“使える”セキュリティ・クリアランス法制のために積み残されている課題

2024 年 2 月 19 日
主任研究員
小木 洋人

本稿は、Foresight（フォーサイト）にも掲載されています。
（上）https://www.fsight.jp/articles/-/50431
（下）https://www.fsight.jp/articles/-/50432

岸田文雄総理は、本年 1 月 30 日の経済安全保障推進会議において、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関する法案の通常国会提出に向けた準備を加速するよう高市早苗経済安全保障担当大臣に指示を行った。これは、それに先立って、本制度に関する有識者会議において議論の「最終とりまとめ」が提出されたことを受けたものである。筆者は、有識者会議での議論が始まった 2023 年 2 月に、所属する地経学研究所でコメンタリーを発表し、当該制度に関する誤解を解きつつ論点整理を試みた。しかし、制度そのものの複雑性・専門性が高いゆえに、当時も存在していた誤解に基づく議論は、現在もまだ残っている。また、有識者会議の最終取りまとめで示された法制化の方向性においても、当初論じられていたニーズを本当に手当てできるのか課題が残る箇所がある。

そこで本稿では、改めてセキュリティ・クリアランス法制に関する論点を整理するとともに、有識者会議による最終取りまとめにおいて残された課題を特定し、今後の議論の具体化に貢献したい。

セキュリティ・クリアランス法制は防衛産業と基本的には関係ない

セキュリティ・クリアランス法制に関する議論で頻出する誤解が、同制度が存在しなかった日本でこれが初めて法制化されることで、同盟国等との防衛装備協力・防衛産業協力が進展するというものだ。これは特に、海外のシンクタンクにおける議論や報道で良く見られるものであり、なかなか訂正されない。セキュリティ・クリアランスとは、政府が秘密情報として指定したものが適切に秘匿されるようにするため、それを取り扱う者や施設の資格を審査する制度である。秘密情報を含む国際共同研究や海外政府の調達案件に日本企業が参加するためには、セキュリティ・クリアランスが要求される事例があり、それなしでは企業の円滑な国際展開に支障が生じるとの問題意識に基づき、議論が進められてきた。

しかしながら、最終取りまとめにも明示的に記載されているとおり、日本においては従来、特定秘密保護法によりセキュリティ・クリアランス制度が規定されてきた。機微な防衛、外交、テロ等の情報を特定秘密として指定した上で、民間の適合事業者を含め、政府による調査等を経て資格要件を満たした者にのみその取扱いを認める制度である。防衛装備品に関してはこのほかに、自衛隊法に基づく防衛省秘（自衛隊法上罰則規定のある自衛隊員のみならず、2023 年に成立した防衛生産基盤強化法により、契約関係にある事業者の従業者（民間人）への罰則も法定（装備品等秘密））や、日米相互防衛援助協定等に伴う秘密保護法に基づく特別防衛秘密（米国製防衛装備品の場合）に指定された情報を取り扱う場合にも、企業の従業者がセキュリティ・クリアランスを取得する必要があるとされる。

一方、今回の法整備の対象は経済安全保障分野に関する情報であり、「国家及び国民の安全を支える我が

国の経済的な基盤の保護に関する情報」を対象とすることが念頭に置かれている。つまり、特定秘密保護法等の適用分野である防衛、外交等の情報に限られていたセキュリティ・クリアランス制度を、経済安全保障の分野に拡げることが目的だ。したがって、「セキュリティ・クリアランス制度はこれまで日本に存在しなかった」との言説は誤りである。また、国際共同開発など防衛装備品に関する協力に従事する民間人にとっては、今回の法整備により直接何かが変わるわけではない。

新法制の制度設計

それでは、今回の法整備でセキュリティ・クリアランスによって担保された秘密情報（CI）の対象となる分野は具体的に何であるのか。最終取りまとめでは、「国家及び国民の安全を支える我が国の経済的な基盤の保護に関する情報」に当たる例として、「サイバー関連情報（サイバー脅威・対策等に関する情報）」、「規制制度関連情報（審査等に係る 検討・分析に関する情報）」、「調査・分析・研究開発関連情報（産業・技術戦略、サプライチェーン上の脆弱性等に関する情報）」及び「国際協力関連情報（国際的な共同研究開発に関する情報）」が挙げられる。

