスが必要かと思う。

○　資料２の２ページについて、セキュリティ・クリアランスの対象者の規模を考えた際、サイバーセキュリティ部門の人員全員がセキュリティ・クリアランスを取得しないといけないことになるのか、あるいは、ごく一部、セキュリティに直結するようなところにだけレポーティングラインが限定されていてそこだけ取得することになるのか。人数のイメージが分かれば教えていただきたい。

企業より回答

○　一部分という認識。機微な情報に直接アクセスをして、社として何をすべきなのか

を判断し、部門内に指示できるだけの人数がセキュリティ・クリアランスを取得すればよいと考えており、それほど多くの人数は考えていない。当社の場合、１０名前後いれば十分だと思う。異動があるので一定程度のラップができればよい。

○　第２回の事務局資料２の情報区分のイメージ図で考えると、民間で発生したインシデント情報は「D」に当たると思うが、これが果たして国家機密なのかどうか。他方で政府の方で発生したインシデント情報は「A」に当たると思うが、果たして特定秘の対象となっているのかどうか。多分なっていないのだろうと思うが、そうであれば、保秘はどうなっているのか。国家公務員法の下での守秘義務がかかっているだけなのかどうか。

事務局より回答

○　詳細は改めて確認する必要があるが、インシデント情報が「D」なのか「E」なのかという論点がある。情報が政府に共有された結果、付加価値が付いた状態になり、それが更に民間側に共有されるようなときは、「A」や「D」になるのではないかと考えており、その扱いは整理する必要があると思う。

○　現状、政府側が持っているインシデント情報については、おそらく、他国から共有された場合であれば、ものによっては「A」に当たるものはあると思う。

○　また、特定秘密を関係省庁がどう指定しているかは数字が公表されている。それを見ると、インシデント情報を特定秘に指定していれば１とカウントされるだろうが、経済官庁の多くで特定秘密が指定されていないことから推察するに、経済官庁においては、インシデント情報そのものを指定しているということではないのだろうとの推測が成り立つ。

○　インシデント情報は共有することに意味がある一方で、共有をためらう事業者が多いのも実態。レピュテーションを含めた副作用を気にしているところもある。攻撃に関する属性情報と被害を受けた組織の情報を切り分けて、攻撃情報は今後の防御なり対応に役立つ情報なので、被害者情報と切り離す形で報告・共有する枠組みを考えていこうという取組もいま議論されている。

○　政府が認知したインシデント情報のほとんどは、特定秘密には指定されていないと認識している。一方で外国との情報交換の過程で提供されたものは特定秘密になっているのではないかと思う。

○　質問にあったように、仮に政府で被害を受けたものが「A」に分類されたとしても、基本的に官であろうと民であろうとインシデント情報とそれに付随するものは開示することで防御に資する性質のものだと理解するのが正しいと思う。それに対する防御策も秘密の度合が高いので、それがどの領域にカテゴリーされるかは今後検討していくことだと思う。

○　官か民かという２分法で話があったが、民でサイバーインシデントが起こり官に共有した場合、アトリビューションを定める能力は政府の方が高いため、その部分は政府が何らかのレベルの秘密指定をするはず。官民どちらに発生したかによって議論するのは難しい。

○　社長はいろいろ兼務しているのでセキュリティ・クリアランスは難しいとの意見があったが、社長にはセキュリティ・クリアランスを課すのがアメリカの制度。

企業より回答

○　現在の体制では、社長は最終的に責任を負うが、現場のオペレーションは全てセキュリティ担当役員が責任を負っている。

○　内閣サイバーセキュリティセンターでは色々なインシデント情報を集めて民間企業に情報提供する仕組みがあると聞いているが、水道とか電気とかガスとか通信とか、災害や事故があって使えなくなると国民生活に直結するような重要インフラ事業者は、世界中で今どんな攻撃、マルウェアがあるのかというのはただちに知りたいはずで、防御策についても国と共有したいだろう。そうなると会社できちんとした体制を整えて、それがセキュリティ・クリアランスになるのだろうが、国としてそういう方向に向かうべきなのではないかと考える。

○　資料２の最後のページについて、民間企業間の信頼関係がある会社同士の情報交換については、イメージとしては２ページの図にある、セキュリティ・クリアランスが必要とされる範囲である青色同士での情報交換ということか。

