係強化にも資するため、各国は戦略的に取り組んでいる。

参照　Ⅰ部4章4節（防衛生産・技術基盤をめぐる動向）

第2節　わが国の防衛生産・技術基盤を取り巻く環境

わが国においては、今や「新しい戦い方」を踏まえたわが国独自の「新しい守り方」を可能とするための優れた装備品等を早期に獲得することは急務である。その獲得は、わが国国内における技術的知見の蓄積や、高度な技能を有する人材の育成、特殊なニーズを満たす製造設備・施設の整備・維持などといった、長期にわたる不断の取組によりようやく実現することが可能となる。

このため、政府は、2022年12月に策定した国家安全保障戦略などにおいて、防衛生産・技術基盤を取り巻く厳しい現状を直視し、優れた装備品等の確保に不可欠の要素である防衛生産・技術基盤を、いわばわが国の防衛力そのものと位置づけることによって、その抜本的な強化に取り組んでいく方針を明確に示した。

まず、わが国における防衛生産・技術基盤には、いくつかの特徴がある。前提として、工廠（装備品等の製造などを行う国営工場）を持たないわが国においては、基盤の重要な役割を、プライム企業と呼ばれる防衛省から直接受注を受ける大企業のみならず、サプライヤーと呼ばれる多くの中小受託事業者といった民間企業に大きく依存している。また、装備品に携わるサプライヤーは非常に多く、例えば戦車や戦闘機は1,000社以上、護衛艦は8,000社以上の企業が、各種部品の製造や組立てなどに携わっているとも指摘されている。防衛力の抜本的強化が求められるなか、自衛隊の任務遂行に必要な装備品等の確保を担保する防衛産業の重要性はますます高まっている。

そのうえで、装備品等の製造等[1]にあたっては、高度な機能・性能の要求および情報保全措置などへの対応に多大な経営資源の投入が必要となり、企業がそのための投資に踏み切るためには、経済合理性の観点から一定の予見可能性が必要となる。また、これらの企業は多品種少量生産を求められるほか、装備品等の運用期間の長さから、長期にわたる製造などの体制確保も必要となる。さらに、顧客は基本的には防衛省・自衛隊のみであることから、生産数は極めて限定的となり、企業にとって投資回収の機会は限られる状況が続いている。加えて、防衛事業に対して忌避観やレピュテーションリスクを抱く企業も依然として存在する。

こうした状況にも起因し、防衛事業からの撤退や事業規模の縮小を決断する企業が断続的に現れるなど、わが国の防衛産業は様々な課題に直面している。その結果、自衛隊の運用に必要不可欠な装備品等の安定的な調達に支障が生じるだけでなく、長期的には、適正な競争環境やイノベーションが失われ、安全保障分野におけるわが国の技術的優位性を喪失するおそれもある。

これらに加え、近年、防衛関連企業の契約履行環境のDX（デジタルトランスフォーメーション）化が急速に進展するなかで、機微な情報を保有する防衛産業においては、情報システムやネットワークに対し、国家が関与する疑いのあるサイバー攻撃の脅威が高まっている。例えば、2021年には、中国軍が関与している可能性が高いとされるサイバー攻撃集団によって、わが国の防衛関連企業を含む国内の約200の企業や研究機関などに対して大規模なサイバー攻撃が実行されたことが公表された。また、2024年には、わが国の研究機関が管理する通信機器が侵害され、サーバが不正アクセスを受け、業務に関する情報が漏えいしたことが公表された。

さらに、重要な物資の囲い込みが国際的に進むなか、例えば、外国政府による輸出規制によって原材料などが輸入できなくなり、装備品等の安定的な供給が確保できなくなるリスクも現実味を帯びている。

防衛省・自衛隊としては、こうしたわが国の防衛生産・技術基盤を取り巻く環境を踏まえ、これを維持・強化するための各種施策を講じている。

1　製造、研究開発および修理ならびにこれらに関する役務の提供。

視点

わが国の防衛産業が直面する課題

防衛研究所　社会・経済研究室　主任研究官　小野（おの）　圭司（けいし）

日本の防衛産業には「構造的な問題」が存在しています。装備品の高度化、国際環境の緊張、技術覇権競争の激化が重なるなかで、従来型の調達・生産モデルは限界を迎えつつあります。特に①供給網（サプライチェーン）の安全性、②熟練人材の減少、③サイバーセキュリティの脆弱性は、防衛産業基盤そのものを揺るがしかねない深刻なリスクです。

第１は供給網の安全保障です。装備品は数千点規模の部材・電子部品・ソフトウェアの集合体であり、その一部でも信頼性が揺らげば、装備全体の安全保障リスクに直結します。近年は海底通信インフラや半導体製造装置など、軍民両用性の高い技術が国際的な安全保障上の焦点となっています。海外企業の買収を巡る投資審査の強化や、特定国によるレアメタル輸出規制は、供給網の地政学的リスクを示しています。弾薬、センサー、パワー半導体などの生産が影響を受ける可能性がある以上、トレーサビリティの強化、代替調達先（レアメタルの都市鉱山も含む）の確保、戦略物資の備蓄拡充などは必須です。

第２に人材基盤の弱体化があります。装備品の製造・整備には、高度な加工技術や暗黙知を有する熟練工の存在が不可欠です。しかし団塊世代の大量退職が進む一方、若年層の採用は進まず、技能伝承が追いついていません。特に中小サプライヤーでは、受注の不安定さや低収益性が人材確保を阻んでいます。防衛産業は少量多品種生産が中心であり、技能の喪失は即座に品質低下や納期遅延につながります。また装備品は民生品に比べて市場規模が小さく、輸出も限定的であるため、企業が設備投資や人材育成に踏み切りにくい構造的制約があります。

第３に、供給網下流を起点とするサイバー攻撃の増加です。近年はセキュリティ体制の脆弱な下請企業を経由して機密情報を窃取する手法が増えています。国内でも、一般産業分野でのランサムウェア被害が相次ぎ、情報管理の弱点が外部から突かれ得ることが明らかになりました。防衛関連企業の場合、設計図面や試験データが流出すれば、技術的優位性の喪失のみならず、国家安全保障上の重大な損失となります。供給網全体を対象としたセキュリティ基準の統一、監査制度の導入、ゼロトラスト型の情報管理体制の構築が求められますが、中小企業にとってはコスト負担が重く、実装面での支援策が不可欠です。

これら３つの課題は相互に連関しています。今後は、効率性と冗長性の再均衡を図りつつ、防衛産業を国家安全保障の基盤インフラとして再定義する視座が求められます。経済合理性だけでは測れない「安全保障としての産業政策」が、今まさに問われています。

（注）本コラムは、研究者個人の立場から学術的な分析を述べたものであり、その内容は政府としての公式見解を示すものではありません。