DEFENSE × DUAL-USE × INTELLECTUAL PROPERTY

防衛デュアルユース分野における企業知財戦略の現状と今後の課題

経済安全保障・グローバル市場・制度統合の観点から

修正版（第 2 版）

原案作成支援	Gemini（生成 AI）
修正・検証	公開一次資料および提示資料に基づく再編集
作成日	2026 年 8 月 21 日
情報基準日	2026 年 8 月 21 日
版	第 2 版（誤り・出典・体裁修正版）

利用上の注意

本報告書は、2026 年 8 月 21 日までに公表された一次資料および提示資料に基づく調査・分析であり、個別案件に関する法的助言を構成しない。法令、政府調達条項、輸出管理、サイバーセキュリティ要件および運用は変更され得るため、実際の出願、技術移転、輸出、共同研究または政府調達契約では、最新の法令・公示・契約条項と専門家の助言を確認する必要がある。

エグゼクティブサマリー

防衛デュアルユース市場では、ハードウェア単体の性能だけでなく、AI、データ統合、ソフトウェア更新、エッジ通信、サイバーセキュリティおよび運用ノウハウが競争力の中心へ移っている。したがって、企業の知財戦略は、特許件数の最大化ではなく、権利帰属、納入物、利用権、アクセス権、データ、ソフトウェア、営業秘密、輸出管理および情報セキュリティを一体で設計する「事業・安全保障一体型知財アーキテクチャ」として構築する必要がある。[1,2,3,4]

- **市場評価：**本報告書に掲げる市場規模は、引用元の記事が提示する推計モデル・シナリオ上のポテンシャルであり、公的統計による確定市場規模ではない。日本の 2040 年 16.8 兆円は、8.6 兆円のベースラインと 8.2 兆円の波及効果を加算したシナリオ値である。[3,4]
- **日本制度：**特許出願非公開制度は、第一次審査、保全審査、保全指定後の各段階で法的効果が異なる。保全審査の所要期間に法律上の上限はなく、保全審査中は出願の取下げが可能である一方、保全指定後は取下げが禁止される。[11,12]
- **政府契約：**日本版バイ・ドール規定により一定条件の下で受託者帰属が可能であるが、政府利用、移転、専用実施権等は法令および個別契約に左右される。米国 DFARS の Data Rights は技術データ・ソフトウェアに関するライセンスであり、それ自体から特許ライセンスが生じるものではない。[17,18,20,21,22]
- **実務優先順位：**BIP/FIP の事前区分、開発履歴の証拠化、契約前の納入物・データ権マトリクス、特許化・秘匿化判定、第一国出願制限・輸出管理・CUI 対応の統合審査を、研究開始前から実装することが最も重要である。[12,18,20,25,29]

本修正版の位置付け

市場推計の計算関係、特許出願非公開制度の 10 か月・取下げ・適正管理、損失補償、日本版バイ・ドール、DFARS の第三者開示・マーキング・特許権との関係、CMMC の現状、AI 関連発明の保護可能性、企業事例における確認事実と筆者分析の区別を再整理した。

1. 序論：防衛デュアルユース市場の構造変化と知財の役割

世界の安全保障環境の変化と先端技術の急速な進展に伴い、防衛技術と民生技術の境界を再定義する「防衛デュアルユース（軍民両用技術）」の重要性が高まっている。従来の防衛産業は、重厚長大なハードウェア、政府の直接調達、長期の開発サイクルを中心としてきた。しかし近年は、AI、自律制御ソフトウェア、宇宙通信、サイバーセキュリティ、海洋センシング等、民生分野で発展したデジタル技術が防衛能力の中核を担う構造へ移行している。[1,2]

2026 年 7 月 21 日に決定された「日本成長戦略」は、AI・半導体、情報通信、防衛産業、航空・宇宙、海洋等を含む戦略 17 分野を掲げる。防衛産業は独立した一分野であるだけでなく、複数の先端技術分野を接続する需要側・実証側のハブとなり得る。防衛投資を通じて技術基盤を高度化し、民生市場へ展開するスピルオーバーと、民生イノベーションを防衛装備へ取り込むスピンオンを循環させる制度・契約設計が重要となる。[1,2]

