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５回）　議事要旨

１　日時

令和５年４月 25 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　特別中会議室

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
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

（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
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
遠藤　顕史	内閣官房内閣審議官
小松　克行	防衛装備庁装備政策部装備保全管理官

４　議事概要

（１）高市経済安全保障担当大臣挨拶

○　委員の皆様におかれては、御多忙の中、第５回有識者会議に御出席いただき、心より感謝。

○　これまで電機メーカーや重要インフラ事業者から様々なお話を伺ってきた。本日は、事務局から、スタートアップ企業におけるニーズや事例の紹介を行うほか、内閣官房や防衛省から、情報保全制度などについて説明が行われる予定。これらを踏まえた本日の自由討議においては、目指すべき制度の方向性について、更に議論が深まるのではないかと期待している。

○　引き続き、委員の皆さまの御知見をお借りしつつ、政府としても検討作業を鋭意進めてまいりたい。本日も活発な御議論のほどよろしくお願いする。

（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）関係省庁説明（内閣官房内閣情報調査室）

内閣官房内閣情報調査室から、資料３の内容に基づき、特定秘密保護法の概要について、説明があった。

（４）意見交換

○　資料３の６ページの適性評価の調査項目については、防衛省や外務省等の行政機関が司々で対象者に聞くことになると思うが、①～⑦の項目をざっと見ると、⑤（精神疾患に関する事項）や⑥（飲酒についての節度に関する事項）、⑦（信用状態その他の経済的な状況に関する事項）といった項目は警察等の協力を得ないと把握や確認ができない情報だと思う。どういう運用状況となっているのか。

内閣官房より回答

○　精神疾患や飲酒の節度に関する事項等はプライバシーに関わる事柄であるが、各行政機関においては、人事管理を通じて、各職員の日頃の健康状態等を把握していることが多い。④（薬物の濫用及び影響に関する事項）といった項目についても、上司等が平素のコミュニケーション等を通じて、そうした事情があれば把握しているものと思われる。

○　適性評価に係る調査の方法は、まず、本人に詳細な質問票に自己申告をしていただく。同時に、その本人をよく知る上司等にも調査票により関連する質問に回答いただく。

○　その過程で、例えば、精神疾患の通院状況の申告があれば、必要に応じて、通院先の病院に照会をすることもできる。

○　このように、各行政機関において調査事項に関する情報を把握し、確認を行っている。

○　適合事業者の適性評価について、これまでにクリアランスを取得できなかったケースはあるか。
○　質問票による調査に疑問が生じた場合、上司等に調査がなされるとのことだが、これまでにそうしたケースはあったか。

内閣官房より回答

○　民間事業者は、特定秘密保護法上、適合事業者に認定された後にその従業者のクリアランス（適性評価）をしていくこととなるが、その適性評価において、「特定秘密の取扱いの業務を行った場合にこれを漏らすおそれがない」と認められなかったケースはこれまでのところ承知していない。
○　資料３の６ページ上に、調査の過程で疑問が生じた場合に、更に質問や照会をすると記載しているとおり、質問票の自己申告の内容と上司等による調査票の内容等から矛盾点があるなどの場合、本人に対する面接までは行わずとも、本人やその上司等に事実確認をすることは行われている。
○　運用基準では、調査を適切に実施するため必要があるときは、手続の順序を入れ替えて実施することを妨げないとされており、実効性のある形で調査は進められる。
○　各適合事業者において、適性評価の対象となる候補者の選定の段階で、それまでの様々な情報を総合して適任者を選定しているといった状況があるとみられ、クリアランスが認められなかった者がいないということにつながっていると推察している。

