

防衛と民間の デュアルユース徹底調査

市場・技術・各国政策・企業モデル・知財／輸出管理・責任ある利用

結論を一文で

デュアルユースの競争力は、汎用技術そのものではなく、政府を含む複数市場で同じ技術コアを再利用し、実証・量産・データ・知財・安全保障管理を一つの事業システムとして回せるかで決まる。

エグゼクティブ・リサーチレポート

調査基準日 2026 年 8 月 14 日 | 公開情報のみ

エグゼクティブ・サマリー

本調査は、ユーザー提供の3本の記事を出発点に、2026年8月14日時点の政府・国際機関・企業開示などの一次資料で検証した。結論は、デュアルユースを「軍でも民間でも使える技術の一覧」とみるだけでは不十分であり、需要、実証、量産、データ、知財、資本、人材、輸出・情報保全、責任ある利用を結ぶ事業システムとして設計すべき、ということである。 ^{〔A1〕}

〔A2〕 〔A3〕

- 【確認済み】 公的文書・法令・企業の法定開示等で裏付けられる事項。
- 【試算】 外部推計または本レポートの計算。前提を明示し、実測値・公的予測と区別する。
- 【分析】 複数資料から導く解釈・提言。事実そのものではない。

01 技術ではなく循環 民生→防衛（spin-on）と防衛→民生（spin-off）を、実証・人材・標準・供給網まで含めて循環させる。	02 500兆円の読み方 2040年451兆円（約500兆円）は5つの広い隣接民生市場を合算した強気TAMであり、防衛市場の公式予測ではない。
03 米国の更新 米国の重点技術は2025年11月に14技術群から6つの任務志向CTAへ再編。旧14分野は歴史資料として扱う。	04 日本の転換点 FY2026は研究開発約7,095億円、装備移転は全完成品等を制度上原則可へ。ただし専用予算・輸出実績とは同義でない。
05 勝ち筋 汎用コア＋任務別アダプター＋保護データ層に分け、同じコアを複数市場で再利用する。現場実装力が模倣困難性をつくる。	06 死の谷 試作件数より、量産予算・ユーザー受入れ・認証・保守・資金繰りがボトルネック。入口資金だけでは移行率は上がらない。
07 知財は権利の束 特許だけでなく、データ、重み、ソース、API、試験証拠、更新権、製造ノウハウを資産単位で管理する。	08 管理は成長基盤 輸出・秘密・研究セキュリティ・責任あるAIを設計初期から組み込み、後工程の停止や市場分断を防ぐ。

意思決定者が押さえる4つの問い

問い	誤りやすい見方	判断基準
どの市場か	防衛予算、隣接民生TAM、企業売上、投資額を足す	予算／契約上限／実支出／売上／資金調達／TAM／GVAを分離
何を共通化するか	軍民の全仕様を一体化する	汎用コアは共通、任務・秘密・輸出管理部分は分離
何を守り、何を開くか	全て特許化、又は全て秘匿	IF・試験法は開き、モデル・データ・工程・校正値は閉じる
いつ止めるか	完成後に法務・輸出審査	用途確定前からG0-G7のゲートで再判定

本レポートの実務的な答え

政府は「ミッション提示→90 日級の契約→試験環境→移行予算→量産」の一貫経路をつくる。企業は「共通コア→モジュール境界→IP／データ台帳→管理組込み→民生還流」の順で設計する。評価は試作件数ではなく、移行率、実支出、現場稼働、民生売上、更新速度、安全・遵守実績で行う。

目次

章	内容
1	デュアルユースの定義と分析枠組み
2	なぜ今なのかー世界の需要・資本・技術サイクル
3	市場規模をどう読むかー『2040 年 500 兆円』の検証
4	重点技術ポートフォリオ
5	企業モデルーPalantir、Anduril ほか
6	各国モデルと日本の制度的位置
7	知財・データ・契約・標準化
8	輸出管理・情報保全・研究セキュリティ・責任ある AI
9	政策提言と企業実行計画
10	2040 年シナリオと結論
付録	記事ファクトチェック／ステージゲート／出典

注：目次は文書内の論理構成を示す。ページ番号は閲覧環境による再レイアウトを避けるため付していない。

1. デュアルユースの定義と分析枠組み

デュアルユースとは、同じ製品が軍と民間で使われることだけを指さない。技術、部品、ソフトウェア、データ、研究人材、試験手法、標準、製造設備、保守網が、民生と安全保障の間を双方向に移動する現象である。しかも、規制上の『デュアルユース』は品目の固定属性ではなく、用途、需要者、提供方法、統合先、地域、版数によって変わる。^{〔27〕} ^{〔31〕} ^{〔32〕} ^{〔34〕}

1.1 四つの経路

経路	意味	代表例	事業上の要点
Spin-on	民生技術を防衛へ取り込む	クラウド、AI、商用衛星、ドローン、電池	民間の速度・量産・価格を保ちつつ、耐環境・秘密・任務保証を追加
Spin-off	防衛起点の成果を民生へ展開	堅牢通信、PNT、耐環境設計、危機時指揮	軍仕様をそのまま売らず、規制・コスト・UX を民生向けに再設計
Spin-around	初めから軍民の共通課題を共同開発	災害・物流ロボ、海底監視、分散電源	共通コアと用途別レイヤー、複数アンカー顧客、共通試験法
Dual-market	同じ技術コアを別製品として継続販売	Palantir のデータ基盤、SAR 解析、サイバー	売上・データ・学習効果を分散し、単一予算依存を下げる

1.2 三層アーキテクチャ

層	共有度	典型資産	設計方針
共通コア	高	OS、データモデル、センサ処理、通信、電源、製造工程	広い市場で再利用。標準 IF、サイバー・バイ・デザイン、版管理
任務アダプター	中	任務ロジック、耐環境、HMI、規制・認証、特殊部品	顧客別だがモジュール化。コアへの個別仕様混入を防ぐ
保護データ／運用	低	機密データ、標的・脅威情報、鍵、校正值、戦術・運用ログ	環境分離、最小権限、輸出・再移転・利用目的を厳格管理

分析

最も収益性が高いのは『軍用品を民生にも売る』ことではなく、共通コアの研究・製造・更新費を複数市場で回収し、任務固有部分だけを切り替えられる構造である。逆に、全顧客仕様をコアへ直書きすると、認証・秘密・輸出規制が民生版へ伝染し、成長を止める。

1.3 波及効果は自動ではない

防衛需要が産業成長を生むためには、次の五つの変換が必要である。

1. **需要変換**：部隊・行政の課題を、企業が解ける非機密のミッション仕様へ翻訳する。
2. **技術変換**：民生技術に耐環境性、信頼性、セキュリティ、相互運用性を付加する。
3. **契約変換**：試作契約を量産・保守・更新予算へ接続し、資金繰りを切らさない。
4. **市場変換**：防衛で得た検証証拠・人材・標準を、災害、物流、製造、医療、海洋等へ移す。
5. **管理変換**：秘密・輸出・倫理の制約を製品構成に埋め込み、民生版を隔離して拡張する。

2. なぜ今なのかー世界の需要・資本・技術サイクル

2.1 需要側：安全保障支出とレジリエンス投資

SIPRI による 2025 年の世界軍事支出は 2 兆 8,870 億ドル（実質前年比 2.9%増）、世界 GDP 比 2.5%。米国 9540 億ドル、中国 3360 億ドル、NATO 合計 1 兆 5,810 億ドルとされる。日本は 622 億ドル、実質 9.7%増、GDP 比 1.4%であった。NATO の 2025 年ハーグ合意は、2035 年までに GDP 比 5%（中核防衛 3.5%以上、インフラ・サイバー・レジリエンス等最大 1.5%）を目標とし、『防衛』と『民生インフラ』の政策境界を広げた。〔1〕〔2〕

注意

軍事支出は需要の背景であって、デュアルユース市場の売上ではない。予算額、契約上限、支払済額、企業売上、民間資本、TAM、経済波及額は相互に合算しない。

2.2 技術側：商用サイクルが戦力化を先導

AI、クラウド、半導体、衛星、無人機、通信、サイバー、バイオでは、商用市場の研究開発と量産サイクルが防衛専用品より速い。防衛当局は『自ら発明する』比率を下げ、民間の成熟技術を短期に評価・統合・更新する能力を競っている。ウクライナ等で示された低価格無人機、ソフトウェア更新、分散通信、商用衛星データの有効性は、この転換を加速した。