そして、これらの経済分野における情報を、情報漏洩による影響度合い等に応じて階層的に秘密として指定・管理するため、有識者会議の最終取りまとめは新法制を特定秘密保護法とシームレスな形で取り扱うことを提唱している。米国等において、情報の重要度等に応じ、秘密がトップ・シークレット、シークレット、コンフィデンシャルと複数の階層に分かれて指定されていることを踏まえたものだ。この示唆を受けて、冒頭で触れた岸田総理の発言では、「コンフィデンシャル級の情報を保護の対象とする制度を新法により創設」するとともに、「特定秘密保護法の運用基準の見直しの検討を含め、必要な措置を講じる」ことが具体的に指示されている。この方向性は、最終取りまとめでは具体化されていなかったもので、この段階で初めて出てきたものだ。

これらを踏まえて総理指示を字義どおり読むと、今後の方向性としては、①特定秘密よりは重要度や罰則も軽いコンフィデンシャル級の情報であって、経済安全保障に関するものを新法の対象としつつ取扱資格制度（クリアランス）を定めるとともに、②トップ・シークレット、シークレット級の秘匿度の高い経済安全保障関連情報についても、特定秘密保護法の運用改善によって指定しやすくする、ということが目指されていると推察する。

このうち上記②は、有識者会議において、特定秘密に指定できる情報として、経済に関連するものがあるにもかかわらず、経済官庁による秘密指定の実績がなく、硬直的な運用となっていることが問題視されたことにヒントを得たものかもしれない。

確かに、特定秘密保護法の運用基準は、同法別表に特定秘密に指定できる事項として掲げられている防衛、外交、テロ等の項目の細目を列記しており、貨物の輸出入や資産の移転といった経済関連の情報も規定されている。この運用基準を改正し、経済安全保障関連の情報を指定しやすい運用とすることは、一つの方向性かもしれない。ただし、防衛装備品の製造・開発と関係しない先端民生技術に関する情報を直接的に読み込める事項が法律の別表本体にないので、運用基準の改正では限界がある。したがって、新法のカバレッジをどう定めるかは、引き続き政府内で検討が続く可能性がある。

いずれにせよ、既にクリアランス制度が確立されている特定秘密保護法に屋上屋となるような新法を被せるのではなく、両者の切り分けを丁寧に調整しつつシームレスに運用しようという方針は妥当である。

最も重要な論点は民間由来情報の扱い

しかしながら、最終取りまとめで示された方向性には、三つ大きな課題が残されている。それらはいずれも、本

来示されていたセキュリティ・クリアランス制度に対するニーズを本当に手当てできるのか分からないという点に関わる。

本来示されていたニーズとは、防衛装備品の契約に関係しない国際共同研究等の案件における機微な情報の取扱資格を政府が定めることにより、日本企業の国際展開を円滑化するというものであった。

これについては第一に、秘密指定する情報の性質が問題となる。最終取りまとめでは、有識者会議での議論で示された事務局（政府）の方針を踏まえ、新たな法制で秘密指定の対象となるのは、「政府が保有している情報」であるとされた。民間から提供された情報に政府が分析等の付加価値を付けた上で秘密として指定することは妨げられないものの、その出元となる民間情報そのものが秘密指定されることはないとされる。このような整理は、特定秘密保護法におけるそれを踏襲したものであり、法律論としては整合的なものである。

しかしながら、もの作りや調査・研究開発の実態を踏まえた場合はどうか。特定秘密保護法では、秘密指定できる事項として、防衛装備品の製作、検査、修理等の方法が規定されている。整理としては、政府が保有する特定秘密を契約に基づき民間の適合事業者（防衛企業）に提供した上で、防衛装備品の製造を請け負わせることとなるので、情報の原保有者はあくまで政府となる。しかし、製品の製造そのものを行う機能のない政府において、製作や検査の情報を元々保有しているわけではないので、その製品の開発段階では、政府からの研究委託や試作品の製造請負を通じて企業に開発・製造させる。その過程では、政府のニーズという機微な情報が民由来の製造技術に付加されることになる。そして、それらを含め政府が秘密指定した上で、改めて契約に基づいて企業事業者にその秘密情報を提供し、防衛装備品の製造を請け負わせるというのが法的な整理だろう。加えて、防衛装備品の研究開発における試作品請負契約の場合、研究開発の過程で得られた技術資料は原則国に帰属することになっているので、指定の実務上も無理がない。