○　適合事業者の数の内訳に中小企業は入っているか

内閣官房より回答

○　中小企業については、詳細は申し上げられないが、規模の小さいところもあったと承知をしている。

○　適合事業者の中で適性評価を行う対象は、情報に直接アクセスする者だけか、それともマネージャーも含むか。

内閣官房より回答

○　基本的には、特定秘密を取り扱う者ということになるが、管理職であったとしても、特定秘密を使って仕事をしなければならないということであれば対象になる。

○　特定秘密を扱う人がいるとして、マネージャーにしろ、社長にしろ、その情報に触れないのであれば適性評価は不要ということか。

内閣官房より回答
○　そのとおり。

○　資料３の９ページで、各役所でかなりの数の方が特定秘密を取り扱うことができるとなっている。役所は、局長・課長・担当者といったピラミッド型の組織だと思うが、ある担当者が特定秘密に触れるためにクリアランスを得たとして、その上司に当たる人は、特定秘密に触れないのであればクリアランスは不要ということか。
内閣官房より回答
○　そのとおり。全く触れないのであれば適性評価は不要。少しでも触れる可能性があるのなら必要。

○　クリアランスがない人は、役所の中であっても、特定秘密の内容を聞いてはいけないということか。
内閣官房より回答
○　そのとおり。

○　調査事項の中に、帰化歴や渡航歴も含まれているのではなかったか。
内閣官房より回答
○　質問票により、渡航歴や外国政府機関との関係等は、自己申告をしてもらっている。また、家族・同居者について日本国籍を有しているか、帰化歴があるかを申告してもらっている。プライバシーに配慮しつつ、必要な事項は申告してもらっている。

○　資料３の１ページの法律解釈適用で、報道・取材の自由について書かれているが、特定秘密保護法の逐条解説には、「報道機関による、たまたま入室可能な状態となっていた部屋に入り、閲覧可能となっている状態のパソコン画面あるいは紙媒体の特定秘密を閲覧した、そういう行為は、処罰対象とはならない」ということが書かれているところ、逐条解説にはこのように色々な例が明記されている。これは運用基準にも明記されているのか。こうした行為により特定秘密が新聞等で報道された場合、それは、施設保全を行うべき公務員側の責任になるのか。
内閣官房より回答
○　御指摘の逐条解説の記述は運用基準に記載されていない。

○　ただし、公務員側は、過失又は行為そのものについて罰せられると理解。
内閣官房より回答
○　しかり。

○　先日、防衛省の特定秘密の漏えい事案があったが、関係国から信頼のある制度としていく観点から考えていかなくてはならない点があると思う。

○　１点目として、先ほどの内閣官房からの説明は、諸外国、主にアメリカを念頭に置いた説明なのだと思うが、相手国のトップシークレットやシークレットは特定秘密保護法上の３つの要件に該当すれば特定秘密となり、コンフィデンシャルは、通常、特定秘密に該当しないとのことだった。考え方の整理は諸外国によって違うのかもしれないが、アメリカでは、トップシークレットは「例外的に重大な損害」が引き起こされる情報、シークレットは「重大な損害」が引き起こされる情報、コンフィデンシャルは「損害」が引き起こされる情報、と整理されている。一方、特定秘密保護法の条文上では、特定秘密は「その漏えいが我が国の安全保障に著しい支障を与えるおそれがあるため、特に秘匿することが必要であるもの」とされている。この特定秘密の解釈が、トップシークレットの「例外的に重大な損害」及びシークレットの「重大な損害」に対応しているという整理なのか。特定秘密は４分野に限られるという別の論点はあるとは思うが、どのような整理になっているのか御教示いただきたい。

事務局より回答

○　１点目の質問について、我が国は諸外国との関係で情報保護協定があり、通例、相手国のトップシークレットとシークレットに該当する情報は我が国では特定秘密と明記されており、そこに対応関係がある。また、相手国のコンフィデンシャルに該当する情報ついては、我が国では行政文書の管理に関するガイドラインの秘文書に相当するとの仕切りになっており、それに基づき各省において保全措置がとられている。今後、経済安保分野におけるセキュリティ・クリアランス制度を検討するに当たり、コンフィデンシャルに相当する情報の取扱いについて、規制強化も含めどのように管理していくのか検討する必要がある。

