「経済安全保障時代」におけるスタートアップ・エコシステムの発展に向けて

～経済安全保障リスクをどのようにヘッジし、エコシステムを駆動させるべきか～

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　和大
業務・IT 戦略コンサルティング部　コンサルタント　水木　香那

1　はじめに

1）経済安全保障政策とスタートアップ支援政策

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日本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」（経済安全保障推進法）が公布され、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「重要経済安保情報の保護及び活用に関する法律」（重要経済安保情報保護活用法）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成長・事業化を目指すスタートアップへの支援策も急速に充実している。新 SBIR 制度※2 に基づく補助金の充実（2021）や、スタートアップ育成 5 か年計画（2022）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。これら経済・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の展開については十分に検討されているとは言い難い。

経済安全保障政策とイノベーション政策はある面では相反する関係にある。イノベーションは、技術や知識が特定の組織や集団を超えて対流することによって促進される。技術革新によって産業化が期待されるフロンティア領域においては、国や地域の枠を超えた国際共同研究や、高スキル人材のリクルーティングといったことが重要である。他方、経済安全保障という観点では、国家間対立の激化を背景とした「経済の武器化」を考慮し、特定の国への経済的な依存や、資源・技術・人材等の流出を抑制する方向で政策の検討を行わなければならない。

2）問題の所在と本稿の狙い

上述のように、日本では経済成長の起爆剤、イノベーションの源泉としてスタートアップに期待が集まり、急速に施策が充実している。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ための体制構築に取り組むことができていないケースも多い。

本稿では、スタートアップ・エコシステムに潜む経済安全保障リスクを整理した上で、経済安全保障の重要性が高まるこれからの時代において、こうしたリスクをヘッジしながらエコシステムを発展させ、日本産業の成長・強化を実現するための方向性を提示することを目指す。

なお、本稿は、NRI マネジメントレビュー 2024 年 12 月号 NRI Insight「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」で論じた内容についてより詳細な検討を行い、加筆・修正をしたものである。

※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

※2　SBIR とは、Small Business Innovation Research の略であり、米国における中小企業・ベンチャー向けの研究開発制度を範として日本において導入されたスタートアップ向けの補助金制度を指す

2　スタートアップ・エコシステムに潜む経済安全保障リスク

1）スタートアップの「経済安全保障リスク」とは

本論に入る前に、スタートアップ・エコシステムに潜む経済安全保障リスクを考察するにあたり、本稿における「経済安全保障リスク」の定義を整理する。

経済安全保障という言葉に明確な定義はないが、経済安全保障推進法に基づく政府の基本方針を定めた「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基本的な方針」の以下の記載が経済安全保障という言葉の大枠を捉える上では有用である。以下の内容からは、国家および国民の安全を経済面から確保することが、経済安全保障関連政策の目的であり、これが脅かされることが「経済安全保障リスク」であるといえよう。

> *「安全保障の裾野が経済分野へ急速に拡大する中で、国家及び国民の安全を経済面から確保すること」*

（出所）内閣府「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基本的な方針」

さらに、スタートアップの特性から経済安全保障リスクを考えてみよう。スタートアップは、外部のさまざまな主体と相互に関わりながら急速な成長を目指す。一般的な中小企業と比べて、資金調達の手段・出資者も多様であり、共同研究等オープンイノベーションを前提とした事業開発を行う。リクルーティングもグローバルレベルで行うとともに新規株式公開（IPO）や企業の合併・買収（M&A）等、出資者の意向も加味した、いわゆる EXIT を目指すことが一般的である。こうした外部とのヒト・モノ・カネ・情報のやりとりは、社内の管理体制やルールの整備が十分に進んでいない創業初期から行われる。さらに、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領域を扱う企業も多い。したがって、スタートアップは、技術情報の流出リスクが高く、国家および国民の安全に直結するような情報を取り扱っているケースも多いと考えられる。

