■企業も大学も「機微技術」の管理を急げ

米中技術覇権で問われる「アクセス天国・日本」の対応

中部大学特任教授
細川昌彦
ほそかわまさひこ
1955年生まれ。東京大学法学部卒業。通商産業省（現・経済産業省）で通商政策局米州課長、貿易管理部長などを歴任。在職中にスタンフォード大学客員研究員、ハーバード・ビジネス・スクールAMP修了。中部経済産業局長として「グレーター・ナゴヤ」構想を提唱。2009年より現職。テレビコメンテーターとしても活躍中。著書に『メガ・リージョンの攻防』『暴走トランプと独裁の習近平に、どう立ち向かうか？』。

米中合意でも深層部分は対立激化

米中貿易交渉の第一段階の合意が署名された。市場はポジティブに反応して一応両国の狙い通りだ。しかしこのようなトランプ大統領による関税合戦は、米中対立の表層部分に過ぎない。深層部分の対立は着実に激化している。

深層部分とは〝オール・ワシントン〟（米議会などワシントンの政策コミュニティー）による中国に対する技術覇権争いだ。最近はさらにこれに人権問題も加わっている。

この深層部分はオール・ワシントン主導で根深く、トランプ大統領も勝手に中国とディール（取引）させてもらえない。従って中長期的に続くと見るべきだろう。中国側も覚悟して長期戦の構えだ。

背景にあるのは、戦後の欧米主導の価値観とは相容れない中国の国家資本主義だ。これは共産党統治のための経済システムだ。国家計画「中国製造２０２５」も単なる産業政策ではない。中国は軍事力の高度化と一体となった世界最強の製造強国をめざしている。米国はそうした中国に対して技術優位を失うと、安全保障上の重大リスクになるとの厳しい認識だ。こうした認識を持つのは米国だけではなく、欧州における対中警戒感の高まりも見逃してはならない。

米国の基本的な対中認識を示すのが、二〇一七年十二月に発表された国家安全保障戦略と、一八年十月のペンス副大統領による演説だ。それを具体的な政策に落とし込んでいるのが一九年、二〇年度の国防権限法だ。

米中は「脱・依存」のせめぎ合い

注目すべきは安全保障上の中核的な産業分野として、国防権限法に半導体とレアアースが挙げられている点だ。

半導体は米国に依存する中国にとってアキレス腱になっているため、自前生産に躍起となっている分野だ。「中国製造２０２５」において自給率を二〇年までに四〇％、二五年までに七〇％をめざしている。そのために資金力を武器に、技術と人材の取り込みを加速している。

レアアースは米国が中国に依存しているために、米国にとってその弱みから脱却することが安全保障上急務の分野だ。ミサイルなど軍事用途に直結するだけに深刻で、米国は供給多角化や備蓄に向けて手を打ちつつある。

一方、中国が戦略的に自給率を高めるのは半導体だけではない。ロボット、大型航空機など「中国製造２０２５」の一〇大戦略産業はもちろん、情報システムといったソフトの国産化方針も打ち出している。

安全保障に直結する通信インフラは米中の綱引きが激しい分野だ。５Ｇを巡る覇権争いだけではない。通信衛星における米国のＧＰＳに対抗する中国版ＧＰＳ「北斗」、日米欧が独占する海底ケーブルへの中国のチャレンジなど争いは熾烈だ。

さらに米国による金融制裁のリスクを考えれば、中国にとって基軸通貨であるドルへの依存からの脱却は急務だ。そのカギは中国の広域経済圏構想「一帯一路」と「デジタル通貨」だ。「一帯一路」は人民元経済圏を広げる戦略でもある。またデジタル人民元の発行もドルに依存しない戦略の一つだ。

このように安全保障の根幹にかかわる経済分野において、米中それぞれが相手国からの依存脱却に躍起になっている。

最近、「エコノミック・ステイトクラフト（economic statecraft）」というコンセプトが注目されている。これは地政学的な戦略目標を達成するため、軍事力ではなく、経済的手段を用いて実現する国家の政策手法である。米中はこうした経済的手段を積極的に使おうとしている。米中

によるエコノミック・ステイトクラフトに晒されて、日本はどう対処すべきかが問われているのだ。

米国の「部分的な分離」戦略

今、ワシントンでは米中間「部分的な分離（Partial Disengagement）」がキーワードだ。

かつて冷戦時代の米国の対ソ政策は「封じ込め政策」であった。そして冷戦後の対中政策は西側諸国の価値観に収斂していくことを期待した「関与政策」であったが、その期待は裏切られた。しかし今や冷戦時代の「封じ込め政策」に戻ることはあり得ない。現在はグローバルな相互依存の経済構造がすでに出来上がっているからだ。