したがって、特定秘密保護法のこの建付け自体に問題があるわけではない。しかし、これを防衛装備品の製造に関係しない経済安全保障上の重要技術に当てはめると、無理が生じる場合がある。というのも、政府が民間に秘密情報を提供する場合、契約に基づき何らかの製品の製造や役務（調査等）実施を請け負わせるという政府調達が考えられるのだが、防衛に関係しない政府調達において、先端的な重要技術が含まれるケースがさほど想定されないためだ。そうなれば、防衛装備品製造以外の場合において、民間由来の重要技術情報を保護する契機が乏しくなり、情報保護が宙に浮いてしまうおそれがある。

例外として、有識者会議の議論でもニーズとして挙げられていた宇宙やサイバーといった領域であれば、防衛装備品以外の政府調達案件もあるので、新法制による指定事例としても想定される。一方、それ以外の AI、無人、量子といった経済安全保障推進法に基づく重要技術育成プログラム（K プログラム）が対象とするような領域では、研究開発への政府資金提供スキームは考えられるものの、政府が製品や技術を直接調達することはあまり想定されない。あるいは、有識者会議の議論で事務局側から例示された、政府が分析等の付加価値を付した情報を民間に提供するという場合にしても、その情報を民間に提供して何の役務を委託するつもりなのかという点が判然としない。

この点、米国では、政府資金の提供を受けた契約事業者や委託研究者が秘密情報を自ら生成し得る場合があることを想定し、そうした情報を秘密指定する例外的手続が定められている。大統領令第 13526 号は、政府資金の受給者等が自ら秘密指定を要する情報を創出したと判断した場合に、当該情報を管轄する政府機関にその旨を通知すべきことを規定しており、その通知を受けて、政府は当該情報を秘密するか否かを決定することとしている。各省庁による運用の実態は不明だが、この規定の存在が、大統領令第 13526 号が秘密指定の対象に含む「国家安全保障に関する科学技術又は経済的事項」の指定の間口を実際に担保するものとなっていると

言える。

こうしたことから、日本の新法制において、これと同様の規定が盛り込まれず特定秘密保護法における整理を厳格に踏襲した場合、実際の秘密指定事例が著しく狭いものとなる可能性が高い。最終取りまとめで指定できる情報の分野は幅広く概念された一方で、指定の対象が政府保有の情報に限られたためである。これにより、指定の契機となるような政府の行為が具体的に何なのかという点が不明確となっている。

元々のニーズが経済安全保障分野において国際的に通用し得る秘密取扱資格制度の創設であったことを踏まえれば、実際の秘密指定事例が狭められかねないことは大きな課題となるだろう。当然のことながら、秘密指定されない情報に与えられる取扱資格（クリアランス）はないからだ。指定対象の情報の範囲が狭ければ、クリアランスを保有する民間人も増えない。

2023 年 10 月の段階で、有識者会議の議論においても、委員の一人から当該例外規定についての問題提起がなされたことはある。しかしそれ以前、企業ヒアリングの段階（2023 年 3 月）で、一つの企業から、民保有の機微な技術情報は CUI（controlled unclassified information、秘密ではない保護情報あるいは注意情報）であるとして秘密指定に慎重な姿勢が示されたことが意図せずその後の議論を方向付けてしまったような印象がある。その後の議論では、秘密指定の対象となるのは民間由来であるにせよ政府保有の情報のみであるとされ、民間の機微な情報としてこの場で位置付けられた CUI については、セキュリティ・クリアランス制度の枠組みの外における管理の必要性が検討される方向となった。

このような秘密指定制度を超えて機微な情報を管理していく裾野の広い考え方そのものは、何ら否定されるべきものではない。しかしながら、元々のニーズが防衛装備品に関係しない機微情報の取扱資格の策定にあったことに鑑みれば、そのような方策は当該ニーズに十分対応できるものではない。セキュリティ・クリアランスは秘密取扱いに際して付与されるものであり、秘密ではない情報の取扱資格がこれを代替することはできないからだ。当然ながら、米国等の諸外国においても秘密取扱資格として通用するものではない。そして、日本企業の国際展開の円滑化に資するのか疑問が持たれる。