- **ソフトウェア定義**：性能がハードの交換より、データ・モデル・コードの更新で改善する。
- **量産性**：少数の最高性能品だけでなく、安価・大量・消耗前提のシステムが必要になる。
- **相互運用性**：単体性能より、センサ、通信、意思決定、効果器を結ぶインターフェースが価値を持つ。
- **レジリエンス**：平時効率だけでなく、妨害、断絶、災害、供給停止でも動く能力が民生にも求められる。

2.3 米国の重点技術は 14 から 6 へ

添付記事が参照する米国防総省の 14 Critical Technology Areas（2022 年）は、Trusted AI & Autonomy、Space、Integrated Sensing & Cyber 等を並べた技術別分類である。しかし OUSD(R&E)は 2025 年 11 月 17 日、6 分野へ再編した。これは旧分野の単純廃止ではなく、AI-first、争奪環境の兵站、情報優越、量産可能な指向性エネルギー・極超音速という『任務成果とスケール』に束ね直したものと読むべきである。 [3] [4] [5] [A2]

現行 6 CTA	中心課題	旧 14 との関係（本調査の分析）
Applied AI	意思決定・自律・開発／運用の AI 化	Trusted AI & Autonomy、Advanced Computing & Software、HMI を横断
Biomanufacturing	バイオ製造、材料、医療・供給能力	Biotechnology に製造・材料要素を統合
Contested Logistics	妨害・攻撃下の輸送、電力、修理、供給	Energy/Storage、Materials、製造、無人化を横断
Quantum & Battlefield Information Dominance	量子、通信、センシング、サイバー、宇宙/PNT	FutureG、Network SoS、Sensing/Cyber、Space、Microelectronics 等を束ねる
Scaled Directed Energy	指向性エネルギーの量産・配備	Directed Energy をスケール重視へ
Scaled Hypersonics	極超音速の量産・配備	Hypersonics をスケール重視へ

注：米政府は旧 14 と新 6 の一対一対応表を公表していない。上表 3 列目は本調査の分析であり、OSC 等の投融資適格範囲が 6 分野だけに縮小したことを意味しない。 [9]

2.4 米国の『研究→試作→量産→資本』

米国の強みは単一機関ではなく、DARPA、SBIR/STTR、In-Q-Tel、DIU、Office of Strategic Capital、各軍プログラムが異なるリスクを分担する点にある。DIU は FY2016～2023 に 450 件の試作契約を扱い、完成試作の 51%が量産へ移行したと自己報告する一方、量産契約 55 億ドルは契約上限であり、実支出・企業売上ではない。GAO は契約の 85%が 90 日目標を超え、平均約 172 日だったと指摘した。 [6] [7] [8] [9]

Defense Innovation Board は、2021 年以降の防衛テック新興企業への民間資本を 1,300 億ドル超としながら、量産規模を実証し始めた企業は『少数』にとどまると分析する。資金流入と調達移行は同義ではなく、R&D 予算と 2〜3 年前に編成される量産予算の時間差が『死の谷』をつくる。^{〔10〕}

3. 市場規模をどう読むかー『2040 年 500 兆円』の検証

3.1 結論：防衛市場ではなく、5 つの隣接民生市場の強気 TAM

添付記事の数値は、2025 年 24 兆円から 2040 年 451 兆円、CAGR 21.6%であり、本文では『約 500 兆円』に丸められている。対象は①産業別フィジカル AI 実装、②ソブリンクラウド・産業データ統合、③高速・高信頼通信インフラ、④高速宇宙通信網、⑤海洋インフラ監視・海洋データ産業である。これは Arthur D. Little による潜在市場シナリオであり、米国政府や統計機関が公表した防衛デュアルユース市場ではない。^{〔A1〕 〔A2〕}

【算術確認】24 兆円×(1+21.6%)^15=451.0 兆円。記事の CAGR と終点は整合する。

【未開示】各市場のドル原典、為替、名目／実質、地域範囲、売上／投資、重複除去方法。

【評価】中心予測ではなく、重複を含み得る広義 TAM の強気上限として利用する。

3.2 二重計上と定義リスク

論点	なぜ重要か	安全な表記
対象重複	AI 端末、通信、クラウド、衛星、解析が同じ売上を含み得る	『5 関連市場の単純合算、重複排除未確認』
市場と投資	設備投資、サービス売上、政府支出、企業価値は別指標	指標種類を列で分け、合算しない
名目／実質	15 年ではインフレだけでも大差が出る	価格基準年と物価前提を明記
為替	451 兆円は換算レートでドル値が大きく変わる	原通貨と換算レートを併記
地域範囲	『米国市場』に国外売上・供給網が含まれる可能性	国内売上／企業売上／最終需要の区分を確認
比較対象	451 兆円は 1 ドル 150 円で約 3.0 兆ドル、世界軍事支出に近いが分類が違う	規模感の参考に留め、比較・合算しない

CBO が示す米国名目 GDP の長期成長率は概ね年 3〜4%台であり、21.6%が 15 年間続く仮定は経済全体を大幅に上回る。新市場の立上がりとして不可能とはいえないが、定義拡張・価格・普及率・競争による成長鈍化を織り込む必要がある。^{〔43〕}

3.3 CAGR 感応度

2025→2040 CAGR	2040 年規模 (24 兆円起点)	読み方
10.0%	100.3 兆円	高成長だが経済全体との差は比較的小さい

2025→2040 CAGR	2040 年規模（24 兆円起点）	読み方
15.0%	195.3 兆円	複数の新市場が同時に立ち上がる強気ケース
20.0%	369.8 兆円	長期継続には大規模な価格・用途・地理拡張が必要
21.6%	451.0 兆円	記事の試算。『約 500 兆円』の算術的根拠
25.0%	682.1 兆円	極端な上限。定義拡張・重複の影響が支配的

3.4 日本の 8.6 兆円／16.8 兆円シナリオ

添付記事は、日本の 5 関連市場を 2025 年約 2.0 兆円、2040 年 8.6 兆円（現状延長、年率約 10.2%）とし、防衛投資・技術／人材移転によって米国型の成長軌道に近づく場合 16.8 兆円まで拡大すると試算する。上振れ 8.2 兆円は政府予測でも因果推定でもなく、政策効果を仮定したシナリオ差である。^[A1]

シナリオ	2040 年	含意／成立条件
制約ケース（本調査）	4.2 兆円	2 兆円起点で年率 5%。試作止まり、データ・輸出・人材・量産の制約が残る
記事ベースライン	8.6 兆円	年率約 10.2%。現行の民生市場成長が継続
記事アップサイド	16.8 兆円	年率換算約 15.2%。政府需要、移行予算、人材、民間展開が同時に機能

注：制約ケースは比較用の本調査試算。すべて名目・実質や為替等が統一された公式予測ではなく、投資判断には分野別ボトムアップの SAM/SOM 検証が必要である。

3.5 波及効果を測る KPI

段階	入力 KPI	成果 KPI
研究	採択額、民間共同負担、研究者・特許	技術成熟、再現性、公開／秘匿の適切性
試作	契約数、契約日数、試験環境	現場評価、性能・単価、次段階移行率
量産	移行予算、発注数量、製造能力	実支出、納期、可動率、原価低下、供給網冗長性
民生還流	共通コア比率、標準・認証、人材移動	民生売上、輸出、民間投資、災害・生産性成果
ガバナンス	審査日数、台帳網羅率、教育	違反・事故・用途逸脱、更新再審査、是正時間

4. 重点技術ポートフォリオ

添付記事の 5 重点領域は、2026 年日本成長戦略の 17 分野と広く接続し、国際的な重点とも整合する。ただし、投資対象を『AI』『宇宙』のような名詞で選ぶと範囲が広すぎる。防衛と民生の双方に共通するミッション、再利用可能なコア、試験可能な成果で絞る必要がある。^{〔A1〕}

