

経済安全保障の確立とスタートアップ促進両にらみの施策の展開を

社会システムコンサルティング部
シニアコンサルタント 本田 和太

国際情勢が目まぐるしく変化する中で、経済・産業政策の側面からわが国の安全を確保するための制度・施策の整備が急ピッチで進められている。2022年には「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」が交付され、24年にはセキュリティ・クリアランス制度^{*1}について定めた「重要経済安全保障情報の保護及び活用に関する法律」が成立した。経済安全保障関連施策と時期を同じくして、革新的な技術を核として急速な成長を目指すスタートアップ支援策も急速に充実化が進む。新SBIR制度に基づく補助金の充実化（21年）や、スタートアップ育成5か年計画（22年）等施策の後押しもあり、スタートアップの数や資金調達の額も増加トレンドにある。このように、時期を同じくして経済産業政策上重要な二つの政策の整備が進む一方で、双方を一体的に組み合わせた施策については十分に検討されているとは言い難い。

スタートアップの事業領域は、重要インフラや軍事・民生双方に活用できるデュアルユース技術を扱うものも多く、経済安全保障関連制度の規制等の対象となりうる。一方、多くのスタートアップは、少ないリソースで事業を展開しており、技術流出に対応する体制構築が十分でないケースも多い。さらに、グローバル市場を志向するスタートアップは、経済安全保障への対応の必要性について認識が不十分であるケースも見られる。公安調査庁では、重要技術の流出が起きやすいシーンを取りまとめているが（図表）、特にスタートアップは、投資の受け入れ、海外機関・企業との共同研究、外国籍の従業員の受け入れ等について、事業拡大に向けて積極的に取り組む傾向にある。体制面や認識不足も相まって、これらの経路で重要技術の流出が起きるリスクは大きい。

政府には、スタートアップの事業拡大という「攻め」の施策と、経済安全保障の確立という「守り」の施策を一体的に進めることが求められる。例えば、スタートアップ向けの補助金の審査において、経済安全保障を考慮した体制構築や事業戦略を評価項目とすることや、採択後の伴走支援としてこれらの整備を支援すること等が挙げられる。また、多くのスタートアップが事業等の売却を出口戦略に据えていることを考慮し、事業売却先の制限を補助条件として設けることも考えられる。さらに、ベンチャーキャピタル等スタートアップを取り巻くプレイヤーの意識醸成を進めることも有効である。

スタートアップが急速に活性化しつつあるこのタイミングだからこそ、経済安全保障の視点を盛り込んだ施策の充実化を行うことで、わが国のイノベーションの促進と経済安全保障の確立の両立実現につながるだろう。

（監修：駒村 和彦）

図表 スタートアップに関連する重要技術の流出経路

投資・買収	●懸念国の投資家が日本企業を買収することで、重要技術やデータ、製品等が流出するリスク ●スタートアップの場合海外のファンドの出資を積極的に受け入れたり、エグジットとして海外ファンドへの売却を行ったりするケースも多くリスクが大きい
不正調達	●輸出管理を回避するために、複数の企業等を経由することで最終需要者を秘匿する手口により、重要技術やデータ、製品等が不正調達により海外に流出するリスク
留学生・研究者の送り込み	●経歴を秘匿した海外の研究者等が日本企業に参画し、重要技術やデータを持ち出すリスク ●スタートアップの場合、自社の革新的な技術の開発に資するスキルを持つ留学生や海外の研究者等を積極的に受け入れるケースも多くリスクが大きい
共同研究・共同事業	●外国企業や機関との共同研究や事業を通して、技術者等がリクルートされたり、重要技術が目的外の用途に転用されたりするリスク ●スタートアップの場合、外部とのオープンイノベーションにより事業成長を進めるケースが一般的でありリスクが大きい
人材リクルート	●外国企業による高度な技術・技能を有する専門人材のリクルートにより、重要技術やデータが流出するリスク ●グローバル市場での競争を前提とし、人材の流動性が高いディープテック系のスタートアップにとっては、重要技術を取り扱う人材が外国企業に移るケースも多いことが想定される
情報活動	●展示会や講演会といった機会の中でターゲットとされた人材に対して、公私の場を問わず接触する手口によって、重要な技術に関する情報が流出する ●スタートアップも国際展示会や講演会等でネットワーキングを行い、販路や協業相手先を開拓することが一般的であり、多くの企業と同様にリスクがある
サイバー攻撃	●メールに添付されたマルウェアや、外部からのサイバー攻撃による不正アクセスにより、重要技術・データが流出するリスク ●創業間もないスタートアップの場合、重要技術を取り扱っていても情報セキュリティ体制や投資が不十分であるケースも多くリスクが大きい

注) 公安調査庁資料に取りまとめられている流出経路について、特にスタートアップにとつてのリスクが大きいものについて NRI でその内容を補記している
出所) 公安調査庁「経済安全保障の確保に向けて 2022」に基づき NRI 作成

^{*}1 セキュリティ・クリアランスとは、政府が保有する情報について、安全保障上重要であると指定された情報を取り扱うことができる者を制限する仕組みを指す