○　２点目として、指定権限のある行政機関の長として、例えば国土交通省が入っていない。経済安全保障上の基幹インフラやサイバー分野における重要インフラ等、国土交通省の管轄には安全保障に影響がある重要分野が含まれていると思うが、指定権限者になっていない理由は、国土交通省が保有する情報は４分野に該当せず特定秘密にはならないからなのか。指定権限を有する行政機関が限られていることの背景について御教示いただきたい。

内閣官房より回答

○　２点目の質問について、特定秘密に該当するかは、３つの要件を満たしているどうかで判断される。そのうちの１つの要件は、安全保障に関する情報で４分野のいずれかに該当するかどうかである。重要インフラだからという理由で指定されるわけ

ではない。

○　特定秘密保護法の目的は、国の存立に関わる外部からの侵略等に対して国家及び国民の安全を保障することとされているが、以前、重要インフラ事業者から説明のあった、インフラを制御するシステムに関する情報は機微な情報であり、法の目的にまさに該当するのではないかと思う。このように、重要インフラや電力・通信等は特定秘密ではカバーできていないと思うが、法改正すればカバーできるようになるのか。

○　また、特定秘密は国が保有する情報ということであるが、民間企業が保有する情報は対象にはならないのか。

○　制度の制定当時、指定行政機関を決める際に、内閣官房において国家安全保障に関する情報があるかどうかを各省に尋ねたが、その際に指定の可能性も含めて「無い」と回答した各省には指定権限が付与されなかったと聞いている。各省からは、指定権限のある行政機関に「なりたくない」との回答がほとんどであり、10 年前の状況は、「安全保障という分野にタッチしたくない」というものであったと聞いている。特に当時、基幹インフラはサイバー攻撃を受けるため安全保障に関わるという議論が進んでなかったこともあるのであろう。なお、指定行政機関は政令で定めるとされているため、仮に分野が横に広がった場合は、内閣官房において指定行政機関の見直しがされるのではないか。

事務局より回答

○　特定秘密保護法でカバーできない部分をどう考えるかについては、まさに有識者会議で各企業からヒアリングをしたところであり、現行法ではクリアランスを得られないという声も上がっている。そのため、現行法の運用改善若しくは法改正して対応するべきという声が出ているということかと思う。

○　また、特定秘密保護法は、政府が持っている情報を個別に指定し秘密とする。それを民間に共有する場合には適合事業者に共有することになる。したがって、純粋に民間が保有している情報を特定秘密に指定する仕組みはない。

内閣官房より回答

○　テクニカルに言えば、法改正をすれば特定秘密に該当することになるのはその通りであるが、法律の目的は、我が国の存立に関わる外部からの侵略等に対して国家及び国民の安全を保障するものであり、この枠を変えるのであれば、そもそもの法律の目的も変えることになる。

○　今の内閣官房による特定秘密保護法の説明で、「国の存立に関わる」という点につ

いて、安全保障に関わる定義規定に対する議員修正があったと思うが、列挙されている事項に何らかのものを加えると法律の性格が変わってしまうという説明があったが、それは違うと考える。国の存立に関わるということは、安全保障の定義という形で記載されており、その下の要件が１項目増えたところで、法律の内容が変わるとは言えないと考える。

内閣官房より回答

○　ここの目的を変えるとすれば、法律の目的が変わってしまうという趣旨で申し上げた。

○　今の指摘は特定秘密の定義規定についてであって、目的の部分についてではないのではないか。「国の存立」というのは、安全保障の定義規定であって、その下の部分に新しいものが入ったからと言って法律の解釈が変わるというのはおかしいのではないか。

○　特定秘密保護法の４分野には緊急案件も含まれると思うが、例えば、クリアランスを保有している担当者が、直ちに政府としての対応が必要であるため上司に報告しなければならないという場面で、当該上司がクリアランスを保有していないために情報共有できないといった不都合は想定されないのか。今後、クリアランスの対象を経済分野に拡大した際に、課長や部長、取締役まで知らないといけないような情報なのかという論点にもつながる質問ではあるが、現状どのような運用なのか。クリアランスを保有する担当者の上司もクリアランスを保有しているという認識で良いか。