このように、スタートアップの通常の事業活動においては、日本の重要技術が流出し、国家および国民の安全を経済面から脅かすことにつながるリスクが存在する。本稿では、経済安全保障リスクをスタートアップやスタートアップを取り巻くエコシステムの側面から捉え、リスクをヘッジするためのポイントを整理する。

2）想定される技術流出リスク

公安調査庁では、重要技術の流出が起きやすい経路として「投資・買収」「不正調達」「留学生・研究者の送り込み」「共同研究・共同事業」「人材リクルート」「諜報（ちょうほう）活動」「サイバー攻撃」を挙げている。こうした経路を通してスタートアップが保有する重要技術情報が外部に流出することを防がなければならない。近年急速にディープテック系のスタートアップが増加した日本においては、スタートアップ・エコシステムにおける経済安全保障リスクは幸いにも顕在化していないものの、顕在化する前にリスクを想定し、対応をしておく必要がある。

ここでは、想定されうるスタートアップ・エコシステムに潜む経済安全保障リスクについて、スタートアップの特性や、関連するプレーヤーとの関係に着目して整理する。

(ア) 投資の受け入れにおけるリスク：投資家を介した流出

スタートアップは、一般的な中小企業と異なり、事業開始直後の売り上げが立っていない段階からさまざまな投資家による出資を受け入れ、研究開発や事業開発へ投資を行う。特に創業間もない段階では、ベンチャーキャピタル（VC）や企業だけでなく、エンジェルと呼ばれる個人投資家からの投資を受け入れるケースも多い。エンジェル投資家は、自ら起

図表 1　重要技術の流出が発生しやすい経路と想定されるリスク

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
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
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
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
諜報活動	● 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リスク
サイバー攻撃	● メールに添付されたマルウエアや、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

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

業を経験し事業の売却益を原資とし、個人として投資活動を行っていることが一般的である。起業経験を生かしたメンタリングや人的ネットワークの提供など、スタートアップにとって、金銭面以外のメリットも大きい。しかし、個人であることから、企業体のような情報管理体制を敷いていないことも想定され、投資家個人の所属するコミュニティーや人脈を介して情報流出が起きる可能性もある。

また、個人投資家でない場合でも、議決権を背景とした経営参画や、出資元企業との共同研究を通して、重要な技術情報が意図せず流出するリスクもある。特に、スタートアップがグローバル市場をターゲットとして、活動する場合は、外国企業や、外国企業の資本が入った企業からの投資の受け入れの際の技術流出リスクも想定される。

(イ) 人材移動やリクルーティングにおけるリスク：社員を介した流出

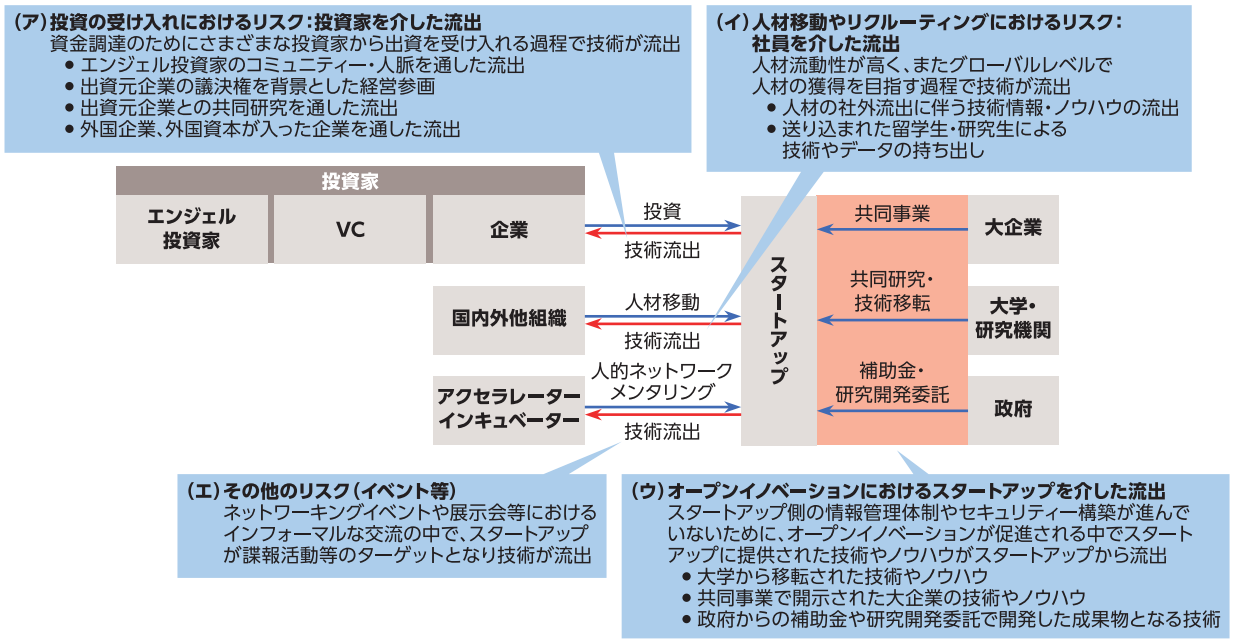
ディープテック系の領域で事業を展開するスタートアップは、グローバルレベルでエンジニアや高スキル人材の獲得を目指すことが一般的である。また、人材の流動性も高い。