そこで第三の道として、米国圏と中国圏という「分断（デカップリング）」が進むのではないかとの懸念が広がっている。しかし経済全般の「分断」はもはや不可能で非現実的だ。

他方で、安全保障上の対中懸念の現実を無視して、自由貿易をナイーブに唱えているだけでは済まない。むしろ安全保障に直結する機微な技術（以下、機微技術）の分野を特定して、部分的に中国を分離していく。それが米国の指向する「部分的な分離」戦略だ。

こうした米国の「部分的な分離」戦略は当然、同盟国、友好国を巻き込む。

例えば、昨年十一月、半導体製造装置大手のオランダのASMLが、半導体の性能を高める次世代装置を中国政府系の半導体大手に納入する案件を保留しているとの報道があった。これも明らかに米国の要請を受けた動きだ。日本の半導体製造装置メーカーなども、サプライチェーンにおける重要パートナーとして巻き込まれる可能性大だ。

また台湾の半導体大手TSMCに対して、米中それぞれが圧力をかけて米国生産、中国生産をさせようと綱引きが過熱し、同社が股裂き状態になっているのも象徴的だ。その結果、TSMCに部材供給している日本企業も余波を受ける。

日本企業もすでに「股裂き」の状況に直面している。例えば、ファーウェイが米国のエンティティ・リスト（事実上の禁輸措置にするブラックリスト）に掲載された後、米国とファーウェイのはざまで困惑した日本企業も少なからずあった。

さらに中国は米国への対抗策の一つとして「中国版のエンティティ・リスト」制度の導入準備を進めている。これは、米国の規制によって中国企業への供給をやめる外国企業に対して、「不当な供給制限」として制裁を加えるものだ。その結果、企

業が米中双方のエンティティ・リスト間で〝踏み絵〟を迫られる恐れもあるのだ。

米国が徹底する「技術管理の強化」

こうした機微な特定分野を念頭において、米国が手を打っているのが「技術管理の強化」だ。その二本柱が「投資管理」と「輸出管理」である。

中国を念頭に、外国企業による米国企業への投資を通じた技術流出を阻止すべく、二〇一八年八月、対米外国投資委員会（CFIUS）による審査が拡大・厳格化することになった。欧州でも同様の懸念から投資管理が強化されている。

一八年八月以降、米国は安全保障上懸念のある中国製の通信・監視機器について政府調達を禁止するだけでなく、民間取引も禁止して米国からの締め出しを図っている。

また中国企業のエンティティ・リストへの掲載も相次いでいる。最近だけでもファーウェイの他、監視カメラ、スーパーコンピューター、原発関連企業など二〇〇社近くがリストに追加されている。

「買わない」「使わない」から「売らない」「作らせない」にまで及んでいるのだ。

さらに今年は輸出管理で米国に大きな動きがある。輸出管理改革法（ECRA）が制定され、「新興技術」や「基盤技術」という新たな概念を導入して、これまで規制されていなかった領域の技術まで輸出管理を強化しようとしている。前者はAI、量子技術などが、後者は半導体製造などが挙げられている。

現在、米国政府内においてそうした技術の特定化作業が行われている。日本企業にも大きな影響を与える動きであり、目が離せない。

輸出管理は「新型・対中COCOM」へ変貌

中国に対する技術管理に取り組むうえで、忘れてはならないポイントがある。「軍民融合」と「国家情報法」の存在だ。

軍民融合の方針の下では、中国の民間企業に供与された民生技術でも常に軍事転用の危険に晒される。民生用と軍事用の区別が意味をなさないのだ。

さらにそのリスクを高めているのが国家情報法だ。民間企業も含むあらゆる主体が、中国政府の指示があれば得られた情報を政府に提供することを義務付けられている。

その結果、各国の輸出管理も大きく変貌する必要に迫られている。これまで輸出企業が輸出管理を行う際は、軍事用途に転用されないことを確認することに主眼が置かれていた。

しかし、これでは現在の中国に対応できなくなっている。これが米国の対中・技術管理のベースとなる認識だ。

そこで機微技術について軍民を問わず、中国への流出を阻止するというアプローチが必要となる。

かつて米ソ冷戦期には共産圏に対する技術上の優位を維持するために、西側諸国によってココム（対共産圏輸出統制委員会）が実施されていた。冷戦終了後、九〇年代からは懸念国への兵器の拡散を防ぐための輸出管理に衣替えした。

