

政策提言

科学・技術・産業・安全保障の エコシステム構築

—日本の総力を挙げた国家安全保障の実現を—

2026年10月

公益財団法人 笹川平和財団
経済安全保障技術・産業力強化戦略研究会

政策提言

科学・技術・産業・安全保障の エコシステム構築

—日本の総力を挙げた国家安全保障の実現を—

2026年10月

公益財団法人 笹川平和財団

経済安全保障技術・産業力強化戦略研究会

提言目次

提言者一覧	ii
はじめに	1
提言要旨	3
本提言の問題意識と提言の概要	11

第1部 デュアルユース技術 21

提言 1 「安全保障関連技術推進基本法」の制定及び「安全保障関連デュアルユース技術推進基金」の設置	21
---	----

コラム 「最先端技術（CET）」だけでなく「基盤技術（FT）」も—基盤的デュアルユース技術の空洞化という論点—	24
---	----

提言 2 安全保障デュアルユース技術開発実装のためのエコシステムの構築	25
-------------------------------------	----

提言 3 安全保障上重要なデュアルユース技術を実装・事業化につなぐ知財・技術資産戦略—技術を持続的な能力に結実させる支援制度への転換—	37
---	----

コラム 上流からの一体設計—光学センサーの設計から知財・技術資産戦略まで—	47
---------------------------------------	----

提言 4 進化し続ける防衛装備品へ—ソフトウェア時代の産業技術基盤：三者一体（MOSA・SBOM・RMF）とDevSecOps—	49
--	----

提言 5 安全保障に関連する機器・システムの調達先企業の選定に関するガバナンスルールの導入	59
---	----

第2部 防衛装備品 61

提言 6 緊急時における防衛装備品の優先的確保に係る施策	61
------------------------------	----

提言 7 有事における継戦能力確保のための取り組み	63
---------------------------	----

提言 8 防衛装備品の更なる移転推進のための施策	65
--------------------------	----

提言 9 部隊レベルのニーズを反映した新たな調達制度の導入	67
-------------------------------	----

提言 10 シンクタンク等におけるセキュリティ管理システムの導入	69
----------------------------------	----

第3部 官民連携 73

提言 11 官民の研究者の交流の促進	73
--------------------	----

提言 12 SDA（宇宙領域把握）と天文学会の連携による宇宙関連等学術データの安全保障への活用	77
---	----

提言者一覧

- 赤 石 浩 一（元科学技術・イノベーション推進事務局長、
元デジタル庁デジタル審議官、笹川平和財団上席フェロー）
- 油 木 清 明（パウワーグループアジア（BGA）日本代表）
- 磯 部 晃 一（元東部方面総監、元陸将）
- 兼 原 信 克（笹川平和財団常務理事、元国家安全保障局次長）
- 河 上 康 博（笹川平和財団 日米・安全保障研究ユニット 総括・交流グループ長、
元防衛大学校教授、元海将補）
- 土 本 英 樹（元防衛装備庁長官）
- 西 山 淳 一（元三菱重工業株式会社 航空宇宙事業本部 副事業本部長）
- 真 部 朗（元防衛審議官）
- 宗 像 直 子（元特許庁長官、笹川平和財団上席フェロー）
- 渡 辺 秀 明（元防衛装備庁長官）

※五十音順

【事務局】

- | | | |
|---------|---------------------|----------|
| 河 上 康 博 | （笹川平和財団 総括・交流グループ長） | 【事務局長兼務】 |
| 柴 山 真里枝 | （同上 研究員） | 【事務局】 |
| 洞 口 雅 恵 | （同上 主任） | 【事務局】 |

はじめに

国際秩序の大変容が始まった。ロシアによるウクライナ侵略は長期化する一方、中国は大規模な軍備増強を進め、北朝鮮も核・ミサイル能力の強化を継続している。米国・イスラエルとイランの戦争は、ホルムズ海峡の封鎖を引き起こし、アジア全域におけるエネルギー安全保障上の重大な懸念となっている。このように我が国を取り巻く安全保障環境は、戦後最も厳しく複雑なものとなっている。

世界経済秩序も大きく変容している。戦争やパンデミックは、地球規模で張り巡らされたサプライチェーンが容易に寸断され得ることを証明した。また、急速に台頭した中国による、最先端軍事技術の急速な追い上げ、経済的相互依存関係の武器化や、基幹産業の生産基盤の中国移転とそれに伴う先進国産業の空洞化は、経済安全保障上の深刻な懸念を引き起こしている。

さらに、現代の戦場には、大量のソフトウェアを搭載した廉価な無人兵器（ドローン）が投入され、人工知能（AI）、自律システム、量子、サイバー、宇宙等の「ゲーム・チェンジング・テクノロジー」が戦闘の様相を一変させている。今日、デュアルユース技術と軍事技術は不可分であり、明日の戦場は今日の戦場とは全く異なるものとなり得る。

国民の生命と幸福な暮らしを守ることは国家の一丁目一番地の責務である。国家安全保障は、国家の政策体系の最高位に位置する。科学技術の発展こそは国家安全保障の中核である。

しかしながら、国家安全保障が国民生活や経済活動の大前提であるという国際社会において当然の考え方が、我が国においては広く共有されていない。我が国においては戦後長きにわたり、「安全保障と科学・産業技術の断絶」という特殊な問題が存在し、アカデミア及び防衛産業を除く民間企業の双方で、防衛技術開発に対する忌避感が根強くあった。安全保障上のニーズが産学のデュアルユース技術のシーズと結びつかないことに加え、そもそも安全保障分野に限らず、産学の技術シーズをグローバルビジネスに育て上げるためのマインドが育っておらず、エコシステムも十分に整備されていない。

デュアルユース技術が安全保障能力を左右する時代には、イノベーション・エコシステムの弱さは、そのまま抑止力の弱さにつながる。安全保障を根柢にイノベーションを強くし、そのイノベーションの力で安全保障を強くする。この好循環を生み出すことが、日本にとって喫緊の課題である。そのためには、日本の優れたデュアルユース技術を国家安全保障に活かすとともに、安全保障上の厳しいニーズを日本の科学技術と産業のイノベーションにつなげていかなければならない。

こうした問題意識の下、公益財団法人笹川平和財団は2024年6月、防衛省及び経済産業省の元政策立案者並びに防衛産業に関する有識者等の参加を得て、「経済安全保障技術・産業力強化戦略研究会」を立ち上げた。以来、2026年9月までに計14回の研究会を開催し、防衛産業・技術開発及び経済安全保障に係る現状を分析するとともに、諸外国の先進事例も参照しながら、安全保障関連技術の推進と産業基盤の強化に必要な政策及び制度について検討を重ねてきた。

本提言は、その議論を踏まえ、安全保障関連技術とデュアルユース技術の間の垣根を取り払い、日本全体として官産学及び自衛隊の協力を実現する方策を示すものである。「強い防衛」と「強い経済」の双方を底支えするものが、「先端デュアルユース技術基盤」である。この基盤を強化することこそが、我が国の経済安全保障を確立し、政府の掲げる成長戦略の実現に大きく寄与すると考える。本提言が、政府、産業界及び学术界をはじめとする幅広い関係者の議論と行動につながることを期待したい。

最後に、本研究会に貴重な知見をご提供いただいた研究会メンバー及び有識者の皆様に、心から御礼を申し上げます。また、本研究会の運営並びに本提言の取りまとめに当たっては、事務局である河上康博 総括・交流グループ長、柴山真里枝 研究員、洞口雅恵 主任の尽力なくして完成に至ることはなかった。ここに深く謝意を表したい。

2026年10月

公益財団法人笹川平和財団 常務理事

兼原 信克

提言要旨

第1部

デュアルユース技術

提言

1

「安全保障関連技術推進基本法の制定」及び「安全保障関連デュアルユース技術推進基金」の設置

日本の優れた科学技術を国家安全保障に活かすために、安全保障関連技術推進のための基本法として「安全保障関連技術推進基本法」を制定し、総理主宰の本部を設け、国家安全保障局監督の下、内閣府にその事務局を設け、5か年計画を策定して、政府全体の安全保障関連技術関連業務を総括し、主要な特定技術を指定し、その発展を支援する。毎年、執行状況を確認するため年次報告書を策定する。

元自衛官、元官僚、産業界の経営者及び技術者、学界の研究者等からなる総理直轄のディフェンス・ボードを作り、5か年計画原案を総理から諮問する。安全保障関連技術に関する内外の軍事情勢、技術情報を収集するために、自衛官、官僚、外事警察関係者、学識者、研究者からなる調査部を、上記の内閣府事務局に設ける。

企業、スタートアップが負えない予算的リスクを政府が安全保障理由として負うこととし、特定の有望技術の支援のために、官民で10兆円（運用型なら30兆円規模）の基金として「安全保障関連デュアルユース技術推進基金（仮称）」を立ち上げる。さらに、安全保障関連技術育成促進のための知財・技術資産戦略を策定する（提言3参照）。

また、同5か年計画においては、ソフトウェア中心となる今後の防衛装備の調達の方法の改変、有事における防衛省の継戦能力の確保、資材の優先利用、工廠の設立やGOCO（Government Owned and Contractor Operated）制度の活用必要性等についても、その内容に含めることとする。

提言

2

安全保障デュアルユース技術開発実装のための
エコシステムの構築

日本が安全保障に資するデュアルユース技術を育成するには、課題設定から研究開発、スタートアップ支援、資金供給、政府調達、海外市場獲得まで一貫した「包括的エコシステム」が必要である（知財・技術資産戦略については提言3参照）。米国はDARPA（国防高等研究計画局）・DIU（防衛イノベーションユニット）・In-Q-Tel（CIA系ベンチャーキャピタル）・OSC（戦略資本金局）・OTAs（柔軟な新技術調達制度）などを組み合わせた包括的かつ実効的な仕組みを持つが、日本は課題設定の曖昧さ、硬直した会計制度、資本不足、調達制度の制約、国内外の参入市場の不在などが障害となっている。これを克服するため、米国エコシステムの本質的な点を取り入れた日本版DARPA・DIUの構築、国家安全保障ベンチャーキャピタル（VC）やOSC型金融支援、柔軟な調達制度、そして10兆円規模の「安全保障関連デュアルユース技術推進基金（仮称）」（提言1参照、年間1兆円規模の支援を想定）と基金運用／エコシステム支援のための「包括的安全保障関連技術育成実装機構（仮称）」を創設、研究から産業化・市場獲得までを一体で支援する体制を構築すべきである。

提言

3

安全保障上重要なデュアルユース技術を実装・
事業化につなぐ知財・技術資産戦略—技術を持
続的な能力に結実させる支援制度への転換—

研究開発を支援するだけでは、安全保障上必要な技術も供給能力も国内に残らない。先端デュアルユース分野で「技術で勝って事業で負ける」失敗を繰り返してはならない。政府は、達成すべきミッションと利用ニーズを明確にし、技術の探索から市場展開までを一貫して設計するとともに、知財・技術資産の価値を契約条件と価格に反映し、知財評価や契約実務を担う専門人材確保のため、その対価を支援額・契約額に組み込む。政府の利用・改良能力と企業の改良・再投資条件の確保はゼロサムではなく、企業を成長させ技術供給基盤を持続させる事業戦略として捉える。このため、防衛省版SBIR（いわゆる「ファストパス調達」）、「包括的安全保障関連技術育成実装機構（仮称）」（提言2参照、以下「新機構」）、「安全保障関連デュアルユース技術推進基金（仮称）」（提言1および提言2参照、以下「新基金」）等に、①ミッション起点の入口評価、②知財・契約・事業化の伴走支援、③初期需要から調達・量産・市場展開への移行の3機能を組み込む。利用部門が個別案件を主導し、新機構・新基金が専門家と支援を組み合わせ、防衛省・防衛装備庁には知財・技術データと契約・調達を一体的に扱う専門機能を整備する。また、試作・実証段階での低価格中国製部材への過剰依存を防ぐため、国内・同志国供給網の活用を促す。目指すのは、安全保障上必要な能力を自ら定義し、技術・企業・供給網・市場を一体的に形成する能力の構築である。

進化し続ける防衛装備品へ —ソフトウェア時代の産業技術基盤：三者一体 (MOSA・SBOM・RMF)とDevSecOps—

装備品の性能と能力向上の速度は、機体や素材、センサーといったハードウェアに加え、内部で動くソフトウェアに大きく左右されるようになってきている。しかもソフトウェアは「造って終わり」の製品ではない。現代のソフトウェアは、オープンソース、商用製品、独自開発のコードを組み合わせで構築されることが多く、配備後も新たな脆弱性が次々に明らかとなる一方、適用すべき新しい技術も次々に現れる。従って、米国防総省は「ソフトウェア近代化実施計画（2025～26年度）」において、現代の戦場を「ますますソフトウェアが規定する戦場（increasingly software-defined battlespace）」と位置付けている。装備品は配備した後も、不具合を直し続け、能力を高め続けられる構造でなければならない。これは防衛に限った話ではなく、自動車・通信・重要インフラなど、ソフトが価値を決めるあらゆる製品に共通する、産業全体の構造変化である。

特に防衛においては、「進化し続ける装備品を生み出す技術基盤」を持つ国だけが、これからの先端技術を利用して、不安定な安全保障環境を勝ち抜くことができる。その技術基盤こそが、①機能を交換可能な単位に分ける「モジュール・オープン構造（MOSA、Modular Open Systems Approach）」、②ソフトウェアの中身を見える化する「SBOM（Software Bill of Materials）」、③リスクを管理して運用を承認する「RMF（Risk Management Framework）」の三者と、これらを分断なく一つの流れで回すDevSecOps基盤である。日本は、この技術基盤を無人機を出発点として最初から一体の更新サイクルとして設計し、アジャイル開発による早期装備化、常時のセキュリティ確保、スタートアップ参入による新技術導入を同時に達成することで、バランスのとれた戦闘力を最大に発揮できる防衛力を築くべきである。

提言

5

安全保障に関連する機器・システムの調達先企業の選定に関するガバナンスルールの導入

防衛施設や政府機関、基幹インフラ等で利用される機器・システムは、AIやIoTの普及により継続的にデータを収集・送信するものが増えている。このため、防衛装備品のみならず、一見すると安全保障とは直接関係のない設備やハードウェアについても、機微情報が国外へ流出するリスクを考慮する必要がある。

このため、安全保障に関連する機器・システムの調達に当たっては、外国政府への協力義務の有無を含めた企業ガバナンスを総合的に評価する仕組みを導入すべきである。こうしたガバナンスルールを整備することにより、安全保障上信頼できる製品・システムの普及を促すとともに、我が国企業の技術開発や設備投資を後押しし、技術安全保障基盤の強化につながっていく。

併せて、こうしたガバナンス要件を適用する分野の判断や、調達先選定後の運用段階においても、取り扱うデータや機器が使われる工程の機密度に応じて、利用可能な機器・通信機能・データ移送経路等を段階的に制限する仕組みを組み合わせることが有効である。

提言

6

緊急時における防衛装備品の優先的確保に係る施策

半導体など汎用部素材に関しては、市場原理に基づくと防衛装備品に優先的に供給されにくい傾向がある。事態が緊迫し近い将来に武力攻撃事態等を認定する蓋然性が高まりつつある状況になった場合、民生・軍用双方に利用可能な汎用部素材や、民生需要に対応してきた技術力・製造ラインを防衛装備品向けに優先的に確保することが必要となる。このため、国家安全保障会議（NSC）で防衛装備品の確保を優先的に措置すべき旨決定した場合、防衛大臣から経済産業大臣に所要の防衛装備品確保のため汎用部素材を防衛装備品向けに優先して納入・生産してもらう、また製造ラインを民需から防需に向けてもらいたい旨要請し、経済産業大臣から製造事業者に上記内容を要請するというスキームを構築する。その際、併せて事業者には機会損失等に係る補填措置を行うこととする。このスキームの実効性を確保するため、「安全保障関連技術推進基本法」（提言1参照）の中にプログラム的に盛り込み、新たに実施法を制定することとする。

提言

7

有事における継戦能力確保のための取り組み

5年近く続く戦闘においてウクライナは弾薬・誘導武器・ドローン等を大量に消費しており、厳しさを増す安全保障環境の中、我が国においても長期戦に対応できる生産能力・維持整備能力の確保は喫緊の課題となっている。防衛装備品や我が国の存立のため必須となると考えられる装備品に関して、有事における継戦能力の確保や経済安全保障における戦略的自立性の確保などの観点から、現在の防衛生産基盤強化法に規定されており、ラストリゾートと位置付けられているGOCO（Government Owned and Contractor Operated）の制度を積極的に活用し、特に長期間にわたる戦闘行為において特に消耗が激しいと考えられる弾薬、誘導弾、ドローン等についてGOCOによることとする。なお、平時には、GOCOの枠組みによる生産数量の確保の観点から、積極的にこれらの装備品を海外に輸出したり、ドローンについては民生需要にも対応することとする。さらに、武力攻撃事態認定以降も一定の生産量を確保するとの観点から、当該施設の安全が確保される限り業務を継続する旨契約で担保し、併せて有事において当該業務に従事する労働者については、国から特別の手当を支給するほか、万が一の際の補償についても自衛官並みとなるように新たに法律を制定する。

提言

8

防衛装備品の更なる移転推進のための施策

我が国の安全保障環境の改善を目的として政府主導で防衛装備移転を強力に推進するためには、装備移転対象国を特定し、交渉・合意し、合意に基づく装備品を取得し、それを移転するための新たな制度が必要となる。組織面での強化のために、まず、NSCを司令塔と位置付け、国家安全保障局（NSS）に装備移転担当部署を新設するとともに、防衛装備庁に「装備移転部（仮称）」を新設する。さらに、新たに「装備移転推進機構（仮称）」といった法人を新設し、官民から人材を派遣して、各国の装備品需要の調査、対象国関係機関及び国内関係企業との移転実施に係る実務面の調整、防衛産業への支援策、納期管理、部素材安定供給のための調整などの実務を処理することとする。さらに、納期管理等を徹底させ、可能な限り単納期で装備移転を実現する等との観点から、重要技術を含む防衛装備品に関してはG-G契約（日本版FMS：Foreign Military Sales）を新たに制度として導入することとする。

提言

9

部隊レベルのニーズを反映した新たな調達制度の導入

安全保障分野におけるデュアルユース活用推進の方策として、防衛省の地方調達システムを、消耗品などの購入手段に限らず、現場ニーズを起点としたイノベーションのツールとして再定義することが必要となる。

第一に、随意契約を再定義し、その上限を引き上げるべきである。安全保障分野に限り、これを「特定企業の技術に戦略的にフォーカスする手段」として位置付け、対象を新領域の装備・研究開発・実証等に限定しつつ、情報公開や第三者チェック等のガバナンス強化を前提に、その活用余地と限度額を拡大する。

第二に、地方調達を拡充し、部隊単位の調達制度を構築すべきである。平時有事の境が曖昧化し、陸海空に加え宇宙・サイバー・電磁波・認知の領域までを担い、多様な編成をとる現在の自衛隊においては、現場に一定の権限を移し、中央調達品目であっても地方で調達できるよう、防衛省の調達制度を改正するべきである。

第三に、デュアルユース技術の活用である。中小企業の機動力とデュアルユース技術の転用可能性を活かし、現場ニーズに即した技術の取り込みを進めることが必要となる。

シンクタンク等におけるセキュリティ管理 システムの導入

米国政府系シンクタンクであるRAND（ランド）研究所、MITRE（マイター）研究所などFFRDC（連邦研究開発センター）においては、政府指定の「秘」を取り扱うために、セキュリティ管理区域を設置し、研究員もセキュリティ・クリアランス（Security Clearance、以下SC）を保有している。一方、CSIS（戦略国際問題研究所）、ハドソン研究所（Hudson Institute）などの民間非営利シンクタンクでは「秘」に関する研究を行わず、組織として「秘」を扱う制度・施設を保有していない。研究者個人ではSCを持っている人がおり、組織が制度・施設を持たなくても個人が保有できる仕組みがある。これに対し日本の場合、退職するとSCは失効する。

一般に有識者はリタイアした人（経験有識者）が多く、「秘」を含む経験・知見を活用するための制度が必要である。現役時代にSCを保有していた人を「経験有識者」としての活用が可能となるようなSCの管理機関と制度を整備すべきである。

第3部

官民連携

提言

11

官民の研究者の交流の促進

現行法制度上、官民の人材の双方向の交流に関して「官民交流法」があるが、例えば、民間から官に派遣された場合、交流元企業の契約関連業務に従事できないことに加え、民間企業復帰後2年間は派遣先との契約の締結等に関する業務や派遣先との折衝や情報収集に関する業務に従事できないと制度上されている。

防衛省の研究者は防衛装備庁技術戦略部や各研究所で研究開発業務に従事するが、防衛省が発注する研究開発に関する契約やその履行に研究者は携わることとなる。かかる事情から、上記に述べたような官民交流法における各種規制との関係で、これまで防衛省の研究者と防衛産業の研究者との官民交流は、官民交流法施行後、実績がないまま推移している。

防衛省と防衛産業の研究者は、相互にお互いの組織を知り、特に防衛産業側の研究者にとっては防衛省・自衛隊の運用ニーズやスピード感を踏まえた装備品の研究開発の実態を知ることが、研究者として民間企業に復帰後も有益な経験となり、かかる観点からも研究者の相互交流の活性化が望ましい。このような事情を踏まえ、研究者に限定した官民交流法を新規に制定し、現行法の利益相反防止に係る制度に代わる新たなチェック機能を導入することにより、研究者の官民交流の活性化を図ることとする。

提言

12

SDA（宇宙領域把握）と天文学会の連携による宇宙関連等学術データの安全保障への活用

宇宙空間の利用は、国家安全保障はもとより、人々の毎日の生活に欠かせないものとなっている。宇宙利用が進めば進むほど、大量の人工衛星が打ち上げられ、大量の衛星が軌道を周回し、その後廃棄されることとなる。その副次的影響として、宇宙デブリ（ゴミ）が増大し、宇宙空間の安定的利用への脅威となっている。宇宙の安定的利用のためには、宇宙デブリの監視が喫緊の課題であり、将来的にはデブリ除去が求められる。

我が国において宇宙デブリの監視は、防衛省とJAXAの役割分担により政府に統合化されたが、観測体制は決して十分とはいえない。それを補完するために天体観測データを宇宙デブリ監視のデータとして活用する。具体的には、天体観測を行っている天文台のデータを防衛省に提供することにより、宇宙デブリ監視に役立てる。天文台の観測データを宇宙利用の安全のために使うことができる制度を整備すべきである。