内閣官房より回答

○　通常、担当者は業務状況を上司に報告する必要があり、その際に上司も当該情報に接し得ることが想定されるため、上司もクリアランスを保有する必要があるのだろう。

○　内閣官房で危機管理に携わる者については、特定秘密に接しなければならない局面もあるため、基本的には全員クリアランスを持っているという理解でよいかと思う。

（５）関係省庁説明（防衛省）

防衛省から、資料４の内容に基づき、防衛産業保全について説明があった。

（６）意見交換

○　例えばイギリスと共同するプロジェクトは、その際の法律上の立て付けとしては、特定秘密保護法ということになるか。

防衛省より回答

○　しかり。我々は、様々な国と保全に関する国際協議を実施しており、その際、実質的同等性を議論するときに何が重要かと言えば、法律がどうなっているかというのも重要だが、より重要なのは実際に何をやっているか、実行の部分で何をやっているか、である。例えば、先ほど紹介のあった、シークレット、トップシークレットが特定秘密であり、コンフィデンシャルが秘であるのはなぜかと言えば、そういうふうに決めたから、という部分もあるが、それよりも、そこでとられている秘密保全上の措置が実質的に同等かどうかという点がポイントになってくるので、一番大切なのは何を実行しているかということである。

○　実質的同等性に関し、制度改正を目指すのであれば、防衛省としては、特別防衛秘密において行われているような手続が基本的には望ましいと考えているか。

防衛省より回答

○　我々としては、特定秘密・特別防衛秘密を含め、現行の保全制度を活用しながら国際協力を含めて実施していく。その前提で、戦略３文書上の施策を含め、様々な施策を進めている。

○　防衛装備品の周辺技術についての協力についてはどう考えるか。

防衛省より回答

○　今、軍事技術というのは、各国とも、デュアルユース技術を含めてうまく活用している。その意味で、しっかりと周辺技術も管理されるべきと当然考えている。ただ、その手法が秘密保全制度なのか。秘密保全制度というのは、国家が指定した秘密を相手に渡したときに、企業に守ってもらうための制度であり、これが産業保全制度の概念である。しかし、会社が作り出した秘密を社外秘として守る制度や外為法の制度等をどう組み合わせていくのかが重要なテーマとなってくる。防衛省としても、このような取り組みに防衛の視点から協力すべく引き続き検討していく必要がある。

○　説明の中で、法人に対しては、アメリカのＦＯＣＩのようなものを実施しているとのことであったが、アメリカのＦＯＣＩの場合、株式会社では取締役会議長（会長）とＣＥＯのクリアランス取得が要件となっている。我が国では、防衛産業に関わっている者に対して、会長とＣＥＯに対してセキュリティ・クリアランスを実施しているのか。

防衛省より回答

○　ＦＯＣＩに関して、セキュリティ・クリアランスを誰まで付与するかについて、まず、会社において、防衛省と関係する機微な情報にアクセスする範囲を会社で決め

てもらう。その際には、Need-to-know の大原則に基づき、知る必要のある者にのみ付与することになっている。これを踏まえ、一般的に言えば、大会社については取締役に関しては防衛部門の長だとか、現実的に秘密情報にアクセスして判断を行う者などについては必ずセキュリティ・クリアランスを取得してもらうことになる。他方、アクセスする予定がない者にセキュリティ・クリアランスを付与することはない。また、規模が小さい会社については、社長がセキュリティ・クリアランスを取得するケースもある。

○　日本企業がアメリカに法人を設立するなどしても、ＮＩＳＰOMの規定により、原則として極秘までの情報しか交換できないはずであり、それを超える場合にはアメリカ政府による国家利益決定が必要になると思うが、今回防衛省から説明のあった「外国のプロジェクトに参画する日本企業との秘密保護契約」に関する制度においては、極秘を超える情報について情報交換が可能なのか。