そして今や中国を念頭においた「新型・対中ココム」（仮称）へと変貌しようとしているのだ。

既存の国際的枠組みは中国を巡る新たな状況にそぐわなくなったが、米国だけが独自に規制しても効果が限定される。そこで同盟国との国際連携が必要とされているのだ。日本にも同調が求められるのは必至だ。

日米欧の有志国による新たな国際輸出管理体制という潮流が見えてきた。

「シャドウ・ラボ」の恐ろしさ

もう一つ米国の対中・技術管理のうえで重要なポイントがある。それは研究開発段階から中国への技術流出を阻止することだ。米国の大学は中国による国家主導の技術獲得の主要なターゲットとされており、対応が急務になっている。

二〇〇八年にスタートした中国政府による「千人計画」がある。中国政府主導の海外の研究人材の招致プログラムで、米国にいる中国人研究者が主な対象だ。これが組織的な技術流出に利用されることを米国は警戒している。

米デューク大学の中国人研究者もその一人だった。米国防省の受託研究で特殊素材を使った「透明マント」の研究情報を窃取して中国に帰国後、中国政府の支援を受けている事件は有名だ。

「シャドウ・ラボ」という、中国による組織的な技術窃盗を表す言葉がある。盗んだ情報をもとに、研究室にあった装置のコピーを中国国内に作って、研究室をそっくりそのまま再現するのだ。

そのため米国では中国人研究者に対するビザ発給を厳格化するだけでなく、大学でも自主的な管理強化の動きが強まっている。多くの大学がファーウェイからの資金提供を拒否し、共同研究の実施を停止している。

日本が〝抜け穴〟になる恐れ

こうした状況で、日本が技術流出の〝抜け穴〟になることは許されない。まず政府が制度的な〝抜け穴〟をふさぐ必要がある。経済と安全保障の一体化が進む中で、経済安全保障の重要性が叫ばれているが、取り組むべきは投資管理と輸出管理からなる「技術管理」を強化する制度整備だ。

投資管理については、先の国会で承認された「外為法」の改正がそれだ。これは欧米各国において中国を念頭に、安全保障上の投資管理を強化する動きが相次いでいることが背景にある。これで日本もやっと欧米レベルの投資規制に近づいた。ただし、これで十分な訳ではない。米国CFIUSが強化された投資管理の適用除外国としているのは、諜報情報を共有する英、豪、加のみだ。

問題はこれだけではない。米国の動きをにらんだ、輸出管理の抜本的強化が大きな課題だ。今後、欧州も含めてすり合わせを行い、日米欧の有志国による新たな対中・輸出管理体制をめざすべきだろう。

欧米の対応など面的広がりを持って見る。多様な対応手段を見る。「木を見て森を見ず」にならず、多角的な視野を持って「技術管理」の全体像を描いて、戦略的に取り組むべきだ。

企業に必要な「情報セキュリティ」の仕組み

対応を迫られるのは政府だけではない。企業や大学も情報セキュリティという技術管理が急務だ。

法令を遵守するのは当然だが、米国では企業や大学が、機微技術の管理の観点から、自主的な経営判断として管理強化に動いている。そして共同研究のパートナーから技術が流出することがないよう、パートナーにも同レベルの管理体制を求めることも検討している。

日本企業が技術的な競争力を持つことは不可欠であるが、それは自国だけで達成できるものではない。欧米諸国との共同研究が重要だ。そのためには日本企業もこうした状況に対応していかなくてはならない。

例えば、同じ会社の中で、米国の大学とも中国企業とも共同研究をしている日本企業は多い。その際、社内で両者の間に情報セキュリティのファイアウォールが設けられているかだ。設けていない場合、もはや米国の大学・企業とは付き合ってもらえないというリスクもあるのだ。

日本の大学も同様だ。近年、多くの大学で中国人研究者や留学生を受け入れている。また研究資金不足にあえぐ大学にとって、潤沢な研究資金を有する中国の大学や企業との共同研究は魅力的だ。そこに落とし穴がある。ごく一部を除き、危機意識がなく無防備で、中国にとって「機微技術のアクセス天国」になっている。このままでは日本が米国の共同

研究のパートナーから排除されるリスクもあるのだ。

日本の企業や大学に欠けているのは具体的な社内の情報セキュリティの仕組みだ。中でも人とサイバーがポイントだ。

人については、機微技術にアクセスする従事者の適格性を確認をする制度（セキュリティ・クリアランス制度）の導入だ。米国企業では十数万人規模の人々をこうした制度の適用対象にしている。