本提言の問題意識と提言の概要

1. 急速に悪化する我が国の安全保障環境

国際秩序の大変容が始まった。国連安全保障理事会における常任理事国であるロシアがウクライナを侵略している。アジアでは、核兵器を含む大軍拡に舵を切った中国が、南シナ海に複数の軍事拠点を設けて沿岸国を威圧し、また、台湾の民主主義を踏みにじって共産党一党独裁を押し付けようと併合への野望を隠さない。尖閣諸島では連日、中国「海警」公船が押しかけてくる。北朝鮮はロシア側に立ってウクライナ戦争に派兵し、核武装に余念がない。米国及びイスラエルとイランの戦争は、ホルムズ海峡封鎖を引き起こし、アジア全域においてエネルギー安全保障上の重大な懸念となっている。日本の安全保障環境がこれほど急速に悪化したのは、戦後初めてのことである。多くの日本国民が国際政治のリアルを肌を感じ始めている。

特に、日本が懸念すべきは、台湾有事である。もし、中国が台湾に侵攻すれば、米軍は日本の基地から出動する。それが「日米安全保障条約」第6条の仕組みである。与那国島まで台湾から僅か110キロである。日本はフィリピンと同様、前線国家となる。太平洋の米国同盟国は、日本以外に豪州、韓国、フィリピン、タイしかない。大国と呼び得る同盟国は日本だけである。さらに、中国は、尖閣が台湾の一部であり、沖縄（琉球）の地位は未定であると主張している。かつて安倍首相が述べたとおり「台湾有事は日本有事」との覚悟を持つ必要がある。

台湾有事の経済的打撃は、対中貿易途絶、株と為替の暴落、それに伴う外貨準備の枯渇、台湾周辺海域の封鎖、戦域化する東・南シナ海及びマラッカ海峡・ロンボク海峡の商船通航停止、膨大な戦費と破壊されたインフラ等の戦後復興費など、平時には想像を絶するものがある。太平洋戦争で経験したとおり、戦争の惨禍は、自然災害よりも遥かに大きい。

日本は、この急激な安全保障環境の悪化に対して、第二次安倍政権、菅政権、岸田政権、石破政権、高市政権と続く中で、国家安全保障局設置、国家安全保障戦略策定、国家防衛戦略及び防衛力整備計画策定、防衛装備移転三原則策定といわゆる「5類型」廃止、特定秘密保護法制定、平和安全法制制定及び限定的な集団的自衛権行使是認、経済安全保障法制制定、GDP（国内総生産）2%への防衛予算増額方針、サイバー対処法制定、自衛隊統合作戦司令官及び統合作戦司令部創設、国家情報局設置等と足早に安保政策を充実させてきた。

2. 世界経済秩序の動揺と経済安全保障

世界経済秩序も大きく変容している。冷戦終了時から2020年頃まで、世界秩序はマーケットの力が支配するべきであるという自由主義的な経済思想が主流であった。当時、中国は未だ西側と良好な関係にあり、WTO（世界貿易機関）に加入して急速な経済発展を遂げた。新生ロシアは、G8の一員に迎えられた。テロの横行はあったが、それでも平和と繁栄の新世紀が来るというユーフォリアが生まれた。しかし、それは短命であった。

2014年、2022年のロシアによるウクライナ侵攻や、2020年に世界に広がったコロナ禍は、世界経済が、脆い土台の上に立っていることを思い起こさせた。当時、既に地球的規模でサプライチェーンが毛細血管のように張り巡らされていた。投資家目線に立てば、途上国に直接投資し、安く製品を作って、それを先進国で高く売るのは当然のことであった。先進国が産業空洞化、少子高齢化に悩み始める一方、多くの途上国が若い労働力を生かし、先進国との自由貿易と先進国からの直接投資を活用して発展を遂げてきた。世界経済をけん引し始めたグローバルサウスの台頭である。しかし、戦争とパンデミックは、このサプライチェーンをいとも簡単に寸断できることを証明した。「地経学」、「経済安全保障」という考え方が登場した。

現在、特に大きな問題となっているのが、急激に台頭した中国が引き起こす様々な懸念である。2010年に日本の経済規模を抜いた中国は、その後すぐに日本の4倍の経済規模に達した。共産党一党独裁の下で、習近平国家主席という復古主義的な指導者を得た中国は、強国思想を前面に押し出し、大軍拡に舵を切り、米国との覇権争いを目指すようになった。米国は、第一次トランプ政権から、激しい反発を見せた。対中関与政策は終わりを告げ、「米中大国間競争時代」が幕を開けた。中国は、未だ中国の経済規模より大きな西側経済に深く依存しながら、同時に、西側の政治体制に背を向けて、ロシア、北朝鮮との関係を深めつつある。ここにイランが加わる。冷戦初期のような対立の構造が生まれつつある。西側経済と深く統合されたまま、中国が戦略的方向性を反転させつつある。それがもたらす懸念が、西側諸国の経済安全保障政策を推し進めていると言っても過言ではない。主要な懸念とは次のようなものである。

第一に、中国の最先端軍事技術の急速な追いつきが引き起こす安全保障上の懸念である。中国は、台湾有事を念頭に、米国と対等な軍事力を持つようとしている。「軍民融合」のスローガンの下、巨額の補助金が人民解放軍と関係の深い大学及び研究機関や国有企業に注ぎ込まれる。こうした投資を、一過性の資金供給に終わらせない仕組みも並行して築かれてきた。習近平は2014年、自主イノベーション能力の強化を国家戦略の中核に据え、2015年には「中国製造2025」と知的財産強国建設に関する国務院文書を相次いで発表した。知的財産権保護は、党中央政治局委員が総書記の主宰で特定テーマを学ぶ「中央政治局集団学習」（年数回のみ開催）の議題にも選ばれ、2020年には習近平自身がこのテーマで直接発言している。中国は、イノベーションを生み出し続ける制度基盤そのものを覇権競争の対象と捉え

ている。宇宙、サイバー、量子、バイオ、先進コンピューティング、AI、ドローンなど、デュアルユース技術を用いた最新の軍事技術の進展は、日本を遥かに凌駕して、米国に肉薄している。米国は、対中技術流出に関して厳しい対抗措置を取り始めた。特に、先進コンピューティングやAIの要である半導体に関しては、最先端半導体及びその製造機械の中国への輸出を厳しく制限し始めた。また、米国の科学者がエネルギー省の研究予算を受け取る際には、中国からの研究助成の経験の有無を報告するように義務付けた。中国人留学生の受け入れについても査証発給の際に軍事関係者ではないか厳しい審査が行われている。

第二に、中国による経済的相互依存関係の武器化がもたらす経済的威圧に関する懸念である。2010年のミンシンリョウ事件で、中国は日本へのレアアースの輸出を全面禁輸とした。台湾の貿易事務所を開設したリトアニアは、貿易を完全遮断された（関税表から国名が消えた）。コロナウィルスの発生源を調査せよと中国に迫った豪州はワインの輸入を止められた。台湾からはパイナップルの輸入が、フィリピンからはバナナの輸入が止まった。2025年、第二次トランプ政権が、対中関税を145%にしたとき、習近平は対抗関税を発動したのみならず、直ちにレアアースの禁輸を打ち出して、トランプ大統領を屈服させて貿易停戦に持ち込んだ。中国は、戦略的に西側諸国に対する貿易上のチョークポイントを握り、それを武器化しようとしていることが明らかになった。経済的威圧の対象となった国々は中国の圧力に輸入代替先の確保などで対抗しようとしているが、巨大な国力を以て中国に対峙する米国と、貿易政策を欧州委員会が一元管理している欧州連合（EU）を除き、成功しているとはいえない。

第三に、鉄鋼、造船などの基幹産業の生産基盤の中国移転と先進国産業の空洞化である。中国は市場競争の力を巧みに国家戦略に組み込んできた。中国政府は、技術を習得すると、西側企業を中国マーケットから締め出し、過剰な生産能力を実現し、集中豪雨的な輸出で西側先進国市場を席卷することにより、先進国の基幹産業を空洞化させ、基幹産業面で中国に依存させるという戦略を意図的に取っているように見える。その結果は、巨額の対中貿易赤字だけではない。西側先進国においては、産業基盤、企業の技術開発基盤そのものが失われつつあり、中国が生産力、技術力の双方で優位に立ちつつあるのである。その姿は1970年代末から80年代にかけて対米貿易摩擦に直面した、かつての日本を思い起こさせる。しかし、日本はプラザ合意の円の急騰により、輸出国家から投資国家へと変貌し、米国から産業を奪う国から、米国産業に投資する国へと変貌し、日米貿易戦争は終息した。同盟国だから取れた道であった。米国と覇権争いに立ち上がった中国に同様の道はない。むしろ中国では、プラザ合意は日本が米国に屈服した結果と認識されており、対米貿易戦争での永続的な勝利を目指しているように見える。

3. 急激に変わる現代の戦場

現代の戦場は、急激な変化に見舞われている。それはハードウェア中心主義から、ソフトウェア中心主義への移行である。明日の戦場は、今日の戦場とは全く異なるものとなる。

1991年の第一次湾岸戦争では、米国が情報処理能力を著しく向上させつつ、偵察衛星やGPS衛星などの宇宙アセットを戦術的に利用して、イラク軍を一蹴した。RMA（軍事革命、Revolution in Military Affairs）と呼ばれた。2014年のロシアによるクリミア半島等の奪取に際しては、ロシアがサイバー攻撃能力と非正規部隊を駆使して、ウクライナ軍を混乱させ屈服させた。2020年のアゼルバイジャンとアルメニアによるナゴルノ・カラバフ紛争では、トルコから大量のドローンの提供を受けたアゼルバイジャン軍が、ロシアを後ろ盾とするアルメニア軍を一蹴した。現在のウクライナ戦争では、ウクライナの無人航空機による攻撃がロシアを苦しめている。

大量破壊兵器である核兵器の時代から、精密誘導兵器により敵の戦力を無害化する時代に移り、そして今日、これらの高価な兵器から、無数の廉価な無人兵器が襲い掛かる時代に移りつつある。この進化を支えているのが情報処理技術の進歩である。最近、そこにAIが加わった。軍隊自体が大きく変貌しつつある。

将来の戦場では、無人の航空機や船舶やロボット兵士が先兵となる。個々の無人兵器は、AIによって自律して索敵し、敵を殲滅する。後方の司令部では、索敵、攻撃、兵站に関わる情報を、AIを用いた先進コンピューティングで一括処理し、瞬時に最も効果的な作戦を立案するようになる。それによって作戦遂行のための命令系統（キルチェーン）が著しく効率的になり、高速化する。将来の戦場では、この流れに乗り遅れた国の軍隊は、まるでスローモーション動画のように見えるであろう。

新しい戦場に投入される兵器には、大量のソフトウェアが埋め込まれる。ソフトウェアは定期的に更新されねばならない。まるでスマートフォンのアプリのように、次から次へとアップデートが必要となる。その定期的な交換のためには、兵器をモジュール化し、パーツ、パーツを取り変える必要がある。それは兵器の開発と調達の仕事の抜本的な変更を必要としており、我が国も急ぎ対応する必要がある。

4. 日本に特殊な問題の存在—安全保障と科学技術・産業技術の断絶

経済安全保障を考えると、日本には、特殊な問題が存在する。安全保障と科学・産業技術の断絶である。GHQによる初期占領政策は、日本の徹底的な非軍事化を望んだ。日本国憲法第9条第2項の「陸海空軍その他の戦力は、これを保持しない」という規定はその象徴である。「その他の戦力」とは、外務省が「other war potential」を訳したものであるが、そのまま読めば、ドイツが石炭、鉄鋼、原子力産業を欧州連合によって国際化させられたように、日本から自前の重工業を排除するという意味にも解釈できる。

冷戦の開始及び朝鮮戦争の勃発によって、米国は日本再軍備に舵を切るが、日本独立後（1952年）、今度は、東西冷戦の強い磁場が日本を襲う。日米同盟に舵を切った政府・自民党と、東側陣営に強い共感のあった社会党・共産党の激しい対立が構造化された（55年体制）。高度経済成長、福祉国家実現前の日本では、マルクス主義、共産主義の影響力は大きかった。アカデミアでは、特にその傾向が強かった。防衛産業を除く産業界にも軍需産業、「死の商人」と呼ばれることに強い忌避感があった。

ソ連は、平和攻勢を以て、日本の赤心の平和主義を利用した。その結果、冷戦の最前線に立った外務省、防衛省、警察庁、公安調査庁を除いて、経済官庁、経済界、特にアカデミアの一部に平和主義志向、中立主義志向が浸透し、軍事を忌避する傾向が生まれ、日米防衛技術協力、安全保障関連技術の開発に強い拒否感を示すようになった。それが戦後80年の長い間、日本のデュアルユース技術の安全保障への活用には厳しい壁となって立ちのびてきた。特に、学術会議をトップとするアカデミアには、その傾向が強く見られた。

逆に他の国々では、科学技術の発展こそが国家安全保障の中核であるという常識が根付いている。例えば米国では、年間20兆円近い科学技術予算の半分が国家安全保障関係の研究に当てられる。エネルギー省傘下の優れた研究所や安全保障に関わる研究を志す大学に巨額の研究開発資金が落ちる。そもそも科学技術の発展は人類の希望であり、安全保障に関連する研究をしてはいけないという垣根を設ける方がおかしい。発展する科学技術をどう活用するかしないかは政治と政策の問題である。昨今ではデュアルユース技術が著しい進歩を遂げており、そのような垣根自体に意味がなくなっている。

また、米国防総省の国防高等研究計画局（DARPA）では、スタートアップに資金を提供して、優れた技術を育てマーケットに送り出す。そうすることで「死の谷」と呼ばれる研究開発と市場化・製品化の橋渡しをしている。AppleもModernaもここから生まれた。防衛産業関連では、GOCO（Government Owned and Contractor Operated）と呼ばれる制度がある。政府が投資した設備を民間企業が運営することによって、企業に利益を確保させつつ、防衛産業基盤を維持している。このような産官学軍を横断するエコシステムが大きな成果を上げている。特に、米国の「CHIPS法」に見られるように、今日、デュアルユース技術が軍事技術と不可分になっていることを踏まえて、巨額の安全保障関係の委託研究や投資支援（補助金）がWTOのルールの外で産業界、学界に流されるようになってきている。

日本には、このような仕組みが最近まで存在しなかった。戦後の経緯から、しようにもできなかったのである。

岸田政権の下で、「経済安全保障重要技術育成プログラム」（通称「Kプログラム」）が作成され、2年間で5,000億円の予算が積まれた。かつての学術会議に代表されるように日本の学術界が冷戦時代から強いイデオロギー的分断の下で、防衛省との協力を頑なに拒んできたことを思えば大きな進歩である。

また、防衛省自身が推進する「安全保障技術研究推進制度」（通称「防衛省ファンド」）は、当初の学術会議からの拒否反応も収まってきており、企業の応募も増えているが、アカデミアからの応募はまだまだ少ないことに加え、防衛省側の予算規模の更なる拡充が望まれる。防衛省は、防衛装備庁、陸・海・空の各自衛隊の研究所に優れた研究者を擁しているが、今後、更に民間技術の積極的な導入・活用が欠かせない。安全保障関連技術の進歩のために官民の一層の交流が必要であり、そのための制度的拡充が望まれる。

残念ながら、現状では、安全保障に関する本質的なニーズが研究者、技術者に伝わらず、一方で、そこでの研究成果が本当に実際の場面において安全保障に活かされるか極めて疑問な状況にある。Kプログラムも、防衛省ファンドも、優れたデュアルユース技術を有する民間企業と連携して、国家安全保障のために政府が民間企業のラボなどに資金提供等を行うのみならず、政府が企業側のリスクを軽減して経営に貢献し、さらには技術の一層の発展に資するための仕組みとして有効に機能しているとは未だ言いがたい状況にある。

最も根深い問題は、「戦闘員として自らと部下の死を覚悟して祖国防衛に当たる」という自衛官の壮烈な死生観と、「だからこそ死なずに戦争を終わらせるための優れた技術が欲しい」という切迫した彼らの要望が、政府部内にも、産業界にも、アカデミアにも十分伝わっていないことである。それが伝われば、現在の戦場がどのように変貌しているか、どのような技術が戦場を変えているか、どうすれば勝てるのかという発想が自ずから湧いてくるはずである。

5. デュアルユース技術の国家安全保障への活用

日本が取り組まねばならない課題は多く、未だ連山のように聳えている。その最たるものが日本の優れたデュアルユース技術の国家安全保障への活用である。どこの国でも当たり前のことが、戦後80年間、日本ではできてこなかった。先述のとおり、アカデミア、防衛産業を除く民間企業の双方に、防衛技術開発に対する忌避感があったからである。

AI、自律システム、量子技術、サイバー、宇宙といった「ゲーム・チェンジング・テクノロジー」は、現代の戦闘様相を一変させ、国家間の競争において極めて重要な要素となりつつある。ウクライナ戦争が示すように、こうした先端技術を迅速に装備化し、社会実装する能力は、従来の戦力差をも補完し、状況を大きく好転させる可能性を秘めている。

我が国において防衛装備庁「防衛イノベーション科学技術研究所」（イノベ研）の設立など、画期的な技術（ブレークスルー）を生み出すための研究体制の整備が進められている。しかし、研究開発組織がその真価を発揮するためには、それを支える産業界とアカデミアの「足腰」の強さが不可欠である。具体的には、AI、量子、半導体といった「先端デュアルユース技術基盤」が国内に強固に存在してこそ、防衛省が目指す次世代装備の研究開発においても、優れた性能の実現が期待できる。

この技術基盤の重要性は決して防衛分野にとどまらない。高度な防衛装備品を製造できる技術力は、自動車産業のように世界をリードする民生品の開発・製造基盤としても機能し得る。すなわち、「強い防衛」と「強い経済」の双方を底支えするのが「先端デュアルユース技術基盤」であり、この基盤を強化することこそが、我が国の経済安全保障を確立し、政府の掲げる成長戦略の実現に大きく寄与すると考えられる。

今の日本の喫緊の課題は、先端デュアルユース技術供給基盤の確保である。当該政策の実効性確保のためには、研究開発支援に加え、技術供給主体の競争力及び事業継続能力を補強する包括的な制度的対応が不可欠である。

特に、スタートアップ及び技術特化型中小企業は、新技術導入、用途転換及び市場適応において重要な役割を果たし得る主体であり、特別に注目する必要がある。これらの類型に特有の経営制約及び成長上の課題を踏まえた支援の仕組みの検討が必要である。

研究開発成果が事業化及び持続的成長に至る過程における、いわゆる「死の谷（Valley of Death）」問題（試作から量産化への移行段階で事業化が停滞してしまう問題。資金不足として語られることが多いが、より根本的には、事業として収益を生み出す経営力不足が伴っていると考えられる。「死の谷」問題と通称される。）は、各国共通の構造的課題である。主要国においては、企業の通過確率及び生存可能性を高める観点から、研究開発支援、商用化支援、調達制度の柔軟化、契約制度の最適化、競争力基盤の補強などを含む多層的な制度的対応を実施している。

6. 防衛産業の強化と有事における継戦能力の確保

安保三文書を策定した2022年12月から4年近く経とうとしており、2026年12月には新たな安保三文書が策定されることとなっている。

このような中、ロシアのウクライナ侵略は5年近く続く長期戦の様相を示しており、かかるウクライナの教訓反省等を踏まえると、防衛産業を取り巻く環境には大きな変化が生じている。

第一に継戦能力の脆弱性が露呈したことである。ウクライナでは砲弾を少なくとも約2,000発／日消費している（2024年3月時点）といわれているが、防衛産業への投資が低調であった等の理由により欧米諸国では生産能力がひっ迫するとの課題が明白となった。第二に、ウクライナ・ロシア双方とも多くの安価なドローンを投入し、戦場を可視化した上で敵の高価なアセットを安価に破壊する非対称的な手法で優勢を獲得しようとするといった形で敵に「Cost Imposing」な戦術をとるなど「新しい戦い方」が顕著となってきている。さらに、ウクライナ侵略、中東情勢、中国の重要物資の輸出規制等により、サプライチェーンのリスクが顕在化するなどしており、我が国においても、長期戦にも対応して抑止力を高めることのできる国内生産・維持整備能力の確保や、有事に必要な増産対応能力の確保に資する防衛装備移転の推進等が必要となってきている。すなわち、防衛産業に係る新たな施策を導入することにより、上記の変化に対応できる強靱性を備えた国内防衛産業基盤の確立を図ることが必須となっている。この点、諸外国においても、例えば米国では2024年1月に策定された「国家防衛産業戦略」において、同盟国等を含めた需要増、予期せぬ混乱への対処等に不可欠な予備生産能力にインセンティブ付けとされているほか、英国においても2025年9月に策定された「防衛産業戦略」において、十分な弾薬や補用品の在庫確保、迅速な供給、迅速かつ継続的なイノベーションサイクルの重要性を強調している。

このような観点から、有事を見据えた生産能力の確保や防衛省が必要とする装備品をタイムリーに調達できるようにするための新たなスキーム（防衛装備品の優先的確保措置）を設けることにより、有事に必要な防衛装備品の納入・生産を確実なものとする。さらに、有事における継戦能力確保のためにレピュテーションリスク等のため企業の自主的な投資が進みにくい一方で有事において消費が著しく所要の増大が見込まれる防衛装備品分野（例：弾薬）については、官による直接の関与を強めることとし、具体的にはGOCOを活用することにより、所要の生産能力の確保に努めることとする。その際、武力攻撃事態等の認定以降も業務に従事する防衛産業従業員に対して手当等を支給する特別立法も併せて措置することにより、所要の労働力の確保を担保する。

さらに、我が国にとって望ましい安全保障環境の創出や同盟国・同志国との連携強化・拡大といった目的に加え、有事に必要な増産対応力の確保に資するため防衛装備移転を積極的に推進するため、政府内における防衛装備移転のための司令塔組織の新設、重要技術を含む防衛装備品に関するG-G契約（日本版FMS：Foreign Military Sales）の導入、防衛装備移転の実務を担う新たな法人の設立などの各種施策も併せて措置することが必要となる。