人材の移動による技術流出については、法的には不正競争防止法による規制がある。企業の重要技術は「秘密管理性」「有用性」「非公知性」の要件を満たすことで営業秘密として法的に保護される。一方で、適切な秘密管理措置が取られていないこと[※3]や、従業員等への秘密管理意思の表明を行っていない場合、法的に保護されない。創業間もないスタートアップは、重要技術を保持していても秘密管理や情報管理体制を整備していないことも考えられ、不正競争防止法上の保護を受けられないという可能性もある。さらに、こうした要件が認められうる場合においても、経営体力に乏しいスタートアップにとっては、訴訟を起こすこと自体もハードルが高い。さらに、ディープテック系の領域においては、例えば製造技術等のノウハウも競争力の源泉となるが、従業員個人にひもづいたノウハウはこうした不正競争防止法による保護対象とはなりづらいという課題もある。

また、公安調査庁の調査にあるように、留学生や研究者を企業に送り込み重要技術やデータを持ち出すといった事案も見られる。急速な人員拡大を目指すスタートアップの場合、必ずしも採用の際にバックグラウンドチェックを十分に行っていないことが想定され、重要技術を狙う企業等にターゲットにされるリスクも想定しておかなければならない。

※3　例えば、情報にアクセスできる者を制限することや、情報にアクセスした従業員等が、当該情報が企業の秘密情報であることを認識できる状態にあることが求められる

図表 2　スタートアップ・エコシステムにおける経済安全保障リスクの概念



出所）NRI 作成

(ウ) オープンイノベーションにおけるスタートアップを介した流出

スタートアップの事業化においては、大学からの技術移転を前提とした共同研究や、大企業のアセット、販路・ネットワーク等を活用した共同事業等、オープンイノベーションが重要である。企業の「自前主義」がイノベーションを抑制しているのではないかという課題認識が官民双方に広まり、近年日本においてもオープンイノベーションの取り組みも一般的になりつつある。こうした動きは、国内産業の成長という観点ではプラスであるものの、経済安全保障の観点から考えるとリスクもある。

オープンイノベーションにおいて、スタートアップは重要技術流出の「原因」にもなりうる。例えば、大学が保有する革新的な技術やこれを扱うためのノウハウが、共同研究を通してスタートアップに移転された後に、スタートアップを介した意図せぬ流出につながるということが考えられる。特に創業間もないスタートアップであれば、社内の秘密管理体制の整備が進んでいないことや、前述のように十分なバックグラウンドチェックを行うことなしに国内外から投資の受け入れや採用活動を行っている可能性もある。また、人材の流動性が高く、人材移動（流出）の範囲がグローバルレベルであることもリスク要因となる。