企業より回答

○　他の重要インフラ事業者のサイバーセキュリティ部門との間の情報交換という意味。ネットワークは狭いが、お互いのレベル感がそこで分かり、刺激になってセキュリティレベルをどう上げるか、という議論をしている。

（４）企業からの説明（２社目）

重要インフラ事業者・Ｂ社から、資料３の内容に基づき、経済安全保障分野においてセキュリティ・クリアランス制度が導入された場合に影響が生じる可能性のある具体的事例、課題等について、説明があった。

○　当社の従業員のうち、ごく一部の外国人が外国のセキュリティ・クリアランスを保有しており、サイバーセキュリティに関する部隊に所属している者もいる。ただ、業務内容はブラックボックスであり、日本本社には伝えられないのが現状。

○　資料３の２ページ、「１．セキュリティ・クリアランス制度に関連がある事例」とし

て、１つ目はサイバーセキュリティ関連情報の入手である。最近公表されたアメリカのサイバーセキュリティ戦略の中に、民間との機密情報を共有する戦略ということで、セキュリティ・クリアランス要件や機密指定情報のポリシーを適宜見直す旨が含まれている。官民で協力する際、機密情報を解除することもアメリカでは行っているようであり、民間との秘密情報の共有が進んでいくと思われる。これらの情報はアメリカ国内でも厳格に管理されているであろうから、仮に、こうした情報がアメリカの現地法人で入手できるようになったとしても、これらを日本本社に共有することが難しいのではないかと思う。

○　２つ目がアクティブ・サイバー・ディフェンス（ＡＣＤ）である。昨年 12 月に発表された「国家安全保障戦略」で、「国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する」と書かれている。あわせて、「国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するために、所要の取組を進める」と書かれている。事業者に協力義務をかけようとすると法的な手続きが必要となるし、これに伴う従業員に対する人的なセキュリティ・クリアランスも必要となってくる。

○　３つ目について、防衛産業以外で国際連携に影響が生じる可能性のある分野として、宇宙がある。例えば、相手国のシステム等と連携しようとする際、相手国のシステム等の仕様の提案要件の中にＣＵＩ（Controlled Unclassified Information）のみならずＣＩ（Classified Information）が含まれる場合があり、セキュリティ・クリアランスを取得しないと、連携が出来ないということが考えられる。

○　最後に、３ページに関連して、政府がセキュリティ・クリアランス制度を導入する場合には、３点申し上げたい。一つ目は、日本でセキュリティ・クリアランスを入れてもアメリカとの相互認証ができないと負担だけが増えるため、日本のセキュリティ・クリアランスをクリアすれば、アメリカなどの政府や企業に受け入れられる制度にしていただきたい。２つ目は、アメリカの社員がセキュリティ・クリアランスを取得した場合は日本でも有効にしてほしい。３つ目は、このセキュリティ・クリアランスは背景調査を伴うものなので、人権問題と常に裏腹である。背景調査を求める場合には、これを民間の裁量に任せるのではなく、政府の責任において、明確な制度を法制度上担保してほしい。法的担保のないまま行政指導で求めると企業は板挟みになる。背景調査を求める場合は、政府の責任で調査してほしい。

○　こういう類のものは、中途半端な行政指導でもなく、やるなら法的な手当てをしてほしい。

（５）意見交換

○　資料最終ページの①「日本国のクリアランスをクリアすれば、米国等の政府や企業に受け入れられる制度とすること」とあるが、日本でも同様の制度を作り二国間協議を経れば共有が可能となる可能性がある。

企業より回答

○　サイバーセキュリティ関連情報について、仮に日本のセキュリティ・クリアランス制度が整備され、諸外国と相互認証されても、民間企業が政府を経由せず海外政府に直接データを提供してもいいのかという問題がある。日本政府を通じてアメリカ政府に情報を提供する必要があるとなると、これは単にセキュリティ・クリアランスの問題に留まらず、日本とアメリカの政府間でルートを開かないと、双方でレシプロカルにはできない。

○　ＡＣＤについては、機密（Top Secret）より上位の通信等が該当する機微区画情報という区分があり、アトリビューションを決める際に外国のインテリジェンス情報が必要であるところ、これらに触れる業務については、おそらくアメリカでも民間人にはアクセスを認めておらず、政府機関から出向した者や元職の者が対応しているものと思われる。