〔23〕 〔26〕 〔27〕

4.1 添付記事の 5 重点領域

重点領域	防衛ミッション	民生ミッション	共通コア／主なボトルネック
① フィジカル AI・自律システム	無人偵察、輸送、対処、群制御、危険作業	物流、点検、建設、農業、災害救助	認識・航法・制御・電源・量産／非 GPS、通信断、停止、安全ケース
② 多様データ統合・セキュリティ	C2、ISR、意思決定支援、兵站、サイバー	製造、医療、金融、重要インフラ、行政	オントロジー、データ権限、MLOps、監査／データ権原、ロックイン、敵対入力
③ 抗たん性通信	メッシュ、低帯域、妨害下通信、水中通信	災害、離島医療、遠隔保守、海洋 IoT	無線・光・海中、エッジ、時刻同期／周波数、相互運用、暗号更新
④ 航空・宇宙／衛星インフラ	SATCOM、PNT、SDA、ISR、データ中継	観測、防災、通信、航海、金融時刻	小型衛星、光通信、地上局、解析／軌道・周波数、打上げ、再輸出
⑤ 海上・海中センシング	MDA、UUV/USV、海底状況把握	海底ケーブル保守、資源、環境、洋上設備	ソナー、磁気・光、航法、長期電源／通信、回収、海況データ、責任

4.2 補完すべき 5 領域

補完領域	デュアルユース価値	閉じるべき資産	主要ガードレール
半導体・フォトニクス	エッジ AI、レーダー、通信、宇宙、電力の全てを支える	PDK/GDS、工程条件、歩留まり、テスト	輸出管理、トラステッド製造、長期供給、第三者 IP
量子・PQC	非 GPS 航法、高感度計測、時刻、暗号移行	素子工程、校正、制御、誤り訂正	誇大 TRL、国外クラウド、長期秘匿データの収穫後解読
エネルギー・先端材料	分散電源、無人機航続、耐熱・軽量、AM、修理	組成、熱処理、粉末、製造ファイル	重要鉱物、人権・環境、危険物、供給途絶
バイオ・医療	CBRN 監視、現場診断、外傷救護、バイオ製造	配列、細胞株、試料、製造プロセス	BWC/CWC、DURC、バイオセーフティ、個人・遺伝情報
デジタル製造・造船	デジタルツイン、自動溶接、AM、整備・補給	設計、工程、品質・故障データ	サイバー、認証、設計データ輸出、単一サプライヤー

4.3 優先順位の付け方

軸	高評価の条件	警戒シグナル
共通課題	災害・物流・医療等にも同じ性能指標がある	防衛固有仕様だけで価値が成立
コア再利用率	製品原価・コード・データ処理の 60～80%を共有可能	顧客ごとに別設計・別認証・別供給網
検証可能性	6～18 か月で実環境の証拠を得られる	試験データ・ユーザー・環境がない
量産学習	民生数量が品質・原価・供給網を改善	小ロット専用品で学習曲線が働かない
管理分離	秘密・輸出管理対象をモジュール単位で隔離	コア全体が規制・機密化する
顧客ポートフォリオ	防衛、他省庁、重要インフラ、海外同盟国がある	単一プログラム・単年度予算に依存

ポートフォリオ原則

『最高性能』だけでなく、①低コスト大量、②更新速度、③通信・PNT 断絶下、④相互運用、⑤保守可能性、⑥サプライチェーン継続を評価する。民生側の量産学習が防衛側の価格・可用性を改善する領域を優先する。

5. 企業モデルーPalantir、Anduril ほか

5.1 Palantir：データモデルと現場実装が堀になる

Palantir は 2003 年創業。Gotham（政府・防衛）、Foundry（企業データ基盤）、AIP（生成 AI／AI 運用）、Apollo（継続配備）を展開する。中核はデータを単に集めることなく、人、物、場所、事象、権限、業務ルールの関係性を『オントロジー』として表現し、意思決定・行動につなげることにある。Deployment Strategist と Forward Deployed Engineer が現場に入り、短い反復で運用へ組み込む点も重要である。^{〔A3〕} ^{〔39〕}

2025 年確認値	数値	読み方
売上	44.75 億ドル	前年比 56%増。市場評価ではなく実績売上
政府／商用	54%/46%	政府 24.02 億ドル、商用 20.73 億ドル。二市場モデルが定量確認可能
米国顧客比率	74%	米国依存と高成長の双方を示す
従業員	4,429 人	売上／人は約 101 万ドル。ソフトウェア型の高いスケール性
残存契約価値	112 億ドル	全オプション行使を仮定し、解約可能。確定売上ではない

防衛で鍛えられた異種データ統合、権限管理、監査、低帯域・複雑環境への配備は、製造、物流、金融、医療へ展開できる。一方、機密契約、政府の任意解約、政府による成果利用権、セキュリティ・クリアランス、人権・プライバシーへの批判は、同社自身が 10-K でリスクとして開示する。 [39]

Palantir からの教訓

模倣すべきは『AI 製品』の名称ではなく、①共通データモデル、②役割・権限を含む運用設計、③現場常駐による短期反復、④継続更新、⑤政府と商用の売上バランスである。現場導入プロセス自体が無形資産になる。

5.2 Anduril : VC 型経営で防衛専用サイクルを短縮

Anduril は Lattice を自律システムの指揮・制御・センサ統合基盤とし、無人機、対無人機、監視塔、海中システム等を垂直統合する。2026 年 5 月の Series H で 50 億ドルを調達した。重要なのは、民生売上が大きい真正な二市場企業というより、商用技術スタック、VC 資本、ソフトウェア開発手法、量産工場を防衛専用市場へ持ち込む『defence-first / commercial-method』モデルである点だ。 [40] [41]

- **強み**：製品先行開発、自己資金リスク、ソフトとハードの一体更新、量産前提の設計。
- **弱み**：大型量産契約への集中、資本集約、任務・輸出・倫理リスク、顧客による仕様・予算変更。
- **民生展開**：Lattice を公共安全・重要施設等へ応用できるが、監視・プライバシーの統治が必要。 [41]

5.3 代表的な四つの企業型

企業型	代表例	価値創出	主要リスク
共有基盤型	Palantir、サイバー企業	同じデータ／セキュリティ基盤を政府・企業で再利用	データ権利、ロックイン、監視、人材・信用
民生先行スピニン	SpaceX/Starshield、商用 SAR	商用量産・打上げ・解析を国家安全保障へ	容量優先、政府依存、再輸出、宇宙責任
防衛先行 VC 型	Anduril、Helsing	民間資本とプロダクト開発で取得サイクルを短縮	量産需要、評価額期待、集中、倫理
真正二市場ハード	測量／農業ドローン、海洋ロボ、電池	共通部品・工場・試験で原価と品質を学習	規制伝染、仕様分岐、低粗利、供給網

SpaceX の Starshield は、Starlink の小型衛星量産、再使用打上げ、ネットワーク運用を国家安全保障用途へ転用する民生先行型である。ここでも技術そのものより、製造・打上げ・地上運用を一体化した産業能力が参入障壁となる。 [42]

5.4 日本企業への含意

日本はセンサ、材料、半導体部材、ロボット、造船、精密製造、通信、宇宙・海洋に厚い技術基盤を持つ一方、政府ユーザーへの近接、ソフトウェア製品化、非機密データ、迅速契約、長期成長資本、海外保守網が弱い。大手プライムだけで閉じず、スタートアップの速度と大手の品質・量産・認証・輸出能力をモジュール契約で組み合わせることが要点である。

6. 各国モデルと日本の制度的位置

6.1 各国モデル比較

地域	制度の核	強み	弱点／注意
米国	DARPA、SBIR/STTR、IQT、DIU、OSC、軍調達	大需要、非希薄化資金、OT、VC、実運用	予算断絶、平均契約日数、少数企業集中、輸出・機密
NATO/EU	DIANA/NIF、EDF/EUDIS、EIB、SAFE	多国テスト、標準、共同研究・融資・VC	制度重層、加盟国需要断片化、融資と予算の混同
英国	UKDI へ統合、年 4 億ポンド以上	中央窓口、3 か月契約目標、調達予算 10%方針	実運用定着と量産需要の検証が必要
イスラエル	MAFAT/INNOFENSE、部隊、輸出	ユーザー・人材・起業・輸出の距離が短い	小国内需、紛争・人権・輸出評判リスク
中国	国家主導の軍民融合／標準・大学・SOE	規模、長期動員、供給網・インフラ統合	透明性、非市場価格、技術流出・制裁、民需の軍事転用
日本	ATLA/DISTI、K Program、基盤強化法、移転改革	製造・部材・センサ、政府横断資金、政策転換	移行 KPI、需要確約、府省分散、スタートアップ固定費