1.1 市場ポテンシャルと試算上の留意点

項目	米国デュアルユース市場	日本デュアルユース市場
2025 年の推計規模	約 24 兆円	約 2.4 兆円
2040 年のシナリオ値	約 500 兆円 （引用元の推計モデル）	約 16.8 兆円 （ベースライン 8.6 兆円＋技術・人材転用効果 8.2 兆円）
推計の性格	過去の技術波及速度等を踏まえたシナリオ推計	引用元によるポテンシャル試算。公的統計上の確定市場規模ではない
主な波及領域	専門技術サービス、電子部品、クラウド、データ処理、システム設計等	輸送機械、鉄鋼、電子部品、素材等。今後は AI・クラウド・データ統合への波及拡大が課題

計算関係の注記

日本の「過去 CAGR 10.2%」は、引用元が示す過去の成長実績・参照指標であり、2.4 兆円から 8.6 兆円を算出する単純複利率として扱うことはできない。2.4 兆円から 8.6 兆円への 15 年間の単純年率換算は約 8.9%である。仮に 10.2%を 15 年間機械的に適用すれば約 10.3 兆円となり、8.2 兆円を加算した合計は約 18.5 兆円となる。このため、本報告書では 16.8 兆円を引用元の独立したシナリオ値として扱う。[3,4]

市場が拡大しても、企業が防衛デュアルユース事業へ参入・拡大する際には、民生事業とは異なる知財上の制約が生じる。政府委託・調達における権利帰属と利用許諾、特許出願非公開制度、第一国出願制限、輸出管理、CUI 等の情報管理、政府への納入データ・ソフトウェアのライセンスが交差するためである。したがって、知財戦略は、特許化、営業秘密管理、契約交渉、データ・ソフトウェア管理、輸出管理、サイバーセキュリティを統合した経営設計でなければならない。[11,18,20,25,29]

2. 防衛デュアルユース企業の知財・事業モデルと国内動向

防衛デュアルユース領域におけるグローバルな知財・事業戦略を理解するには、米国防衛テック企業のプラットフォーム型モデルと、日本国内で進む大企業・スタートアップ・政府研究機関の連携を対比することが有効である。本節では、会社の公式発表等で確認できる事実と、本報告書による分析・将来展望を区別して記載する。[5,6,7,8,9,10]

2.1 米国防衛テック企業：公表事実と筆者分析

Palantir Technologies

Palantir の公式資料によれば、Ontology は、プラットフォームに統合されたデータセット、仮想テーブルおよびモデルの上に位置する業務運用層であり、設備、製品、受注、取引等の現実世界の対象とデジタル資産を接続する。多くの環境で、意味要素とアクション・機能・動的セキュリティを含む組織のデジタルツインとして機能すると説明されている。[5]

公開情報を踏まえた筆者分析では、同社の競争優位は、個別アルゴリズムや特許のみではなく、顧客固有のデータ構造、アクセス制御、業務フロー、意思決定ロジックを再利用可能なプラットフォーム構造へ落とし込む能力にあると考えられる。FDE 等による現場実装は、その蓄積と継続的改善を支える一因とみられるが、社内での知財区分や競合排除効果は公開資料から直接確認できる事実ではなく、本報告書の分析である。[2,5]

Anduril Industries

Anduril は、無人航空機、水中無人機、対ドローン等のハードウェアと、Command & Control、Mission Autonomy、Mesh、SDK 等からなる Lattice ソフトウェア群を組み合わせている。第三者システムとの接続、通信制約下での運用、複数機体・センサーの統合を重視した製品体系を公表している。[6]

公表された製品体系からは、ハードウェアを含む垂直統合を維持しつつ、継続的な差別化と収益化の中核をソフトウェア基盤、接続仕様、エッジ自律制御および更新可能性に置く事業構造を志向していると分析できる。ただし、ソフトウェアの利益率や知財管理の詳細は非公開であり、「高利益率」を確認事実として断定すべきではない。災害対応、重要インフラ監視、物流、建設、海洋監視等は、既存の一部実績を除き、主として転用可能性として評価する。[6]

