第２回会議の議論の整理（主なポイント）

資料１

１．セキュリティ・クリアランス制度へのニーズ、あるべき方向性

（１）国際的なビジネス・共同開発等でのニーズ

- ある海外企業から協力依頼があったが、機微に触れるということで十分な情報が得られなかった。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。
- 防衛装備品の国際共同生産において、相手国政府のＣＩ（Classified Information）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、相手国から信頼されていれば、短縮された可能性もある。
- 自衛隊の装備品とは関係ない国際共同開発において、セキュリティ・クリアランス保有者がいなかったために、ＣＵＩ（Controlled Unclassified Information）の開示を受けるまでに長い時間を要したにも関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、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関わらず、双方で十分な意思の疎通ができなかったケースもある。
- 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、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。
- 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。脆弱性情報や攻撃情報といっ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。
- アメリカでは、政府を中核としつつ、主要企業が、セキュリティ・クリアランスを持った上で、サイバーセキュリティ関係の機微な情報を共有できる枠組みがあると聞く。こうした場が日本にも必要なのではないか。
- 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に参加する際、Clearance Holder Onlyであるセミナー・コミュニティがあり、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。
- 特定秘密保護法では、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。
- 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を期待。

第２回会議の議論の整理（主なポイント）

１．セキュリティ・クリアランス制度へのニーズ、あるべき方向性

（２）国際的な枠組み

- 諸外国ではＩＳＡ（Industrial Security Agreement）という仕組みがあり、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。
- ＮＴＩＢ（National Technology Industrial Base）は、現在、アメリカ、カナダ、オーストラリア、イギリスの４か国が加入しているが、加入したアメリカ現地法人はＣＩにアクセスするＮＩＤ（National Interest Determination；国益決定プロセス）に関する承認手続きが免除されており、円滑にＣＩへのアクセスが可能。
- 機密指定が関与するような情報を、政府が全く関与することなしに民間企業同士で交換することは恐らくあり得ない。

（３）情報保全の必要性

- 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確保するかが重要。
- 産業界のニーズと並行して、日本の安全保障にどうつながるかという議論が必要。
- 民間企業は、政府に情報共有するのを一般的に嫌がる傾向はあるので、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。
- 官民双方の「情報保全」能力の向上が一丁目一番地である。
- 人物チェックだけでなく、組織の情報管理の在り方も含めてクリアランスがあるということ。

（４）諸外国に通用する制度

- 他国からも同等性が認められることが重要。まずは外国の制度を精査し、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。

第２回会議の議論の整理（主なポイント）

２．ニーズにこたえるための制度設計の方向性

（１）政府一体となった検討

- 防衛分野を中心として既に情報保全制度があるので、今回の検討が防衛分野を切り離したものとされると、運用コストや管理コストが増す。防衛も含めて政府一体となって検討していただきたい。
- 複数の機関で調査を受け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。

（２）プライバシー・従業員との関係・企業負担

- 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、意義のある仕事として、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。
- 誇りをもってやっている従業員に金銭的に報いられているか分からないため、国として支援したらよいのではないか。
- 誇りを持っているだけでは済まされず、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。
- 防衛産業からの撤退が進んできており、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無いようにしないといけない。
- 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。

（３）ＣＵＩ

- これまでの国際共同開発は防衛分野が一般的であったが、デュアルユース分野が次第に増えてくるという観点での検討が必要。
- 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。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。
- 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を早期の検討課題とすべき。

第２回会議の議論の整理（主なポイント）

２．ニーズにこたえるための制度設計の方向性

（４）情報の指定

- 事務局資料２でいうところのＤやＥを指定するに当たっては、十分な検証が必要。企業のヒアリングを是非していただきたい。
- 一旦指定されるとなかなか解除もされないということも問題。経済安保、デュアルユースの世界では、特にそういった硬直性が支障にならないか。
- 民間の意見や学術的な判断を経た上で、状況に応じ、機動的に変えることも必要。
- 制度の安定性からも、解除する際には関与している者と十分に議論することも重要。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。
- 技術分野で範囲を切ろうとすると難しいので、国際共同開発ということで切るとやりやすいのではないか。
- 画期的な技術が生まれると、民生技術がいきなり最高の技術になる可能性もあり、ＣＩやＣＵＩに指定した方が良い状況もあるのではないか。
- 経済やインフラ分野などをどう扱うか、諸外国の運用や制度も含め検討する必要。

（５）その他

- 契約・案件ごとにクリアランス作業を行うことは企業・政府双方の負担。クリアランスホルダーの育成という観点からもマイナス。契約単位ではなく、一定程度の期間有効なものとすることも検討する必要。諸外国とも同一条件になるのではないか。
- 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、これらの整合性を図りつつ、今回の制度が重複した規制になることは避けるべき。
- イギリス、ドイツ、フランスのクリアランスの調査は困難。諸外国比較は大変かもしれないが、まずは、アメリカは調べるということ。
- ＦＯＣＩ（外国による所有・支配・管理）も検討する必要がある。
- 日本の大学においても、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。
- 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、退職後の情報保全をいかに確保するかという問題について、アメリカでも解決が難しい問題とされ、わが国においても、方策を検討する必要がある。