企業より回答

○　ＡＣＤについては、諸外国の中には、政府機関の人が出向していなくても民間の事業者に相当厳格にセキュリティをかけることで実施していると聞いたことがある。

○　宇宙関係情報は日本とアメリカ間でＩＳＡ（Industrial Security Agreement；産業保全協定）を結ぶことができれば、最初に共有が可能なものであると考えられる。

企業より回答

○　宇宙は制度的に手当てすれば進みそう。

○　例えばＣＵＩがあったとして、これを扱う人に対して社内の人事部門が国籍等を聞くなど、ＣＩを扱うための詳細なバックグラウンドチェックまでは至らないもののある程度までのチェックは実施すべきであるという意見についてはどう考えるか。

企業より回答

○　最終ページの要望でも記載しているが、どれくらい何を調べるかは明確にしてほしい。そして背景調査を行うのであれば、そこは国でお願いしたいということ。国の政策として行うのであれば、明確な調査基準を設け、国の責任において調査を実施してもらいたい。これを企業にやれといわれても実際にできない。

○　バックグラウンドチェックの観点から、企業においてこういった事項を聞くべきであるというようなガイドラインを国が設けることについて、企業の立場からどう考えるか。企業の人事部門にとっては、バックグラウンドチェックが容易になるとも考えられるがいかがか。

企業より回答

○　セキュリティ・クリアランス制度がどういった場面を想定しているか定かではないが、国の必要性に基づいて実施するセキュリティ・クリアランス制度であれば国の方できちんと調査をするべきであろう。他方、ビジネスのために企業がやりたければ、企業が自らの責任において同意を得た上で調査を実施することになるであろう。

○　ＡＣＤに伴うセキュリティ・クリアランスであれば、これに協力する企業に対して、企業がやりたければやってもらうといった制度は無理があると思う。

○　我が国の法制では、官民どちらが調査を行うにしても本人の同意は絶対に必要であり、同意がなければできないと思う。

○　ガイドラインに従い本人の同意のもと人事部が調査した場合、アメリカが認めるかというとおそらく絶対に認めないだろう。何故かというと、民間企業の人事部では、アメリカが敵対視している国家のインテリジェンス機関の者と調査対象者が交流をしているかといった情報は保有していないためである。

○　なお、ＣＵＩであればきちんとした基準がないため、人事部が行った調整であっても認められる可能性はある。

○　政府や経済界の方々がアメリカ保有の情報、特にＣＩの共有を受けたい場合は、国の制度による背景調査が必要である。

○　宇宙分野の話について、海外のシステム等と連携するとなるとセキュリティ・クリアランスの取得は不可避である。さらにいうと、本当に機密保護の世界になるため、大変重要なテーマになると思う。

（６）自由討議

○　本日の資料２の２頁における「セキュリティ・クリアランス制度の活用範囲」における説明と＜活用イメージ＞における図を見ると、同資料を提出して下さった我が国の重要インフラ事業者においても、まだ法人に対するセキュリティ・クリアランス制度についての認識が十分に行き渡っていないのではないかと思われる。これは、この＜活用イメージ＞の図において、社長が「セキュリティ・クリアランスが必要とされる範囲」から除かれている点に表れている。アメリカでは、国家産業保全プログラム（National Industrial Security Program）における施設クリアランス

（Facility Clearance）の一部として法人に対するセキュリティ・クリアランスが必要になるが、株式会社（Corporation）の場合、経営幹部（Key Management Personnel）のうち、取締役会会長（Chairman of the Board）及び最高経営責任者（CEO）（あるいは、社長（President））には、セキュリティ・クリアランスが必要である。今後、我が国で同様の制度構築を検討する場合においても、この点に変わりはないものと思われる。さらに、サイバーセキュリティ部門において、機密指定された情報を扱う社員、及び、これらの方々に対して指揮命令権を持っている方々にはセキュリティ・クリアランスが必要になると考える。