秘密指定を受けた情報の厳格管理やその取扱資格獲得に要する負担・コストと、それによって得られる国際的なビジネスチャンスは表裏一体のものであり、便益のみ選択することは不可能だ。政府は新制度の法制化に当たり、本来のニーズに立ち返った上で、科学技術の自由な発展の視点にも留意しつつ、上記で挙げた米国の例外規定も参考により実効的な内容を検討すべきである。

もっとも、制度のみ創設しても、先端的な民生技術を秘密指定する基準を持つことは容易ではない。しかし、上記の米国における例外規定を見ても、政府が民生技術を一方的に秘密指定する枠組みではない。有識者会議では、ヒアリングを受けた企業も、機微な企業情報が秘密指定を受けることを完全に否定しているわけではなく、企業と相談しながら慎重に進めるべきだと発言している。技術を生成した企業・研究所等と相場観を共有していくしかないだろう。

誰にその権利が帰属する情報か

第二の課題は、米国大統領令第 13526 号の例外規定と同様の基準を導入する場合、知的財産の帰属関係をどうするかという問題だ。具体的には、政府資金を提供した研究成果のうち機微な技術（知的財産権）を国の帰属とすることを検討する必要がある。

現状、国の委託による研究開発は、防衛分野を除き、研究成果としての知的財産権の帰属が委託先の企業や研究機関となっているものが多いと考えられる。これは、民間の産業競争力強化を目的に、産業技術力強化

法に基づき導入された日本版バイ・ドール制度を根拠としている。科学技術振興機構（JST）や新エネルギー・産業技術総合開発機構（NEDO）といった研究開発法人の委託研究契約条項を見ても、そのような措置が可能となるよう規定されている。

これを変えることは、これまでのプラクティスに反する部分も出てくる。しかし、少なくとも秘密指定し得るような機微な研究成果に限っては、国の知的財産とすることを検討すべきだ。むしろ、権利が民間に帰属したまま、その知財の利用についてのみ秘密指定制度で制限をかけるのは一貫性を欠く。他方、有識者会議の事務局が主張するような「付加価値を付加した情報」のみが秘密となり、情報の原保有者たる民間人にその効果が及ばないとする整理は、概念上は可能だったとしても、技術には色がない以上、現実性に乏しい。

加えて、研究開発関連情報についてはさらに処理が必要な論点がある。それは、特定秘密保護法の場合、独立行政法人が取得した情報が対象となっておらず、同法人には特定秘密の指定権限がないことである。特定秘密保護法策定の過程では、民主党政権時代の有識者報告書において、国の行政機関のみならず、独立行政法人や大学が取得・保有する情報も対象に含めることが提案されていた。ところが、政権交代を経て特定秘密保護法が策定された際には、その提案が組み込まれることはなかった。

しかし、宇宙開発の主体である宇宙航空研究開発機構（JAXA）や、K プログラムの推進主体である JST・NEDO など、国の研究開発の担い手は、独立行政法人の一類型である国立研究開発法人だ。現状の法制では、その取得・保有情報を特定秘密に直接的に指定する手段がない。政府資金を提供する研究委託の契約主体がこれらの法人であることを踏まえれば、新法制ではこの点をセットで見直し、これら法人の情報も指定対象に含めることができるようにする必要があるだろう。

国際的な通用性という壁

第三の課題は、以前別稿で指摘したとおり、セキュリティ・クリアランス制度を国内で構築したとしても、それがそのまま海外で通用するわけではないことだ。例えば米国ではセキュリティ・クリアランスの取得を米国市民に限っており、日本のクリアランスが米国で直接通用するわけではない。この論点は、必ずしも有識者会議における最終取りまとめの方向性やそれを受けた総理指示に内在する問題ではなく、国内法制に加えて不可欠となる取り組みである。