7. 宇宙関連等学術データの経済安全保障への活用及びシンクタンク等におけるセキュリティ管理

国家安全保障において、宇宙空間の利用は今や必須の空間であり、今日では戦闘補助空間というよりも、戦闘を行う空間として認識され始めている。さらにGPSの利用等、宇宙空間の利用は人々の毎日の生活にも欠かせないものとなっており、最近ではStarlinkに代表されるように低軌道コンステレーション型の小型多数衛星が打ち上げられ、高速インターネット回線の衛星通信が活用されている。

宇宙利用が進めば進むほど、大量の人工衛星が打ち上げられ、大量の小型衛星が利用され、その後廃棄されることにより、その副次的影響として宇宙デブリの増加は否めない。結果的に、宇宙デブリ（ゴミ）が増大し、宇宙空間の安定的利用への脅威となっている。

宇宙の安定的利用のためには、宇宙デブリの監視が喫緊の課題であり、将来的にはデブリ除去が必要となる。我が国において宇宙デブリの監視は、防衛省とJAXAの役割分担により政府に統合化されたが、観測体制は決して十分とはいえない。それを補完するために天体観測データの活用が考えられる。天体観測データには天文学者にとっては「ノイズ」とでもいうべき宇宙デブリの軌跡が含まれている。このノイズとして利用されないデータを宇宙デブリ監視のデータとして活用すべきである。我が国が天体観測を行っている天文台のデータを防衛省に提供することにより、宇宙デブリ監視に役立てるべきであり、そのための制度を整備すべきである。

また、経済安全保障における特定重要技術の開発支援において、シンクタンクは守秘義務を求められている。つまり、セキュリティ体制の構築が求められ、それはセキュリティ・クリアランス（Security Clearance、以下SC）を有する研究員が必要であると解釈される。

米国のシンクタンクでは、政府系のRAND（ランド）研究所、MITRE（マイター）研究所などFFRDC（連邦研究開発センター：Federally Funded Research and Development Center）では、政府指定の「秘」を取り扱うために、セキュリティ管理区域（SCIF：Sensitive Compartmented Information Facility）を設置し、研究員もセキュリティ・クリアランスを保有している。

一方、CSIS（戦略国際問題研究所）、ハドソン研究所（Hudson Institute）などの民間非営利シンクタンクでは一般に「秘」に関する研究を行っていない。よって、組織（シンクタンク）として「秘」を扱う制度・施設を保有していないが、研究者個人でSCを持っている人がいる。つまり、米国には組織（シンクタンク）自体が制度・施設を持たなくても個人が保有できる仕組みがある。

日本の場合、退職すると同時に業務上のNeed to knowが無くなるので、SCは失効する。前述のように米国におけるSC保持者は個人としての資格であり、SCが必要な仕事（Need to knowが生じた時）に登用できる仕組みができています。

一般に有識者はリタイアした人（「経験有識者」と呼ぶこととする）であり、その経験・知見を活用するための制度が必要である。これら「経験有識者」を活用する場合、「秘」に該当する内容も含めることを想定し、現役時代にSCを保有していた人の活用が可能となるようなSCの管理機関と制度を整備すべきである（ここでいう「秘」は政府が指定する「秘密情報」である）。

8. 「安全保障関連技術推進基本法」の制定

本提言は、このような問題意識を踏まえて、Kプログラム及び防衛省の安全保障技術研究推進制度の強化も視野に入れつつ、さらに、もう一步を踏み出して、日本の民間企業、特にスタートアップ企業のデュアルユース技術を国家安全保障に取り込み活用するために、安全保障関連技術とデュアルユース技術の間の垣根を取り払い、日本全体として官産学自の協力を実現する方策を検討し、具体的提言を行うものである。そのために「安全保障関連技術推進基本法」を制定し、同法下での新しい諸制度導入を提言するものである。

**「安全保障関連技術推進基本法の制定」及び
「安全保障関連デュアルユース技術推進基金」の
設置**

米国、中国が鎬を削る安全保障関連の最先端技術は、宇宙、サイバー、電磁波、AI、ドローンなど現代の戦場を大きく変化させている。戦後、安全保障と科学技術の遮断という特殊な国内事情に苦しんできた日本が、安全保障関連技術開発において先頭を走る米国や中国等と伍していくためには、政府全体として官民の協力を推進することが不可欠である（本稿コラム参照）。

そのためには、安全保障関連技術開発・実用化を推進するための基本法を制定し、総理直轄の安全保障関連技術推進本部を立ち上げ、総理が諮問する安全保障関連技術有識者による会議（ディフェンス・ボード）の設置と基本戦略の策定、諸外国における最先端技術を目利きする調査部の設置、資金の提供、「死の谷」克服のための具体的支援、その関連事務を総括する内閣府部局の創設等を一括して講ずる必要がある（資金提供に関する提言については提言2参照）。

具体的には、新法として「安全保障関連技術推進基本法」を策定し、下記のような制度を設ける。

- ① 総理主宰の「安全保障関連技術推進本部」（閣僚レベルの会議。総理、官房長官、防衛大臣、経済産業大臣、文部科学大臣、総務大臣、外務大臣、サイバー担当大臣、海洋担当大臣、宇宙担当大臣、その他、総理の指名する大臣をメンバーとする。）を設ける。同本部は、定例会を毎年12月に開催する。事務局として、国家安全保障局の管轄の下、内閣府に「安全保障関連技術推進事務局」を設ける。
- ② 安全保障関連技術推進本部は、5年に一度、「安全保障関連技術推進5か年計画（原案）」（公表）を策定する。また、毎年、その執行状況を確認するために「年次報告書（原案）」（公表）を採択する。上記5か年計画及び年次報告書は、安全保障関連技術推進事務局が、国家安全保障局の指導の下で関係省庁と協議の上作成し、本部決定の後、閣議決定する。上記5か年計画においては、Kプログラム、安全保障技術研究推進制度、防衛生産基盤強化法、経済安全保障推進法における施策に加え、ソフトウェア中心となる今後の防衛装備の調達の内訳の在り方の改変、有事における防衛省の継戦能力の確保、資材の優先利用、工廠の設立やGOCO（Government Owned and Contractor Operated）制度の活用等の必要性等、本提言書で提案されている様々な新制度の運営の基本方針を提示する。

- ③ 安全保障関連技術推進5か年計画の策定に当たっては、政府として注力すべき技術分野を明示する。政府が既に指定している「危機管理投資」及び「成長投資」の「戦略17分野」(AI・半導体、造船、量子、合成生物学・バイオ、航空・宇宙、デジタル・サイバーセキュリティ、コンテンツ、フードテック、資源・エネルギー安全保障・GX(グリーントランスフォーメーション)、防災・国土強靱化、創薬・先端医療、フュージョンエネルギー(核融合エネルギー)、マテリアル(重要鉱物・部素材)、港湾ロジスティクス、防衛産業、情報通信、海洋)等を参照し、国家安全保障の観点から、向こう5年間、特に留意すべき「国家安全保障関連特定技術分野」を指定する。
- ④ 上記の指定に当たって、急速に変化する現代軍事技術に対応するために、内閣官房に官民の一流の研究者及び技術者、有識者、元官僚、元自衛官、情報機関関係者、防衛産業関係者からなる「安全保障関連技術推進参与会議」(ディフェンス・ボード)を設ける。同参与会議は、上記5か年計画策定に際し、「国家安全保障関連特定技術分野リスト(案)」及び「安全保障関連技術推進5か年計画(案)」を総理に答申する。また、毎年の「年次報告書(案)」を閣議決定前に了承する。その他、同参与会議は随時会合を持つことができることとする。参与は総理大臣任命とする。
- ⑤ 安全保障関連技術推進事務局に、「安全保障関連技術調査部」を設け、内外の軍事技術及びデュアルユース技術の進展状況を把握し、同時に、国内外のどのような企業や研究所が国家安全保障上、どのような有益な技術を持っているかを調査し、マッピングする(テクノ・インテリジェンスの収集)。このようなインテリジェンスの収集は、民間企業が有する技術シーズと防衛省・自衛隊の防衛ニーズのマッチングを促進する上で必要不可欠である。同調査部には、官民共同でシーズとニーズのデータベースを構築・運営させる。
- このようなテクノ・インテリジェンスに関する部局は、これまで政府部内に存在しない。諸外国では、このような部局は情報部門と絡んだ重要部局として存在する。既存のシンクタンクは、縦割り行政の影響を受けており、①大学の研究者の範囲内にとどまっている、あるいは、②軍事技術に特化しており、民間の幅広いデュアルユース技術に関する世界の最先端動向を追い切れていない等の制約がある。国家安全保障に関する技術情報は、場合によっては、最高度の秘密指定を付与することが必要な場合もある。このようなことから、秘密保全のしっかりとした「安全保障関連技術調査部」(テクノ・インテリジェンス調査部)を設置する必要がある。
- ⑥ 同調査部の調査員としては、米ランド研究所など諸外国の研究所等を参照しつつ、防衛省、防衛装備庁、文部科学省、総務省その他の省庁及び傘下の研究所の研究者、技官、自衛隊関係者(元自衛官を含む)、防衛産業及びデュアルユース技術を有する企業関係者並びに外国諜報員が狙っている日本の技術を追っている外事警察関係者を選抜して充てることとする。調査員には政府の機微情報にアクセスするセキュリティ・クリアラ

ンスを付与する。政府が支援することとなる民間技術が機微なものとなる場合には、民間の研究者などに対して資金提供等の条件として秘密技術扱いとする。

- ⑦ 安保関連特定技術分野が定まれば、それに該当する技術開発を行う者及び当該技術を実装する者に対して資金的支援を行う。そのために10兆円規模（運用型なら30兆円規模）の「安全保障関連デュアルユース技術推進基金（仮称）」を立ち上げ、毎年、その元本と利回りを無償・有償（資本投入、貸し付け、債務保証等）の支援に充てるとともに、これまでの枠組みにとらわれない柔軟で迅速な資金配分・支援を行う新機構を立ち上げる（提言2参照）。
- ⑧ なお、防衛省が専管する防衛装備品の研究開発は、防衛省が主体であり、企業は所要の試作を請け負う形でそれを支援するのが建前であるが、上記基金による研究開発委託では、企業に研究開発そのものを委託し、防衛省をはじめとする関係省庁はそのプログラム・マネージャーに徹するのが適切である。また、委託先を複数化できるようにすれば、受託企業間で競争原理が働き、より優れた技術開発が期待できる。

コラム

「最先端技術（CET）」だけでなく「基盤技術（FT）」も
—基盤的デュアルユース技術の空洞化という論点—

本稿③で提言した「国家安全保障関連特定技術分野」の指定に当たっては、AI・半導体・量子といった「最先端技術（CET：Critical Emerging Technology）」だけでなく、既に量産段階にある「基盤技術（FT：Foundational Technology）」についても、諦めるべきではない。米国が第一次トランプ政権以来、2018年輸出管理改革法（ECRA）において「最先端技術（CET）」と「基盤技術（FT）」双方を特定・規制対象と位置付けてきたのはこのためである。

中国は中国工業情報化部（MIIT）を中心に、政府系ファンドによる資本注入・低利融資といった国家主導の誘導と、民間企業同士の過当競争（「内巻」）による市場原理主導の価格破壊とを組み合わせ、「大量生産 → 価格破壊 → 中位市場支配 → 高性能領域進出」という「二段階侵食」を高速かつ大規模に回している。第一段階は大量生産・低価格による各国中位市場の空洞化、第二段階は依存関係を利用した輸出規制・供給停止による圧力行使であり、「依存」を戦略的武器として利用する構造である。ここでいう中位市場とは、最先端品ではないが産業の裾野を形成する大量使用品群であり、これを失えば最終的に高性能領域も支えきれなくなる。

日本の状況は深刻である。国内SiC（炭化ケイ素）パワー半導体大手は今期（2026年3月期）1,500億円超の最終赤字を計上し、国内大手3社による事業統合協議後でも、合算した世界シェアは1割程度にとどまる見通しである。GaN基板、耐電食・高速・長寿命ベアリング、カーボン開繊薄層複合材、省電力AIサーバー基盤、基幹化学品・先端金属などの分野でも、日本の基礎技術は劣らないにもかかわらず、量産・自動化・国際市場展開の段階で頓挫し、中国側の量産能力が急速に追い上げている。この分野で必要なのは新規の研究開発ではなく、政府調達・既存認証・同志国相互承認を組み合わせ、これら出口段階を制度として保証する「国内アンカーテナンシー → 輸出 → 同志国供給網」という三段階の出口戦略である。

技術で先行しても量産競争で敗れば、市場も供給網も失う。これは個別企業の経営問題ではなく、国家としての技術基盤喪失の問題である。「国家安全保障関連特定技術分野」の指定においては、最先端領域の指定と並行して、こうした基盤技術の量産基盤維持についても対象範囲に含めることを検討すべきである。

政府は国家戦略として「戦略17分野」（防衛産業、造船、フュージョンエネルギー、航空・宇宙、AI・半導体等）を策定した。「先端デュアルユース技術基盤」の中核をなす重要分野である。

これらの分野で我が国の安全保障にも資するデュアルユース技術が育つためには、

- 1) 明確な課題設定
- 2) 当該課題を踏まえた迅速柔軟な技術・製品開発
- 3) 当該技術を社会実装するためのスタートアップや新産業支援（安全保障上の懸念のある投資の阻止を含む）
- 4) 立ち上がった産業をスケールするための大規模な資金供給枠組み
- 5) 政府調達も含めた関連市場の創設
- 6) さらにグローバルな市場獲得

に至るまで「包括的な先端デュアルユース技術開発実装エコシステム」を育む必要がある。

本分野で圧倒的に進んでいる米国の安全保障関連技術エコシステムを例に取ってみると、

- ① 汎用的な技術開発（米国防高等研究計画局（DARPA）等。基礎／一般技術）
- ② 個別具体的な技術開発（米国防総省（DoD）の防衛イノベーションユニット（DIU）¹等）
- ③ 新産業への投資枠組み（CIA傘下のIn-Q-Tel²など）
- ④ 産業スケールアップのための民間資金のレバレッジ（OSC（Office of Strategic Capital、戦略資本局）およびSBICCT（Small Business Investment Company Critical Technologies Initiative））³
- ⑤ 新技術調達枠組み（OTAs）⁴
- ⑥ 海外展開支援（国を挙げて安全保障関連技術・製品・ビジネスを海外展開）

という包括的枠組みが揃っており、そういった枠組みの中で現代の安全保障を担う技術開発が行われ、Palantir Technologies⁵やAnduril Industries⁶などの新たな防衛関連企業（Neo Primes⁷）やSpaceX等が育ってきている。

我が国においても研究・技術開発については、内閣府の経済安全保障重要技術育成プログラム（Kプログラム）や防衛装備庁の安全保障技術研究推進制度などが存在しているものの、米国との比較において課題設定が不明確であるほか、一般的な公会計制度に縛られていることもあり、目的達成型の柔軟迅速な研究開発を行うことが困難である。

また、新産業創出については、「スタートアップ育成5か年計画」⁸など新産業育成に向けた投資を一般的に支援する仕組みはあるものの、安全保障の観点から柔軟、迅速かつ大胆に投資を行う仕組み等は存在していない。なお、安全保障に関する投資の仕組みは、関連するスタートアップ育成に寄与するだけでなく、重要なデュアルユース技術を保有する既存の企業に対する敵対的買収を阻止する意味でも重要である点に留意する必要がある。

さらに、「戦略17分野」で想定される先端デュアルユース技術の多くは、巨額の設備投資と長い回収期間を要する「ハードウェア（ディープテック）」と密接不可分である。

そのため、ソフトウェア産業と比較してリスクが高く、金融機関や民間投資家（ベンチャーキャピタル、以下VC）からの資金供給が慎重になりがちであり、その結果、資金不足により試作から量産化への移行段階で事業化が停滞してしまういわゆる「死の谷（Valley of Death）」に直面するケースが日本には多く散見される。この課題に対処しなければ、技術基盤そのものが空洞化し、将来的に防衛省の研究開発能力や民間の産業競争力に影響が及ぶ懸念があると言わざるを得ない。

そして何とんでも先端デュアルユース技術を活用した製品やサービスの「市場」が我が国にはほとんど顕在化しておらず、それが本分野への新規プロジェクト、新規参入、資金投入、新技術開発の最大の課題となっている。海外には巨大な市場が存在し、飛躍的に拡大しつつあるものの、我が国においては武器輸出に係るこれまでの制度的制約・心理的制約・政策的制約が根強く残っており、海外市場の開拓もこれからという段階である。

我が国がそういった過去の遅れを取戻し、一足飛びにデュアルユース技術の開発／実装を促すエコシステムを構築するために、以下の提言を行う。

1. 安全保障関連技術開発実装エコシステム創設戦略の策定

提言1にある「安全保障関連技術推進5か年計画」において、個別分野の技術開発やアドホックな制度創設だけでなく、新たな技術開発枠組みからスタートアップ創設、スケールアップ、内外市場獲得を一貫して支援する枠組み、すなわち上記のエコシステム創設に向けた包括的な戦略を構築する。

2. 日本版DARPAの設立（安全保障ニーズと我が国の優れた研究・技術のマッチング機能を有するもの）

DARPA型の研究開発枠組み創設については、我が国でも長い間議論されてきており、内閣府の戦略的イノベーション創造プログラム（SIP）やKプログラムなどDARPAを手本に様々な研究枠組みは作られてきたものの、安全保障担当部局（米国防総省）の直下／明確な問題意識／客観的な採択基準／実装を念頭においた評価／関連する研究開発に関する強力な権限／年間約50～60億ドルの予算／高リスク研究を許容／プロジェクトマネージャーに強い裁量／軍事技術と民生技術を一体で推進、といったDARPAの本質的特徴はほとんど取り入れられていない。

日本でDARPA型組織ができない背景として、省庁縦割り構造、高リスク研究への文化的抵抗、防衛研究への社会的反発、予算規模の不足、司令塔機能の弱さなど指摘されるが、提言1に記載した安全保障関連技術推進事務局の下に安全保障部局としてのDARPA型研究推進部局を創設し、同じく提言1に記載した「安全保障関連デュアルユース技術推進基金（仮称）」による安定的なファンディングで活動を支えるべきである。要すれば既存のKプログラムなどを換骨奪胎し、ここに統合することも考えられる。

3. 日本版DIU = DISTIの抜本的強化

我が国においても、米国の防衛イノベーションユニット（DIU : Defense Innovation Unit）に倣って防衛イノベーション科学技術研究所（DISTI : Defense Innovation Science & Technology Institute）が設立された。

これは防衛装備庁の研究開発を補完するため、ブレークスルー技術の創出（量子、AI、無人機など）、外部プログラムマネージャ（PM）を活用した挑戦的研究の推進などを行う組織とされている。米DIUを参考に設計されたといわれるが、米国のDIUはスタートアップ等の有する「民間技術を安全保障分野に転用」することを明確に目標として掲げ、商用技術（AI、宇宙、無人機など）を軍に高速導入するために、スタートアップとの契約を数ヶ月で実現、プロジェクト内容においても商用技術の転用を重視、調達改革（OTAs）を使い迅速にプロトタイプを採用するなど、「技術を実践的に活用する」という点が際立っている。実際の運用でも、米国ではスタートアップなどの民間企業が技術開発・移転の中核にいるのに対して、我が国のDISTIの受託者は、全体としては大学や研究機関が委託対象の多くを占めている（科学者主体）。民間企業の参画も増加傾向にあるものの、大企業が中心であり、スタートアップの参画比率は依然として低い。

DISTIの試みは野心的なものであるが、手本とした米国のDIUの本質を踏まえ、制度設計を商用民間技術（デュアルユーステック）の活用にも軸足を移し、予算規模を拡大するだけでなく、調達の仕組みも根本的に見直すべきである（本稿「6. 日本版「新技術調達枠組み」の構築」参照）。

4. 安全保障関連資本投入枠組みの構築

技術開発だけではスタートアップは育たない。そこに資本が投入されて初めて社会実装の種がまかれる。我が国でも徐々にVCなどが育ってきているが、デュアルユース技術関連企業（特にスタートアップ）を成長させるためには、一般的なVCでは時間的・資金的・能力的な限界がある。そもそも一般のVCは投入資金回収が大前提であるため、安全保障上いかに重要な技術を有するスタートアップや企業であっても、投入資金回収の見込みが立たなければ、VCもその他の金融機関も資金投入はできない。

膨大なVCを擁する米国においてさえ、CIAが敢えてIn-Q-Telを創設した理由も同様である。民間VCは国家安全保障に必要な企業・技術であっても、収益性が低いもの、投資回収まで長い時間がかかるもの、市場が想定できないもの、には原則投資をしない。CIA傘下のVCであれば、CIAのニーズを理解し技術を選別／スタートアップに長期資金を提供し政府向け技術を育成／CIAと企業の橋渡し（契約・技術移転）／機密性の高い技術を安全に取り扱う／国家安全保障に必要な技術を最速で確保などが可能となる。

In-Q-Telの場合、きちんとした潜在的ニーズも踏まえて投資を行っていることから、Palantir TechnologiesやKeyhole（Google Earthの基盤となった企業）など大成功を収めた投資もあり、結果的に財政的にも安定しているといわれる。我が国においても適切な技術を見極めて迅速柔軟に安全保障の観点から「資本注入／投資を行う組織」を安全保障関連技術推進事務局のもとに構築すべきである。

5. 「死の谷」を乗り越えスケールするための金融的支援（日本版OSCの創設）

上記枠組みを活用し、技術開発から企業体の創設までこぎ着けても、次の厳しい試練がある。

冒頭に指摘したいいわゆる「死の谷（Valley of Death）」を克服し、強靱な技術基盤を構築する上で、有力な参考モデルとなるのが米国防総省の戦略資本局（OSC：Office of Strategic Capital）の取り組みである。従来の政府支援は「補助金の給付（Spending）」が中心であったが、巨額の資金を要するハードウェア産業をそれのみで支えることには限界がある。そこでOSCでは、より効果的な以下の手法を採用しているとされる。

① 手法の転換（支出から融資／出資へ）

直接的な支出だけでなく、政府が「融資」や「債務保証」を行うことでリスクを分担し、民間銀行や投資家の資金を呼び込む（呼び水効果）手法である。具体的にはSBA（中小企業庁）と共同でSBICCT（Small Business Investment Company Critical Technologies Initiative）を設計、防衛・重要技術に投資するVC／PEファンドに最大1.75億ドルのレバレッジ（借入枠）を提供しており、既に複数のファンドがSBICCTとして認定、活動を行っている。これにより民間ファンドの投資余力が数倍に増幅されているといわれている。