防衛省より回答

○　アメリカとどのレベルの秘密まで共有できるかについて、日米のＧＳOMＩＡにおいては、トップシークレット以下全て情報共有できることになっている。個別のプロジェクトについて、どの範囲まで情報共有するかは、委員御指摘の米国の制度との関係も含め、個別の状況によることになる。

○　ＣＵＩに関するサイバーセキュリティ基準について、これは優れた施策と思うが、ここには機密指定された情報、すなわちＣＩに関する我が国のサイバーセキュリティ基準についての記載がない。我が国がアメリカから機密指定されたサイバーセキュリティに関する情報を共有してもらった場合、これを我が国の民間事業者に配信する際には、アメリカで行われているように国家安全保障システム（National Security Systems）と同じレベル・要件を満たしたシステムが必要になると考える。なぜなら、外国の秘密情報を送付する場合には、アメリカと同様に高度な秘密保全措置がなされたネットワークシステムである必要があるためである。そう考えると、アメリカの国家安全保障システムと同等のものを、民間企業への配信も含め、どのように策定するべきと考えるか。

防衛省より回答

○　防衛省が政府として保有している情報システムについて、ＮＩＳＴ　ＳＰ８００－３７に規定のＲMF（Risk Management Framework）を防衛省の全体システムに導入しようとしている。そこでの検討の状況を踏まえながら、防衛産業における秘密の取扱いについて、どのようにしていくかは今後検討していく。

○　アメリカがＦＯＣＩで考えているのは、社長や取締役の Need-to-know ではなく、

これらの者が外国から影響を受けている場合、あるいは、脅されるなどしている場合には、会社法上の権限により、機密指定された情報にアクセスする恐れがあることから、セキュリティ・クリアランスを要件とするというのがアメリカの仕組みである。その点を防衛省ではどう考えているか。

防衛省より回答

○　まさにそのように認識。アメリカの制度は洗練されている。冷戦の終わりからＦＯＣＩを導入しており、相当な経験をもって今の制度を作ってきている。他方ＦＯＣＩは国際的に発展途上の制度であり、国によって相当異なっている。防衛省としては秘密を取り扱う企業が外国の影響について評価した上で契約していくことは重要な論点だと考えている。現行制度は、令和元年から導入している制度であるが、今後も検討していく。

○　アメリカだけが全てではないということなのだと思うが、他国がＦＯＣＩあるいは類似の制度を持っている場合、どういう形でセキュリティ・クリアランスをかけているのか、是非情報共有をお願いしたい。今後制度設計をしていく上での一つの大きな論点ではないかと思う。

○　コンフィデンシャルが特定秘密の対象になっていないというやり取りの中で、行政文書の管理に関するガイドラインにおける秘文書の扱いを新しい制度設計の中でどう扱うかは要検討だとの説明が事務局よりあったが、その問題意識で言うと、防衛省の秘密区分ではコンフィデンシャルの部分は特別防衛秘密ということでセキュリティ・クリアランスがかかっている。今後新たな制度で、いわゆる技術というものに対して、秘密保全をしてセキュリティ・クリアランス制度を導入していくに当たっては、防衛省でやっているようなコンフィデンシャルに対するセキュリティ・クリアランスの扱いは、参考材料になると思う。その観点では、技術の中でもいわゆるデュアルユースになると防衛も非防衛も関係ない。同じ技術に対して、防衛省としてはコンフィデンシャル情報としてセキュリティ・クリアランスをかけている。これは新しい制度ではどうするのかという問題にも関わってくるので非常に重要。特に、これまでの企業ヒアリングの中には、防衛も含めて政府一体となった制度設計を期待するという声もあったところ。情報保全制度の全体の中でどう位置付けていくのかということかと思う。