日本企業もこうした制度の基準に合致していなければ重要な情報を共有できるセキュリティがないと米国企業からみなされて、今後は情報のやり取りさえできなくなる恐れもあるのだ。

サイバー攻撃に対する備えも急務だ。機微技術を有しているにもかかわらず無防備な企業も多い。米国は中国のサイバー攻撃による技術窃取には極めて神経質になっている。

例えば、中国が大型ジェット旅客機でボーイング、エアバスに一気に追いつこうと、自主開発と自称するC919を開発した。これは米仏の部品メーカーへのサイバー攻撃の結果、米仏合弁企業のエンジンと極似のエンジンを製造したものだ。

最近、防衛産業の代表的な企業である三菱電機が中国軍とのつながりもあるハッカー集団によるサイバー攻撃の標的にされたことで衝撃が走った。日本企業ではサーバー攻撃も他人事のように思っている経営層がいかに多いことか。自社のサイバー攻撃のリスク分析もせず、社内にサイバーセキュリティの専門人材がいない企業が依然多い。

米国では国防調達に限らず、広範な裾野の間接的な取引先にも、政府指定の厳しいセキュリティ措置への準拠を求めている。外国企業でも準拠しなければ、米国のサプライチェーンから外されるリスクもあるのだ。

安全保障のアンテナ低い日本企業

経済と安全保障が一体化した今、安全保障に対するアンテナを高くし、こうした米中双方の動きを他人事ではなく、自らの経営リスクとして受け止めるべきだろう。

そのための社内体制も重要だ。従来の輸出管理だけでは大きな経営リスクを抱えることになる。輸出管理部門、技術開発部門、情報システム部門がバラバラに対応するのではなく、経営層直轄で、安全保障の視点で一体的に取り組む体制が必要になってくる。

米中両国とビジネスで付き合う日本企業にとって、安全保障上機微な技術分野の見極めが重要になってくる。AI、量子技術、5G、監視カメラのような特定分野については米国の動きを踏まえた慎重な対応が必要だ。虎の尾を踏むわけにはいかないのは、一九八七年の東芝機械ココム違反事件を思い出せば明らかだ。そしてこうした特定分野におけるサプライチェーンの分断を、経営リスクととらえる必要があるだろう。

さらに、米国の規制との関係では、法的なチェックさえすればよいわけではない。仮に「米中対立はビジネスチャンスだ」として「漁夫の利」を得ようとすれば、違法行為でなくても、米国からは利敵行為とみなされて制裁対象にもなり得るのだ。エンティティ・リスト掲載企業との取引は慎重にすべきであることを経営層は理解しておくべきだ。

他方、中国との関係では中国企業との共同研究に合意して満足していると、研究データを日本に持ち出す際に、サイバーセキュリティ法で中国政府の許可が必要になると知り、慌てふためいている企業もある。

今、中国は米国に対抗する経済的手段を持とうと躍起になっている。米国と同様の武器をそろえるべく、新しい制度の導入も目白押しだ。輸出管理規則の制定、中国版エンティティ・リストの公表がそうだ。

今年一月一日から施行された「暗号法」も、中国でビジネスを行う外国企業にとって機密保護ができなくなる可能性が懸念されている。

こうした米中双方の動向をすべて経営リスクとして経営層がとらえているかどうかだ。

米中のイノベーションを取り込むために

他方で、中国における自主的なイノベーションの展開も目覚ましい。これを冷静かつ正当に評価することも重要だ。

中国の潤沢な研究費や高待遇といった研究環境は、海外の優秀な研究人材を引き付けている。さらには大量の資金を投入する技術開発のエコシステムが出来上がっているのだ。研究開発費、研究者数は米国と一位、二位を競うレベルだ。その結果、論文数や特許出願数で目覚ましい躍進を遂げている。中国全土が日本の〝特区〟のようで、社会実装のスピードも圧倒的だ。

日本企業は今や自前の技術開発だけでは立ちゆかず、オープン・イノベーションが企業の競争力のカギになっている。そうした中で米国だけでなく、同じく巨大市場とイノベーション力を有する中国と付き合っていくことも重要になる。

その際、必要なのは安全保障の視点でのリスク管理と技術管理だ。これは米中技術覇権争いによって直面する新しい経営課題だ。その向き合い方が企業の存立を左右する。