さらに2025年7月に成立したいいわゆる「OBBBA（One Big Beautiful Bill Act）法」に基づき、OSCは15億ドル（約2,200億円）程度の予算計上で、その政府信用力を背景に、最大2,000億ドル（約30兆円）規模の融資枠を保証する権限を有している。少ない元手（真水）で大きな資金を動かすレバレッジ効果が期待できるのである。

② ハードウェアへの重点化

この資金枠は、ソフトウェア分野よりも、半導体、先端素材、バッテリー、重要鉱物といった「国の存立に関わるが、民間だけでは投資判断が難しいハードウェア・サプライチェーン」に重点的に向けられている。

このように、公的資金を呼び水として、その数倍から数十倍の民間資金を動かす仕組みは、製造業基盤の再構築に向けた有効なアプローチの一つとして機能しているようである。

日本が掲げる「戦略17分野」の実現、そして防衛省の研究開発と民生産業の双方を支える「先端デュアルユース技術基盤」の確立には、こうしたOSC型の資金供給メカニズムの導入が有効な選択肢となり得る。

上記のようなメカニズムを実現するためには、提言1に掲げた「安全保障関連デュアルユース技術推進基金（仮称）」は無償の資金提供のみならず、政府からの有償資金を民間融資と組み合わせて、相応の融資を実現する制度を内包すべきである。具体的には下記のとおり。

- ① 日本版レバレッジの活用：米国の事例を参考に、日本においても1,000億円程度の国費（真水）を充てることで、1兆円以上の規模のリスクマネー（融資・保証枠）を創出することを目指す。
- ② 投資対象の明確化：この資金を低利の有償資金として、「戦略17分野」の中でも特に「死の谷」が深いとされる「量産化段階のハードウェア（造船、AIインフラ、宇宙、ドローン等）」へ重点的に配分することが効果的であると考えられる。
- ③ 民間資金の呼び水（Patient Capital）：政府が長期的な視点でリスクを取る姿勢（Patient Capital：忍耐強い資本）を示すことで、民間金融機関の予見可能性を高め、防衛・経済安全保障分野への投資を促進することが期待される。

OSCモデルを参考とした「量産化・産業化支援」の仕組みを整えることは、日本の「先端デュアルユース技術基盤」を盤石なものとし、将来にわたる防衛力と産業競争力の維持・強化に資する有力な方策となると考えられる。

6. 日本版「新技術調達枠組み」の構築

安全保障に関連する研究開発やスタートアップ支援の最大の障害が、政府の予算会計制度である。

米国の通常の政府調達も、連邦調達規則（FAR : Federal Acquisition Regulation）という巨大な規則に縛られている。その基本的考え方は政府予算の透明性・公平性を確保するものであるが、機械的に厳格に適用された場合には、イノベーション推進には決定的な障害となり得る。特に安全保障の観点からは致命的になりかねない。具体的には、契約までに時間がかかりすぎる（公募 → 入札 → 審査 → 抗議対応 → 契約まで 1 ～ 3 年といった長いプロセス前提）、膨大な書類作成（数百ページに及ぶこともある）、政府調達仕様・規格に合わせる必要（商用技術が使えない）、価格競争が中心で、イノベーションが評価されない、知的財産権（IP）の扱いが厳しすぎる、などの多くの問題が幅広く指摘されている（知財の扱いについては提言 3 参照）。

この問題は我が国でもほぼ同様であり、JST（国立研究開発法人科学技術振興機構）や NEDO（国立研究開発法人新エネルギー・産業技術総合開発機構）等の行う研究開発がなかなか実装に結びつかなかったり、政府の関与する技術開発にスタートアップ（先端技術を有する海外企業を含む）の参画や国際共同研究が困難であったりする要因の多くは、予算会計制度（会計法／予算令／会計検査院制度等）に起因する。政府予算の透明性公平性客観性確保と、迅速柔軟な予算執行のバランスは重要であり、みだりに予算会計制度を逸脱することは適切ではない。しかしながら、制度的制約があるがゆえに、研究開発の成果が出ない、イノベーションが起きないというのであれば、それは本末転倒である。

いわんや、国家安全保障に関わる部分において、予算会計制度を厳格に遵守するがために産業や国家が危機に陥るようなことはあってはならない。

米国防総省はこうした問題意識に基づき、OTAs（Other Transaction Authority/Other Transaction Agreement）と呼ばれる、通常の政府調達枠組みとは異なる柔軟な調達手法を採用している。

FAR（連邦調達規則）に縛られない特別な契約権限であり、研究開発・試作・新技術の迅速導入を目的として使われる。従来の契約よりもスピードが速く、要件が少なく、スタートアップや非伝統的防衛企業を取り込むために広く活用されている。FAR 契約は仕様策定・入札・審査が重く、数年かかることもあるが、OTAs はこれを大幅に短縮できる。調達金額に特段の上限は設定されておらず、米国防総省の OTAs 義務付け額は近年急増、2024 年度には 180 億ドルを超えている（2016 年度は 18 億ドル）。なお、米会計検査院（GAO）は、試作段階 OTAs の成果がどれだけ量産・実戦配備に結びついたか、米国防総省自身が体系的に追跡できていないと指摘しており、日本が同種の枠組みを導入する際は、当初から効果検証の仕組みを組み込む必要がある。

また、技術仕様の厳格な遵守が不要であり、成果の範囲を広く設定することが可能であ

る。そのため、非伝統的企業（スタートアップ等）の参入促進を図り、AI・量子・自律システムなどの民間先端技術を迅速に軍事利用するために活用可能であることから、新技術の試作・実証に適しており、完成品調達よりも研究開発・試作段階で多用され、米国防衛産業の新たなプライムといわれるPalantir Technologies、Anduril Industries、あるいはSpaceXなども活用しているといわれている。

本来、我が国においてもOTAsのような制度を幅広く研究開発やイノベーション分野に入れていくべきであるが、まずは安全保障分野、なかんずく提言1に基づく「安全保障関連デュアルユース技術推進基金（仮称）」の執行にあたっては、既存の予算会計制度とは異なる枠組みを導入していくべきである（本稿「8.「安全保障関連デュアルユース技術推進基金」の設立」参照）。

7. 海外市場の開拓／最先端動向の把握

デュアルユース技術が育つためには、国内市場にとどまっていたには限界がある。海外の巨大な市場を視野に入れる必要があるが、ロシアのウクライナ侵攻により、海外、特に欧州での安全保障関係調達の様相は大転換しつつある。

具体的には、ウクライナの戦場での技術の進展があまりにも早く、これまで有用とされていた技術が現場で役に立たなかったり、これまでは全く考えられなかった技術が活用されたりするため、現場で実際に役立つかどうか、役立ったかどうか、が安全保障関連装備調達の大前提となりつつある。そのため、ウクライナはBrave1⁹と称する防衛テックの国家イノベーション拠点を設立し、ドローン・ロボティクス・電子戦・AIなどの新技術を実戦投入するための仕組みとして機能するほか、スタートアップ支援、試験・認証、資金供給を一体化することで、数週間で戦場投入まで持っていく加速器としての役割を果たしている。EUと欧州防衛庁（EDA）は2026年4月、BraveTech EU（ウクライナの防衛テック拠点であるBrave1と連携する技術開発支援策）Phase 2 協定に署名し、EDAは選抜された技術をウクライナ戦争の運用シナリオに基づき試験・評価することとなった。

特に重要なのは、Brave1が持っている、ウクライナで実際の戦場から出てきた実戦上のニーズ（ウクライナ軍のユーザー、スタートアップ、試験環境、実戦データ・フィードバック）を、EU側の企業・スタートアップ、研究機関・防衛産業に直接つなぎ、EUにおいてもこれまでにない速度で有用な技術開発を行うエコシステムを構築していることである。対象はウクライナの軍事活動の大半をカバーしており、ドローン、自律型UAV（Unmanned Aerial Vehicle、無人航空機）／UGV（Unmanned Ground Vehicle、無人車両）／USV（Unmanned Surface Vehicle、無人水上機）、AI・機械学習、電子戦（EW：Electronic Warfare）、SIGINT（Signal Intelligence、通信情報を用いた諜報活動、「シギント」）、防空、レーダー、GPS妨害環境での航法、通信、ミサイル、センサー、ロボットなど広範に及ぶ。

ロシアと対峙する欧州がUkraine Battle Testedを重視するのは当然であるが、安全保障関連技術はロシア側からも連携国に急速に展開され、米国にとっても死活的に重要であることから、米国の関連企業が多く関与しているといわれている。我が国がデュアルユース技術開発に実質的に取り組むのであれば、こうした世界最先端の技術導入・活用・開発状況を十分に理解しておく必要があり、Brave1のような枠組みとの関わりの在り方を真剣に検討すべきである。

具体的には、「Brave Tech Japan（仮称）」を日・ウクライナ技術開発のプラットフォームとして早急に設立し、我が国の安全保障関連技術・装備の幅広い海外展開に結び付けていくべきである。我が国の装備品移転には未だ様々な制約があるが、それでも日本政府は今年、「同盟国・同志国の抑止力・対処力を強化するため、防衛装備移転を更に推進する」という方向を明確にしている。世界最先端の実戦状況を理解せずして、我が国に必要な安全保障能力

を定義し、技術・装備を開発することはできない。その経験を我が国自身の能力形成と安全保障関連技術・装備の海外展開の双方につなげていくことを議論の出発点とすべきである。

8. 「安全保障関連デュアルユース技術推進基金」の設立

上記の安全保障関連技術開発実装に関する包括的エコシステムを構築するため、技術開発から実装に至るまで一貫して支援を行う「安全保障関連デュアルユース技術推進基金（仮称）」を安全保障関連技術推進事務局（提言1参照）のもとに創設する。

（ニーズの把握）

当該基金は、実質的・具体的な安全保障上のニーズに基づき、実際に現場で役に立つ技術開発～実装、を支援する必要がある、そのためにニーズを擁する政府の安全保障関連部局と密接な連携を確保することとする。

（基金規模）

当該基金の規模については、米国の防衛関連技術開発経費は米国防総省だけで10兆円強、中国も数兆円規模の支出をしていることを踏まえると、我が国においても最低限年間1兆円程度を安定的に支出ができる体制が必要と想定される。そのため、取崩し方式であれば10兆円（10年間）程度、運用方式であれば30兆円程度（年間3%強の利回りを想定）の基金規模を確保することとする。なお、既存のKプログラムなどの基金は目的、枠組み等が本質的に異なるため、そのまま一体化することは不可能であるが、既存の基金を換骨奪胎し、当該基金に統合することは考えられる。

（機能）

国家安全保障デュアルユース技術開発実装に係るエコシステム構築の趣旨に基づき、研究委託から補助金による支援、民間企業に対する出資や融資、債務保証、関連VCへの資本投入、試作品調達、市場獲得支援など、幅広い多様な機能を有するものとする。

（予算執行の在り方）

当該基金の支出にあたっては、米国OTAsなどに倣い、既存の会計規則とは異なる柔軟でリスク耐性のある迅速・アジャイルな支出を可能とする。

（プロジェクトの評価）

米国のDARPAが日本のプロジェクト評価と決定的に異なる点は、明確な目的、独創性、実現可能性、インパクトなどを評価する「Heilmeier Criteria¹⁰」を用いている点にある。一般的な研究開発や科研費などとは異なり、本基金の執行にあたってはプロジェクト採択の段階から安全保障上の明確な目標設定を行うこととし、その評価も実際に社会実装ができたか、それに貢献したか、など、具体的でクリアなベンチマークによって行うこととする。

9. デュアルユース技術開発促進支援法人の設立

上記基金を執行し、縦割りを打破して、明確な目標の下、基礎研究からグローバル市場獲得に至るまで安全保障関連技術の開発と実装を支援するため、内閣府に設置する安全保障関連技術推進事務局（提言 1 参照）の下に「包括的安全保障関連技術育成実装機構（仮称）」（以下「新機構」）を創設する¹¹。

現代・将来の安全保障ニーズを踏まえると、新機構の機能は技術開発支援にとどまらず、それを社会実装するために、どれだけスタートアップ企業・スタートアップビジネス育成を行うことができるかが鍵となる。

そのため、テーマ選定、プロジェクト構築段階から実装を明確に視野に入れたプロジェクトを扱うこととし、グローバルマーケット獲得を視野に入れた徹底した伴走型支援ができる体制を整える。また、企業が知財・技術資産の管理や契約条件によって技術の価値を回収し、政府も運用・改良に必要な権利を確保できるよう、知財・技術資産戦略の実行機能を新機構が担う（詳細は提言 3 参照）。加えて、安全保障関連プロジェクトを扱うことから、秘密事項の取扱い、セキュリティ・クリアランスなどもそれに見合った枠組みを構築する。

-
- 1 米国防総省（DoD）が民間の先端技術を迅速に軍事利用へ取り込むために設置した組織で、スタートアップや民間企業とDoDをつなぐ技術導入のフロントドアとして機能。2015年にDIUxとして設立され、2018年にDIU（防衛イノベーションユニット）として常設化。米国防総省全体のアジェンダを明確に把握しその全体課題を扱うこと、米国防総省の長官直轄であること、OTAs（本稿「6. 日本版「新技術調達枠組み」の構築」参照）活用で高速調達が可能であること、In-Q-Tel（脚注 2 参照）から防衛調達まで次のフェーズに橋渡しができること、において、日本の類似する機関とは異なる。
 - 2 CIA（米中央情報局）が支援する非営利の戦略的ベンチャーキャピタル（以下VC）で、民間の先端技術を米国の諜報機関が迅速に取り込むために1999年に設立された組織。
情報分析、AI、サイバーセキュリティ、バイオテック、電子工学など幅広い分野のスタートアップに投資。投資件数は累計数百件規模と推計される。米国の防衛産業関連スタートアップであるAnduril Industries、Palantirはいずれも支援対象。
 - 3 OSC（Office of Strategic Capital、戦略資本金局）及びSBICCT（Small Business Investment Company Critical Technologies Initiative）は、米国で防衛関連技術をスケールアップ（量産・商用化・産業基盤の拡大）するための制度。両者は「民間資本を国家安全保障に動員するための新しい金融インフラ」として2022～2024年に整備。前者は主に戦略を構築するとともに、実際に、長期融資（最大1億ドル超）で製造設備などを支援。後者は重要技術特化型ファンドの育成、政府保障付きの低コスト資金のファンドへの共有などを行う。
 - 4 OTAsは「Other Transaction Authority/Other Transaction Agreement」の略称であり、柔軟な新技術調達の枠組み。詳細は本稿「6. 日本版「新技術調達枠組み」の構築」参照。
 - 5 CIA系VC（In-Q-Tel）の支援で誕生したデータ解析企業。テロ対策・軍事作戦・諜報活動・サイバー防衛などで利用。代表製品はGotham（政府向け）とFoundry（企業向け）。米軍・政府機関のデータ統合・AI分析の中核的役割を担う。
 - 6 Oculus創業者パルマー・ラッキーが設立した防衛スタートアップ。AI+自律ドローン+センサー+指揮統制を統合した防衛システムを開発。代表製品はLattice（AI指揮統制）とGhost、Anvil（自律ドローン）。DIUや米軍とのOTAs契約で急成長中。
 - 7 米国防衛産業で台頭している“新世代の防衛大企業候補”のこと。従来のロッキードやレイセオンのように

な巨大防衛企業に対し、ソフトウェア・AI・自律システムを武器に急成長しているPalantir Technologiesなどの新勢力が含まれる。

- 8 2027年度までにスタートアップ投資額を現在の約8,000億円から10兆円規模へ10倍以上に拡大することを国家目標とし、人材育成・資金供給・オープンイノベーションの3本柱で、起業家教育、海外派遣、VC育成、公共調達拡大、M&A促進などを総合的に推進する。ユニコーン100社・スタートアップ10万社の創出により、日本をアジア最大のスタートアップハブにすることを長期目標とする。
- 9 Brave1はウクライナ政府が設立した防衛技術イノベーション・プラットフォーム。スタートアップや研究機関を支援し、ドローン、AI、電子戦、ロボットなどの軍事技術を開発・実用化。戦場のニーズを迅速に技術開発へつなげるDefenseTechエコシステム。現在、約2,500社、5,000以上の製品が参加、UAV、UGV、電子戦、SIGINT、ミサイル、AIなど非常に広い分野を扱っているといわれている。海外との関係では、欧州とはBraveTechEUを通じて防衛技術の共同開発・実証を推進、米国やイスラエルとも、防衛技術やイノベーション分野での協力・交流を進めている。
- 10 米DARPAが研究プロジェクトを評価するための以下の8つの基本質問のことをいう。「その研究は本当に価値があり実現可能でインパクトがあるのか」を見極めるためのチェックリストとして機能している。
 - ① 何をしようとしているのか？（専門用語なしで説明できるか）
 - ② なぜそれが重要なのか？（誰のどんな問題を解決するのか）
 - ③ これまでの方法では何が問題なのか？
 - ④ あなたのアプローチは何が新しいのか？
 - ⑤ 成功したら何ができるようになるのか？
 - ⑥ 成功をどう測るのか？（評価指標）
 - ⑦ どんなリスクがあり、どう対処するのか？
 - ⑧ どれくらいの費用と期間が必要か？
- 11 これまでの政府の研究開発関連法人は、一般の技術開発を行う観点からは機能してきたと考えられるものの、法的・予算的・体制的・歴史的制約などから、安全保障上の課題に関する明確なニーズを踏まえ、迅速・効果的・効率的に技術開発を行うには必ずしも適していない。

安全保障上重要なデュアルユース技術を実装・事業化につなぐ知財・技術資産戦略—技術を持続的な能力に結実させる支援制度への転換—

1. 問題の所在

(1) ミッションを実装可能な知財・技術資産戦略に結実させる機能が欠けていた

冒頭で述べられているとおり、日本には安全保障と科学技術・産業技術の断絶という特殊な事情があり、ミッションを起点に技術・制度を逆算して設計する発想が定着してこなかった（「本提言の問題意識と提言の概要」4参照）。また、研究開発支援に加えて技術供給主体の競争力及び事業継続能力を補強する包括的な制度的対応が不可欠であることも、既に示されている（「本提言の問題意識と提言の概要」5参照）。提言1の「安全保障関連技術推進本部」及び「安全保障関連技術推進参与会議」（以下、ディフェンス・ボード）は前者に対応するものであり、本提言は後者のうち、知財・技術資産戦略の在り方に関わる。

「死の谷」は、資金供給の強化だけでは越えられない。ミッションが定まり資金が投じられても、技術がどの用途に接続されどのような知財・契約条件を必要とするかを探索段階から見通す機能が伴わなければ、先端デュアルユース分野で「技術で勝って事業で負ける」失敗を繰り返すこととなる。中国が民生分野で築いた量産基盤で軍事用ドローン・ロボットを支えているように、デュアルユース品の基盤は民生分野における競争力にある。しかし、防衛専用品は技術情報を秘匿するのが通常であり、その発想のままでは民生市場で供給できない。民生市場で供給する場合、外形的な構成など秘匿できない部分は、公開前に特許化するほか、事後的に保護する手段がないためである。先端デュアルユース分野で「技術で勝って事業で負ける」失敗を繰り返さないためには、民生市場での競争力を左右する知財・技術資産戦略が不可欠である。

(2) システムを支配する企業が、技術の価値を取り込む

現代の競争では、個々の要素技術に加え、それらを組み合わせ、運用し、継続的に改良するシステム全体の能力が競争力を決める。複数のドローンを連携させる群制御システムに、日本企業が高性能なセンサーや画像処理ソフトウェアを提供したとする。製品の売上げは得られる。しかし、システム全体を統括する外国企業が、実際の運用データと利用者のニーズを集約し、システムの改良と市場展開を主導すれば、日本企業には次に何を改良すべきかという知見が十分に蓄積しない。これは外国企業との協業に限らず、国内の主契約者と供給企業の間でも生じる問題である。

部品・要素技術を供給する企業が取り得る対応は、システムの統括者へと立場を広げることだけではない。中国のヒト型ロボット政策では、減速機、モーター、軸受等を組み込んだ電動一体化関節について、感知、知能学習、柔軟制御、モード切替、振動抑制、遠隔診断・

遠隔更新、状態監視、自己診断等の「知能化要求」を定める標準化が進められている。米国でも、ロボットのマジュール化や部品間のインターフェース、相互運用性等の標準化が進められている。こうした動きはヒト型ロボットに限らず、ドローン等の自律システムにも広がる可能性がある。部品として供給する立場にあっても代替されにくい位置を確保するためには、こうした部品の知能化を先取りし、部品そのものに知財・データの価値を埋め込むとともに、インターフェースや標準の形成に早期から関与することが重要となる。知能化や標準化が進んだ後では、他者が形成した仕様や標準への適合を迫られ、競争上の主導権を確保することが難しくなり得る。

日本では、完成品メーカーとサプライヤーの長期取引を通じて投資を回収する仕組みが弱まる一方、知財・技術資産の価値を製品価格に包摂する慣行と、サプライヤーがその対価を独立して求めにくい取引関係が残っている。供給企業が技術の価値に見合う収益と成長機会を得られなければ、国内の技術、人材及び供給能力が失われる。防衛分野では、それが国の継戦能力と選択の自由の喪失に直結する。2026年6月に公正取引委員会、中小企業庁及び特許庁が公表した「知的財産権・ノウハウ・データの適切な取引のための優越的地位の濫用等に関する指針」は、こうした取引慣行を是正し、知財・ノウハウ・データの価値を取引価格に反映する方向を示しており、システムを統括する企業との関係においても、同じ発想が求められる。

(3) 調達側の交渉体制が伴わなければ、政府自身も必要な権利を確保できない

知財・技術資産戦略の必要性は、供給企業側だけの問題ではない。装備品のライフサイクルを通じた運用、維持整備、改良及び増産に必要な技術データ・利用権を確保できるかどうかは、調達時点における政府側の交渉体制に左右される。国内外いずれの企業から調達する場合であっても、政府が自ら調達を主導していれば当然に必要な権利を確保できるわけではなく、知財・技術データに関する専門的な交渉能力を欠けば、契約条件の設計が供給企業側の都合に委ねられ、後になって必要な権利を欠いていたことが判明する事態を招きかねない。他方で、政府が必要以上の権利を一方的に求めれば、供給企業の事業性を損ない、技術供給そのものが持続しなくなる。調達側には、自らに必要な利用権を確保しつつ、供給側の事業としての持続可能性にも目配りするという、双方のバランスを見極める交渉能力が求められる。