防衛省より回答

○　一点、デュアルユースの技術は民間で使っている技術であるが、国家が指定した秘密というのはコンフィデンシャルも含め国が全面的に管理するということになる。民間企業が独自に、防衛省と無関係のところで生み出した技術をいきなり国が指定するというのは現実には難しいので、むしろ外為法や投資審査などまさに経済安全

保障の業務として行っていくのが合理的かと思う。

○　デュアルユース技術について言えば、経済安全保障推進法上の「経済安全保障重要技術育成プログラム（Kプロ）」では罰則が１年となっている。そうすると、防衛省からすれば、罰則が 10 年ではなく１年なので、罰則１年で保護できる程度の情報しか提供することができないため、せっかく作った制度が発展しにくくなる。Kプロを活用していくためには、罰則１年では足りないのではないかと思う。仮に第５分類みたいなものを作り、経済安全保障の分野にまで広がる中でセキュリティ・クリアランス制度ができ上がり、罰則が 10 年となれば、Kプロの制度も活用しながら、防衛省自身が提供できる情報が広がりやすくなると思う。更に言えば、米国と一緒に共同研究する道も開かれるのではないか。Kプロをより活かすという意味においても、経済安全保障という領域を広げていくことは重要ではないかと考える。

事務局より回答

○　Kプロについては、政府側から提供した情報については守秘義務がかかり、漏えいした場合の罰則は１年。これは、国家公務員は国家公務員法上の守秘義務がかかるため、これと同等の情報を提供する場合には並びで守秘義務を求めるというもの。Kプロについて、現状どういう技術や研究プロジェクトを対象にするのかということについては、基礎段階から応用段階に少し上がったものを念頭に置いており、技術熟成度（ＴＲＬ）で言えば、まったくの基礎研究ではないが少し上に行ったものというふうに考えている。したがって、特定秘密に該当するような情報をKプロで渡すのは事実上考えにくい。他方で、Kプロとは別に、将来的な在り方はまさに今後の検討課題。より機微度の高い研究を政府と民間で共有しながら進めていく場合が生じれば、別の枠組み等も含めて検討する必要があると考えている。

○　別の枠組みを作る必要はないのではないか。現在のKプロの枠組みのままでも、経済安保関連でセキュリティ・クリアランス制度ができれば罰則 10 年の上乗せがかかるので、そうした人に対しては、その部分については防衛省がより機微な情報を提供できることにつながるのではないか。

事務局より回答

○　本当に機微度の高い研究で保全をかけた情報共有の枠組みを作るのであれば、更に多くの論点、例えば、保全の在り方、成果の扱い方も考えた枠組みにすべきではないかと考えており、更に検討が必要と考えている。

○　企業を契約で縛ることの意味合いについてお尋ねしたい。先ほどの罰則の話は個人・自然人に対するサンクションだと思うが、契約の中には違約金条項や解約条項など、いわゆる契約違反をしたときに企業側に何らかのサンクションが与えられる

という構造になっていて、当然法的拘束力はあるのだと思うが、これは法人に対して実際どのくらいの縛りになっているのか、あるいは契約を守ろうというインセンティブを与えられるものになっているのか。資料の最終ページでは、秘密保護契約は無償契約となっており、これは単純に秘密保持だけ定めるということになっていると思われるが、違反したときに罰則など何かしらのサンクションが無いとこれだけで意味があるのかと思うが、どうか。

防衛省より回答

○　契約に基づいて、保全規則の作成、保全教育の実施、保全施設の設定をしたりするが、こうした規則の内容や施設の中身も防衛装備庁の方で基準を作っており、これを満たすものをやってくださいということを義務付けている。契約に基づく措置は産業保全制度の根幹であり、アメリカにせよイギリスにせよカナダにせよ契約に基づき保全措置をとっていると認識している。仮に漏えいを起こせば、いわゆる施設クリアランスや適合事業者性を見直さなければならないほか、状況によっては契約において競争上不利になる。加えて、個人に関して特定秘密であれば懲役刑がかかる可能性もある。防衛産業において秘密情報を取り扱っている方や企業の保全施設を見せていただいても、本当に気を配って作業しており、現行の契約に基づく産業保全制度は機能していると考えている。