EU の EDF は 2021～2027 年に約 73 億ユーロ。SAFE の 1,500 億ユーロは加盟国共同調達向けの長期融資、Readiness 2030 の最大 8,000 億ユーロは加盟国追加支出余地を含む動員構想、NATO Innovation Fund の 10 億ユーロ超は VC であり、いずれも EU の単年度調達予算ではない。

[12] [13] [14] [46] [47]

NATO DIANA はアクセラレーターと 200 超のテストセンターを結び、NIF は 24 同盟国が支える VC として資本を供給する。英国は DASA 等を UKDI へ統合し、年 4 億ポンド以上をリングフェンスする。イスラエルの INNOFENSE は株式を取らない初期支援と知財の企業保持を特徴とする。

[11] [12] [15] [16] [17]

中国のモデルは VC 橋渡しより、国有企業、民間企業、大学、地方政府、共通インフラ、標準を国家主導で統合する。規模を過小評価すべきでない一方、軍事売上、基金の重複、非市場価格のため、他国と同じ市場指標で比較できない。

[18]

6.2 日本の制度パイプライン

段階	主な制度	役割	未解決点
----	------	----	------

段階	主な制度	役割	未解決点
① 戦略・需要	三文書、7 重点機能、日本成長戦略 17 分野	必要能力と産業方向を提示	非機密ミッション、長期需要・数量の可視化
② 探索	安全保障技術研究推進、K Program	目的指向基礎研究、公的・民生利用、流出管理	防衛調達への移行率、公開研究と機微化の境界
③ 成熟化	先進技術橋渡し、DISTI ブレークスルー	民生成果を試作・実証へ	プログラム責任者、試験データ、失敗許容
④ 迅速実装	早期装備化、ファストパス、防衛省版 SBIR	随契、アジャイル、伴走支援	新設直後で量産移行・支払・原価監査の実績未検証
⑤ 量産・供給	通常調達、防衛生産基盤強化法	供給網、効率化、サイバー、事業承継	民生品は基本対象外。併用設備への波及は可能
⑥ 市場拡大	装備移転改革、基金、政府間協力	輸出可能性、共同開発、生産・整備共有	協定、個別審査、認証、金融、現地保守、案件獲得
⑦ 保護	特許非公開、重要経済安保情報、研究セキュリティ	機微情報・技術流出を管理	大学・スタートアップの固定費、透明性・外部監督

6.3 FY2026 の数値—母数を混同しない

項目	公表値	解釈上の注意
整備計画対象経費	歳出 8 兆 8,093 億円／契約 8 兆 2,607 億円	防衛全体の母数。デュアルユース／スタートアップ専用ではない
研究開発	約 7,095 億円（他分野除外 2,907 億円）	再掲を含む。単純に他重点分野と加算しない
安全保障技術研究	129 億円	公開・非秘密の目的指向基礎研究。装備応用可能性は審査項目ではない
ブレークスルー／橋渡し	237 億円／141 億円	成熟度・目的が異なる。採択額と量産需要は別
生産基盤	957 億円（他分野除外 678 億円）	指定装備品の安定製造が中心。民生併用設備は認定可能
SHIELD	1,001 億円	FY2027 中構築を目指す UAV/USV/UUV 取得。民生市場額ではない
移転基金	FY2026 400 億円	基金への補助。輸出契約売上や交付済額と区別

FY2026 予算は、デュアルユース技術やスタートアップの先端技術を幅広く取り込み、成果を社会へ還元するエコシステムを明記する。安全保障技術研究推進制度は成果公表を制限せず、秘密指定を行わず、日本版バイ・ドールの条件下で知財を受託者へ帰属させ得る。2026 年度から医学・生物学の基礎研究も追加された。^{〔19〕} ^{〔20〕}

K Program は 2021・2022 年度補正で合計 5,000 億円の政府横断基金を形成し、海洋、宇宙・航空、領域横断・サイバー、バイオ等を支援する。ただし防衛省の調達予算ではなく、装備化

を保証しない。DISTI は 2024 年 10 月開設で、外部人材、リスク許容、短期実証を通じた橋渡しを担う。〔21〕〔22〕

6.4 2026 年 4 月の装備移転改革

2026 年 4 月 21 日の改正は、国産完成品を救難・輸送・警戒・監視・掃海の 5 類型に限る制約を撤廃し、完成品、部品、技術、修理等役務を制度上『原則可』とした。非武器は移転先制約を設けず、武器は国連憲章に適合した使用を義務付ける協定締結 17 か国に限定し、現に戦闘中の国へは原則不可（日本の安全保障上、特段の事情がある場合を除く）。武器は国家安全保障会議の判断後、国会通知、審査項目拡充、移転後モニタリングが求められる。〔25〕

評価

これは『全面自由化』ではなく、許可可能性の範囲を広げた個別厳格審査型への転換である。輸出実績を増やすには、国際仕様、認証、相互運用性、供給能力、現地保守・訓練、輸出金融、政府間交渉が別途必要になる。

6.5 日本の構造ギャップ

- **移行責任の谷**：基礎→橋渡し→装備化、K Program→防衛調達の公開移行率・責任者・標準期間がない。
- **需要の谷**：PoC 後の最低購入量、量産時期、保守・更新予算が見えず、企業の設備・人材投資を誘発しにくい。
- **法的境界**：防衛生産基盤強化法は基本的に民生品を対象外とし、両市場の育成制度は府省に分散する。
- **オープン／機微の谷**：基礎制度は公表・非秘密だが、実装段階は保全・クリアランスが必要。セキュア研究拠点構想の詳細は未確定。
- **参入固定費**：原価・会計、サイバー、保全、資格、長い支払、政府 IP・データ権がスタートアップの速度と資金繰りに合わない。
- **スピンオフ KPI**：政府自身が防衛→民生の波及不足を認識するが、民生売上、人材循環、ライセンス、原価低下の追跡が弱い。

統合イノベーション戦略 2026 は、防衛から民生への社会実装の波及が十分でないとの認識の下、防衛省版 SBIR、アジャイル契約、民間資金、試験評価基盤、大学・国研のセキュアなオフキャンパス研究機能等を掲げる。方向は妥当だが、2026 年 8 月時点では将来計画を含み、運用実績・権利・監督の詳細は未確定である。〔27〕

7. 知財・データ・契約・標準化

7.1 競争優位の中心は『特許数』から権利の束へ

デュアルユースでは、特許だけを数えても競争力を把握できない。ソースコード、モデル重み、学習・評価データ、製造条件、校正值、試験ログ、脆弱性、API、標準提案、更新権、保守ノウハウが一体で価値を持つ。案件ごとに IP-SBOM（権利・規制・秘密の部品表）をつくり、一行

一資産で権利者、原資、利用範囲、情報区分、輸出・アクセス、証拠を記録する。〔48〕〔52〕〔54〕

資産群	記録すべき事項	典型的な保護
発明・設計	発明者、出願国、BIP/FIP、共同持分、政府資金	特許、意匠、回路配置、契約
ソフトウェア	ソース／バイナリ、OSS、API、ビルド、SBOM、版	著作権、営業秘密、ライセンス、エスクロー
データ／AI	原データ、ラベル、合成、特徴量、重み、RAG、ログ	契約上の利用権、個人情報、営業秘密、アクセス制御
製造・試験	工程条件、校正、歩留まり、治工具、評価スイート	営業秘密、限定提供、施設・人の管理
標準・IF	寄書、必須特許候補、適合性試験、FRAND	特許＋標準 IP ポリシー＋認証
運用・更新	任務データ、脆弱性、パッチ、更新・停止・監査権	契約、秘密、輸出・再移転条件

7.2 オープン&クローズ

開く層	閉じる層	理由
API、メッセージ、データ形式	実装アルゴリズム、重み、特徴量	相互運用と競争調達を可能にしつつ性能差を守る
機械・電気インターフェース	材料組成、製造条件、校正值	複数供給者と保守を可能にし、工程ノウハウを守る
安全・品質・サイバー試験法	脅威データ、脆弱性、対抗策	信頼性の共通尺度を作り、悪用情報は限定する
モデル／データカード様式	学習データ本体、任務ログ	説明・監査可能性とデータ保護を両立