2. 各国の実例

優れた技術が生まれても、それだけで事業化や社会実装につながるわけではない。研究開発成果を実際に使われる製品・サービスへ育て、持続的な事業と産業基盤につなぐことは、日本だけでなく米国や欧州でも長年の政策課題となってきた。

(1) 米国 — ミッションから調達・事業化まで、段階に応じた専門機能

1957年のスプートニク・ショックを契機に設立されたARPA（現DARPA、米国防高等研究計画局）は、達成すべき国家的ミッションを明確にし、そこから逆算して必要な技術的課題を設定する。少数のプログラム・マネージャーに大きな裁量を与え、期間を区切って高リスク・高インパクトの研究開発を進める。

こうして生まれた技術的課題を民間技術に接続する経路は、技術の成熟度に応じて使い分けられている。SBIR（中小企業イノベーション研究制度）は、まだ実用段階に達していない中小企業の技術をPhase I（実現可能性検証）、Phase II（本格的な研究開発・試作）と段階的に育成し、開発・生成された技術データについて企業は原則20年間所有権を保持する。DIU（防衛イノベーションユニット）は、既に商用段階にある技術を、短期間の試作・実証を経て、部隊への導入や本格調達につなげる。In-Q-Tel（米国情報機関の戦略的投資機関、提言2脚注2参照）は、情報機関が必要とする新興商用技術を投資と技術開発契約を通じて政府利用につなげる。

DIUが主に用いる契約手段が、FAR（連邦調達規則）及びDFARS（国防総省連邦調達規則補足）の標準的な知財・データ権のルールから離れたOTAs（柔軟な新技術調達の枠組み）である。通常の契約では、技術データが政府資金・自己資金いずれで開発されたかに応じて政府が得る権利の範囲があらかじめ区分され、自己資金で開発した部分を守るには企業側の表示が必要とされる。継続的に更新されるAIモデルのようにこの区分が困難な技術を持つ企業、とりわけスタートアップには、この画一的な区分が参入障壁となる。OTAsはこの区分を離れ、商用知財と政府の利用権を案件ごとに個別交渉できるようにすることでこの障壁を取り除く（通常契約の中でも、同様の交渉を認める（specifically negotiated license rights）が別途ある）。

他方、政府が必要な権利を確保できなければ、後の維持整備、改良又は競争調達に支障が生じる。米会計検査院（GAO）は、F-35計画が長年知財戦略を欠いていたために特定企業への依存が固定化していたと指摘しており、同計画は2025年7月によりやく知財戦略を策定した。個別交渉の柔軟性を活かすには、企業の参入促進と政府の利用可能性の確保を両立させる高度な交渉スキルが求められる。

このスキルを支えるのが、知財を専門に扱う横断的な体制である。米国防総省が2025年5月に公表した「知的財産ガイドブック」は、知財戦略を契約交渉段階の事後処理事項では

なく、入札公告前のプログラム初期段階から検討し、調達ライフサイクル全体で継続的に管理すべき戦略要素と位置付ける。国防省の調達規則は、政府が任務遂行に必要な範囲の権利だけを取得し、納入させる技術データを個別項目として区分・価格付けすることを求めている。これを支えるIP Cadre（知的財産専門組織）は、法務・契約・技術・兵站・産業基盤政策に加え、コスト・価格分析及び知財の価値評価を含む専門人材で構成される。また、米国の政府契約制度では、専門家・コンサルタント費用、契約上必要な特許関連費用等を、合理性、契約との関連性等の要件の下で契約価格の形成に反映し得る仕組みがある。

研究開発を事業化・量産・市場拡大へ橋渡しする機能も、知財・技術資産戦略と一体で設計されている。DARPAのCSO（商業戦略室）は、研究チームに起業・事業化の経験を持つ人材を組み込む「事業化人材伴走支援イニシアティブ（EEI）」を展開する。応募段階で知財管理戦略の提示を求め、審査でも知的財産及び政府の使用権の扱いを評価要素とすることで、企業が商業的知財価値を保持しながら政府の使用権を確保する道筋を築く。ARPA-E（エネルギー高等研究計画局）のSCALEUP（有望エネルギー技術の商業化に向けた規模拡大支援）は、研究室規模からパイロット規模への移行、製造工程の確立、性能・コストの検証を支援する。NASA（米航空宇宙局）のCOTS（商業軌道輸送サービス）は、企業が開発・実証費の過半を負担する対価として、法律上可能な最大限の知財を企業側に残す契約設計とし、後続のCRS（商業補給サービス）契約による調達につなげた。

（2）EU — 成果活用・知財・標準化を研究開発の入口から設計

欧州は高い科学研究力を持つ一方、研究成果を新事業や急成長企業、産業競争力へ転換する力が相対的に弱いという「欧州のパラドックス」に長く直面してきた。2021年に開始されたHorizon Europe（ホライズン・ヨーロッパ、EU研究・イノベーション枠組み計画）は、科学的成果に加え経済・社会へのインパクトと成果活用を重視し、公募・契約の段階から、参加者が事前に保有する既存の知財・データと、プロジェクトで新たに生まれる成果を区別した上で、互いのアクセス条件を整理する。プロジェクトの実施に必要なアクセスは原則無償、成果の活用に必要なアクセスは公正かつ妥当な条件とされ、実施段階と活用段階とで切り分けている。標準化、規制対応、実証、市場導入も研究計画に組み込まれ、欧州イノベーション会議（European Innovation Council）を通じて企業の事業化と成長を支援している。

(3) 中国 — 産業・供給網の要所に技術資産を蓄積

中国では、製造業の規模が拡大する一方、中核部品、高度材料、製造装置、産業ソフトウェア等を海外に依存し、供給網の要所を自国企業が掌握していないことが課題となった。2018年以降の米中技術摩擦を契機に、2019年から国家レベルの専精特新（「専門化・精密化・特色化・革新能力」を備えた中小企業を育成する政策）「小巨人」企業の選定が本格化した。「小巨人」企業は、その中でも特定市場や産業チェーンの重要部分を担う企業として選定し、研究開発・技術成果の産業化、知的財産、財政・金融、市場開拓、政府調達上の優遇措置等を通じて育成する。産業・供給網上の弱点を特定し、その要所を担う企業に技術、知財、人材、設備、製造ノウハウ、顧客基盤を継続的に蓄積させる政策である。

専精特新の支援策に知的財産が当初から組み込まれているのは、産業振興と知財支援を一体で設計する制度基盤が、これに先立って既に築かれていたためである。制度基盤の整備は、2015年の国務院文書「新情勢下における知的財産強国建設加速に関する若干の意見」を起点に加速されてきた。同文書は、2020年までに達成すべき具体的な施策として、主要産業計画や重点投資プロジェクトそのものを対象に知的財産評価を実施する制度の構築や、経営学・経済学に知的財産の専攻を設けるなどの経営と知財を横断する専門人材の育成を掲げていた。

(4) 共通するもの

これらの事例に共通するのは、技術を実用化・事業化につなげるために必要な専門機能を、技術の探索・選定から開発、実証、調達、量産及び市場展開に至る過程に組み込んでいくことである。技術と具体的な需要を結び付け、事業主体、顧客、資金、知財、技術データ、標準、規制、製造、調達を相互に整合させる仕組みが形成され、企業が中核技術、優秀な人材、自己資金を投入できるよう、知財・技術データの利用条件、将来市場への展開可能性、後続調達の見通し等が設計されている。

3. 提言：知財・技術資産戦略を一体で設計する制度への転換

（基本的な考え方）

日本が目指すべきは、安全保障上必要な能力を自ら定義し、国内外の技術を探索・選択して組み合わせ、実運用に適合させ、量産、維持整備、継続的な改良及び有事の増産まで行える体制を形成することである。

任務遂行に不可欠で、危機時に供給制約を受けやすく、失えば再構築に長期間を要する能力については、設計、システム統合、製造、保守、改良及び増産の中核を国内に確保しなければならない。同志国や外国企業を活用する分野でも、複数供給源、必要な技術データ、利用・改良権及び代替製造能力を確保する必要がある。

優れた技術の存在だけでは、この能力は形成されない。技術を担う企業が量産、改良、人材確保及び次世代技術への再投資を継続できる事業基盤が必要である。

この能力を実現する中核が、知財・技術資産戦略である。これは、技術の探索から開発、実証、調達、量産及び市場展開までを見通し、次の三つを同時に満たすよう、権利化、秘匿、標準化、契約、輸出管理を一体として設計することを意味する。第一に、企業が技術の競争優位を守り、市場・用途を広げながら、その価値を対価として回収し、継続的な改良・再投資につなげられるようにすること。防衛専用品では、性能を秘匿することが安全保障上不可欠であり、区画管理や関係者限定のもとで全てを秘匿するのが通常である。しかし、デュアルユース技術は、民生市場や同志国市場を含めた広い販路で投資を回収して初めて事業として成立する。防衛専用品と同じ発想で全てを秘匿すれば、投資回収の道を自ら狭めることとなる。第二に、政府が運用、維持整備、改良、相互運用及び増産等、任務遂行に必要な範囲の権利及び技術データを確保すること。第三に、第三者の知財・契約によって実装、改良又は供給の継続が妨げられないようにすることである。

この三つは、ゼロサムではない。企業が事業として存続し、改良・再投資を続けられなければ、政府が確保した利用権も持続的な供給に結びつかない。政府が必要とする範囲を明確にすることは、企業にとっても投資判断の前提となる。技術が防衛用途以外にも展開されれば、量産によるコスト低下は政府の調達条件にも及ぶ。知財・技術資産戦略とは、この三つを、企業を成長させ、技術供給基盤を持続させるという一つの目的のもとで、一体的に設計することである。この設計は契約締結時点で完結するものではなく、装備のライフサイクルを通じて生じる維持整備、改良、代替調達及び増産の必要に応じ、双方の利益を高める選択肢を、あらかじめ用意しておくことを含む。

(1) 三つの機能を制度に組み込む

日本は防衛産業を含む「戦略17分野」に2040年度までに官民で370兆円超を投資しようとしている。既に防衛省は令和8年度より、スタートアップ企業等の技術を本格的な研究開発段階につなげるSBIR型の調達制度（防衛省版SBIR、いわゆる「ファストパス調達」）を開始し、伴走支援体制の整備を進めている。これは、個別プロジェクトの採択・出資段階で知的財産の価値を評価する仕組みを、こうした既存制度・新制度の双方に制度横断的に組み込む絶好の機会である。

第一 達成すべき目標から逆算した入口評価

達成すべきミッションと利用ニーズを起点として、技術の性能だけでなく、実運用への適合性、量産・改良可能性、知財・技術データの確保、第三者特許リスク、標準化・認証、供給網、調達・市場への参入可能性、事業性及び投資回収の見通しを評価する。

第二 知財・契約・事業化を一体とした伴走支援

採択企業とともに、政府に必要な利用権を確保し、企業が改良と横展開を行える契約条件を設計する。知財、秘密管理、標準化、輸出管理、実証、調達及び資金調達を一貫して支援する。知財・技術資産の価値は契約条件と価格に反映し、必要な専門人材の費用も支援額及び契約額に織り込む。

部隊レベルで迅速な試験運用・調達を行う場合（提言9参照）には、運用データへのアクセス、既存技術の取扱い、改良・再実証に必要な利用権等の基本条件を標準的な契約ひな形により迅速に合意し、詳細な条件は試験運用の結果や事業化の見通しを踏まえて確定できる仕組みを整備する。企業には中核技術の権利と商用化・横展開の余地を残し、政府には運用、評価、維持整備、改良等の任務遂行に必要な利用権を確保することを基本とする。供給途絶、事業撤退等の場合に必要となる追加的な権利についても、あらかじめ条件を定めておく。

第三 初期需要から調達・量産・市場へ移行する仕組み

開発・実証のマイルストーンと、その達成後の政府調達、大企業購買その他の具体的な需要をあらかじめ設計する。初期需要を企業の設備投資、民間資金、量産及び国内外の市場につなげ、そこで得られた収益、技術及び事業基盤を次の技術開発・改良と安全保障需要につなぐ循環を形成する。

(2) 利用部門と知財専門機能が一体で実行する体制を整える

安全保障関連技術推進本部及びディフェンス・ボードが示す方針を踏まえ、個別案件では、実際に技術を利用する部門が、解決すべき課題、運用場面及び制約条件を具体化し、調達部門、企業及び知財・契約等の専門家とともに、必要な権利、技術データ、利用・改良条件及び調達への移行条件を設計しながら、開発、実証及び調達を進める。プログラム・マネージャーとしての役割は、技術的な解決策を指示することではなく、利用部門が具体化した課題・運用条件を的確に伝え、その解決の設計は企業の裁量に委ねることにある。既存の早期装備化やスタートアップ参入促進の取組にも、利用部門の入口からの関与と、知財・技術データ・契約条件を実証及び調達と一体で設計する機能を組み込む必要がある。

機能	主たる担い手
ミッション・需要の定義	利用部門・調達部門
技術・事業・知財の入口評価	利用部門＋新機構・新基金＋専門家
知財・技術データ・契約設計	新機構・新基金の専門チーム＋政府側専門機能
実証・改良	利用部門＋企業
調達・量産への移行	利用・調達部門＋新機構・新基金
民需・同志国市場・資金への接続	新機構・新基金＋企業＋民間資金

「包括的安全保障関連技術育成実装機構（仮称）」（提言 2 参照）及び「安全保障関連デュアルユース技術推進基金（仮称）」（提言 1 および提言 2 参照）等には、資金配分機能に加え、個々の案件について、需要設定から技術選択、実証・改良、知財・契約、調達、量産及び国内外の市場展開までをつなぐ横断的な支援機能を持たせる。この支援においては、知財・技術データ、契約、標準化・認証、実証、調達、量産、市場展開、価値評価及び資金調達を個々の案件に応じて組み合わせて提供する。支援に当たっては、秘密として管理すべき技術情報を企業自身があらかじめ特定できるよう助言する機能も持たせる。共同研究、実証、委託製造又は人材の移動を通じて技術情報が流出しても、社内で秘密として管理されていないければ、営業秘密としての法的保護を受けられない。

防衛省・防衛装備庁には、米国防総省のIP Cadre（知財・技術データと契約・調達上の課題を一体的に扱う専門人材・支援体制）に相当する専門機能を整備する。政府に必要な利用・改良能力を確保しながら、企業の技術優位、参入意欲及び成長余地を損なわない契約を設計する。企業の事業撤退、経営悪化又は買収が生じた場合にも、安全保障上重要な技術、技術者、製造設備及び供給能力が国内から失われないよう、他企業への技術移転、事業承継の仲介又は政府による一定の権利確保を検討する。

知財・技術資産戦略の欠如は、安全保障関連デュアルユース技術に限られた課題ではない。AI、量子、サイバー、宇宙、ロボティクス、半導体、通信、電池、素材など、将来の防衛能力を左右する技術の多くは、当初から防衛用途として生まれるとは限らず、民生市場や重要インフラ分野で先に育つ場合も少なくない。「戦略17分野」への官民投資が動いている今を逃せば、この横断的な体制を組み込む機会は再び巡ってこない。防衛省・防衛装備庁のIP Cadre相当機能は、内閣府、経済産業省、特許庁、関係調達機関、INPIT（独立行政法人工業所有権情報・研修館）、NEDO（国立研究開発法人新エネルギー・産業技術総合開発機構）、JST（国立研究開発法人科学技術振興機構）、JETRO（独立行政法人日本貿易振興機構）、JSA（一般財団法人日本規格協会）国際標準化戦略推進センター等と連携し、政府横断の「知財・標準・調達専門ネットワーク」として展開すべきである。これにより、防衛用途として育つ前の段階から、技術の価値を取りこぼさない体制とする。

（3）試作・実証段階からの中国部品依存を防ぐ支援を設ける

安全保障に関わる分野では、中国製部品・素材の採用には、情報漏洩、供給途絶、保守・更新への依存等のリスクが伴う。他方、デュアルユース技術の多くでは、中国企業が巨大な民需と量産基盤を背景に圧倒的な価格競争力を持ち、将来の量産を見据えた低価格で試作品を提供することも多い。国内企業の試作品が実費ベースで高額となれば、開発企業はリスクを認識していても、試作段階で中国製品を選択しやすい。

試作段階で採用する部品・素材・モジュール等は、その後の設計、性能、知財、標準及び量産体制を大きく左右する。この段階で中国製品を採用すれば、中国依存が製品設計に組み込まれ、後から国内・同志国供給網へ切り替えることが困難となる。

このため、戦略分野の試作・実証において、国内・同志国企業の重要部品・素材・モジュール、加工・試作サービス等を将来の量産価格に近い条件で利用できるよう、試作品価格と量産想定価格との差額を補う仕組みを設けるべきである。これは、技術開発の初期段階から国内・同志国の供給基盤、知財、標準、認証及び量産可能性を製品設計に組み込むための初期需要形成策である。

制度運用では、価格差、代替困難性、供給持続性、知財の所在・管理、標準・認証への適合可能性及び量産時の供給能力を確認し、採用後の改良、標準化及び量産移行につなげる。必要に応じて、知財・技術データ及び契約条件の整理を担う専門家支援とも連動させる。

なお、中国依存を避けるための同志国企業への発注拡大は、日本単独では確保できない量産規模を得て中国の規模の経済に対抗し、西側装備全体のコストを引き下げる上で望ましい。ただし、同志国企業であっても、その利便性から過度に依存すれば、災害その他の事情により供給が滞るリスクは残ることに留意が必要である。

(空 白)

技術を持続的な力に変える第一歩は、要求に立ち返って設計することである。

システムを作る場合、ニーズ（要求）を把握し、それを基に要求性能を明確にする。要求を達成するため装置への要求仕様を作成する。その仕様を基に設計を行い（必要な技術がない場合は研究開発を行う）、装置の製造を行い、完成した製品を納入し、ユーザーが運用する。

これを整理すると、「ニーズ（要求）→ 要求性能 → 要求仕様 → 設計（研究開発）→ 製造 → 運用」の流れとなる。

ここでは、可視光の光学センサーシステムを一例として考えてみる。光学センサーの要求には対象物は何か、その対象物の何を見たいのか（形状を見たいのか、動きを見たいのか等）を明確にする。

装置としては、光を集める光学レンズ系、その次に光を電気信号に変える検知部が必要となる。光の有無だけを検知（光によるオンオフ制御）するのであれば、検知部は1素子でよいが、画像として認識する場合は多数の画像素子が必要となる。例えば、一般のパソコンについているWebカメラの場合は、（207万倍に当たる）207万画素を用いることで、フルHDのカラー画像を得ることが可能となる。

このように、求める情報は何かを分析し、製品設計につなぐ一体的設計が必要である。これは、センサーで得たデータの画像処理についても同様である。形状を捉えたいのか、動きを捉えたいのかによって、必要となる画像処理のアルゴリズムも異なる。

こうしたデュアルユース技術のシステムを、防衛装備向けにのみ販売するのではなく、将来、民生向けにも展開する場合には、新規性があり分解などにより容易にその構造が理解され模倣されてしまうものについては、特許出願のタイミングや権利化する技術の範囲に留意する必要がある。例えば、専用の出力形式のまま一度製品として納入・公開してしまえば、その後に追加した出力対応や関連する改良について新たに特許を取ろうとしても、既に世に出た製品の仕様が新規性を否定する先行技術となり、権利化できないことがある。また、多少の改良を加えた製品を他人が自由に製造、販売できることとなり、それまで苦労した研究開発にただ乗りされてしまうこととなる。技術は後から広げられても、その技術を守る特許は後から追加できるとは限らない。技術を公開する前に周到なビジネス戦略と知財標準戦略が必要である。

この光学センサーが、複数のドローンを連携させる群制御システムに組み込まれる場合、センサーを納入するだけでは、実際の運用データを見て初めて分かる「何を改良すべきか」という知見が蓄積しない。その知見を基に改良発明が生まれた場合、その権利（フォアグラウンド知財）の帰属や共有も、契約条件によって決まる。決めておかなければ、プラットフォーム側の設計・データ管理の都合がそのまま既成事実となる。入口段階では、データ利用や改良発明の扱いを細部まで確定させることはできないが、データ利用の手続、改良発明の帰属原則、仕様変更時の協議手続といった骨格は定められる。実証段階で必要なデータや改良点が明らかになれば、一から交渉し直すことなく、その骨格に沿って具体的な条件を詰め、継続的な改良と価値の創出につなげることができる。

進化し続ける防衛装備品へ —ソフトウェア時代の産業技術基盤：三者一体 (MOSA・SBOM・RMF)¹とDevSecOps—

1. 三つの仕組みと一つの基盤に係る基本的な考え方

まず、本提言で扱う三つの仕組みの概念について整理する。

- ① **モジュール・オープン構造 (MOSA)** は、無人機をセンサー、通信、航法、AI、動力といった機能単位 (モジュール) に分け、そのつなぎ方 (インターフェース) を政府や認められた企業が利用できるようにする設計・取得のアプローチである。単なる構造設計ではなく、主要な接続仕様の管理、政府による必要な技術データ権の確保、モジュール単位の競争環境の整備までを含む。部品を差し替えるように能力を更新でき、機体全体を作り直す必要がなく、特定企業への依存 (ベンダーロックイン) も抑制できる。ただし「交換可能」とは無試験で差し替えられることではなく、電力・重量・熱・電磁両立性や安全・耐空性等の適合確認を伴う (図1 参照)。
- ② **SBOM (ソフトウェア部品表)** は、装備品に入っているソフトウェア部品の一覧であり、食品の原材料表示に例えられる。新しい脆弱性が公表されたとき、機体・製品・版の構成管理情報と結び付けて照合することで、影響を受ける可能性のある装備品を迅速に絞り込むことができる。なお、防衛用途のSBOMは一般公開を前提とするものではなく、取得当局、運用者、評価機関等にアクセスを限定して運用できる (図2 参照)。
- ③ **RMF (リスク管理枠組み)** は、サイバーリスクを評価し、必要な対策を実装・確認した上で、残るリスク (残余リスク) を明らかにして権限者が運用の可否を判断し、配備後も監視を続ける仕組みである。「完全に安全になるまで使わない」のではなく、「リスクを把握し管理しながら、早く使い始め、使い続ける」ための枠組みである (図3 参照)。
- ④ **DevSecOps** は、開発 (Dev)・セキュリティ (Sec)・運用 (Ops) を分断せず、試験や証拠の作成を自動化しながら一つの流れで回す共通基盤である。三者はこの基盤の上で初めて、連続した更新サイクルとして機能する。 (図4 参照)。