○　契約そのものでサンクションを何か定めているということではなく、それを違反したことによって施設クリアランスが失われたり、入札に今後参加できなくなったり、そういった周辺のサンクションが非常に大きいので、そこの重しが効いていると理解。

（７）自由討議

○　防衛省の委託研究や公募研究などの研究に関してお伺いしたい。民間の研究機関や国立の研究機関に秘密情報を提供して、委託研究等を行う場合のルールや実際の運用について教えてほしい。

防衛省より回答

○　基本的に、企業や国立研究開発法人において秘密情報を管理する必要がある場合には、資料に記載の契約に基づく保全措置をとることとなる。他方で、防衛省が大学等に資金提供して行ういわゆるファンディングについては、オープンの研究を行っていただくものであり、秘密情報を提供する前提で行われているものではない。

○　資料４において、ＮＩＳＰＯＭを参考にして防衛産業保全マニュアルを現在策定中とあることから、その前提となる資料であるＮＩＳＰＯＭの行政規則と、関連する

国防総省マニュアルの第一部及び第二部について、庁内で翻訳されているのではないかと思い事務局に確認したが、ないとのことだった。また、事務局にも翻訳はないとのことであった。なお、ＮＩＳＰOMが行政規則化される前のＮＩＳＰOM第２版については、防衛整備基盤協会が翻訳したものが公開されている。そこで、事務局へのお願いだが、事務局等の予算を使って現行のＮＩＳＰOM規則と関連文書の全訳を外注していただき、事務局で翻訳をチェックした上で、配布先はお任せするが、少なくとも本委員会の委員にファイルで配信してほしい。これらの英語文書は、Ａ４横打ちで３５０ページほどあり、個人で翻訳すると疲弊してしまうので、是非ともお願いしたい。これがあれば、本委員会の委員の中で、アメリカのセキュリティ・クリアランスの民間企業に対する制度の理解が一気に進み、ＮＳＳの事務局における業務が円滑に進むと思うので、是非とも検討していただきたい。

○　アメリカから提供される機密指定されたサイバーセキュリティ関連の情報は、非常に有用であると聞いている。アメリカでは、これを重要インフラを担う民間企業に配信するため、国防産業基盤（Defense Industrial Base）を保護するためのプログラムで公開情報と機密情報の双方を扱う高度サイバーセキュリティサービスを、これらの企業にも適用することにした。アメリカは、当初、防衛産業に限ってこれらの情報を配信していたが、サイバー攻撃が激しくなったことから、重要インフラ企業にも配信するための制度を整えたのである。また、そのために必要となる商用サービスプロバイダーの認定も行っている。今回の法制か、その先になるか分からないが、我が国も同じようなシステムを整えない限り、重要インフラがサイバー攻撃にさらされる可能性が高くなる。この点につき、国家安全保障局かＮＩＳＣの事務局に計画や考えがあれば伺いたい。

事務局より回答

○　今直ちに事務局の方でそのような計画があるわけではない。

○　事務局へのお願いだが、第１回会合でも発言したとおり、関係省庁による説明として、特定秘密保護法や防衛省の話について、現在どのような運用をされているかという御説明を伺ったが、これから先のことを考えたときに、例えば経済官庁にも説明してほしい。経済官庁には、あまり関与したくないという雰囲気がいまだにあるのではないかと推測する。産業界が制度整備を要望している中で、経済官庁自身が当事者意識をもって取り組まなければ、どのような制度を作ろうとも動かなくなってしまうと思う。経済官庁自身がどういうポジションでどういう貢献をしていく所存なのか聞くことが大事だと思う。やり方は事務局に任せるが、そのような機会を設けていただきたい。