標準化団体へ寄書する前に発明届と出願を行い、IP ポリシー、特許開示、FRAND、著作権、秘密保持、輸出管理を確認する。『標準化＝無償公開』ではなく、インターフェースを開いて実装コアを閉じ、適合性試験・認証を市場形成に使う。

7.3 BIP／FIP の契約設計

Background IP（BIP）は契約締結前に名称・版、権利者、第三者制約、提供形態、研究／製品化／量産／保守、防衛／民生、地域、期間、再許諾、終了後利用、輸出制約を別紙化する。『研究に必要な一切の BIP を無償許諾』は範囲が読めず、民生コアを失うため避ける。〔52〕

Foreground IP（FIP）は、技術モジュール・発明群ごとの単独帰属と限定クロスライセンスを第一案にする。日本の共有特許は各共有者が原則自己実施できる一方、持分譲渡・第三者ライセンスには他共有者同意が必要で、スタートアップの資金調達・M&A・SEP 許諾を止め得る。共同発明だけを共有し、出願国、費用、第三者許諾、権利行使、放棄、支配権変更を先に決める。

政府資金の注意

安全保障技術研究推進制度は日本版バイ・ドールの条件下で受託者に知財を帰属させ得るが、国または指定第三者への実施許諾、移転・専用実施権設定の承認等が問題になり得る。資金制度ごとの公募要領・契約条件を一般論で処理しない。〔20〕〔58〕

7.4 データ・ソフトウェア・AI 契約

『データは甲の所有』だけでは足りない。閲覧、複製、改変、結合、学習、評価、派生作成、再配布、第三者支援、輸出、保存、削除、監査という動詞で権限を分ける。原データ、ラベル、合成データ、特微量、重み、チェックポイント、プロンプト、RAG、テレメトリを別資産とし、ソース、API、ビルド環境、SBOM、パッチ、モデル／データカード、評価スイートを納入物として明記する。

争点	推奨条項	避ける表現
政府・支援業者の利用	目的、利用主体、環境、期間、再委託、監査を限定	『政府目的で無制限』
モデル更新	重要変更基準、再試験、再法務審査、ロールバック	『常時最新版を自動適用』
学習利用	データ群別に学習可否、派生重み、再識別、削除を定義	『サービス改善に利用できる』
終了・競争調達	IF 文書、必要技術データ、エスクロー、移行支援	全ソース譲渡／又は情報提供ゼロ
脆弱性・事故	通知期限、是正、パッチ、ログ、規制当局対応を分担	責任主体・時間軸がない一般条項

7.5 特許化・秘匿化・FTO

- **特許向き**：製品から解析される、標準に入る、広く開示する、独自開発が予想され、侵害を外部から立証できる。
- **営業秘密向き**：製造条件、歩留まり、校正、学習／評価データ、重み、運用ノウハウ、脆弱性など、外から発見しにくい。〔54〕
- **防御公開／標準化向き**：エコシステム形成を優先する IF、試験方法、データ形式。ただし寄書前出願と FTO を行う。

FTO は製品名ではなく、『予定行為（研究・製造・輸入・販売・使用・クラウド処理・保守）×法域×構成版』で行う。モジュール、SEP、OSS、データ契約、営業秘密混入、大学・政府権利を含め、クレームチャートと構成管理を結ぶ。特許非公開制度により先行出願が公開されない探索限界も残るため、FTO は無侵害保証ではなく、回避設計・ライセンス・無効資料・更新監視を含むリスク低減である。

8. 輸出管理・情報保全・研究セキュリティ・責任ある AI

8.1 特許出願非公開—出願前より前に動く

日本の特許出願非公開制度は 2024 年 5 月 1 日に開始。特定技術分野に属する出願は JPO の第一次審査を経て内閣府の保全審査へ送られ得る。保全指定中は出願公開・査定等が留保され、発明の開示・実施、共有、外国出願等に制約が生じ、通常生ずべき損失の補償制度がある。

[29] [49]

2025 年度は JPO から内閣府へ 106 件が送付されたが、保全指定は 0 件。外国出願禁止の事前確認は 922 件、内閣府へ送付しない旨の通知は 771 件であった。指定ゼロは制度が無関係という意味ではなく、国外代理人への明細書送信、国外 Git／クラウド保存、外国共同研究先への詳細開示より前に事前確認が必要な実務負担を示す。 [30]

発明届の必須欄

安保関連性／外国出願予定／国外共同発明者・国外サーバ／公表予定／対象技術の民生用途／秘密・輸出区分。発明届→非公開制度確認→国内出願→外国出願・公表の順を標準化する。

8.2 輸出管理—物より広い『技術提供』

日本の外為法管理は、物品だけでなくソースコード、設計図、モデル重み、学習手順、製造条件、遠隔保守、クラウド／Git の国外アクセス、学会発表、非居住者や特定類型該当居住者への技術提供を含む。2025 年 10 月 9 日の補完的輸出規制見直しも踏まえ、版・需要者・用途・アクセス場所が変わるたび再判定する。 [31] [51] [61]

順序	確認	成果物
1 対象	物、ソフト、技術、クラウド、役務、試料、モデル、更新	構成・版・提供方法一覧
2 法域	日本外為法、米国由来 EAR/ITAR、EU、契約再輸出条件	法域マップ
3 リスト	部品、暗号、量子、半導体、材料、製造装置等の該非	該非判定書
4 キャッチオール	WMD／通常兵器、用途、需要者、インフォーム	用途・需要者審査
5 技術／みなし輸出	外国人、特定類型、国外クラウド、遠隔支援	アクセス承認・記録
6 最終用途	実質所有者、統合先、運用人、第三国移転、制裁	最終用途証明・契約条件
7 継続監視	版、仕向地、需要者、用途、許可条件の変更	構成管理と再審査ログ

米国では EAR が多くの商用品・デュアルユース品と技術・ソフトを、ITAR が USML 上の防衛物品・役務・技術データを扱う。EU 規則 2021/821 は輸出、仲介、技術援助、通過、移転を対

象とする。米国由来技術・部品を組み込む日本製品では再輸出条件が事業・M&A・クラウド運用に及ぶ。 [32] [33] [34]

8.3 情報保全とセキュリティ・クリアランス

営業秘密、契約上の保護情報、防衛調達保護すべき情報、重要経済安保情報、外為法上の規制技術、個人情報とは別制度である。同じデータが複数に該当し得るため、一つの資産台帳へ統合しつつ、法的根拠と取扱いを別欄にする。防衛調達情報セキュリティ基準は、保護情報を扱う下請へもフローダウンし、基本方針、システムセキュリティ実装計画、取扱者、検知・対応・復旧等を求める。 [50]

重要経済安保情報保護活用法は 2025 年 5 月 16 日施行。政府が指定した重要経済基盤情報を適合事業者へ提供し、取扱者を適性評価で制限する。官民・同盟国間の情報共有を可能にする一方、適合事業者認定、認定場所、取扱記録、教育・施設等がスタートアップや大学の固定費になり得る。社内の全デュアルユース技術を自動的に秘密指定する制度ではない。 [28]

- **区画化**：民生環境と保護環境を論理・物理分離し、承認済み移送ゲートを置く。
- **最小権限**：人、端末、場所、データ、操作を結び、異動・退職時に即時剥奪する。
- **下請管理**：成熟度を契約前評価し、同じ管理、事故通知、監査、返却・消去を流す。
- **解除設計**：秘密理由、期間、解除条件をデータ単位で持ち、プロジェクト全体の過剰機密化を避ける。

8.4 研究セキュリティー開放と保護の二層化

研究セキュリティの目的は国際共同研究の一律縮小ではなく、リスクに比例した保護によって信頼できる協力を継続することである。相手機関、実質支配・資金源、制裁、軍・情報機関との関係、研究者の兼職・外国資金、アクセスする設備・データ、国外クラウド、再委託を確認する。国籍だけでなく役割・アクセス・関係・用途に基づき軽減措置を設計する。 [48] [53]

- 公開ワークパッケージと保護ワークパッケージを分け、コアだけをセキュア環境へ置く。
- 研究者申告を採択時だけでなく、年次・兼職・資金・メンバー変更時に更新する。
- 公表ゲートで発明届、第三者 IP、輸出、秘密、個人情報、バイオリスクを同時確認する。
- 疑義を研究者個人へ負わせず、研究・知財・輸出・セキュリティ・人事・国際・法務の窓口へ上げる。