三者一体の意味は明快である。本提言では、この三者をDevSecOps基盤の上で連携させる考え方を「三者一体」と呼ぶ。MOSAが「交換できる構造」を、SBOMが「中身の見える化」を、RMFが「変更後も安心して使える承認」を担い、DevSecOpsがこれらを一つのサイクルとして高速で回す。どれか一つが欠ければ、影響の特定、修正、審査のどこかが滞

¹ MOSA : Modular Open Systems Approach
SBOM : Software Bill of Materials
RMF : Risk Management Framework

り、更新サイクルの速度と確実性は大きく損なわれる。三者がそろって初めて、更新のたびに戦闘力を高め続ける装備品が実現する。

なお、「オープン」とは内部設計やソースコードを一般に公開することではない。政府、運用者及び承認された供給者が、交換・追加に必要な情報と権利を利用できる状態を指す。

2. 各国の実例

米英・ウクライナは、①交換可能な構造、②構成の見える化、③リスク管理型の承認という三つの機能を、それぞれ別個の制度として発達させてきた。以下、各国の実践を具体的に見た上で、そこから日本が汲み取るべき教訓を整理する。

(1) 米国 — 制度化されたMOSA

米国の特徴は、MOSAを個別プログラムの工夫ではなく、法律・政策・技術標準の三層で制度化した点にある。連邦法（10 U.S.C. §§4401–4403）は主要防衛取得計画に対し、実行可能な最大限の範囲でMOSAを採用し、主要インターフェースを定めて利用できるようにすること、モジュール単位での競争を確保すること、政府が技術データ権を確保すること等を取得戦略に盛り込むよう義務付けている。2019年には陸海空三軍の長官が連名で、将来の装備システムと既存システムの改修の全てにMOSAを適用する方針を示した。米国においてモジュール・オープン構造は、設計上の推奨ではなく取得制度上の要求事項である。

この法的要求を支えるのが技術標準群である。陸軍のCMOSS（C5 ISR／電子戦モジュール・オープン標準群）は、通信、電子戦、測位等の機能を共通規格のカードとして共通シャーシに差し替え可能とする標準であり、航空ソフトウェアのFACE、センサー分野のSOSAとともに、どの機能を共通規格とし、どこに接続点を設けるかを具体的に定めている。法律が方向を示し、標準が接続点を定めることで、初めて第三者が現実に統合へ参入できる。

その効果を最も具体的に示すのが陸軍の無人機Gray Eagleである。米陸軍と製造企業の公表によれば、CMOSS準拠の共通シャーシを搭載した結果、通信情報の収集、電子攻撃、通信中継、対無人機等の任務機能が、機体を再設計することなくカードの追加・交換として順次統合され、製造者以外の企業のセンサーや無線機を短期間で搭載する実証・契約が積み重なっている。任務の追加が「機体の開発」から「モジュールの統合」の作業へ変わったところ、MOSAの効果の具体的な現れである。

さらに、米国防総省の継続的運用承認（cATO）の運用指針では、DevSecOps基盤で生成されるSBOMの提出と脆弱性情報との照合が求められている。MOSAとcATOは別々の制度体系に属するが、両者を通して見れば、構造（MOSA）・可視化（SBOM）・承認（RMF）を一つの更新サイクルとして連携させる方向は、米国において最も明確に現れていると評価できる。

(2) 英国 — PYRAMIDとSecure by Design

英国の出発点は、ミッション・システムのソフトウェアが機種ごとの専用品となり、開発費と改修期間が膨張しているという問題意識であった。将来の航空戦力ではミッション系ソフトウェアが3,000万行を超えると見込まれ、機種ごとに互換性のないソフトウェアを別々に開発し維持する方式は持続できない。そこで国防省はPYRAMID計画を立ち上げ、航空ミッション・システムの機能を境界の明確な部品群に分解した参照アーキテクチャ（PRA）を整備した。同一の参照構造を採用した機体の間ではソフトウェア部品を再利用でき、能力向上は部品の差し替え・追加で実現できる。PRAは公開ライセンスの下で公開され、2025年には英国防規格（Def Stan 00-134）となった。米国のFACE標準との整合も確認されており、英国防省はPYRAMIDを、日英伊で進めるグローバル戦闘航空プログラム（GCAP）を含む個別計画で適用を義務付けており、GCAPに参画する日本にとって直接関わる標準である。

サイバー面では、Secure by Designにより、一時点の認定に代えて開発初期からライフサイクル全体でリスクを管理する方式へ移行しており（2023年から新規プログラムに適用）、米国のRMF・cATOと同じ方向にある。また、国家サイバーセキュリティセンター（NCSC）は、第三者ソフトウェア部品を把握するインベントリの代表形式としてSBOMを示している。

モジュール構造の効果を実運用で示したのが、2025年に公表されたStormShroudである。既存の無人機に他社製の電子戦ペイロードを短期間で統合し、有人戦闘機を援護する電子戦という新たな任務を具体化した。機体と任務装置を別々の企業が開発し、組み合わせて新しい能力を生む—機体と任務装置を分離し、外部の技術を迅速に統合できる構造が可能にした装備品取得の姿である。

(3) ウクライナ — 実戦下の高速な更新

ウクライナの実践は、MOSAという名称を用いてはいないが、モジュール構造の軍事的価値を最も鮮明に示している。ウクライナ国防省は、戦場の変化に対応するため、無人機的设计は実質約3か月ごとに更新する必要があると説明している。この速度を要求する主因は電子戦であり、妨害の周波数や航法妨害の様相が変わるたびに、通信機、映像伝送、飛行制御、航法等の構成部品を替えなければ、無人機は数週間で無力化される。機体全体を作り直しては、この周期に追従できない。構成部品を差し替えやすいモジュール構造は、部品の供給網や迅速な試験と並んで、この短い改版周期を支える中核的な条件である。

短距離FPVでは、通信、カメラ、飛行制御等のモジュール的な部品を組み替え、完成品を生産バッチ単位で高速に改版する方式が定着した。これを支えるのが部品の市場と共通基盤であり、国産部品を登録した「部品ライブラリー」は170点超に拡大し、2025年8月には、前線部隊が戦果に応じて付与される電子ポイントを用い、必要な機体や装備を市場（Brave1 Market）から選択・取得する仕組みが導入され、参加部隊は400を超え、累計の注文は

50万機規模に達している。標準文書によるトップダウンの標準化ではなく、市場に流通する部品の事実上の共通インターフェースを核とする、ボトムアップ型のモジュール・エコシステムである。

長距離攻撃型では逆に、基本機体系列を維持しながら内部を進化させる方式がとられている。リューティは、2024年の採用後も機体の基本形を保ちつつ改良が重ねられ、航続距離2,000km級の能力が公表されるに至った。個々の改良内容の全てが公表されているわけではないが、基本系列を維持しながら内部を進化させ続ける長距離無人機の代表例である。短距離型の「バッチ単位の組み替え」と長距離型の「系列内の版管理」は形こそ異なるが、いずれも「変わらない基本構造+交換可能な内部モジュール」という同じ原理に立つものである。

制度面でも、国家サイバー当局がSBOMを正式に定義し、2025年にはデジタルシステムのセキュリティ承認手が制度化された。同年12月には、日本の防衛省・自衛隊がRMFの実装経験（主として情報システム分野）をウクライナ側へ共有している。名称や成熟度は国ごとに異なるが、実戦の要請から、構造・可視化・承認という同じ機能が急速に整えられつつある。

(4) 各国の実践の評価 — 収斂と残る課題

3か国に共通するのは、三つの機能をそれぞれ別個の制度として整備してきたことである。米国ではMOSAは取得政策、cATOはサイバー承認と系統が分かれ、英国でもPYRAMID、Secure by Design、SBOMはそれぞれ別の取り組みである。ウクライナでは各機能が今まさに個別に整いつつある。少なくとも公表された制度を見る限り、三者を最初から一体の仕組みとして設計した国は見当たらない。

しかし、無人機を速く更新し続けるという共通の要請の下、実践の現場では三つの機能が事実上一つのサイクルとして連動し始めている。Gray Eagleに新しいペイロードを統合するには、CMOSSの構造、ソフトウェア構成の把握、変更の承認が連なって初めて配備に至る。ウクライナのバッチ単位の改版も、英国のStormShroudも同じである。制度が分立していても、運用の必要が三者を結び付けるのである。

同時に、事後的なつなぎ合わせには無理が残っている。米国では承認の遅延がソフトウェア更新の隘路と繰り返し指摘され、cATOはこの遅延への対処として後から生まれた。英国のPYRAMIDは採用の初期段階にあり、ウクライナでは、用途とリスクに応じて前線投入の速度と制度的な保証のバランスを変える実践的な運用がとられており、制度としての体系化はこれからである。各国の実践が示すのは、三つの機能は必然的に連動するという方向の正しさと、別々に作って後からつなぐと不整合が残るという一体設計の必要性の、その両方である。

3. 三者一体とDevSecOpsが実現する三つの目標

実際の更新は、次のような一つのサイクルとして回る。新たな脆弱性が判明した場合は、SBOMを構成管理情報・脆弱性情報と照合して影響を受ける可能性のある装備品を迅速に絞り込み、モジュール・オープン構造により該当部分を中心に修正・交換する。新しいAI・通信・センサーを導入する場合は、任務上の必要に基づいて対象モジュールを選定・統合し、SBOMを更新する。いずれの場合も、変更影響分析に基づく試験とRMFによる運用承認を経て、DevSecOps基盤で配備後の監視へつなぐ。この連携が、日本の防衛力整備に求められる目標を同時に実現する。

目標	三者一体が生む効果
アジャイル開発による早期装備化	更新・向上したい機能があれば、該当するモジュールを選んで、そのモジュールを中心に開発・交換すればよい。審査も変更影響分析に基づき変更部分を中心に行えるため、機体全体を一から開発・審査する場合に比べ短期間で実施でき、新しい能力をはるかに早く発揮できる。
常時のセキュリティ確保	新しい脆弱性が見つかったも、SBOMと構成管理情報の照合で影響を受ける可能性のある機体を迅速に絞り込み、該当部分を中心に修正して速やかに運用へ戻せる。配備後も新たな脆弱性を監視し続ける。
スタートアップ参入による新技術導入	接続の仕様が承認された企業に開示されているため、機体全体を開発しなくても、優れたセンサーやAIが一つあれば参入できる。SBOMにより新規企業の製品でもソフトウェア構成と既知の脆弱性を確認しやすく、審査も円滑となる。

この三つの目標は相互に支え合う。早く更新できるからこそセキュリティを常時保て、新しい企業が参入するからこそ技術が進み、構成が見えているからこそ更新を速くできる。三者をDevSecOps基盤で一体運用することこそ、性能・安全・セキュリティ・スピードのバランスがとれた、戦闘力を最大に発揮できる装備品への道である。

4. 日本の基本方針

以上を踏まえ、日本が採るべき基本方針は次のとおりとすべきである。核心は一つである。各国が別々に整備し、後から個別につないできた三つの機能を、日本は最初から一体の更新サイクルとして設計する。これが後発の利であり、日本の無人機取得の独自性となる。

- (1) **三者一体を基本方針とする。** モジュール・オープン構造（MOSA）、SBOM、RMFを個別の要求として並べず、DevSecOps基盤の上で連携する一つの更新サイクルとして調達仕様に組み込む。
- (2) **日本型として実装する。** 米国制度の複製ではなく、日本の取得制度や企業構造に合わせて設計する。問うべきは名称への適合ではなく、第三者が接続できるか、構成を追跡できるか、試験の証拠を再利用できるかである。
- (3) **共通化する範囲は官が定める。** 任務の分析（ミッション・エンジニアリング）とシステム構造の検討に基づき、機体のどの部分に共通の接続仕様を設けるか、どの技術データ権を政府が確保するかを、運用者、取得当局、試験機関が主導して決める。ただし企業の内部設計には立ち入らず、部品の交換・追加に必要な最小限の接続条件（物理・電気条件、データ形式とその意味、タイミング、セキュリティ、版管理、適合性試験の方法）を示すにとどめる。
- (4) **機種に応じて要求に軽重をつける。** 短距離FPVには簡素な構成管理と迅速な実証を、長距離攻撃型・回収・再使用型には着実な版管理と適合性試験を適用し、全ての機体に同じ重い手続を課さない。
- (5) **承認手続を簡素化し、迅速化する。** 一度評価したモジュールと試験証拠は、対象となる版・用途・前提条件を明示した上で登録・再利用し、変更部分を中心に評価する。サイバー、安全・耐空性、性能の証拠は一つの変更承認パッケージにまとめ、各承認主体が証拠を相互に利用できるようにし、各分野の承認権限と責任分界は初期段階で明確にして維持する。
- (6) **無人機から始める。** 新規の小型・中型無人機、地上管制装置、通信・AIペイロードから導入し、国内の実証環境とDevSecOps基盤で運用実績を積み上げて順次拡大する。なお、三者一体の効果を実際に発揮するには、必要な技術データ権、適合性試験環境、構成管理、脆弱性監視、変更承認の権限、継続的な改修予算を併せて整備する必要がある。

5. まとめ

目指すべきは、装備品を、納入時に性能が固定された「モノ」から、配備後も脅威と技術の進歩に追随して能力を高め続ける「進化するシステム」へ転換することである。その鍵が、モジュール・オープン構造（MOSA）、SBOM、RMFをDevSecOps基盤の上で一体運用する三者一体の取組みである。米国の制度、英国の標準、ウクライナの実戦は、それぞれの形でこの方向の有効性を示している。同時に、公表された制度を見る限り、三者を最初から一体として設計した国は見当たらない。後発の日本には、各国が後からつなぎ合わせたことにより残る不整合を、最初から一つの設計で解消する機会がある。

日本は、無人機を出発点として日本型の三者一体を確立し、アジャイル開発による早期装備化、常時のセキュリティ確保、スタートアップ参入による新技術の導入を同時に達成することで、バランスのとれた戦闘力を最大に発揮できる防衛力を築くべきである。

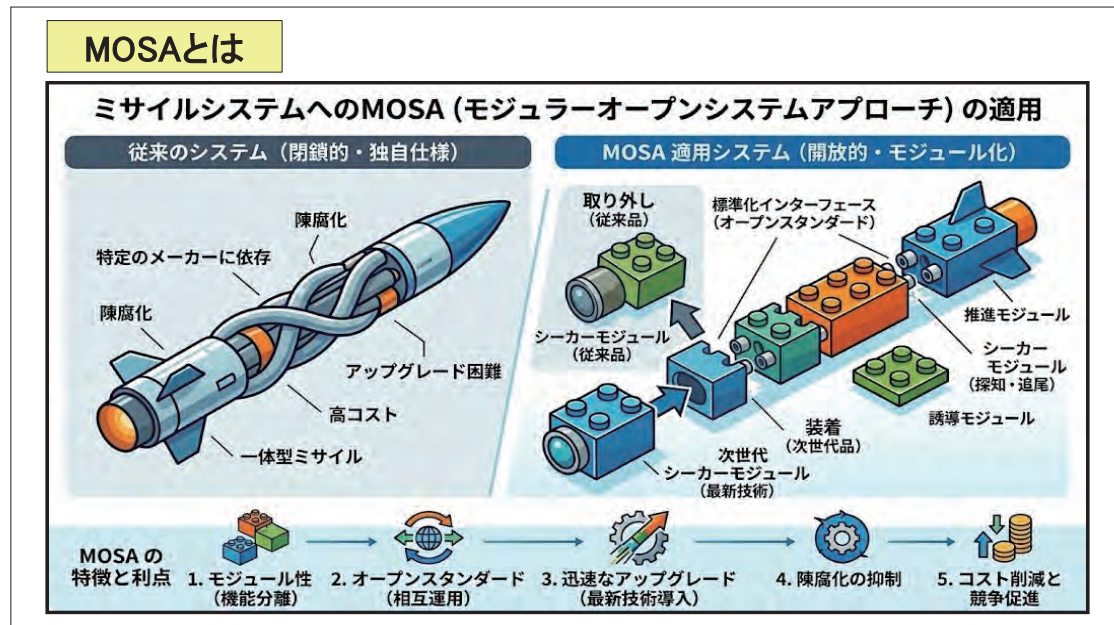
主要参考資料

本文の記述の主な根拠となる一次資料・公表資料は次のとおりである。

- [1] 米国防総省CIO『Software Modernization Implementation Plan FY25-26』（2025年）
- [2] 10 U.S.C. §§4401-4403 (Modular Open System Approach in Development of Major Weapon Systems)
- [3] 米国防総省『Implementing a Modular Open Systems Approach in DoD Programs (MOSA Implementation Guidebook)』（2025年2月）
- [4] 米国防総省CIO『Continuous Authorization to Operate (cATO)』
- [5] 米陸軍・GA-ASI公表資料（MQ-1C Gray EagleへのCMOSS準拠電子戦能力追加契約〔2025年10月〕、及びVanguard実証〔2024年9月〕）
- [6] 英国防省『PYRAMID Technical Standard V1.0』（Def Stan 00-134、2025年2月）及び英国防・安全保障アクセラレータ（DASA）『PYRAMID for Avionics and Mission Systems』競争公示
- [7] 英国防省『Secure by Design』（2023年～）及び英国家サイバーセキュリティセンター（NCSC）SBOM関連ガイダンス
- [8] ウクライナ国防省・デジタル変革省・Brave1公表資料（Army of Drones: Bonus／Brave1 Market、部品ライブラリー等）

別紙 図表

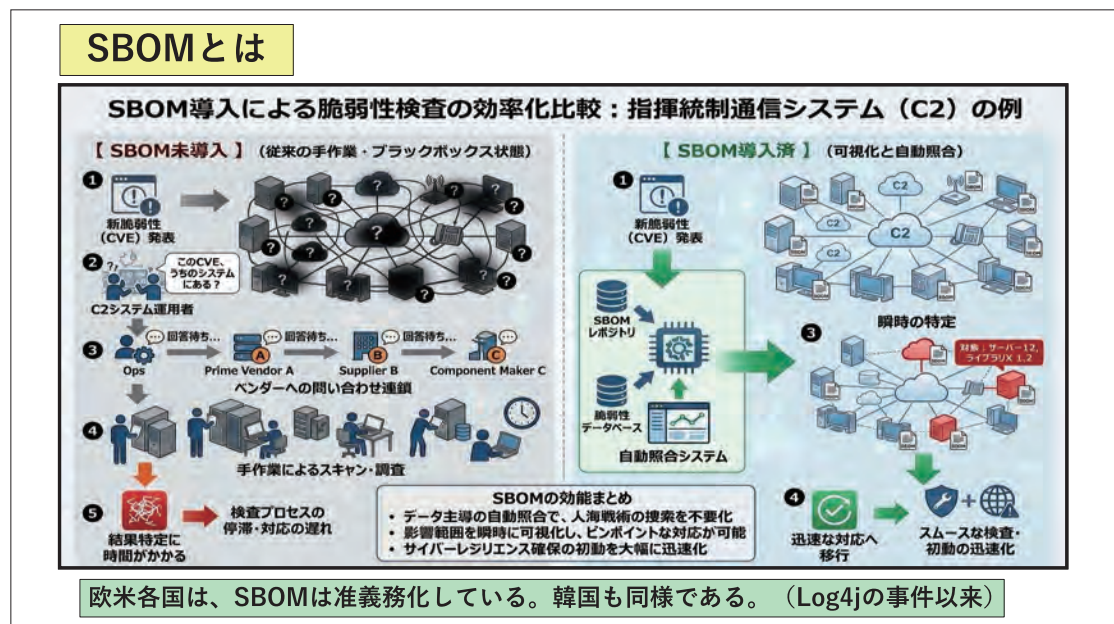
図1 MOSA（モジュール・オープン構造）



特定企業に依存する一体型（左）から、政府と承認された企業が接続仕様を利用し、適合性確認を経てモジュールを交換・追加できる構造（右）へ。新技術導入と競争促進の入口となる。

出典：一般財団法人防衛技術協会作成（概念図）

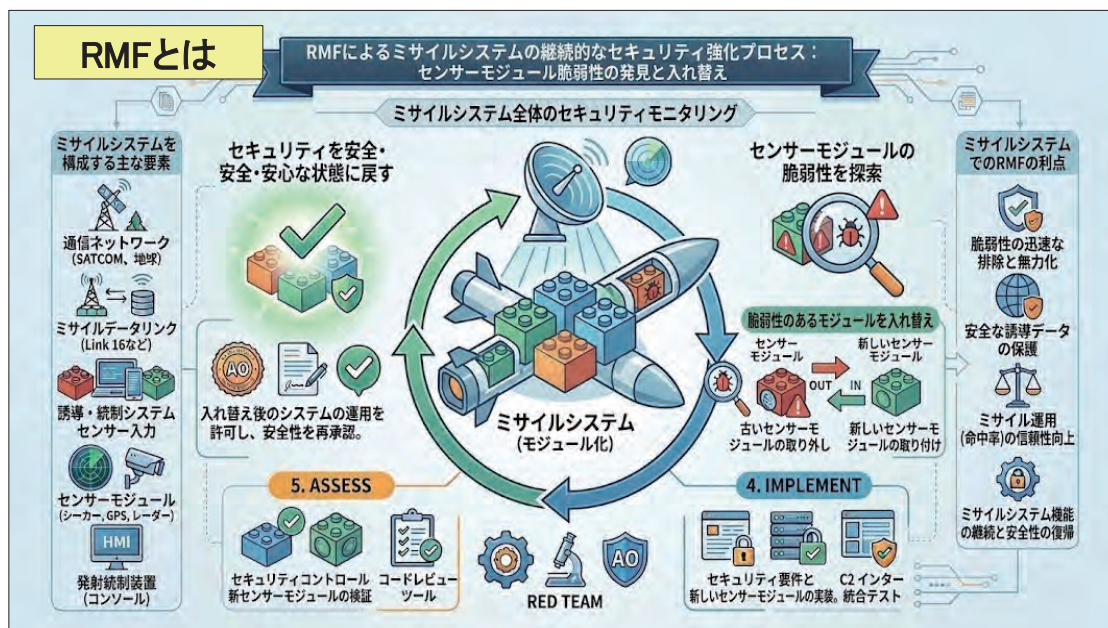
図2 SBOM（ソフトウェア部品表）



SBOMがない場合、影響範囲の把握は供給網への照会と手作業の調査に依存する（左）。SBOMを機体・製品・版の構成管理情報と結び付けて脆弱性情報と自動照合すれば、影響を受ける可能性のある対象を迅速に絞り込める（右）。