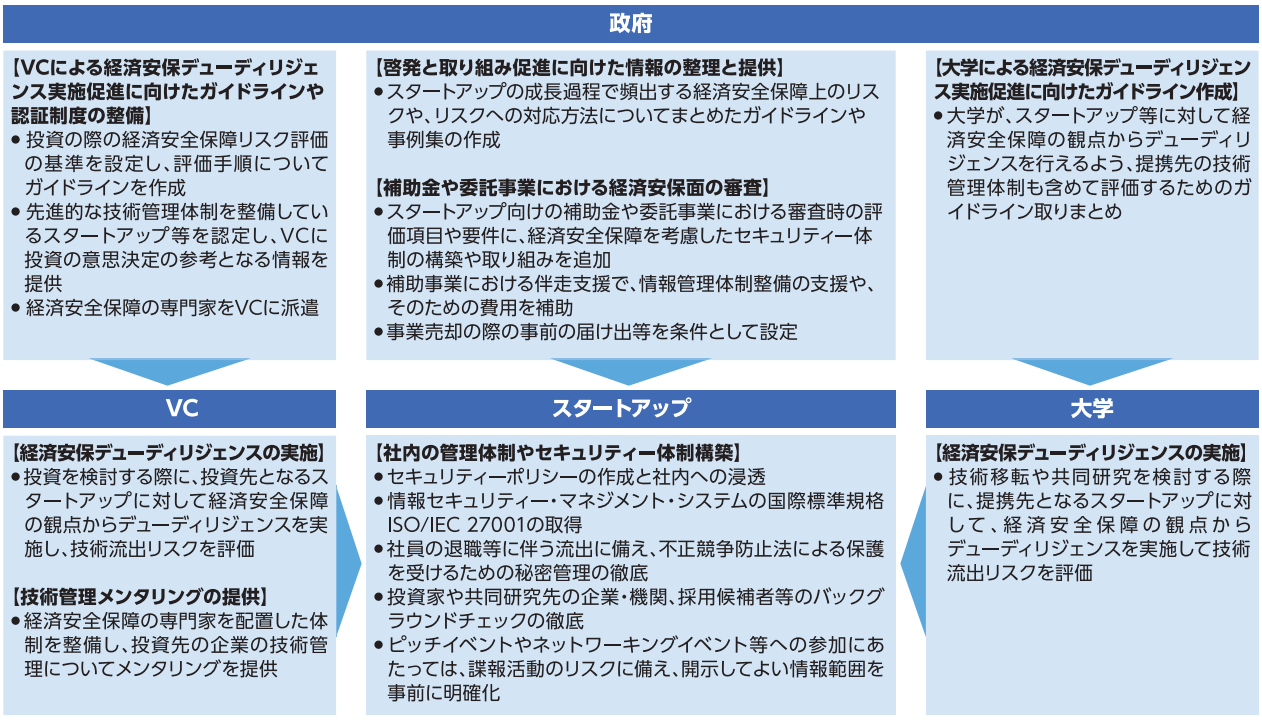
他にも、政府から重要技術の開発についてスタートアップを対象とした委託や補助を行う場合や、国立研究開発法人等の技術移転を前提とした共同研究や委託研究を行う場合も、成果物の流出について上記と同様のリスクがある。

(エ) その他のリスク（イベント等）

その他リスクが高い流出経路として、ネットワーキングイベントや、展示会等におけるインフォーマルな交流が挙げられる。スタートアップ・エコシステムにおいては、資金集めやネットワーキング、販路開拓等を目的としたさまざまなイベントが開催される。イベントにおいては、交流会もセットで行われることも多く、投資家や新規事業に関心を持つ国内外の企業等とスタートアップとのつながりを生み出す重要な役割を担っている。