○　これまで本会議においてプレゼンテーションをして頂いた企業からは、アメリカとＣＩレベルの情報共有をしたいとの希望が出されていた。このレベルの情報共有のために必要となるセキュリティ・クリアランスは、各企業の人事部が行えるものではなく、国によってしか実施することはできないものであると考えられる。そもそも、民間企業の人事部は、自社の社員が外国政府の工作員から接触を受けているといった情報を収集できない。このような情報は、一部の政府機関しか知ることができないものであろう。民間企業が、今後、政府の定めるガイドラインと被用者本人の同意に基づいて実施できる可能性のある調査は、ＣＵＩのレベルにおけるバックグラウンドチェックに限られると思われる。

○　社長や代表取締役権を持つ者をセキュリティ・クリアランスの対象にするかどうかについては、企業ガバナンスとの関係を考えても、そうしないと成り立たないと思う。アメリカの制度云々以前に、論理的に考えてそうならざるを得ないと思う。

○　事務局からのセキュリティ・クリアランス保有者数の説明について、参考で我が国の数字も教えてほしい。

事務局より回答

○　日本の数字をお伝えすると、2021 年時点で、特定秘密のセキュリティ・クリアランス保有者数はストックで約 13 万 4000 人。フローで約２万 7600 件。ストックの約 13 万 4000 人のうち民間は約 3400 人であり、フローの約２万 7600 件のうち民間は約 1100 件である。

○　保有者の数はイメージとしてつかめたが、運用面において、どのぐらいの体制であればこういった資格を与えられる体制を維持できるのか、また、どのぐらいの負担になるかについて、後日参考になる情報があればありがたい。

○　今、日本のセキュリティ・クリアランス保有者数の報告があり、民間についても一定程度の保有者がいることが分かったが、この民間の方々のバックグラウンドチェ

ックは誰が行っているのか。セキュリティ・クリアランスを付す該当の行政機関が行っているのか。それとも特定の調査を行う行政機関が行っているのか。

事務局より回答

○　基本的には行政機関が行うことになっている。例えば防衛産業であれば、防衛省と各種契約を結ぶことになるため、防衛省の長が行うということになる。

○　アメリカでは特定の調査機関が調査を行っていると聞いたことがある。日本では所管省庁が調査を行っているということであるが、所管省庁同士で調査レベルを合わせることは必要になるだろうか。

事務局より回答

○　適性評価を行うにあたり必要があれば、内閣官房が行政機関からの相談に応じ、統一的な回答を行うなど、調査レベルに差が出ないようにしている。

○　適性評価は運用基準に基づき実施することになっており、規範レベルでの斉一性が図られていると認識している。

○　基本的には質問票を用い評価を行うが、当該行政機関の長では分からない部分、例えば渡航歴や当該関係機関にしか分からない部分については、当該行政機関の長は、照会という仕方をとり、知見のあるところに聞いて必要な情報をとる、という形で評価を行う仕組みになっていると理解している。

○　ガバナンスの観点について、社長等会社のトップがセキュリティ・クリアランスを持っているに越したことはないというのはその通りであり、その方がガバナンスを効かせやすいというのも間違いではないと思うが、セキュリティ・クリアランスを持っていないからといって、当該会社が日本の会社法上ガバナンスが効いていないことになるのかというと、必ずしもそうではないと思う。企業からの説明でもあったが、社長がセキュリティ・クリアランスがない場合、確かにセキュリティ・クリアランス対象の情報そのものは見えないことがあるとしても、セキュリティ・クリアランスを持っている人を経営にいれ、当該部門のリスク管理等をその人に適切に委譲しつつ、その他の経営陣においては経営指標その他セキュリティ・クリアランスが必要ない情報等によってモニタリングすること等により、会社全体としてガバナンスを効かせているという整理ができる局面もあるのではないかと思う。例えば、家族の何らかの事情でセキュリティ・クリアランスを失ったら、社長は辞任しなければガバナンスが効いていないことになる、ということにはならないのでないか。ガバナンス上望ましいことは間違いないのだが、必ずしもマストな要件ではなく、違う整理もあり得るのではないかと思っている。どちらかというと、ガバナンスではなく、セキュリティ・クリアランス側からくる要件で必要かどうかを検討するほ

うがロジカルに整理しやすいのではないかと思う。

○　サイバーセキュリティに関して、産業界のニーズに加えて国としてのニーズもあることがはっきりしたのではないか。それ以外にも、特定秘密以外で秘密文書なり重要情報として国が管理しているものがあるはずだが、その中で、セキュリティ・クリアランスが必要となるものがあるのかどうかを、検討材料として今後例示していただけると良いのではないか。