8.5 責任ある AI／自律システム

防衛装備庁の 2025 年ガイドラインは、A-1『国際人道法等の国際法・国内法を遵守できないものでない』、A-2『人間の関与が及ばない完全自律型致死兵器でない』を法的・政策的要件とする。技術要件 B-1～B-7 は、人間の責任、運用者理解、バイアス、検証可能性・透明性、信頼性・有効性・セキュリティ、安全性、適法運用設計である。AI 出力が破壊能力に影響する場合は高リスクとして、構想段階の法的・政策的審査と研究開発中の技術審査を行う。 [35]

保証領域	企業が残す証拠
用途・人的責任	意図用途、禁止用途、運用構想、人間の決定・承認・停止点、責任分担

保証領域	企業が残す証拠
データ・公平性	来歴、代表性、ラベル品質、汚染・敵対操作、防止策、バイアス評価
構成・再現	モデル／ソフト／ハード版、学習設定、SBOM、供給網、再現手順
試験	通常・劣化・通信断・センサ故障・欺瞞・未知入力、誤警報、見逃し、OOD
人間機械 IF	能力・限界表示、自動化バイアス対策、訓練、ログ、縮退・停止
更新・運用	重要変更基準、再試験・再法務、監視、事故／ニアミス、ロールバック

米 DoD Directive 3000.09 も、人間が適切な判断を行える設計、理解可能な HMI、試験・検証、AI 倫理原則、法的レビューを要求する。NATO は適法性、責任・説明責任、説明・追跡可能性、信頼性、統治可能性、バイアス軽減の 6 原則を掲げる。国際的な LAWS の定義は未確定であり、ICRC は予測・限定困難な効果と人間の統制喪失を問題視する。 [36] [37] [38] [56]

8.6 ESG・人権・評判

防衛は自動的に反 ESG ではない。欧州委員会は持続可能金融枠組みが防衛部門への融資を一律に禁止しないと整理する一方、国際条約で禁止される兵器、深刻な人権侵害、懸念国・不透明な最終用途、腐敗、重要鉱物・化学物質・排出・宇宙デブリ等は強い除外・エンゲージメント対象となる。製品、行為、顧客、地域、最終用途で評価する。 [55]

取締役会へ報告する指標	最低限の内容
売上分解	民生／防衛、製品、顧客種別、地域、武器体系との距離
禁止・高懸念	禁止兵器方針、該当／ゼロ／不明、完全自律致死、CBRN
輸出・最終用途	許可・拒否・自主申告、制裁、逸脱、代理店 DD、第三国移転
AI・安全	法的・技術的審査、人的責任、事故・ニアミス、更新再審査
人権・環境	顕著な人権リスク、腐敗、鉱物、労働、化学物質、GHG、水、廃棄物

9. 政策提言と企業実行計画

9.1 政府への 10 提言

- 1. 単一ポートフォリオ責任者：防衛省、経産省、内閣府、文科省、JST/NEDO の案件を同じ成熟度・移行 KPI で追い、次段階の決定主体を一件ごとに置く。
- 2. 非機密ミッション・カタログ：『AI を募集』ではなく、妨害下通信、港湾復旧、海底ケーブル監視等を性能、環境、単価、期限で提示する。
- 3. 移行予算を試作と同時に予約：試験合格時に量産・保守へ進めるオプション、最小発注、年度跨ぎ枠を設け、PoC の墓場を防ぐ。

- 4. **ユーザーと試験データを早期開放**：部隊・海保・消防・自治体・インフラ事業者の共通テストベッドを作り、非機密・合成データを提供する。
- 5. **資本スタックを連結**：補助金、マイルストーン契約、前払、融資・保証、エクイティ、輸出金融をTRL・量産段階に合わせる。
- 6. **IP・データ標準条項**：BIP/FIP、政府利用権、モデル学習、技術データ、IF、終了時移行をモジュール別を選ぶ標準メニューにする。
- 7. **コンプライアンス共通基盤**：輸出、保全、サイバー、クリアランスのテンプレート、相談、共有施設を提供し、中小企業の固定費を下げる。
- 8. **MOSA・認証の相互承認**：開くIFと閉じるコアを明確化し、同盟国・民生規制との試験・サイバー認証の相互承認を進める。
- 9. **輸出をライフサイクル事業化**：許可だけでなく、政府間交渉、現地訓練・整備、部品、アップデート、第三国移転監視まで一体支援する。
- 10. **公開ダッシュボード**：契約日数、試作→量産移行率、実支出、納期、民生売上、民間資本、輸出、事故・違反を指標定義付きで公表する。

9.2 政策 KPI の最小セット

目的	KPI	避ける代替指標
速度	課題提示→契約、契約→試験、試験→量産の中央値	公募件数だけ
移行	成熟段階別の次段階移行率、理由別失敗率	採択件数・採択額だけ
需要	契約上限ではなく実支出、量産数量、保守・更新額	最大契約額の合計
波及	民生売上、民間資本、共通コア比率、ライセンス、人材移動	推計 TAM だけ
産業基盤	納期、可動率、原価低下、国内・同盟国供給源、復旧時間	国内調達比率だけ
責任	事故・用途逸脱・違反、更新再審査、是正完了時間	規程・研修回数だけ

9.3 企業の 90 日実行計画

期間	経営・組織	技術・知財・管理	事業・顧客
0～30 日	取締役会の許容／禁止用途、地域、顧客方針。横断委員会と窓口	既存案件、IP-SBOM、国外アクセス、政府資金、秘密を棚卸し	民生／防衛の共通ミッションとアンカー顧客を選定
31～60 日	案件受付・上申基準、権限、審査SLA	BIP/FIP、発明届、輸出、AI 保証、最終用途テンプレート。上位 20 件 FTO	共通コア／任務層を分け、試験計画と単価仮説を作る
61～90 日	1 案件を G0～G7 でパイロットし、差戻し理由を経営報告	共有権・過大納入・再許諾を是正。開くIF／閉じるコア、標準・認証ロードマップ	政府・民生各 1 ユーザーと実証、次段階契約条件・資金計画を合意

9.4 企業のビジネスモデル設計

論点	推奨	レッドフラッグ
売上構成	防衛、他官庁、重要インフラ、一般民生、同盟国を段階拡張	単一プログラムが売上の過半、終了後の転用先なし
製品構成	共通コア 70%を目安に、任務層・保護データを分離	全顧客仕様がフォーク、民生版も機密・輸出対象
価格	ソフト更新・保守・データ・訓練をライフサイクル価格化	試作の原価回収だけ、量産時の粗利・運転資金がない
資本	助成＋契約＋融資保証＋長期株式を段階別利用	高評価額の株式だけで設備・在庫・遅い支払を賄う
パートナー	大手の量産・認証・輸出と新興のソフト速度をモジュール契約	包括独占、BIP の無償包括許諾、出口・M&A を阻害
ガバナンス	用途・需要者・地域・更新を継続監視し、停止権を持つ	営業が許可・性能・用途を先に約束

10. 2040 年シナリオと結論

10.1 三つのシナリオ

シナリオ	制度・市場の姿	早期シグナル（2027～2030）	日本の 5 関連市場（参考）
A 制約残存	PoC 多数、量産予算・データ・保全・輸出が断絶。個別カスタム化	移行率非公表、支払長期、輸出少数、民生売上横ばい	本調査試算 4.2 兆円
B 管理された拡大	府省パイプラインが接続、共通テスト、MOSA、資本・輸出支援が機能	契約日数短縮、量産移行率上昇、民生案件・同盟国案件増	記事ベース 8.6 兆円
C 加速循環	政府がアンカー需要、企業が共通コアを世界市場へ。人材・標準・資本が循環	複数の二市場企業、継続輸出、原価低下、民間資本・ライセンス増	記事上振れ 16.8 兆円

上表の市場額は同じ品質の統計ではなく、比較用シナリオである。政策評価は市場額の実現だけでなく、国の安全、災害・インフラのレジリエンス、技術自律性、国際法・人権、安全、財政効率を同時に見るべきである。

10.2 最終結論

1 市場

『2040 年 500 兆円』は可能性を示す広義の強気 TAM であって、防衛デュアルユース市場の確定予測ではない。企業は国・分野・顧客・用途ごとの SAM/SOM へ分解し、予算、契約上限、実支出、売上、投資、GVA を混ぜない。