出典：一般財団法人防衛技術協会作成（概念図）

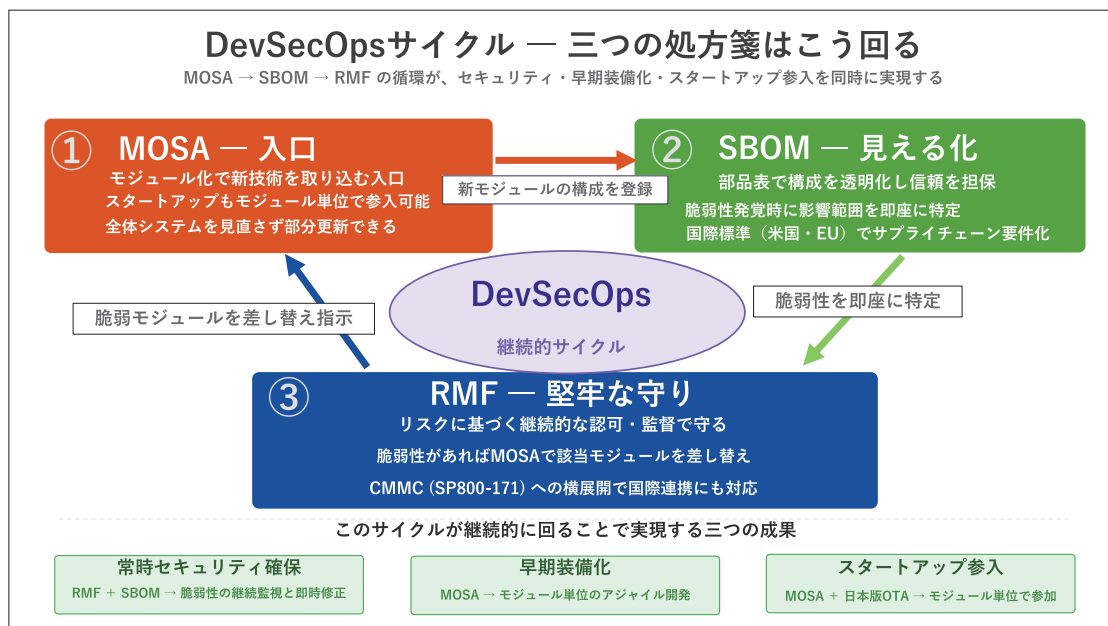
図3 RMF（リスク管理枠組み）の適用例



RMFのうち、脆弱性発見後の変更実装・評価・再承認・継続監視を示す適用例。対処は、ソフトウェア修正、設定変更、緩和策、モジュール交換からリスクに応じて選択する。

出典：一般財団法人防衛技術協会作成（概念図）

図4 DevSecOps — 三者を継続的に回す運用基盤



MOSA（新技術の入口＝交換できる構造）→ SBOM（中身の見える化）→ RMF（守り）を継続的に循環させる。常時セキュリティ確保・早期装備化・スタートアップ参入を同時に実現する。本図は役割分担を示す概念図であり、実際の活動は並行・反復して行われる。図中の「日本版OTAs」は、試作・実証・改良を短期間で反復する柔軟な契約方式を指す。

出典：一般財団法人防衛技術協会作成（概念図）

(空 白)

1. 現状の問題点

我が国の安全保障は、防衛省・自衛隊のみならず、政府機関、基幹インフラなど、官民の幅広い施設・設備によって支えられている。近年、これらの施設ではAI、IoT、クラウド技術の活用が急速に進展しており、多くの機器・システムがネットワークに接続され、継続的にデータを収集・送信するようになっている。このため、防衛装備品や通信設備のような中核システムだけでなく、一見すると安全保障とは直接関係のない設備や、比較的単純なハードウェアであっても、重要情報を取り扱う可能性があり、情報の国外流出リスクを考慮する必要がある。

例えば、仮に防衛施設内で利用される電動モビリティや物流設備がクラウドを通じて管理され、そのデータが非友好国へ送信された場合には、施設内部の配置や運用状況、人員の動線などが推測される可能性がある。また、コンピューターケーブルをはじめとする一見単純な製品にも半導体や制御チップが組み込まれている例があり、こうした部品を経由したデータフローについても十分な注意が必要である。経済安全保障推進法では、基幹インフラ事業者（特定社会基盤事業者）が重要設備を導入する際には所管官庁による事前審査制度が設けられているものの、どのような機器・システムが経済安全保障上信頼に値するのかについて、分野横断的な共通の評価基準は十分に整理されていない。

2. 解決の方向性

上記課題を解決する方策として、安全保障に関連する機器・システムそのものではなく、これら産品等の調達先企業を選定する際のガバナンスルールの導入という方策が考えられる。ここでいうガバナンスとは、株主構成、海外拠点との関係、外国政府との関係、特に外国法令や外国政府との契約等に基づく義務の有無などを含め、これらの要件が我が国の安全保障にリスクとなり得るか否かを総合的に評価するものである。このようなガバナンスルールの考え方は、2025年5月に施行された外為法施行令改正の考え方とも整合する。同改正では、外国法令や外国政府との契約等により外国政府へ協力する法的義務を負う法人等について、我が国の基幹インフラに係る機微情報の流出又は毀損のリスクを防止する観点から、一定の対内直接投資について事前届出が義務付けられている。

この外為法施行令の改正の立法例も踏まえ、安全保障に関連する機器・システムの調達においても、このようなガバナンスルールが導入されれば、これをクリアできる我が国企業などに対して、安全保障の関連市場の獲得に向けた技術開発や投資のインセンティブを提供することができる。この結果、我が国の技術安全保障基盤及び産業競争力の強化にも資することが期待される。

また、調達先の制限をどの分野に導入するか判断や、調達先を選定した後の実際の運用段階においても、取り扱うデータや機器が使われる工程の機密度に応じて、利用可能な機器、通信機能、データ移送経路、保守主体等を段階的に制限する仕組みを組み合わせることが有効である。例えば、①非機密の場合、外国製機器についても、運用側が外部との通信を監視できる隔離ネットワーク上での活用を認める、②生産ノウハウ等を含む場合、信頼性に懸念がある外国製機器については外部通信の遮断や取得データの移送経路の限定等を行う、③高度機密を含む場合、信頼性に懸念がある外国製機器は排除した上で、供給者の信頼性、ファームウェアの真正性等を確認できる機器に限定する、④防衛・重要インフラ等の場合、製品の国籍に加え、サイバーセキュリティ管理体制や、ファームウェア、クラウド、更新・保守主体等まで含めたサプライチェーン審査を行う、等である。

緊急時における防衛装備品の優先的確保に係る施策

1. 問題の所在

防衛装備品に用いられている半導体、チタン（主翼・エンジン等）、タングステン（弾芯・ノズル）といった部素材は民生品と共通しているものが多い。しかし、防衛用途は少量多品種であり、かつ長期運用を前提とすることから、経済原理に基づく通常の市場においては優先的に供給されにくい傾向にある。

また、ニーズの変化や技術進歩に伴い、半導体の製造サイクルは短期化しており、防衛装備品に用いられた特定の半導体が、数年で製造中止（EOL：End of Life）となることもある。実際、コロナ禍におけるサプライチェーンの混乱の下では、防衛省が半導体を調達できなかったために通信システムの納入が遅延したという事例も見られた。

これに加え、防衛装備品の骨格をなすエンジンプロック、変速機ケース、あるいは高度な強度を要する構造材等の鋳鍛造品の製造基盤は、防衛装備品の製造に欠かせない極めて重要な基盤である。しかし、国内の鋳鍛造産業は、人材確保難・後継者不足により供給能力の減退の恐れがある。特に防衛用の鋳鍛造品は、特殊な加工を要する一方で、生産量が極めて少ないため、小規模事業者の廃業や民需を優先する製造事業者の判断によって、製造ラインが消滅するリスクも否定できない。

さらに、防衛装備品を構成するAI、無人化や自動化技術、通信技術などの技術基盤や製造ラインの多くは、民生分野とも共通性が高い。これらの技術や生産基盤は、平時においては、民生需要に対応しつつ、有事、すなわち事態認定された後は、防衛需要へ迅速に転用することが可能である。

2. 解決の方向性

事態が緊迫し、近い将来、武力攻撃事態や武力攻撃予測事態、存立危機事態又は重要影響事態などが予測される段階においては、前述のような民生・軍用双方に利用可能な汎用部素材（例えば、半導体や鋳鍛造用の原材料・製造ライン）や、民生需要に対応してきた技術力・製造ラインを防衛装備品向けに優先的に確保することが、我が国の平和と独立を守り、その存立を全うするため必要となる場合がある。

このような状況下においても、半導体や鋳鍛造品等の部素材の生産・納入が、民間の経済原理のみに委ねられ、結果として民需向けを優先して配分されることとなれば、コロナ禍において見られたような防衛装備品の不足という事態となってしまう可能性も否定できない。

そこで、事態が緊迫時、近い将来に武力攻撃事態等となる可能性が予測され、かつ、防衛装備品の確保が必要と判断される場合には、例えば、国家安全保障会議（NSC）の9大臣会合で「防衛装備品の確保を優先的に措置すべき旨」認定し、閣議決定した上で、防衛大臣から経済産業大臣に対し、必要となる汎用部素材について、防衛装備品向けの納入・生産を優先したり、製造ラインを民需から防需に向けてもらいたい旨要請したりする仕組みを設けることが考えられる。

かかる要請を受けた経済産業大臣は、製造事業者に対し、その旨の要請をすることができるものとする。当該製造事業者が補助金を受けて製造ラインを整備している場合には、補助金の交付条件として政府の要請に従うべき旨の規定が設けられていれば、製造事業者は特段の事情がない限り、これに従うこととする。また、補助金等を受給していない製造事業者が経済産業大臣から要請を受けた場合には、製造ラインの転用に伴う機会損失について、適切な補填措置を受けられるものとする。

かかるスキームは行政指導及び予算措置で行えるものであるが、より実効性を持たせるため、具体的には上記スキームを提言1にある「安全保障関連技術推進基本法」の中にプログラムの盛り込み、新法として「武力攻撃事態等における防衛装備品確保法（仮称）」を制定することとする。

1. 日本におけるGOCOの制度の概要

2023年に成立した防衛生産基盤強化法は、日本の防衛産業を抜本的に強化することを目的としていたが、GOCO（Government Owned and Contractor Operated）については、ラストリゾートと位置付けられており、防衛産業の裾野に広がる多数の中小企業が後継者不足などから廃業を余儀なくされ、事業承継する企業が現れない場合等、限定的な活用に絞ったものとなっている。

本来のGOCOとは、政府が所有し民間企業が運営するという趣旨であり、研究開発、生産基盤のための設備投資に巨額の費用がかかる場合に、政府がその資金を提供し、出来上がった設備は政府が所有した上で、低利で民間企業に貸し出し、その運営を民間企業に委ねるという仕組みである。諸外国においてもかかる運用形態となっていることが多い。

2. 継戦能力の確保とGOCOの活用

5年近く続く戦闘において、ウクライナは弾薬・誘導武器・ドローン等を大量に消費しており、我が国においても長期戦に対応できる生産能力・維持整備能力の確保は喫緊の課題となっている。有事に対応して弾薬等の大規模増産に対応するためには、平時からオーバーキャパシティの供給能力（「遊んでいる」生産ライン）が必要である。

実際、米国が2024年に公表した「国家防衛産業戦略」においては、同盟国等を含めた需要増、予期せぬ混乱への対処等に不可欠な予備生産能力（spare production capacity）にインセンティブ付けする旨の記述が、EUが2025年に公表した「EU防衛産業変革ロードマップ」においては、緊急の需要増加に対応できる柔軟性を確保するため、常時稼働可能な予備産業能力（spare industrial capacities）の構築を支援する旨の記述がなされている。

このように、防衛装備品の生産・維持整備に係るオーバーキャパシティの負担を民間企業に押し付けるのは、国策として誤っているといえる。本来、有事増産用のラインは、政府が出資して増設し、それを民間企業に低利に貸すという、本来のGOCO制度を用いて実施するのが適切である。

3. 新たな制度

このようなことから、防衛装備品や我が国の存立のため必須となると考えられる装備品に関して、武力攻撃事態等の有事における継戦能力の確保や経済安全保障における戦略的自立性の確保などの観点から、GOCOを積極的に活用していく旨のスキームが必要である。その際、管理を委託される事業者は、懸念国からの部素材の調達を排除するとの観点から、政府に当該装備品を製造するに必要となる原材料等の調達や輸入に関して必要な報告又は資料の提出を行うことを義務付け、必要に応じ所管大臣は調達先の変更を命ずることができることとすることにより、戦略的自立性を確保していくこととする。

具体的には、武力攻撃事態等において自衛隊が確実に侵害を排除することができるための装備品等の確保を確実にするとの観点から、長期間にわたる戦闘行為において特に消耗が激しいと考えられる弾薬、誘導弾、ドローン等の防衛装備品については、政府が施設を提供し、民間会社がこれを運営するというGOCOによることとする。この場合、平時には有事のような所要量が出ないことから、海外への輸出やドローンについては民生品としての製造など、平時においてもGOCOの枠組みによる生産量が一定数確保できるようにし、万が一有事になった場合には、GOCOにおける生産は自衛隊のニーズを充足できるように振り向け、継戦能力の確保に齟齬が出ないようにする。

このような枠組みの構築により、当該民間会社は固定資産税等の固定費用を支払う必要が免除されることとなり、武力攻撃事態等においても、業務を継続することを期待することができる。さらに、このように国が施設を準備する以上、当該防衛装備品の部品等を経済的理由から懸念国から調達することは排除されるべきであり、そのためのサプライチェーン調査を義務付けるとともに、必要に応じて、所管大臣は調達先の変更等を命ずることができるスキームも併せて構築することが適切である。さらに、武力攻撃事態以降も業務の継続性を確保する観点から、GOCOの契約において、当該施設の安全が確保される限り業務を継続する旨を契約において担保することとする。その場合、武力攻撃事態以降も業務を継続する防衛産業従事者に対して、国から特別の手当を支給するとともに、万が一の場合の補償についても自衛官並みに手厚くすべく、新たに法律を制定することとする。

1. はじめに

我が国の安全保障環境の改善を目的として、政府主導で防衛装備移転を強力に推進するためには、装備移転対象国を特定し、交渉・合意を経て、合意に基づく装備品を取得した上で、これを移転するという流れとなるが、この流れを円滑に実施するためにも新たな制度を構築することが望ましい。

2. 防衛装備移転推進のための新たな制度

防衛産業側から「日本版FMS（Foreign Military Sales）」の創設が提案されているが、これは防衛装備品の輸出を官民一体で進めるための一つの有力な選択肢である。これまで「日本版FMS」は、民側の輸出事業者が確実に支払いを得るため、日本政府に納入し、日本政府が民間企業に代わって輸出事務を行うことがイメージされてきた。このような機能も事業リスクを負う事業者を支援するために重要なものといえるが、より本質的には、防衛装備移転を戦略的に展開していくためには、①官民一体となった取り組みが必要であり、官と民を横断的に統合する組織が必要となること、②日本政府の中にも中央の司令塔組織が必要であること、③重要技術を含む防衛装備品の移転に関しては、契約主体も日本政府―相手国政府とすること（G-G契約）、が必要となる。具体的な理由は以下三点のとおりである。

第一に、防衛装備移転には必ず国防当局間の交渉が伴う。この中で、輸入国は多くの場合、現地生産や技術移転といった直接型オフセット、又は防衛装備品と直接関係しない産業支援といった間接型オフセット（例えば、防衛装備品購入の見返りにバナナの購入）を求めることとなる。このような場合、いずれも企業単独や防衛省単独では対応が難しいため、内閣官房の国家安全保障局に防衛装備移転の中央司令塔的組織を設置し、かかるオフセットに関する関係省庁間の調整や処理などを担わせることが望ましい。

第二に、防衛装備品の輸出契約を履行するためには、部素材の安定的供給が不可欠である。防衛装備品に用いられる半導体、チタン、タングステン等は民生品と共通しているが、防衛用途は少量多品種かつ長期運用を前提としているため、市場においては優先供給されにくい。市場の変化により数年で半導体が製造中止となることも多く、このような状況下では、防衛装備移転の契約履行に支障が生じてしまう。このため、第一の理由で述べたのと同様に、中央司令塔組織を設け、経済産業省等との連携を緊密に確保し、外部依存性の高い重要物質の安定的供給対策を担わせることが望ましい。具体的には前述のように国家安全保障局に装備移転担当部署を新設する。

第三に、一部の防衛装備品では、国家間契約（G-G）が国際的に主流となってきた。一般に、防衛装備品の海外への輸出を考えた場合、価格、品質、納期の三点が重要となる。価格や品質の重要性はさることながら、最近とみに重要視されているのは「納期」である。

例えば、イスラエルのSIBAT（国際防衛協力局。国防省の独立した部門として、イスラエル国防軍等の運用上のニーズを把握し、イスラエルの防衛産業企業の国際市場への進出や商談を一元管理する組織。装備品や防衛技術の契約交渉を担当し、G-G、B-G契約を担当する）のKulas准将は、2025年6月、各国が長年にわたり品質と価格を追求する中、近年、イスラエルには「納期の速さ」という新たな有利な要素が登場し、競合他社が7年という納期を提示するのに対し、イスラエル企業は2年から3年で対応することで受注を獲得している旨を発言している。このように、近年の目まぐるしく変化する安全保障環境を踏まえれば、「短納期」が一つのキーワードとなっているといえる。

かかる契約履行を保証する枠組みとしては、契約を民間企業に任せるのではなく、日本政府が契約主体となり、価格、品質、納期を保証する履行体制を整えることこそが、国際市場で日本製の防衛装備品が選ばれる条件となると考えられる。短納期や確実な契約履行が競争条件となりつつある現状において、日本の防衛装備品が国際市場で信頼を獲得するためには、政府が契約管理を担う体制を整えることが望ましいといえよう。

このような計画体制とすると同時に、前述の国家安全保障局の装備移転担当部署に加え、官民からなる新たな「装備移転推進機構（仮称）」を設立し、官民から人材の派遣を受け、各国の装備品の需要の調査、対象国関係機関及び国内関係企業との移転実施に係る実務的調整、防衛産業への支援策の実施、納期管理の実務、部素材安定供給の管理実務など、国家安全保障局装備移転担当部署の決めた政策に基づき実務を担うこととする。これに加え、防衛装備庁に「装備移転部（仮称）」を新設し、体制の充実を図る。

なお、政府間契約に関して、全ての防衛装備移転をそのような枠組みとすることは、政府側の事務手続きの増加等、移転の迅速性を欠くことになりかねないので、主として国家安全保障の観点から重要技術を含む防衛装備を対象とする。

1. 現行の調達制度の概要

日本の防衛調達は、防衛省、防衛装備庁、自衛隊各幕僚監部、及び全国に所在する駐屯地・基地など、様々なプレーヤーが多層的に役割を分担している。調達対象は、戦闘機・艦艇などの大型装備から、建設工事、物資、維持整備、研究開発、役務調達まで多岐にわたっている。装備品の調達制度を概観すると、以下のように整理される。

- ・ 契約方式による分類：一般競争契約、指名競争契約、企画競争、随意契約
- ・ 調達実施機関による分類：中央調達、地方調達
- ・ 方法による分類：国内開発、国際共同開発・生産、ライセンス国産、輸入、民生品の活用

新しい戦い方や継戦能力の確保等の観点から、今後の防衛装備品の調達においては、上記のうち、ゴシック体の下線部分を拡大すべきというのが提言である。

2. 随意契約の上限引上げ

現行制度上、随意契約には、競争性・透明性の低下といった一般的なデメリットがあるとされるため、例外的な手段と位置付けられている。しかし、装備品の高度化と現場ニーズへの迅速な対応が国家の存立に直結する時代においては、安全保障分野に限って「特定企業の技術に戦略的にフォーカスするための手段」として、随意契約の役割を再定義することが求められている。

具体的には、防衛装備品のうち、新領域装備・研究開発・実証などに限定し、随意契約の限度額を拡大（例：物品の買入れであれば300万円→1,000万円）することにより、随意契約の活用範囲を拡大する。その際、競争性・透明性を担保するため、情報公開や第三者チェック等のガバナンス強化も併せて導入する。

3. 地方調達の上限引き上げ／部隊単位の調達制度の構築

上記措置により随意契約の限度額は引き上げられるところ、これを地方調達においても実施し、あるいは自衛隊の部隊単位で調達できる制度を構築すべきである。

現在の自衛隊が対象とする事態は、冷戦期とは異なり、平時有事の境目は曖昧で、陸・海・空という領域のみならず、サイバー、宇宙、電磁波、認知の領域までをカバーしなければならない。従来のような陸・海・空領域における脅威に対処するのであれば、中央で一括調達することが合理的かつ効率的であるが、様々な脅威に対処するため、自衛隊は従来のような画一的な部隊編成ではなく、多種多様な部隊編成となっている。新たな脅威に対処するため、現場レベルにある程度権限を移して、中央調達品目であっても部隊特有の装備などの調達は、地方調達や部隊ごとの調達とすることが適切である。

4. デュアルユースの活用

以上述べてきたように、随意契約・地方調達の拡大という制度論（需要サイド）に加えて、「どこの、どのような能力を防衛力として取り込むのか」という供給サイド（企業）の視点からの議論も必要である。

現下の安全保障環境の下で求められているのは、①技術力・発想力・迅速な対応力をもった企業のデュアルユース技術の活用、②現場ニーズに即した製品選定・購入プロセスの構築、③そのためのスキームとして地方調達の枠組みを戦略的に位置付けること、である。

(1) 中小企業の活用と現場密着型の装備導入

防衛分野に未参入の中小企業を活用し、育成する意味において、地方の部隊単位で中小企業から装備や訓練資材、また生活資材を購入することができれば、中小企業の迅速な対応力を活用した部隊装備、資材の導入が可能となる。

