KEIZAI DOYUKAI

「経済安全保障上の重要技術に関する技術流出防止策についての提言 ～国が支援を行う研究開発プログラムにおける対応～」への意見

2024年6月27日
公益社団法人　経済同友会
代表幹事　新浪　剛史
経済安全保障委員会　委員長　柴田　英利
同　委員長　小柴　満信

はじめに

本年6月4日、「経済安全保障法制に関する有識者会議」は、経済安全保障上の重要技術のなかでも「国が支援を行う研究開発プログラム」について、「経済安全保障上の重要技術に関する技術流出防止策についての提言　～国が支援を行う研究開発プログラムにおける対応～[1]」を公表した。

世界では、従来の軍事力・防衛力による戦いだけでなく、経済力と技術力が「武器化」されたパワーゲームが繰り広げられている。その戦いは経済力に欠かせないサプライチェーンや機微技術の保護や強化にとどまらず、半導体、AI、量子コンピュータ、バイオなどの次世代先端技術においても、主要各国が他国に対する優位性の確保するために国の資源を惜しみなく投入している。我が国においても2022年5月に「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法。以下、「推進法」。）」が成立し、サプライチェーン強靭化、先端重要技術の開発支援のために数兆円の政府予算が投入され実行に移されている。

一方で、先端技術の開発には膨大な有形無形のコストが掛かり、開発難度も極めて高いことから、自国や単独企業、大学だけではなく、同盟国や同志国の研究機関や企業との国際共同研究開発は不可欠である。日米民間企業による2nmの先端半導体の共同開発[2]や、米国の先端量子コンピュータとスーパーコンピュータ「富岳」との連携による研究開発プロジェクトの締結[3]はその具体例である。さらに、先端技術の多くは軍事転用可能なデュアルユース技術であり、国際共同

---

[1] https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r6_dai10/siryou4.pdf

[2] Rapidusは米国IBM、ベルギーimec（Interuniversity Microelectronics Centre）と提携して、最先端2nm半導体製造を目指す。

[3] https://newsroom.ibm.com/2024-04-30-RIKEN-Selects-IBMs-Next-Generation-Quantum-System-to-be-Integrated-with-the-Supercomputer-Fugaku

研究開発にあたっては、相手（国・企業）と同等の「共同研究内容及びその成果を保護する仕組み」を備えない限り、先端技術の国際的研究開発の枠組みから取り残されてしまう。

したがって、特に「国が支援を行う研究開発プログラム」において、アカデミアは研究インテグリティ[4]の確保に加えて、研究セキュリティ[5]の確保も必要となり、企業においては自社の営業秘密や研究開発成果の保護・管理体制整備が必要となる。

経済同友会では昨年５月に提言「”Politics meets Technologies.”の時代を生き抜く国と企業の戦略」[6]を公表したが、同提言の趣旨を踏まえ、今回の有識者会議提言に対して、以下の通り意見を取りまとめた。本意見では、主に経済界に関係が深い「経済安全保障上の重要技術の研究開発成果の社会実装と技術流出防止について」に関して言及する。

<u>政府への意見</u>

- 推進法の正式名称にある通り、「経済安全保障」の目的は「経済の発展」やそれを支える「技術優位性の強化・創出」を通じて国家の安全を確保することである。「国が支援を行う研究開発プログラム」が「経済の発展」や「技術優位性の強化・創出」に充分に寄与するためにも、今回の提言を踏まえた技術流出防止策が有効に機能することを期待する。
- 一方で、今回の提言に基づく技術流出防止策が企業の自由で活発な活動を抑制することのないように留意を求める。今回の提言の対象は「国が支援を行う研究開発プログラム」であり、企業が独自で実施する研究開発や保有する機微情報に対する管理を求めるものではない。しかし、その前提条件が十分に周知されていないと考える。今回の提言および今後の制度設計に際しては、官民対話を積極的に行い、誤解のない正確な情報の発信と周知を求める。
- 今後、提言に基づいて国からの支援を受ける際の技術流出防止措置要件やガイドラインを策定するだけでなく、政府は半導体業界における「ロードマップ」のような技術進化の道筋を示すべきである。そのためには政府の技術インテリジェンス強化（シンクタンクの設置）が必須である。ガイドラインと

---

[4] 研究の健全性・公平性。https://www8.cao.go.jp/cstp/kokusaiteki/integrity/integrity_housin.pdf。１ページ、脚注２より。

[5] 経済的、戦略的リスクや国家的、国際的な安全保障上のリスクをもたらす行為者や行動から研究コミュニティを保護する活動。有識者会議提言（脚注１）２ページ、研究セキュリティの定義より。

[6] https://www.doyukai.or.jp/policyproposals/2023/230515t.html

「ロードマップ」を公表することで、企業はリスク、機会の両面で予見性を高めることができる。

・ 経済安全保障に関連する制度は概して企業に組織力や堅牢度の向上を求めるものであり、特に中小企業およびスタートアップにとってはコストと負担の増加は大きな問題である。政府にはガイドラインや「ロードマップ」の公表に加えて、各経済官庁への相談窓口の設置や、企業に対する支援策の検討が求められる。

<u>企業経営者としての覚悟</u>

・ 前述のとおり、今回の提言の対象は「国が支援を行う研究開発プログラム」であるが、企業においても、今回の提言にある好事例なども参考にしながら営業秘密の管理体制などを見直すべきである。技術が「武器化」され、民生技術のデュアルユース化が進行する現代においては、企業が保有する高度な技術やサプライチェーンに関する情報が、国家安全保障上の観点からも重要な意味合いを持つようになってきている。加えて、営業秘密や技術情報の管理体制を確立することは、研究や事業の（諸外国を含めた）パートナーに対しての信頼の証であり、単なるコストではなく企業価値向上にも資する取組みであることを意識すべきである。来年施行予定の「重要経済安保情報の保護および活用に関する法律」に基づくいわゆる「セキュリティ・クリアランス」も、企業にとっては負担だけでなく企業価値向上に資する制度と考えるべきだ。

・ AI や量子コンピューティングなどの先端技術の革新は、2030 年代を迎える前に企業の経営戦略に大きな影響を与えると予想される。我々経営者は、新時代に対応する自社の「準備度(readiness)」を改めて検証するとともに、自社のインテリジェンス機能を磨くために経営資源を投入すべきである。技術革新が企業に与える影響への対応に加えて、経済安全保障の重要性が高まる中で、自社や保有する技術の立ち位置を正しく認識するためにも、インテリジェンス機能の向上は不可欠である。そのために経営リソースをどのように配分するかは、取締役会の役割であることを改めて意識する必要がある。

以　上