○　特定秘密保護法については、立法時の議論を十分に把握していないので、わかる方がいれば教えていただきたいが、今回のテーマでは、対象者の「同意」というところが一つの肝になると思う。ネット上では、「プライバシーポリシー」や「利用規約」に同意してください、というボタンが出てくることがよくある。中身をきちんと読まなくても同意のボタンを押してしまうようなケースもよくある。他方、ヒトゲノム・遺伝子解析研究等においては、対象者の単なる書面による同意だけでは不十分で、研究者が被験者に詳細な研究内容の説明を行うことや遺伝カウンセリングの機会を提供することなどが、国の指針で求められている。つまり「真摯な同意」をとるための工夫がなされている。本テーマでも、「真摯な同意」をとるための方法について検討すべきかと思う。実際のところ、特定秘密保護法では、「同意」をどのような運用・手続きで取っているのか、差し支えない範囲で、教えて頂きたい。

○　セキュリティ・クリアランスの際には、アメリカでもそうだと思うが、基本的に身上調査票を埋めていただくという作業があると認識している。従ってそうした作業についての説明をしなければならないことになっていて、運用基準では同意にあたっての説明事項が規定されていると理解している。同意書の様式もあるかと思う。常識的な形で同意についてはさらっとやるというよりは、法律的に同意は明示されており、下位法令で更に様式的な形で担保しているという理解で良いかと思う。

○　やはり今回、同意をしないと、結局あるプロジェクトに携われないとか、セキュリティ・クリアランスが与えられれば給料を上げた方が良いという意見も過去あったかと思うが、同意をしないと、給料が上がらないという不利益があるかもしれない。会社の人事部門や経営層からしたら、この制度がちゃんと従業員に真摯に理解してもらわないと責任問題になりかねないと思い、その辺を危惧している。

○　特定秘密保護法においては、評価対象者となった方からの同意を得て、運用基準に定められている質問票に記入していただくという手続が必要になる。この質問票には、ご本人のみならず家族や同居人の方に国籍や、帰化歴があるかといった詳細な

情報を記入して頂く必要があるが、非常に時間と手間を要するものである。このため、先ほど例として上がったネット上で同意ボタンを押すというレベルで気軽にできるものではない。また、事前に適性評価についての告知がなされるとともに、一度同意した場合であっても、後で取り下げることができる制度になっている。

○　先程、他の委員からご指摘のあった企業等に関するＦＯＣＩ（Foreign Ownership, Control or Influence；外国による所有権・管理・影響）については、まだ我が国で十分な理解がされていないと思われる。アメリカにおける同制度は、機密指定された情報を政府と共有している企業等が、外国関係者（foreign interests）による株式の保有などにより支配されていないかどうかを事前に審査するものである。これをチェックしないと、外国関係者による機密情報へのアクセスを排除することができない恐れが生じる。なお、外国籍の方が経営幹部にいる場合でも、その方が機密指定された情報にアクセスできないようにする仕組みを整えて政府に認めてもらうことは可能である。また、外国の株主については、当該企業の株式所有に付随する多くの権利を、アメリカ政府によりセキュリティ・クリアランスが認定された取締役会の構成員に譲渡する取決めである議決権信託合意及び委任状合意（Voting Trust Agreement and Proxy Agreement）等の仕組みが整えられており、非常に優れた制度であると評価できる。なぜ我が国でＦＯＣＩが知られていないのかというと、特定秘密保護法には同制度がないためであると考えている。それでは、なぜ特定秘密保護法の下では、法令上ＦＯＣＩの要件がないにもかかわらず、民間事業者等である適合事業者は、政府と特定秘密を共有しうるのであろうか。これは、私の推定ではあるが、適合事業者の大半を占めると思わる防衛産業における該当企業が、すべてＦＯＣＩの要件を満たしており、また、アメリカもこの点を理解しているためであると考えられる。また、特定秘密保護法の下における運用により適合事業者を認める方法では、事務局が紹介した民間企業におけるセキュリティ・クリランス保有者の数字で明らかなように、その人数が非常に少なくなってしまう。また、ＦＯＣＩは企業等の経営組織にかかわる問題であることから、日本経済団体連合会、経済同友会及び日本商工会議所を代表されている委員の方々に、ＦＯＣＩに関する意見や要望を述べて頂く機会があればよいと考える。