2 技術・事業

勝つのは最高性能の単品ではなく、共通コア、標準 IF、短い更新、量産学習、現場導入を複数市場で再利用できる企業である。Palantir が示すのはデータ統合と現場実装、Anduril が示すのは商用開発・資本・量産手法の防衛転用である。

3 日本

探索、橋渡し、迅速実装、生産基盤、装備移転、情報保全の制度部品は揃い始めた。次の課題は制度間の移行責任、量産需要、ユーザー・データ、スタートアップ固定費、民生波及 KPI を埋めることである。

4 ガバナンス

知財、データ、輸出、秘密、研究セキュリティ、責任ある AI はイノベーションの後付け制約ではない。共通コアを安全に複数市場へ展開するための製品アーキテクチャであり、信頼と輸出可能性を生む成長基盤である。

付録 A 添付 3 記事のファクトチェック

主張	判定	検証結果／扱い
日本成長戦略 17 分野と防衛の密接性	概ね確認	2026-07-21 決定は官邸検索と記事で確認。防衛は AI・半導体、通信、宇宙、海洋等と横断。ただし官邸本文 URL は調査時に 404。
5 つの注目技術	分析として妥当	政策上の公式 5 分類ではなく記事著者の選定。K Program、内閣府重要技術、FY2026 防衛予算と方向整合。
米 DoD 14 技術分野	歴史的には正確	2022 年資料。2025-11-17 に 6 CTA へ再編されたため、現行優先順位としては更新が必要。
米国市場 2025 年 24→2040 年 451 兆円、CAGR21.6%	算術整合／定義不足	$24 \times 1.216^{15} = 451.0$ 。5 隣接市場の合算で、重複、為替、価格基準、原典・地域等が未開示。
『2040 年 500 兆円』	丸め表現	451 兆円を約 500 兆円としたもの。防衛調達・企業売上・公的市場予測ではない。
日本 2040 年 8.6／16.8 兆円	民間シナリオ	2 兆円起点の現状延長と政策上振れ。政府予測・因果推定ではない。
防衛 1 兆ドルで 5 産業へ 0.74 兆ドル波及	著者モデル	DoD・BEA 資料を用いた記事著者の産業連関的試算。公的乗数・独立再現値として扱わない。
Palantir 2025 売上 44.75 億ドル、政府 54%／商用 46%	確認	SEC 10-K と一致。従業員 4,429 人も確認。契約上限や時価総額は売上と区別。
Palantir は民生にも展開	確認	Foundry/AIP 等を製造、物流、金融等へ展開。政府・商用の両セグメント売上を法定開示。
技術・人材・供給網の三経路	妥当な枠組み	歴史例と制度は支持するが、波及の大きさは自動でなく、移行予算・標準・需要・管理に依存。

著作権配慮：添付記事の図表・文章は転載せず、主張を要約し、一次資料との照合結果を独自の表に再構成した。

付録 B 企業ステージゲート G0-G7

ゲート	問い	必須成果物	停止・上位承認例
G0 方針・受付	使命・リスク選好、用途、顧客、地域に合うか	用途記述、顧客・地域、技術、民生還流仮説	禁止兵器、用途不明、匿名顧客、方針外
G1 機微性・法域	秘密、輸出、個人、バイオ、AI、自律性は	初期分類、法域、情報区分、AI／バイオ区分	許可見込みなし、完全自律致死、無承認開示
G2 IP・FTO	BIP を使えるか、侵害しないか、特許か秘密か	IP-SBOM、BIP 表、発明計画、FTO、OSS／データ権原	権利者不明、競合秘密、重大 SEP、外国出願未確認
G3 相手方 DD	組織、人、資金、支配、再委託、アクセスは信頼可能か	相手方 DD、研究者申告、アクセス設計、軽減策	虚偽、懸念主体、実質所有者不明、軽減不能
G4 契約・設計	権利、政府権利、標準、秘密、輸出、更新を配分したか	契約、納入物、IF/MOSA、セキュリティ、最終用途	包括 IP 譲渡、無制限再移転、フローダウンなし

ゲート	問い	必須成果物	停止・上位承認例
G5 開発・検証	安全・信頼・適法に使える証拠があるか	試験、保証ケース、カード、SBOM、脆弱性評価	停止不能、重大誤作動、データ不足、版不一致
G6 出願・公表・移転	開示・出願・輸出してよいか	発明審査、外国出願確認、許可、公表審査、用途証明	保全・秘密、許可なし、第三者 IP、用途変更
G7 配備・更新・終了	用途逸脱、再移転、劣化、更新、事故を監視できるか	監視、再審査、監査、再移転、返却・廃棄	無断用途・第三国移転、重大事故、制裁、保守不能

単独レッドフラッグ

禁止兵器／人間の関与が及ばない完全自律型致死構想／制裁対象／虚偽 DD／無許可技術提供／IP 権原不明。合計点が低くても自動承認しない。

付録 C 調査手法と限界

- 基準日：2026 年 8 月 14 日。公開情報のみ。機密情報・非公開契約・内部データは用いていない。
- 優先順位：法令・政府・国際機関・法定企業開示を優先し、添付記事の試算・解説と区別した。
- 市場：定義が統一されていないため、予算、契約上限、実支出、売上、資金調達、TAM、GVA を別指標として扱った。
- 為替・価格：資料の原通貨を優先。円換算は添付記事の前提が未開示であり、比較目的以上に用いない。
- 政策：制度の創設・予算化と、運用実績・成果を分離。新設制度は効果検証前であることを明記した。
- 官邸の 2026 年日本成長戦略ページ／PDF は検索索引で決定を確認したが、直接取得時に 404 であったため、添付記事と他の一次資料を併用した。
- 法務：本報告は実務設計の一般的枠組みであり、個別案件の輸出許可、特許、秘密指定、製品安全、国際法等の法的助言ではない。

参考文献・一次資料

本文中の上付き〔番号〕は、以下の資料へのリンクである。閲覧日は原則 2026 年 8 月 14 日。

〔A1〕 日経テックフォーサイト「防衛デュアルユース、戦略 17 分野と密接 5 つの注目技術」（2026-08-03、ユーザー提供 PDF、file_000000008ab88209bc7ddd6a12850072）

〔A2〕 日経テックフォーサイト「米国のデュアルユース、2040 年に 500 兆円規模 実態と今後」（2026-08-05、ユーザー提供 PDF、file_00000000209c81f8a111c69c1e3b4bc3）

〔A3〕 日経テックフォーサイト「AI が防衛作戦、代表格バランティアは何者か 民生展開も」（2026-08-07、ユーザー提供 PDF、file_00000000566082099d73f7cd56f73c9c）

〔1〕 SIPRI, Trends in World Military Expenditure, 2025 <https://www.sipri.org/publications/2026/sipri-fact-sheets/trends-world-military-expenditure-2025>

〔2〕 NATO, The Hague Summit Declaration (2025-06-25) <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration>