事務局より回答

○　本有識者会議の設置は、経済安全保障推進会議という閣僚級の会議で総理の指示があり、高市大臣にも検討の指示があって始まっており、そこには各閣僚が経済官庁も含めて参加している。また、その後、高市大臣が経済官庁を集め、情報保全制度の検討が始まったので協力をお願いするという御指示を出させていただいた。それを受け、事務局でも経済官庁と勉強会や議論を行ってきている。これについては、有識者会議の議論も踏まえ、必要に応じて、どういう関与をさせていくか検討をしていきたい。

○　特定秘密保護法は、４分野が定められているところ、それが経済分野に広がると、経済官庁にも負荷がかかるという認識である。

○　ガバナンスに関し、ＮＩＳＰOMの和訳があれば米国が民間会社に情報を提供する際の規定が明らかになると思うが、日本も上場企業に関しては、2013、2014 年頃から、ガバナンス・コードが適用されているが、そもそも会社法上、代表取締役は、全部の執行権限を有し、責任も負う仕組みとなっているので、代表取締役や担当取締役が把握できないブラックボックスが社内にあるというのは違和感がある。したがって、株式会社においては、代表取締役や担当役員は、ブラックボックスはあってはならない、つまりセキュリティ・クリアランスを取っておくべきなのかもしれない。大学に関しては、学問の世界では、総長であっても、学内の誰がどのような研究を行っているか知らなくて当たり前であり、知る必要もない。法律的に何か抵触する場合には知らなければいけないことがあるかもしれないが、株式会社と国立大学、私立大学、国研は、法律の立て付け、つまりガバナンスの仕組みが異なるので、そうした法律の仕組みを意識した上で、どういうガバナンスが必要か、もう少し詳細に検討した方がよいと考える。

○　軍事分野でないデュアルユースの機微技術について、産業界において国際連携するときにＣＵＩに当たるものについて、どの範囲の情報がこれに該当し、どのような程度の保全措置が必要となるのか。防衛産業の保全において、上から下までレベルがあることは分かるが、その横の部分、つまり情報区分の表（第２回会合の資料２）における「Ｅ」に相当するものについて、早くもう少し明確になるとありがたい。どういう技術が対象なのか、これを扱う業者においてどのようなセキュリティ・クリアランスを要するか。電磁波攻撃に対してもしっかり体制を作るなど、実際に情報システムの中で Entity List に入っているサプライヤーは使えないなど、この「Ｅ」の部分についてもう少し明確にしていただけると産業界としてありがたい。

事務局より回答

○　防衛省資料と、過去の事務局資料（第２回の資料２）の情報区分の表に関し、後者における政府由来の秘密情報である「A」、民間のものである「D」のレベルは、防衛省資料の７ページにおけるトップシークレット、シークレット、コンフィデンシャル、つまりＣＩの情報のレベルに当たる。まずは、情報保全について今後考えていく上で、経済分野であれ何であれ、まずこの「A」、つまりＣＩ情報が基本であると考えている。その上で、通例であれば、諸外国もこの部分についてセキュリティ・クリアランスを求めている。その下の、米国でいえばＣＵＩに当たる部分については、情報区分の表の「B」や「E」に該当する。ＣＩの中で、トップシークレットやシークレット、コンフィデンシャルがあり、この保全措置が前提としてあり、更に広く見ればＣＵＩがあるので、その保全の在り方がどうとらえられるか。ものによっては背景調査を求めている分野もあれば、求めていないものもある。まずは、ＣＩについて整理して、ＣＵＩをどう考えるか、という順番で検討したい。

○　ＣＩだけの議論はよく分かるのだが、ＣＵＩ部分は、いつ頃議論するのか。

○　これまでの議論の中でも、ＣＵＩについても御意見を頂いてきており、それも踏まえて、考えていきたい。

○　この有識者会議でＣＵＩも取り扱うということよいか。

事務局より回答

○　既に議論に出ているものについて、どのような方向性に持っていけるか議論していきたい。多いのはＣＩに関する議論であり、まずはそこからと考えている。