企業・連携	公表事実（技術・事業）	民生展開	本報告書の分析・将来展望
Palantir	Gotham、Foundry、AIP、Apollo、Ontology。Ontology はデジタル資産を現実世界の対象へ接続する運用層として公表。	製造、ヘルスケア、金融、サプライチェーン等で民生利用を公表。	【筆者分析】データ構造・業務フロー・権限制御を一体化する実装能力が競争優位の一因。社内の「コア知財」区分や競合排除効果は非公開。
Anduril	Lattice C2、Mission Autonomy、Mesh、SDK と無人システム群。第三者接続とエッジ運用を重視。	公共安全等のデュアルユースを公表。災害、インフラ、物流等は転用可能性を含む。	【筆者分析】ソフトウェア基盤・接続仕様・更新機能を継続的差別化の中核に置くとみられる。利益率は公開資料から断定不可。

企業・連携	公表事実（技術・事業）	民生展開	本報告書の分析・将来展望
三菱重工業×PFN	2026 年 6 月、社会インフラ・安全保障分野のミッションクリティカル機器・システム向け国産 AI 技術の共同開発を公表。	社会インフラの自律化、予知保全、危機対応等。	【筆者分析】重工のハード・制御・シミュレーションと PFN の基盤モデル・AI チップ・計算基盤を組み合わせる統合型モデル。
Sakana AI	2026 年 2 月 10 日、DISTI と「複数 AI 技術の組み合わせによる観測・報告・情報統合・資源配分高速化の研究」を約 9.65 億円で契約。SVLM 等を開発。	公表された直接目的は防衛 C2 高度化。行政・産業への応用は将来展望。	【筆者分析】国産 AI エージェント・小型モデルの実証基盤となり得るが、民生展開や権利構造は今後の契約・事業設計に依存。
Skygate Technologies	Synspective と航空自衛隊の「宇宙システムにおけるセキュリティ標準ガイドラインの作成」事業を受注したと公表。	商用衛星通信、宇宙・サイバー防護への展開可能性。	【筆者分析】官需実績を標準・ガイドライン知見へ転換できれば、宇宙セキュリティ領域の信用資産となり得る。

2.2　日本国内における連携の萌芽と構造的課題

日本では、防衛省・防衛装備庁の研究開発投資の拡大に伴い、大企業と先端テック企業の連携が本格化している。三菱重工業と PFN は、重工業メーカーのハードウェア設計、制御、シミュレーション、システム統合と、AI 企業の基盤モデル、AI チップ、計算基盤を組み合わせ、社会インフラおよび安全保障分野の知能化・自律化を目指している。[7]

Sakana AI は、DISTI との委託研究で、陸・海・空のマルチモーダルデータを統合し、観測、報告、情報統合、資源配分を高速化するシステムと、小規模視覚言語モデル（SVLM）の開発を公表している。防衛装備庁の契約公表資料によれば、契約日は 2026 年 2 月 10 日、契約金額は 965,469,765 円である。[8,9]

一方、日本の課題は、政府投資がハードウェア・素材・個別装備に閉じ、民生のクラウド、データ、ソフトウェア、専門技術サービスへ十分に波及しない可能性にある。引用元記事の分析では、米国の波及先が高度デジタル・ソフトウェア産業に広がるのに対し、日本は輸送機械、鉄鋼、電子部品、素材等への比重が大きいとされる。今後は、「ハードウェア単体の売切り知財」から、更新可能なソフトウェア、データ連携、API、モデル、保守・学習サービスを含む「プラットフォーム知財」へ転換する必要がある。[3,4]

3. 国内外の制度的枠組み：特許出願非公開制度と政府調達知財ルール

防衛デュアルユース知財戦略では、技術の優位性だけでなく、制度と契約が権利範囲を決める。特に、日本の特許出願非公開制度、日本版バイ・ドール規定、防衛装備庁・DISTI の個別契約、米国 DFARS の Data Rights、OTA、輸出管理および CUI 保護要件を、案件ごとに分けて確認する必要がある。[11,17,18,20,24,25,29]