一方でこうしたイベントは、参加者のバックグラウンドの厳密なチェックは実施されないことが一般的であり、基本的に事前登録さえすれば誰でも自由

図表３　エコシステムの各プレーヤーに求められる取り組み



出所）NRI 作成

に出入りできる環境にある。イベント会場で秘密情報に該当するような情報を漏らさなかったとしても、会場での接点をきっかけとして継続的にスタートアップに接触を図ることで、重要技術に関する情報を引き出すことを企図する者に狙われるリスクもある。実際に前述の公安調査庁の調査においては、諜報活動の典型的な例として、展示会等でターゲットとした者への継続的な接触の上、心理的ハードルを下げて情報提供を行わせるといった事例が紹介されている。

3　エコシステム全体で経済安全保障リスクをヘッジしていくための取り組み

第２章では、スタートアップ・エコシステムに潜む経済安全保障上のリスクについて、特にエコシステムの当事者が直面しやすいシーンに着目して整理をした。こうしたリスクが現実のものとなり、スタートアップが保有する革新的な技術情報が流出すると、日本の経済安全保障が脅かされるとともに、産業競争力自体も低下してしまう。

経済安全保障リスクをヘッジしつつエコシステムを駆動させ日本経済の成長を実現するためには、スタートアップがその成長過程におけるさまざまなリスクに対応するだけでなく、スタートアップを取り巻くエコシステムのプレーヤーがその機能に応じた役割を果たすことが重要である。

本章では、経済安全保障リスクに対してスタートアップが対応すべきポイントを整理した上で、VC、大学等スタートアップを取り巻くエコシステム内のプレーヤーが貢献できる役割について提言を行う。

1）　スタートアップが取り組むべき対応

まず、全てのリスクに共通する対応として、社内の管理体制やセキュリティー体制の構築にリソースを投入することが求められる。特に創業間もないスタートアップは、創業直後の資金調達や事業開発にリソースを集中させる中で、社内の管理体制やセキュリティー構築を後回しにしがちである。しかし、体制整備が不十分であると、大企業や政府・地方公共団体との取引機会を逸することや、M&A や IPO 等スタートアップの出口戦略にも影響を及ぼしうる

※4。情報セキュリティー対策の詳細には本稿では立ち入らないが、まずはセキュリティーポリシーの作成・社内への浸透に取り組んだ上で、情報セキュリティー・マネジメント・システムの国際標準規格である ISO/IEC 27001 の取得等を目指すことが考えられる。また、重要技術については、社員の退職等に伴う流出等万が一の事態を想定し、不正競争防止法による保護を受けられるよう秘密管理の徹底を行うことも求められよう。

投資の受け入れや共同研究については、多くのスタートアップにとっては魅力的な機会であり、詳細な調査を行うことなしに受け入れてしまうケースも多いと想定される。投資家や共同研究先の企業・機関、採用候補者等のバックグラウンドチェックを徹底することが重要である。さらに契約に進む場合も情報開示の範囲について事前に明確化しておくことが望ましい。同様にインターン生の受け入れや新規採用等で外部から人員を受け入れる場合も経歴等に問題がないかどうかバックグラウンドチェックを行うことが重要である。

さらに、ピッチイベントやネットワーキングイベント等に参加する際には、諜報活動に従事する者が紛れているリスクを認識した上で、事前に話してよい範囲を決めておく等工夫をすることで意図せぬ情報の漏えいを抑制することも求められよう。

2） VC が果たすことができる役割

VC はスタートアップ・エコシステムにおいて、スタートアップの資金需要に応える役割に加えて、その成長を多方面から伴走支援する機能を担う。これらの機能において、VC には「経済安全保障デューディリジェンス」と「技術管理メンタリング」の役割が期待される。

（1）経済安全保障デューディリジェンスの実施

経済安全保障デューディリジェンスとは文字通り、投資を検討する際に、経済安全保障の観点からデューディリジェンスを実施し、投資先となるスタートアップの技術流出リスクを評価することを指す。多くのスタートアップにとって VC から投資を受けることは事業活動において前提となる。VC が経済安全保障リスクを考慮して投資判断を行うようになれば、エコシステムの中で、スタートアップに技術管理体制を整備するインセンティブを与え、経済安全保障リスクをヘッジする流れを生み出すことにつながる。