- [3] U.S. OUSD(R&E), Six Critical Technology Areas (2025-11-17) <https://www.war.gov/News/Releases/Release/Article/4333074/under-secretary-of-war-for-research-and-engineering-emil-michael-announces-six/>
- [4] U.S. OUSD(R&E), Critical Technology Areas (current) <https://www.cto.mil/cta/>
- [5] U.S. OUSD(R&E), 14 Critical Technology Areas (2022 archive) https://www.cto.mil/wp-content/uploads/2022/02/usdre_strategic_vision_critical_tech_areas.pdf
- [6] Defense Innovation Unit, 2024 Annual Report <https://www.diu.mil/2024-annual-report-files/index.html>
- [7] U.S. GAO, Defense Innovation Unit: Actions Needed to Assess Progress and Further Enhance Collaboration (GAO-25-106856) <https://files.gao.gov/reports/GAO-25-106856/index.html>
- [8] DARPA, Commercial Strategy Office <https://www.darpa.mil/about/offices/commercial-strategy>
- [9] U.S. Department of Defense, Office of Strategic Capital FY2025 Investment Strategy <https://media.defense.gov/2025/Jan/02/2003623435/-1/-1/1/FY25-INVESTMENT-STRATEGY-FOR-OFFICE-OF-STRATEGIC-CAPITAL.PDF>
- [10] U.S. Defense Innovation Board, Scaling Nontraditional Defense Innovation (2025) https://stib.cto.mil/wp-content/uploads/2026/01/2025-2_DIB-ScalingNontraditionalDefenseInnovation_250113PUBLISHED_9ee4ae.pdf
- [11] NATO DIANA <https://www.diana.nato.int/>
- [12] NATO Innovation Fund <https://www.nif.fund/>
- [13] European Commission, European Defence Fund https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en
- [14] Council of the EU, SAFE instrument — €150 billion for joint procurement <https://www.consilium.europa.eu/en/press/press-releases/2025/05/27/safe-council-adopts-150-billion-boost-for-joint-procurement-on-european-security-and-defence/>
- [15] UK Government, UK Defence Innovation (UKDI) <https://www.gov.uk/guidance/a-new-era-for-defence-innovation-dasa-diu-and-des-fci-unite-under-uk-defence-innovation-ukdi>
- [16] UK Government, DASA Impact Report 2025 <https://www.gov.uk/government/publications/dasa-impact-report-2025>
- [17] Israel Ministry of Defense, INNOFENSE <https://ddrd-mafat.mod.gov.il/en/innofense>
- [18] State Council of China, Opinions on Deepening Military-Civil Integration (2017) https://english.www.gov.cn/policies/latest_releases/2017/12/04/content_281475964615180.htm
- [19] 防衛省「令和 8 年度予算の概要—防衛力抜本的強化の進捗と予算」
https://www.mod.go.jp/j/budget/yosan_gaiyo/fy2026/yosan_20260408.pdf
- [20] 防衛装備庁「安全保障技術研究推進制度」 <https://www.mod.go.jp/atla/funding.html>
- [21] 防衛装備庁「防衛イノベーション科学技術研究所 (DISTI)」 <https://www.mod.go.jp/atla/disti.html>
- [22] 内閣府/JST「経済安全保障重要技術育成プログラム (K Program)」 <https://www.jst.go.jp/k-program/>
- [23] 内閣府「令和 7 年度 経済安全保障に関する重要技術動向等調査」
https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/technology/doc/r07_emerging_report.pdf
- [24] 防衛装備庁「防衛生産基盤強化法」 https://www.mod.go.jp/atla/hourei_dpb.html
- [25] 防衛装備庁「防衛装備移転三原則・運用指針の見直し」 (2026-04-21)
https://www.mod.go.jp/atla/soubiseisaku/soubiseisakugijutu/boei_sobi_iten_sangensoku_unyo_shishin_kaisei_202604.pdf
- [26] 内閣官房「日本成長戦略会議」 <https://www.cas.go.jp/ip/seisaku/nipponseichosenryaku/index.html>
- [27] 内閣府「統合イノベーション戦略 2026」 https://www8.cao.go.jp/cstp/tougosenryaku/togo2026_zentai.pdf
- [28] 内閣府「重要経済安保情報保護活用法」 https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/hogokatsuyou.html
- [29] 内閣府「特許出願の非公開に関する制度」 https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/patent/patent.html
- [30] 内閣府・特許庁「2025 年度 特許出願の非公開に関する制度における実施状況」
https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/patent/doc/patent_jisshijoukyou_r7.pdf
- [31] 経済産業省「補完的輸出規制 (キャッチオール規制)」 <https://www.meti.go.jp/policy/anpo/catchall.html>
- [32] U.S. BIS, Export Administration Regulations, Part 730 <https://www.bis.gov/regulations/ear/730>
- [33] U.S. DDTC, International Traffic in Arms Regulations (ITAR) https://www.pmdtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987
- [34] Regulation (EU) 2021/821 on dual-use export controls, consolidated 2025-11-15 <https://eur-lex.europa.eu/eli/reg/2021/821/2025-11-15/eng>
- [35] 防衛装備庁「装備品等の研究開発における責任ある AI 適用ガイドライン (第 1 版)」
https://www.mod.go.jp/atla/soubiseisaku/ai_guideline/ai_guideline_ver.01.pdf
- [36] U.S. DoD Directive 3000.09, Autonomy in Weapon Systems (2023) <https://media.defense.gov/2023/Jan/25/2003149928/-1/-1/0/DOD-DIRECTIVE-3000.09-AUTONOMY-IN-WEAPON-SYSTEMS.PDF>

- [37] NATO, Revised Artificial Intelligence Strategy (2024) <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>
- [38] ICRC, Position on Autonomous Weapon Systems <https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems>
- [39] Palantir Technologies, 2025 Form 10-K <https://www.sec.gov/Archives/edgar/data/1321655/000132165526000011/pltr-20251231.htm>
- [40] Anduril, \$5B Series H financing (2026) <https://www.anduril.com/news/anduril-announces-usd5b-series-h-raise>
- [41] Anduril, Lattice dual-use platform for public safety and security <https://www.anduril.com/news/anduril-s-lattice-a-trusted-dual-use-commercial-and-military-platform-for-public-safety-security>
- [42] SpaceX, Starshield <https://www.spacex.com/starshield>
- [43] CBO, The Budget and Economic Outlook: 2025 to 2035 <https://www.cbo.gov/publication/61270>
- [44] 防衛装備庁「防衛産業への新規参入促進／ファストパス」
https://www.mod.go.jp/atla/soubiseisaku/newentry/fastpass_about_r080227.pdf
- [45] 防衛省記者会見（2026-05-12）—スタートアップ参入上の課題 <https://www.mod.go.jp/j/press/kisha/2026/0512a.html>
- [46] European Commission, Future of European Defence / Readiness 2030 https://commission.europa.eu/topics/defence/future-european-defence_en
- [47] EU Defence Spending — €418bn in 2025, projected €454bn in 2026 <https://eda.europa.eu/news-and-events/news/2026/07/16/eu-defence-spending---418-billion-in-2025--projected-to--454-billion-in-2026>
- [48] 内閣府「第7期科学技術・イノベーション基本計画」（2026-03-27）
<https://www8.cao.go.jp/cstp/kihonkeikaku/7honbun.pdf>
- [49] 特許庁「特許出願非公開制度について」 <https://www.ipo.go.jp/system/patent/shutugan/hikokai/index.html>
- [50] 防衛装備庁「装備品等及び役務の調達における情報セキュリティ基準」 <https://www.mod.go.jp/atla/cybersecurity.html>
- [51] 経済産業省「みなし輸出管理」 <https://www.meti.go.jp/policy/anpo/anpo07.html>
- [52] 特許庁「オープンイノベーション促進のためのモデル契約書 ver2.2」 <https://www.ipo.go.jp/support/general/open-innovation-portal/index.html>
- [53] 内閣府「研究セキュリティ確保のための手順書」
https://www8.cao.go.jp/cstp/kokusaiteki/integrity/yushikisha/guidelines_v1
- [54] 経済産業省「営業秘密管理指針」（2025年改訂）
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/forum/reiwa7/05-2_250624_METI.pdf
- [55] European Commission, Notice on sustainable finance and the defence sector (2025) https://defence-industry-space.ec.europa.eu/document/download/ac79ebc7-d2f1-4e7a-a79c-71a06a5fdbf8_en?filename=notice-application-sustainable-finance-framework-and-corporate-sustainability.pdf
- [56] ICRC, Autonomous Weapon Systems and International Humanitarian Law (2026)
https://www.icrc.org/sites/default/files/2026-03/4896_002_Autonomous_Weapons_Systems_-_IHL-ICRC.pdf
- [57] 内閣府「経済安全保障重要技術育成プログラム（K Program）」 https://www8.cao.go.jp/cstp/anzen_anshin/kprogram.html
- [58] 防衛装備庁「安全保障技術研究推進制度 令和8年度公募説明」
https://www.mod.go.jp/atla/funding/koubo/r08/r8koubo_setsumei_2603.pdf
- [59] 防衛省「令和8年版防衛白書」 <https://www.mod.go.jp/j/press/wp/wp2026/pdf/R08zenpen.pdf>
- [60] 防衛装備庁「防衛産業への新規参入促進」 https://www.mod.go.jp/atla/soubiseisaku_newentry.html
- [61] 経済産業省「補完的輸出規制の見直し（2025-10-09施行）」 https://www.meti.go.jp/policy/anpo/apply-01/20251009_catchminaooshi/20251009catchall.html
- [62] 内閣府「経済安全保障推進法」 https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/suishinhou.html