3.1　日本の特許出願非公開制度

経済安全保障推進法に基づく特許出願非公開制度は、2024 年 5 月 1 日に施行された。公にすることにより外部から行われる行為によって国家および国民の安全を損なう事態を生じるおそれが大きい発明について、出願公開等の特許手続を留保し、情報流出防止措置を講じる制度である。審査は、特許庁による第一次審査と、内閣府による保全審査の二段階で行われる。[11,12,16]

第一次審査では、政令で定める 25 の特定技術分野（法令上 47 項目に整理）への該当性が確認される。25 分野のうち 15 分野は分野該当性を基礎として保全審査対象となり得、10 分野は分野該当性に加えて一定の機能・性能、国の委託等の付加要件を満たす場合に対象となる。該当する出願は、出願受理後 3 か月以内に内閣府へ送付される。[12,13]

段階	主な手続・法的効果	出願の取下げ	実務上の留意点
出願前	日本国内でした未公開発明が対象となり得る場合、原則として最初に日本へ出願する。必要に応じ法 79 条の事前確認を検討。	出願前のため該当なし	外国出願禁止の該当性、輸出管理、共同発明地の確認が重要。

段階	主な手続・法的効果	出願の取下げ	実務上の留意点
第一次審査・内閣府送付	特許庁が出願受理後 3 か月以内に定型的選別。送付時は出願人へ通知。	可能	送付は中間的行為であり、保全指定そのものではない。
保全審査中	所要期間に法律上の上限はない。外国出願禁止が原則 10 か月で解除される仕組みを踏まえ、実質的に期間内の終了を想定。	可能。取下げ後も第一国出願義務には留意。	単に保全審査に付された段階では一般的な開示制限はないが、法 67 条 9 項の通知後は当該発明の公開が禁止される。
保全指定後	実施は原則許可制、開示は原則禁止、適正管理義務、外国出願禁止、特許手続留保等が生じる。	不可	指定期間は原則 1 年以内で、必要に応じ延長。解除・不延長で終了。

保全指定後の主要な義務・効果

- **発明の実施制限：**保全対象発明の実施は原則として内閣総理大臣の許可を要する。正当な理由があり、情報保全上の問題がないと判断されれば許可され得る。[12]
- **発明内容の開示制限：**保全対象発明の内容の開示は原則禁止される。業務上必要な共有でも、共有先、必要性、管理措置を確認し、他事業者への共有は所定の承認手続を要する。[12,14]
- **取下げ・外国出願：**保全指定後は出願を取り下げることができず、外国出願禁止が継続する。保全審査中の取下げ可能性と明確に区別する必要がある。[12]
- **適正管理：**指定特許出願人および発明共有事業者は、組織的、人的、物理的、技術的な適正管理措置を講じなければならない。適正管理措置の不備それ自体が直ちに刑事罰となるわけではないが、不備により役職員が正当な理由なく開示し、情報漏えいが生じた場合、出願却下や役職員・法人への罰則が問題となり得る。[12,14]

> **適正管理に関する表現上の注意**
>
> 「管理措置が不十分であれば直ちに出願却下」と単純化すべきではない。内閣府 Q&A は、管理不備により役職員が正当な理由なく開示し、漏えいが生じた場合を前提として、内閣総理大臣の判断による出願却下等を説明している。[12]

損失補償と外国出願事前確認

法 80 条の損失補償は、開発費の実費精算に限定される制度ではない。保全指定との因果関係があり、保全指定により生じることが社会通念上相当と認められる範囲では、製造・販売不能による逸失利益、実施許諾料相当額、外国特許を取得できなかったことによるライセンス機会の喪失、市場優位性を確保できなかったことによる利益差額等が対象となり得る。ただし、開発費・設備投資額それ自体が自動的に補償されるわけではなく、客観的な算定と立証が必要である。[15]

日本出願前に外国出願を行う必要がある場合、法 79 条に基づき、その外国出願が外国出願禁止の対象となるかについて特許庁長官へ確認を求めることができる。ただし、これは当該外国出願の禁止該当性に関する回答であり、将来の保全指定の有無や特定技術分野該当性一般を保証する制度ではない。[12,16]