先行事例として、欧米諸国では民間企業に対して経済安全保障リスクを考慮したデューディリジェンスやリスク評価を求める動きが見られる。例えば、2023 年 6 月 EU 委員会は、EU 理事会、EU 議会、EU の経済安全保障戦略に関する議会に対して、EU 企業が経済安全保障上のリスクをデューディリジェンスやリスク評価プロセスに組み込むよう奨励すべきだとする共同文書※5 を発表している※6。これは EU 内のビジネスに広く向けられたものであり、VC だけを名指ししたものではないが、スタートアップへの投資を担う VC にも考慮することが求められるであろう。

（2）技術管理メンタリングの提供

VC 側で経済安全保障の専門家を配置し、スタートアップに対してメンタリングを行う体制を整備することも有効である。例えば、米国サンフランシスコに本社を置く VC である Shield Capital は、商業および国家安全保障にとって重要な技術を扱う起業家を支援するためのファンドを立ち上げ、投資と

※4　重要技術情報ではないが、自動運転技術を開発するスタートアップ企業が顧客の個人情報の流出が発覚したことで当時の東証マザーズへの上場を延期した事例がある。日本経済新聞電子版「ZMP、顧客情報流出で上場延期『厳粛に受け止める』」2016 年 12 月 8 日

※5　JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL ON "EUROPEAN ECONOMIC SECURITY STRATEGY" 2023 年 6 月 20 日

※6　EU では、既に人権や環境分野については、企業にデューディリジェンスの実施を義務付ける「企業持続可能性デューディリジェンス指令案」が発表されている。出所）JETRO「EU 理事会、人権・環境デューディリジェンス法案採択、2027 年以降に順次適用開始へ」2024 年 5 月 28 日

国家安全保障に精通する人材を配置している※7。これは安全保障領域に特化したVCの事例ではあるものの、重要技術領域を対象とするVCは将来的にはこうした人材を配置し、投資先の企業の技術管理についてメンタリングを行うことが求められよう。

日本には「技術情報管理認証制度」（経済産業省）の中で、技術情報管理認証取得を検討する事業者等に情報セキュリティーの専門家を派遣する取り組みが実施されている。この取り組みを拡大し、経済安全保障の専門家をVCに派遣することで、その専門家が投資先のスタートアップの技術管理体制強化に関するメンタリングを行う体制を整えることも重要と考える。

3） 大学が果たすことができる役割

第2章で述べたように、大学とスタートアップとのオープンイノベーションにおいては、大学が保有する重要技術がスタートアップを介して流出するリスクがある。

こうしたリスクに対応するためには、大学においても、技術移転や共同研究を検討する際に、提携先となるスタートアップに対して経済安全保障の観点からデューディリジェンスを行うことが有効であろう。特にディープテック系のスタートアップにとっては、大学からの技術移転や共同研究は、事業を成長させる上で重要な取り組みの一つである。そのため、大学側が経済安全保障リスクを考慮して技術移転先や共同研究先を選定するようになれば、スタートアップに技術管理体制を整備するインセンティブを与えることにつながる。

現在、研究の国際化やオープン化に伴う研究機関からの技術流出リスクの高まりを受け、大学が技術移転先や共同研究先となる組織に対するデューディリジェンスを行うことを推奨する動きは世界各国で見受けられる。例えば、カナダでは「研究パートナーシップに関する国家安全保障ガイドライン」で、研究者が開発プロセスの初期段階でデューディリジェンスを行うことを推奨し、リスクアセスメントフォームを作成している※8。また日本でも、内閣府が「研究の国際化、オープン化に伴う新たなリスクに対するチェックリスト（雛〔ひな〕形）（大学・研究機関等向け）」を作成し、外国の機関・大学等との連携・契約に関する確認事項を整理している※9。ただし、これらのガイドラインやチェックリストの内容は、大学の連携先となる機関やその組織内の人物が外国政府からの干渉を受けているかどうかについての確認が中心となっており、連携先となる組織自体の技術管理体制そのものの評価を推奨するものではない。一方で、技術流出のリスクは外国政府からの干渉だけではなく、連携先となる組織のセキュリティー対策等にも依存するものである。ゆえに大学が、連携先となる企業の技術管理体制そのものについて、経済安全保障の観点からデューディリジェンスを行えるよう、チェックリストの充実化等に取り組むことも求められよう。