民間人を含む日米間の秘密情報のやり取りは、日米秘密軍事情報保護協定（GSOMIA）の下で行われる。日米 GSOMIA は、互いの秘密情報に相手国において与えられる保護と「実質的に同等の保護」を与えることや、契約企業に秘密情報を提供する場合は当該情報にアクセスする個人が「秘密軍事情報取扱資格」（すなわちセキュリティ・クリアランス）を有すること、秘密情報の送付は「政府間の経路を通じて」行われるべきことなどを定めている。このため、双方の企業・民間人の間での秘密情報の共有は、クリアランスの保有等の条件を満たした上で、それぞれの政府間ルートを通じて行うしかない。

このため、日米国防当局間の共同研究開発や共同調達であれば、日本企業は政府を通じてプロジェクトに応じ参画できる。一方で、秘密情報を含む米国の政府調達や米国企業との共同事業に対し、日本企業が日本政府を介さずして直接参画する手段は、管見の限り現状では存在しない。ここでも、前節で挙げたのと同じ「政府による調達が想定されない非防衛の先端技術分野」の問題が浮上する。すなわち、こうした先端技術分野において、秘密情報を含む米国等の海外のプロジェクトに日本企業がアクセスできるルートが不在となるのだ。

この点、米国は、英国等との間で補足的な「産業保全協定（industrial security agreement）」を締結している場合があるようであり、こうした取極の中で企業を含む秘密情報取扱いのより柔軟な手続を定めている可能性はある。

ただし、その内容は公開されていないので、新制度創設の検討と並行して米国政府と協議する必要がある。また、日米 GSOMIA の対象は「秘密軍事情報」なので、防衛に直接結び付かない経済安全保障関連の機微技術のやり取りを対象に含めるためには、いずれにしても協定の改正等の措置が必要となる。

そもそもセキュリティ・クリアランス制度の中核は防衛関連の情報取扱資格であり、米国においては国防省が制度設計や実施に大きな役割を果たしている。そして米国の国防調達や国防産業は、いわば「一見さんお断り」の閉鎖的な性質を有していることが否めない。したがって、米国の国防産業や国防省が関係している案件や会議においてセキュリティ・クリアランスの保持を理由として情報提供を断られたというような事例では、そもそも対象として米国企業や米国政府と関係の近いファイブ・アイズ（米国・英国・カナダ・オーストラリア・ニュージーランド）の企業しか協力先として想定していなかったという可能性も否定できない。問題の所在は、セキュリティ・クリアランス制度に関する日本国内の事情だけではなく、米国政府の方針にもあると言えそうだ。

そうだとすれば、これは経済安全保障分野と防衛分野に通底する問題だ。2024 年 1 月、米国防省は、初めての文書となる「国防産業戦略」を発表し、国防サプライチェーンの強靭化や柔軟な調達などの必要性を掲げた。サプライチェーンの強靭化の方策としては、同盟国・友好国との防衛生産協力の強化も含まれている。国防省がこれを真に必要な戦略だと考えるならば、その実施に必要な措置も同時に手当てする必要がある。フレンド・ショアリングの対象国として日本を明示的に掲げるならば、なおさらだ。厳格管理を担保した上で、日本企業に秘密情報を伴う事業への参画機会を柔軟に提供することもその手段の一つである。日本政府としても、この機会を捉えて日米産業間協力の促進を米国政府に働きかけるべきである。米国以外のパートナー国との間でも、同様の努力が必要となる。

新たなセキュリティ・クリアランス制度は、このような主張の信頼性を向上させるため極めて重要な取り組みとなるが、同時に、新制度を構築しただけで物事が解決すると考えてはいけない。

防衛と民生技術の境目が曖昧となり、国の安全保障を確保するために経済・民生技術分野における機微な情報の保全も考えなければならなくなっている中、新たな制度の創設は時宜にかなったものである。そして、法案の国会提出を目指し議論を精力的に推進しようとする政府の姿勢も評価に値する。

しかし、そうであるからこそ、実際に“使える”法制としなければならない。その観点から言えば、現在の議論の方向性は、制度に対する懸念への配慮からか、ややスモール・パッケージとなっている感が否めない。本来のニーズに立ち返った思い切りの良い制度設計が求められる。

プロフィール - Profile

主任研究員 小木 洋人

研究分野・主な関心領域

安全保障政策 / 軍事戦略 / 国際軍事情勢 / 防衛産業政策 / 経済安全保障

https://apinitiative.org/experts/ogi-hirohito/