○　２点ある。一つは、先ほど特定秘密保護法の関係で、身上調査票の話が出てきたと思うが、アメリカのセキュリティ・クリアランスでは、国籍とか家族の属性だけではなく、経済状況に関する情報もかなりある。おそらく特定秘密保護法でも同様かと思うが、本人が持っている資産や、いわゆる経済的な活動に関するものを全て出さないといけないので、気軽な同意ではなく、本人しか持ち得ない情報まで出さないといけないと理解している。今後、セキュリティ・クリアランスの制度を検討していくにあたって、どこまでの情報を求めるのかという議論になると思うが、やは

り外国からの資金流入とかも含めて、審査というか情報として持っておくべきものになると思う。これは、アメリカの場合、同意をしない、ないしはセキュリティ・クリアランスを取らずにビジネスを行うという選択の大きな分かれ目になっている点であるかのように聞いているので、注意深く検討しておく必要があると思う

○ もう一つは、今後問題になってくるのが、防衛用に作っていないシステムが防衛目的で使われる場合、どこまでがＣＩ／ＣＵＩになるのか、非常に流動的な状況になる。民間のサービスとしてやっている場合は、機密にならないが、いざ防衛システムと接続された瞬間ＣＩになるという、運用上の変更が起こりうる。これは結構トリッキーな状況で、作っている時はそうではないが、作った後に技術情報やシステムに関わる情報が突然機密指定される可能性があって、そういうやや不規則なケースもあるということを想定しておいた方が良いと思う。

○ 最後の点は、アメリカでどう処理しているのか、かなり細かくケースバイケースでやっているのであろうと思うが、ノウハウが要る世界かと思う。

○ 事後的にセキュリティ・クリアランスが必要になるという状況が生じた場合にどうしたら良いのかというのは、かなり制度の運用上のノウハウが必要になると思う。

○ 詳しく調べたことはないが、アメリカにおいては、国防総省を中心に、今後、軍事技術又は軍民両用技術として発展する可能性のある技術について、各技術分野の専門家が、論文、研究開発助成金獲得のための申請、特許申請等に関する情報収集を常に行うことで、アメリカ政府が知らない間に機密指定すべき技術が外国政府等に流出してしまう事態を防いでいるのではないかと考える。

○ 私もそういうノウハウを持っている人の話は聞いたことがあるが、多分インタビューしても答えてくれないであろう。

○ 各国のセキュリティ・クリアランス保有者数を教えていただき感謝。どこの国も一定程度、むしろ日本と比べると相当数セキュリティ・クリアランス保有者が居るということが分かった。やはり安全保障の分野こういう制度・ニーズがあるということが分かった。

○ 特定秘密保護法の下では、民間のフローの数字は約 1100 人ということで、アメリカはとんでもなく大きいが、日本とかなり似ているドイツでも日本と比べると約 10 倍であるということか。おそらく、特定秘密保護法でカバーしている分野以外の分野で、セキュリティ・クリアランスを取得しているのだろうという実態があるということかと思う。また、大体、有効期間と関係していると思うので、ストックは４

～５倍と考えれば良いのではないか。引き続きこういう情報が得られればそれだけ良いと思うので、情報収集をお願いしたい。

○　それからこういったセキュリティ・クリアランス保有者の人数をどう支えているかということ。それは可能な範囲で知りたいと思う。

（７）高市経済安全保障担当大臣挨拶

○　本日も、有識者会議にご参加いただき、誠に感謝。このセキュリティ・クリアランスの有識者会議の発足以降、かなり頻繁に開かせていただいており、今後ともどうぞよろしくお願いしたい。

○　本日は、企業２社の方から、サイバーセキュリティの観点からも、セキュリティ・クリアランス制度に対するニーズや課題についてお伺いすることができた。

○　これまで企業５社の方々から、貴重なお話を伺いながら、委員の皆様にご議論をいただいた。引き続き、ご知見をいただきながら、スピード感を持って、きちんと制度化に向けて取り組んでまいる所存。どうかよろしくお願いしたい。