4）政府に求められる取り組み

経済安全保障リスクに関する認識が十分に浸透していない中で、エコシステム全体の取り組みを促進するためには、政府が果たす役割が重要である。ここでは、政府に求められる取り組みについて本稿のまとめとして提言を行う。

（ア）スタートアップ向けの政策

前述の公安調査庁の調査等、重要技術流出に関する啓発を行う刊行物は存在するものの、スタートアップをターゲットとした刊行物は現状ほとんど存在しない。スタートアップの取り組みを促す観点では、読者としてスタートアップを想定し、第2章で

※7　Shield Capital ウェブサイト「Shield Capital National Security Venture Capital Fund Launch」2022年3月15日
※8　カナダ政府ウェブサイト「National Security Guidelines for Research Partnerships」2022年10月6日
※9　内閣府「研究の国際化、オープン化に伴う新たなリスクに対するチェックリスト（雛形）（大学・研究機関等向け）」令和5年6月29日版

図表 4　活用できる既存制度や施策とその概要

	活用できる既存制度や施策	概要
1	技術情報管理認証制度 （経済産業省）	●国の認定機関が国の策定基準に基づき、企業の情報セキュリティー対策を審査・認証する制度 ●事業者が自社の情報セキュリティー対策の状況と必要な対策を把握するための「技術情報管理 自己チェックリスト」の作成も進行中 ●認証取得を検討する事業者等に、情報セキュリティーの専門家を無償で派遣し、具体的な情報セキュリティー手法をアドバイスする専門家派遣事業も実施
2	「研究の国際化、オープン化に伴う新たなリスクに対するチェックリスト（雛形）（大学・研究機関等向け）」（内閣府）	●「統合イノベーション戦略推進会議（第9回）」（2021年4月27日）において決定された、研究インテグリティーの確保に係る政府の対応方針に基づいて作成されたチェックリスト ●研究活動の国際化、オープン化に伴う新たなリスクの高まりの中で、大学・研究機関等が、所属する研究者の人事および組織のリスク管理として必要な情報を把握し、適切なリスクマネジメントを行える状態を促進することを目的としている

出所）各種公開情報に基づき NRI 作成

整理したように、投資の受け入れやイベントをきっかけとした諜報活動等、その成長ストーリーに応じた重要技術流出の「あるあるシーン」を整理した上で、具体的にどのような取り組みを実施すればよいか整理することが必要である。

政府補助金や委託事業も日本のスタートアップにとっては、重要な資金供給源である。そのため、スタートアップ向けの補助金や委託事業の審査において、経済安全保障を考慮したセキュリティー体制の構築や取り組みを審査時の評価項目や要件とすることも、スタートアップへの取り組みを促す直接的な効果が期待される。さらに、補助事業の場合は採択後の伴走支援としてこれらの整備を支援することや、セキュリティー構築に向けた費用自体を補助対象とすることも有効であろう。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、事業売却の際の事前の届け出等を条件として設けることも考えられる。

なお、リソースが限られるスタートアップに経済安全保障リスク対応を促すためには、こうした対応が国家の産業政策の観点だけでなく、個社の成長という観点からも必要であるという意識を持たせることが重要である。VC による投資や大学との共同研究、政府による補助事業や委託事業においてこれらの対応状況が問われる環境を構築すると同時に、政府として積極的な啓発を行うことで、スタートアップにおいて経済安全保障リスクヘッジに向けた取り組みの優先度を上げることにつながるだろう。