3.2　日本版バイ・ドール規定と防衛装備庁・DISTI の契約

防衛装備庁の委託研究等では、産業技術力強化法 17 条（日本版バイ・ドール規定）を踏まえ、一定の条件の下で研究成果に係る知的財産権を受託者・研究実施機関へ帰属させることができる。防衛装備庁の FAQ は、研究実施者自身による利用には制約がない一方、知的財産権の移転または専用実施権の設定等を行う際には、あらかじめ官の承認が必要であると説明している。[17,18]

日本版バイ・ドール規定を「国へ常に包括的・無制限の無償実施権が自動的に発生する制度」と理解するのは正確ではない。法令上の条件、公共利益上必要な場合の無償許諾に関する約定、不実施時の第三者許諾、移転・専用実施権等の承認、個別の委託契約・特別条項を確認する必要がある。したがって、政府利用権の対象を FIP に限定すること、BIP ライセンスを必要最小限とすること、民生利用権や更新権限を企業に留保することは、当然に認められる権利ではなく、企業側の契約交渉目標として整理すべきである。[17,18]

DISTI は、防衛分野のブレークスルー研究や迅速な実証・実装を担う組織であるが、国内の DISTI 契約と、米国の Other Transaction（OT/OTA）は異なる法制度である。国内案件では日本法と個別契約条項を、米国案件では OT 契約の個別交渉条件を別々に分析しなければならない。[8,9,18,24]

3.3 米国 DFARS の Data Rights と契約実務

米国国防総省との契約では、特許権の帰属だけでなく、政府へ提出・提供する技術データおよび非商用コンピュータソフトウェアに対するライセンス権が決定的に重要である。技術データは主として DFARS 252.227-7013、非商用コンピュータソフトウェアは同 252.227-7014、SBIR/STTR データは同 252.227-7018 等で扱われる。適用条項、開発資金、開発単位、納入義務、事前の権利主張、表示（marking）を契約単位で確認する必要がある。[19,20,21,22]

区分	典型的な対象・資金条件	政府の主な権利	第三者開示・重要な留意点
Unlimited Rights	政府資金のみで開発された対象データ、FFF、OMIT 等、条項所定のデータ。	政府は目的を問わず使用、修正、複製、公開、第三者提供等が可能。	技術データ・ソフトウェアのライセンスであり、特許ライセンスを当然に含まない。輸出管理・機密・契約上の制限は別途適用。
Government Purpose Rights（GPR）	混合資金で開発された技術データ・ソフトウェア等。	原則 5 年または交渉期間、政府目的で利用・第三者開示可能。期間満了後は通常 Unlimited Rights へ移行。	第三者開示は米国政府目的に限定され、受領者の NDA または所定条項が必要。期間の起算点は開発を要求した契約・変更等の実行時。
Limited Rights	民間自己資金のみで開発された非商用技術データ。	政府内部での利用が中心。製造目的の使用・外部開示は原則制限。	緊急修理・オーバーホール、Covered Government Support Contractor、一定の外国政府評価利用等の例外がある。
Restricted Rights	民間自己資金のみで開発された非商用コンピュータソフトウェア。	単一コンピュータでの使用、バックアップ、所定の修正・保守等に限定。	支援請負業者、緊急修理等への提供には所定の条件・NDA が適用。単純な「外部開示全面禁止」ではない。
SBIR/STTR Data Rights	SBIR/STTR Phase I・II・III 契約等で開発・生成されたデータ。	契約授与日から原則 20 年間の保護期間。期間中は技術データ・ソフトウェアを特別に保護し、満了後は原則として永続的 GPR。	起算点は「契約締結日」ではなく date of contract award。条項・表示・個別交渉を確認。

Data Rights と特許権は別個に分析する

DFARS 252.227-7013 等は、条項上、技術データのライセンスから政府への特許ライセンスが黙示されるものではない旨を明記している。したがって、政府が Unlimited Rights を有するデータを第三者へ提供できる場合でも、第三者による製造・実施が別途特許権を侵害するかは、政府の特許ライセンス、28 U.S.C. §1498 その他の制度を含め、別途検討する必要がある。[20,22]