(2) 製品選定・購入プロセスの改革

従来のような仕様書を先に固定し、紙上での審査で一社を選定するやり方では、現場適合性、運用負荷、整備性、耐久性、ユーザビリティ（隊員の使いやすさ）を十分に把握できないおそれがある。このため複数の競合製品を実戦に近い形で試験運用し、比較・評価するというプロセスの導入が必要である。

(3) 地方調達範囲の拡充と現場主導イノベーション

地方調達は、「中小企業と現場部隊を直接つなぐ役割」や「未来の防衛産業を担う中小企業育成の場」としても再定義すべきである。部隊が自らの裁量で地方調達を活用できる範囲を広げれば、従来の制度では拾いきれなかった多様な中小企業の技術やサービスを、現場レベルで試行しながら取り込むことが可能となる。

1. 米国等の制度の概要

経済安全保障推進法第四章「特定重要技術の開発支援」において、「特定重要技術調査研究機関」としてのシンクタンクは守秘義務を求められている。つまり、経済安全保障に係るシンクタンクにはセキュリティ体制の構築が求められ、それはセキュリティ・クリアランス（SC：Security Clearance）を有する研究員が必要であると解釈される。

米国のシンクタンクにおける実情を見ると、政府系のRAND（ランド）研究所、MITRE（マイター）研究所などFFRDC（連邦研究開発センター：Federally Funded Research and Development Center）¹を運営している機関では、政府指定の「秘」を取り扱うために、セキュリティ管理区域（SCIF：Sensitive Compartmented Information Facility）を設置し、研究員もSCを保有している人を有している。全ての研究が「秘」に該当するわけではないが、いつでも「秘」に該当する研究を実施できる体制を整えている。

一方、CSIS（戦略国際問題研究所）、ハドソン研究所（Hudson Institute）などの非営利民間シンクタンクでは、一般に「秘」に関する研究を行っておらず、組織（シンクタンク）として「秘」を扱う制度・施設を保有していない。他方、研究者個人でSCを持っている人は多くおり、個別に政府の仕事を受けている。このように、米国には組織（シンクタンク）自体が制度・施設を持たなくても個人がSCを保有できる仕組みがある。かかる個人保有に当たっては、個人が直接政府からSCを付与されているのではなく、それを管理する組織が介在する。

さらに、米国の国防科学委員会（DSB：Defense Science Board）は多くの有識者・専門家を集めて安全保障に関する調査分析を行い、報告書を作成している。その報告書はLimited DistributionやSECRETに分類されるものもあり、アクセスするためには適切な資格やSCが求められる。また、これらの調査分析に関わる有識者・専門家は個人の立場で参加しており、所属している組織は契約には含まれていない。このような形態が可能となるのも、個人がSCを保有していることによる。

英国を代表する非営利シンクタンクであるRUSI（Royal United Services Institute for Defence and Security Studies、英国王立防衛安全保障研究所）²は、防衛・安全保障分野を中心に研究を行っている。政府からの委託を受け研究を行っているため、SC保持者が多数存在するとされる。

2. 日本における制度導入の必要性

日本の場合、官庁や防衛関連企業などを退職した場合、自動的にSCは失効する。これは退職により、業務上のNeed to knowが無くなるため、SCが失効するのである。しかしながら、米国におけるSC保持者は個人としての資格であり、SCが必要な仕事（Need to knowが生じたとき）に登用できる仕組みができています。

欧米の場合、SCを持つということは本人にとって、国家へ貢献するという誇りとなっている。日本の経済安全保障シンクタンクに適用する場合、ランド型の国家に直結し秘情報も扱う組織としてのシンクタンクであれば、その組織の職員にSCを与えることとなる。しかし、ハドソン研究所、CSIS型の非営利民間シンクタンクの形を取るのであれば、個人ベースのSCの付与制度も考える必要がある。さらに日本版DSBである防衛科学技術委員会（DSTB : Defense Science & Technology Board）が「秘」に該当する内容を研究するのであれば、どのようにSCを管理し、付与するかについて、新たな制度の構築が必要となる。

一般的に、有識者はリタイアした者が多く、その経験・知見を活用するための制度が必要である。これらの人々を仮に「経験有識者」と呼ぶことにする。

将来的課題の研究・検討に関しては、経験のあるリタイア人材の知見を活用することが適切と考えられる。これら「経験有識者」を活用することで新しいニーズを発掘していくことが可能となるが、その内容によっては「秘」に関連することも含まれると考えられる。

3. 米国の事例と日本におけるセキュリティ対策の見直しの必要性

我が国においての現状は、退職後のごく一部の者にSCを与えている例があるものの、より多くの知見を活用するために現役時代にSCを保有していた者の活用が可能となるようなSCの管理機関と制度を整備すべきである。

2025年11月、トランプ米大統領はAIプラットフォーム構築計画「ジェネシス・ミッション（Genesis Mission）」を発表した³。官民の垣根を超えた強力なパートナーシップを構築するため、米エネルギー省は、OpenAI、Google、Anthropic、NVIDIAを含む24のテクノロジー企業などと提携した⁴。日本は、2026年1月27日、理化学研究所（RIKEN）と富士通が米アルゴンヌ国立研究所及びNVIDIAと覚書を締結した⁵。さらに、2026年6月4日、日本の文部科学省及び経済産業省と米エネルギー省が、日米戦略的パートナーシップに関する意向表明書（SOI：Statement of Intent）に署名した⁶。日米両国で合計10億ドル（約1,600億円）の投資が見込まれ⁷、今後の科学技術協力への大きな足掛かりとなる。

AIジェネシス・ミッションに参加することは、同時に、米国並みの技術管理が求められることである。米国側の研究相手はオークリッジ国立研究所、アルゴンヌ国立研究所、ローレンス・リバモア国立研究所などが含まれており、これらは言うまでもなく核物理の研究を行い核兵器に直結する研究所である。要求される管理体制は一層厳しいものとなろう。

日本においても、セキュリティの観点から管理体制、施設整備、研究者自身のセキュリティの適格性（国籍を含む）などが求められ、管理体制の根本的な見直しが必要となると考えられる。

実施に当たっては、米国政府におけるサイバーセキュリティ確保の肝となるのが「強固な本人確認」、「セキュリティの高いクラウドシステム」、「ゼロトラスト（Zero Trust）⁹の運用」である。具体的には「PIV/CAC⁸」で本人確認→「ゼロトラスト」でアクセス制御→「FedRAMP¹⁰」でクラウドを統一管理、となっており、この三位一体が米国政府のサイバー防衛の中核である。

我が国の政府機関の本人確認システムは未だセキュリティレベルが低く、政府のセキュリティ基準であるISMAP（政府情報システムのためのセキュリティ評価制度）も米国FedRAMP Highのレベルとの関係では大きく劣後するなど、データへのアクセスコントロールは脆弱である。今後、前述の米国の三位一体の例を参考に、日本政府のセキュリティ対策を抜本的に見直していく必要がある。

-
- 1 米国のFFRDCは41機関あり、非政府系機関（大学、非営利団体、又は営利企業）によって運営・管理されている（2025年現在）。ランドは4つのFFRDC、マイターは6つのFFRDCを運営しており、このように一つの機関が複数のFFRDCを運営する場合もある。FFRDCには3種類のタイプがあり、研究開発ラボラトリ（26機関）、研究分析センター（10機関）、システムエンジニアリング及びインテグレーションセンター（5機関）の構成となっている。また、原則としてFFRDCとスポンサーは一対一対応となっている。
 - 2 1831年に英国で創設された「世界最古」のシンクタンク
 - 3 The White House, “Fact Sheet: President Donald J. Trump Unveils the Genesis Mission to Accelerate AI for Scientific Discovery”, November 24, 2025, <https://www.whitehouse.gov/fact-sheets/2025/11/fact-sheet-president-donald-j-trump-unveils-the-genesis-mission-to-accelerate-ai-for-scientific-discovery/>（2026年9月15日閲覧）
 - 4 U.S. Department of Energy, “Energy Department Announces Collaboration Agreements with 24 Organizations to Advance the Genesis Mission”, December 18, 2025, <https://www.energy.gov/articles/energy-department-announces-collaboration-agreements-24-organizations-advance-genesis>（2026年9月16日閲覧）
 - 5 理化学研究所「理化学研究所、アルゴンヌ国立研究所、富士通、NVIDIAが先端的HPC/AIの推進で協力」2026年1月27日、https://www.riken.jp/pr/news/2026/20260127_1/index.html（2026年9月15日閲覧）
 - 6 文部科学省「日本のAI for Scienceの取組と米国の「ジェネシス・ミッション」との連携に向けた日米戦略的パートナーシップについて」2026年6月4日、https://www.mext.go.jp/a_menu/kagaku/kokusai/kyoryoku/mext_00015.html（2026年9月15日閲覧）
 - 7 日本経済新聞「米のAI国家戦略に日本参加、両政府が5年で1600億円投資」2026年6月1日、日本経済新聞電子版、<https://www.nikkei.com/article/DGXZQOSG010CG0R00C26A6000000/?msocid=0634a583dce461d125b8b287dde160f4>（2026年9月15日閲覧）
 - 8 PIV（Personal Identity Verification）/CAC（Common Access Card）。連邦職員（PIV）と軍人・国防総省職員（CAC）が使う米政府公式のICカード型ID。物理入館・PCログイン・システム認証を一体化した強力な本人確認。
 - 9 「誰も信用しない」を前提に、全てのアクセスを継続的に検証する米政府標準モデル。2021年の大統領令で全省庁にZero Trustの導入方針が示され、2022年には2024会計年度末までのZero Trust目標達成が義務付けられた。
 - 10 米連邦政府がクラウドサービスを使う際の統一セキュリティ認証制度。AWS・Azure・Googleなど、米連邦政府にクラウドサービスを提供したい事業者はFedRAMP認証取得が必須。

官民の研究者の交流の促進

1. 研究者の官民交流の現状

現在、防衛装備庁には技術戦略部及び各研究所において、研究職技官が数多く勤務している。同様に、防衛産業においても多くの研究者が勤務しており、防衛省の研究開発事業や各企業が独自に実施している自主研究に従事している。

かかる研究者を含む公務員と民間との間の人事交流に関しては、「国と民間企業との間の人事交流に関する法律」（官民交流法）により、制度的には可能となっている。防衛省を例に取れば、防衛省の職員が民間企業で一定期間雇用される「交流派遣」、逆に民間企業の者が防衛省で一定期間業務に従事する「交流採用」が設けられており、実際に、防衛省のサイバー担当部局や戦略策定部門において民間企業の者が勤務する（交流採用）という実績がある。

しかしながら、防衛装備品の研究開発業務に従事する研究職技官については、交流派遣も交流採用も未だ実績がない。研究職技官は、制度上、「交流派遣」の場合、①防衛省との間の契約の締結又は履行に関する業務、②防衛省に対する折衝又は防衛省からの情報の収集を主として行うこととなる業務、に従事できないこととされている。さらに、防衛省に復帰後、派遣先企業であった民間企業との間の契約の締結又は履行に関する事務をその職務とする官職には就けないこととされている。「交流採用」の場合は、防衛省において交流元企業との間における契約の締結又は履行に関する事務をその職務とする官職には就けず、民間企業復帰後2年間は①防衛省との間の契約の締結又は履行に関する業務、②防衛省に対する折衝又は防衛省からの情報の収集を主として行うこととなる業務、には従事できないこととされている。

さらに、官民人事交流の公平性・透明性の確保のため、一定の交流基準が定められており、交流をしようとする日前5年間にかかる年度のいずれかの年度において国の機関と特別契約関係（契約総額が2,000万円以上かつ当該企業の売上額に占める割合が25%以上（大企業は10%））にあった企業とは人事交流は行えず、さらに、交流をしようとする日前5年以内に、国の機関と民間企業との間の契約の締結又は履行に携わった期間のある国の職員又は民間企業との間の人事交流もできないこととされている。

2. 問題の所在

このように現在の官民交流法は、規制する側と規制される側の利益相反という観点からの制約や、透明性・公正性の確保のための制約が多く設けられているといえる。

他方、防衛省の研究職技官や民間の防衛産業の研究者の場合、艦艇、航空機、ミサイルといったように分野ごとに専門性を有し、かつ基本的に管理職となるまでは当該分野において人事上も垂直管理されることとなる。このような事情に加え、防衛省の研究開発事業に関しては、その事業内容や契約内容等を防衛省の研究職技官自らが精査・策定した上で、民間企業の研究者はその契約に基づき、当該研究開発事業に従事することとなる。このように官民双方の研究者は、研究開発事業の契約の締結や履行に関与し、さらに民間の研究者については、専門性を有する分野についての防衛省との折衝や防衛省からの情報収集にも従事することとなる。したがって、現在の官民交流制度では研究者の交流については制度上可能であっても、実態的にはハードルが高い状況といえ、実際に前述のように研究者の交流実績はない。

防衛装備庁は防衛産業関係者との意見交換の場を設けているが、かかる場において、企業側から研究者の相互交流について積極的に進めてほしい旨の意見表明がなされたことがある。特に企業側の研究者にとって、自衛隊の運用ニーズを踏まえた研究開発の更なる推進のためには、防衛装備庁の研究部門において一定期間勤務し、防衛省・自衛隊の研究開発に係る意思決定プロセスやその運用上のニーズや背景等を知る機会を得ることは、民間企業の研究者のキャリアパスにとって有益なことと考えられる。また、防衛省の研究者にとっても、民間企業の研究開発業務の実態やいかなる研究分野を自主的に取り組んでいくかといったような民間企業側の実態を知ることは、防衛省研究職技官のキャリアパスにとっても有益であるといえる。このように官民研究者の人事交流の促進は、双方にとってウィンウィンの関係となるといえる。

3. 解決の方向性

「国と民間企業との間の人事交流に関する法律」（官民交流法）における第1条の目的規定には、「交流派遣」について、行政の課題に柔軟かつ的確に対応するために必要な知識及び能力を有する人材の育成を図ること、「交流採用」について、行政運営の活性化を図ることを規定しているが、これらの規定はいずれも民間企業側が「効率的かつ機動的な業務遂行の手法」を有していることを前提としている。少なくとも防衛装備品の研究開発業務に携わる官民の研究者にとっては、現在の安全保障環境に適した防衛装備品を可能な限り早く取得するための研究開発に主眼が置かれていることから、官民交流は研究者育成のための一手段と捉えるべきである。

かかる観点から、一般法たる官民交流法の特別法として、研究者を対象とした「研究者官民交流法（仮称）」を制定し、利益相反防止に力点を置いた各種制限事項を研究者については廃止することで、官民の交流を更に活性化させていくべきである。

他方、規制する側と規制される側の公平性・透明性は、本来の目的を損なわない範囲で制度上担保される必要はある。現在、防衛省においては人事交流の計画について、人事関係の審議会に付議し認定を受けることとなっている。研究者の官民交流に関しては、交流採用者又は交流派遣者が防衛省と派遣先又は派遣元の企業との間の契約業務に関与する又は契約の履行業務に従事する場合には、第三者機関たる調達関係の審議会に付議して不正な点はないか等、外部の視点でチェックを受けるといった方策を導入する。これにより、公平性・透明性の担保を図ることとする。

(空 白)

1. 宇宙空間の重要性

国家安全保障において、宇宙空間の利用は既になくってはならない空間であり、今日では戦闘補助空間というよりも、戦闘を行う空間として認識され始めている。また、最近ではStarlinkに代表されるように、低軌道コンステレーション型の小型多数衛星による衛星通信が活用され、打ち上げられている。一方、近年宇宙デブリ（ゴミ）が増大し、宇宙空間の安定的利用への脅威となっている。大量の小型衛星が打ち上げられ、それが廃棄されることにより、宇宙デブリ問題はますます顕在化してくることは否めない。

2. 宇宙デブリ対策

宇宙デブリ対策としては、各国でデータの収集が進んでいる。米国では、宇宙軍が運用する宇宙監視ネットワーク（SSN：Space Surveillance Network）が構築されており、宇宙デブリを含めた観測データを世界に提供している。我が国においては、従来JAXA（国立研究開発法人宇宙航空研究開発機構）が宇宙デブリの観測を行い、宇宙状況把握（SSA：Space Situational Awareness）データとしてユーザーに提供してきた。JAXAの美星スペースガードセンター（岡山県、光学望遠鏡）は、主に静止軌道付近のデブリ監視を、上斎原スペースガードセンター（岡山県、レーダー望遠鏡）では、主に低軌道上のデブリ観測を行っている。2020年、防衛省・自衛隊に宇宙作戦隊（現在の宇宙作戦団）が創設されたことに伴って、防衛省が運用の主体となり、JAXAは高精度観測データと技術を提供する基盤となった。両者のシステムを政府として統合し、内閣府が政策統合、防衛省が運用統合を担い、さらに、防衛省は宇宙を宇宙領域把握（SDA：Space Domain Awareness）として捉え、安全保障の戦略領域として扱うことになった。なお、防衛省は、山口県に宇宙監視レーダーを整備している。

3. 問題の所在

天文学者は天体観測データのうち、自分の研究に必要なデータだけを取り出して使う。他のデータは研究には使われない「ノイズ扱い」である。その中には、多数の人工物体（人工衛星）の画像データが含まれている。これらのデータはSDAにとって貴重なデータであるものの、使われることなく眠っている。日本では、天文学者が国家安全保障への協力に消極的であるという問題があり、SDAのためにこれらのデータを活用しようとしても、「防衛関連には使わせない」として、天文台から提供を拒否され、貴重なデータは死蔵されている。

国民の税金で観測したデータを宇宙の安定利用のため使うことを拒否していることは、天文台が宇宙安全保障利用＝経済安全保障に協力しないこととなる。天体観測データは研究者の独占物ではない。国民の安全・安心のため、積極的に活用すべきである。

4. 解決の方向性

東京大学のトモエゴゼン計画（東京大学大学院理学系研究科附属天文学教育研究センター木曽観測所）では、木曽シュミット望遠鏡用モザイクCMOSカメラを用いた観測を行っている。2019年9月に完成し、広視野かつ高頻度の動画サーベイと高速モニタリング観測を実施中である。日本天文学会が発刊している天文学辞典には「トモエゴゼンのデータには空で発生するイベントが網羅的に含まれるため、地球高層大気の研究、宇宙機や宇宙デブリの状況の把握、リアルデータによる教育・普及など広範囲の分野間連携につながる宇宙科学の展開が期待される。」と述べられている¹。トモエゴゼン計画関連の研究報告では、「地球接近天体や多くの未カタログデブリの検出ができること判明」している。「…Tomoe Gozenカメラからのデータに適用して地球接近天体の早期発見や太陽系の起源の解明、宇宙デブリ問題の解決に役立てていきたい。」²と述べられており、天体望遠鏡による観測データが天文学と同時に地球防衛や宇宙安全保障にも資するとしている。

宇宙空間の利用は人々の毎日の生活にも欠かせないものとなっている。宇宙利用が進めば進むほど、大量の人工衛星が打ち上げられ、その副次的影響として宇宙デブリの増加は否めない。宇宙の安定的利用のためには、宇宙デブリの観測が喫緊の課題であり、将来的にはデブリ除去が必要となる。

我が国において宇宙デブリの監視は、防衛省とJAXAの役割分担により政府に統合化されたが、観測体制は決して十分とはいえない。それを補完するためには、天体観測データの活用をすべきである。

天体観測データには「ノイズ」とでもいうべき宇宙デブリの軌跡が含まれている。このノイズとして利用されないデータを宇宙デブリ監視のデータとして活用すべきである。我が国が天体観測を行っている天文台のデータを防衛省に提供することにより、宇宙デブリ監視に役立てるための制度を整備すべきである。

参 考

日本の代表的な天文台は、以下に示すように多数あり、これら全ての観測データが宇宙監視のために活用できる。

(1) 研究系・大型観測施設

国立天文台（NAOJ）三鷹キャンパス（東京都）、水沢キャンパス（岩手県）、野辺山電波観測所（長野県）、東京大学木曽観測所（長野県）等

(2) 地域の天文台・公開施設

月光天文台（Gekko Observatory、静岡県）、飛騨天文台（京都大学、岐阜県）、久万高原天文台（Kuma Kogen Observatory、愛媛県）、西はりま天文台（兵庫県）、佐治天文台（Saji Observatory、鳥取県）、仙台市天文台（宮城県）等

(3) 日本の「海外設置」天文台

すばる望遠鏡（Subaru Telescope、アメリカ・ハワイ州）、アタカマ大型ミリ波サブミリ波干渉計（ALMA、チリ・アタカマ高地。国際共同プロジェクト：日本・北米・欧州など）、TA（テレスコープアレイ）実験（アメリカ・ユタ州。日本（東京大学など）・米国・韓国の共同）、CTA（チェレンコフ望遠鏡アレイ）計画（チリ：南サイト、スペイン・カナリア諸島：北サイト）

-
- ¹ 公益社団法人日本天文学会『天文学辞典』「トモエゴゼン」<https://astro-dic.jp/tomoe-gozen/>（2026年9月16日閲覧）
 - ² 柳沢俊史・黒崎裕久・Manuel CegarraPolo・吉川真・黒田信介・平子敬一（JAXA）・大澤亮・酒向重行（東京大学）・吉田二美（産業医科大学）・奥村真一郎（JSGA）「重ね合わせ法による高速移動天体の発見観測」2021年度プラネタリーディフェンス・シンポジウム. JAXA. 2021年. https://www.spaceguard.or.jp/RSGC/results/sgr13pdfs/07_PDC2021_T-Yanagisawa.pdf（2026年9月16日閲覧）
満田和真・酒向重行・Tomo-e Gozenプロジェクト「東京大学トモエゴゼンの科学観測データを活用したスペースデブリ監視の取り組みについて」2025年. <https://cir.nii.ac.jp/crid/1390303090624446720>（2026年9月16日閲覧）

公益財団法人 笹川平和財団 経済安全保障技術・産業力強化戦略研究会

政策提言

**科学・技術・産業・安全保障のエコシステム構築
－日本の総力を挙げた国家安全保障の実現を－**

発行 2026年10月

発行者 公益財団法人 笹川平和財団

〒105-8524 東京都港区虎ノ門1-15-16 笹川平和財団ビル

電話：03-5157-5430 | URL：https://www.spf.org

本書に掲載している各提言の見解は執筆者個人のものであり、所属機関および笹川平和財団の見解を代表するものではありません。
無断転載、複製および転訳載を禁止します。引用の際は本報告書が出典であることを明記してください。

 笹川平和財団