（イ）VC 向けの政策

多くの VC にとって、投資先候補企業に対して経済安全保障の観点からデューディリジェンスを行うことは、ノウハウの面からも難しいと考えられる。こうした取り組みを広げるためには、政府が投資の際の経済安全保障リスク評価の基準を設定すること、評価の手順についてガイドラインとして取りまとめることが考えられる。また、先進的な技術管理体制を整備しているスタートアップ等について認定を行うことで、VC に投資の意思決定の参考となる情報を提供することも有効であろう。

既存制度として、日本には「技術情報管理認証制度」があり、国の認定機関が国の策定基準に基づいて企業の情報セキュリティー対策を審査・認証すると同時に「技術情報管理 自己チェックリスト」の作成も進められている[※10]。まずは、このような認証制度やチェックリストの基準を、経済安全保障という包括的な観点から整理し、その基準の活用を VC に周知することで、VC が経済安全保障リスク

※ 10　経済産業省ウェブサイト「技術情報管理認証制度」

を判断する負担を軽減できるのではないか。

(ウ) 大学向けの政策

VC と同様に、知見やノウハウが不足している大学であっても、共同研究や技術移転の際に相手先となるスタートアップ等に対して経済安全保障の観点からデューディリジェンスを行えるように、必要なガイドラインを作成することも有効である。前述のように、内閣府では「研究の国際化、オープン化に伴う新たなリスクに対するチェックリスト（雛形）（大学・研究機関等向け）」を作成しているものの、相手先企業等における技術管理体制については想定されていない。技術管理体制のチェックも含めた大学とスタートアップのオープンイノベーションの際に取り組むべきガイドラインについて取りまとめることで、多くの大学の取り組みを後押しすることが期待される。米国政府は「米国の科学技術研究体制のセキュリティーとインテグリティーの強化に向けた推奨取り組み」を整理しており、リスクに関する考慮要素の一つとして、連携先の技術管理体制を評価する際の参考となりうる「データ共有およびガバナンスに関する規制要件および基準」を含めており、こうした検討の参考になろう[※11]。

4　おわりに

本稿では、スタートアップ・エコシステムに潜む経済安全保障リスクについて整理した上で、エコシステムのプレーヤーそれぞれに期待される役割や取り組みについて提言を行った。これから顕在化するリスクへの「備え」という観点では、スタートアップや VC、大学等の自主的な取り組みだけでは不十分であり、政府による啓発やモデルとなるガイドラインの展開、インセンティブの設定等がカギとなる。

日本においても急速にスタートアップ・エコシステムが発展するにつれて、グローバルレベルでのヒト・モノ・カネ・情報の流動性が高まっている。イノベーション促進という観点ではこうした資源循環は不可欠なものであるが、経済安全保障リスクも同時に高まる。国際関係の変化により、経済安全保障の重要性が高まる今日においては、エコシステムのプレーヤーそれぞれが役割を果たすことによって、経済安全保障リスクをヘッジすることができ、経済安保リスクのヘッジとイノベーションの促進を両立しうるエコシステムの発展、その先のイノベーションによる経済成長へとつながるであろう。

（監修：磯崎　彦次郎）

※11　米国大統領府「RECOMMENDED PRACTICES FOR STRENGTHENING THE SECURITY AND INTEGRITY OF AMERICA'S SCIENCE AND TECHNOLOGY RESEARCH ENTERPRISE」2022 年 1 月

筆者

本田　和大（ほんだ　かずひろ）
株式会社 野村総合研究所
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
専門は、科学技術・イノベーション政策（スタートアップ、知財、大学・高等教育政策等）
E-mail: k4-honda@nri.co.jp

水木　香那（みずき　かな）
株式会社 野村総合研究所
業務・IT 戦略コンサルティング部
コンサルタント
専門は、科学技術・イノベーション政策（スタートアップ、産学連携）、IT 戦略立案・推進
E-mail: k-mizuki@nri.co.jp