権利主張・表示（Marking）と証拠化

DFARS では、契約前後の権利主張と、納入データ・ソフトウェアへの適切な restrictive legend が重要である。無表示で納入された技術データは Unlimited Rights で納入されたものと推定され得る。一定の要件の下で不注意による表示漏れを訂正できるが、原則として納入後 6 か月以内の申請、正当性の立証、訂正前の政府の使用・開示について政府が責任を負わないことの承認等が必要となる。[20,22]

企業は、開発資金の出所を部品・機能・モジュールの最小実務単位で管理し、BIP/FIP、データ種別、納入義務、政府ライセンス区分、表示文言、保存場所、第三者権利を契約前の Data Rights Matrix で確定させる必要がある。[19,20,21,22]

Other Transactions（OT/OTA）

米国の Other Transactions は、一般に FAR ベースの通常調達契約とは異なる柔軟な法的手段であり、研究・試作等の目的に応じて利用される。知的財産、データ権、政府利用、第三者提供、フォローオン生産等の条件を個別交渉しやすいが、「規制を全面的に回避する制度」ではない。適用法、権限、承認、競争、会計、セキュリティ、輸出管理等は別途確認し、交渉結果を契約文書へ明確に反映する必要がある。[24]

4. 防衛デュアルユース企業における知財リスクと課題

4.1 特許出願非公開制度による民生展開の時間・機会リスク

物流ドローン、自動運転建機、スマートファクトリー等の民生用途を想定した技術であっても、明細書等に記載された発明が特定技術分野および付加要件に該当すれば、保全審査へ送付される可能性がある。保全審査・保全指定により、外国出願、出願公開、実施、情報共有等に時間的・法的制約が生じると、民生市場における先行者利益や海外権利化機会を減殺するおそれがある。[11,12,13]

ただし、保全審査に付された時点と保全指定後を混同してはならない。保全審査中は、法 67 条 9 項の通知前であれば一般的な公開制限は生じず、出願の取下げも可能である。企業は、審査段階、通知内容、外国出願禁止の解除時期、開示予定、事業計画を案件ごとに管理する必要がある。[12]

4.2 BIP/FIP の混同と政府利用権の過剰拡張リスク

政府資金導入前から保有するバックグラウンド知財（BIP）と、委託・調達プロジェクトで新たに創出されるフォアグラウンド知財（FIP）を明確に区分しない場合、FIP の実施に必要な BIP まで広く政府利用・納入・第三者提供の対象と解釈されるリスクがある。特に、ソースコード、モデル重み、学習データ、API、設計データ、テスト環境、開発ツール等が一体化している場合、境界の客観証拠が重要となる。[18,19,20,21]

特許権の名義が企業に残っても、政府へ提出した技術データ・ソフトウェアに広範な利用権が設定されれば、競争上の価値が低下し得る。逆に、データ権を限定しても、製品の運用、保守、監査、サイバー対応に必要な納入物を欠けば、政府側の受容性が低下する。BIP の保護と政府の正当な運用ニーズを両立する契約設計が必要である。[18,20,21]

4.3 輸出管理・政府契約・サイバー要件の重複

制度・標準	性格	実務上の主な確認事項
外為法・関連政省令	日本の安全保障貿易管理	貨物・技術の輸出、役務取引、みなし輸出等。特許出願・クラウド共有・共同研究と同期して判定。
ITAR	米国の防衛物品・役務・技術データ規制	USML 該当性、国籍・所在、再輸出・再移転、アクセス管理等を確認。
EAR	米国のデュアルユース品目・技術等の輸出管理	ECCN、仕向地、用途、需要者、米国由来比率、外国直接製品規則等を確認。
DFARS	DoD 調達規則・契約条項	Data Rights、CUI、インシデント報告、下請へのフローダウン等。契約に組み込まれた条項が基準。
NIST SP 800-171	CUI 保護のセキュリティ要件	非連邦システムで CUI を処理・保存・送信する場合の管理要件。NIST の現行刊行物は Rev.3。
CMMC	DoD サプライチェーンの評価・契約枠組み	2026 年 8 月 21 日現在、Phase II 要件は 2026 年 7 月 13 日付で停止。Phase I の自己評価要件は継続。適用は個別契約・最新公式情報で確認。

ITAR・EAR は輸出管理規制、DFARS は国防調達契約規則・条項、NIST SP 800-171 は CUI 保護のセキュリティ要件、CMMC は評価・契約要件化の枠組みであり、法的性格が異なる。これらを単一の「規制」として列挙するのではなく、適用根拠、対象情報、契約条項、システム境界、アクセス者、データ所在、下請フローダウンを分けて管理する必要がある。[23,25,26,27,28,29]

4.4 ソフトウェア・データ知財：特許化と秘匿化の相克

防衛デュアルユース技術の価値は、モデル重み、学習データ、オントロジー設定、エッジ自律制御ロジック、暗号・通信設定、運用データ、テストノウハウ等に分散している。これらを特許出願すれば、原則として出願後 1 年 6 か月で公開される一方、秘匿すれば排他権を得られず、独自開発や適法な解析に対抗できない可能性がある。[16,30,32]

学習データ、モデル重み、ハイパーパラメータ、個別設定値それ自体は、請求項の構成や技術的意義によっては特許保護になじみにくい。他方、学習方法、推論方法、コンピュータシステムとしての構成、学習済みモデル、構造を有するデータ等は特許対象となり得る。保護可能性と侵害立証可能性は、技術内容、請求項、入手可能な証拠に依存するため、「AI モデルやデータは特許保護できない」と一般化すべきではない。[30,31]

営業秘密化により、特許出願非公開制度の手続リスクや出願公開による技術開示を回避し得るが、輸出管理、政府契約上の情報提供義務、CUI 保護、共同研究契約、秘密保持、営業秘密の三要件に沿った管理等の義務は残る。営業秘密化は「制度リスクの遮断」ではなく、他の義務を前提とした保護手段の選択である。[12,20,25,28,32]

5. 今後企業に求められる知財戦略の処方箋

防衛投資を一時的な受託収入ではなく、民生・防衛双方の成長基盤へ転換するためには、技術、契約、証拠、情報管理、輸出管理を研究開始前から一体運用する必要がある。以下は、企業が優先的に実装すべき実務施策である。

5.1 特許出願・営業秘密管理判定マトリクスの導入

- **秘匿化を優先し得る技術：**製品・サービスから解析しにくく、長期間秘密を維持でき、独自開発の追随が容易でない技術。例：学習データの選別・前処理、モデル重み、ハイパーパラメータ、オントロジーマッピング、評価データ、製造・運用ノウハウ。[30,32]
- **特許化を優先し得る技術：**製品から構成を把握しやすい技術、標準化・ライセンス収益を狙う技術、第三者の独自開発に先回りする必要がある技術、侵害証拠を取得しやすいシステム・方法。[30,31]
- **判定項目：**リバースエンジニアリング可能性、秘密寿命、技術陳腐化速度、侵害立証、保全審査該当性、外国出願計画、輸出管理、政府契約の納入義務、標準化、共同研究者の範囲を数値評価する。

> **重要な留保**
>
> 秘匿化しても、契約上の納入義務や政府の監査・サイバー対応に必要な情報まで一方的に拒否できるわけではない。特許化・秘匿化判定は、政府への納入物と Data Rights の設計と同時に行う。

5.2 民生共通構成と防衛固有構成の整理

防衛用途固有の構成（特定軍事規格、任務固有の性能、特殊耐環境仕様、脅威情報等）と、民生用途にも共通する汎用構成（自律走行、一般インターフェース、データ統合、UI/UX、保守・更新機能等）を技術的・事業的に整理する。防衛用途の記載を意図的に隠すための不自然な分割ではなく、技術的に独立した発明単位、製品モジュール、契約納入物を整合させることが重要である。[12,13]

保全審査は請求項だけでなく明細書・図面に記載された発明を対象とし得るため、出願書類全体で機微性を確認する。民生共通構成を別出願・分割出願等で権利化する場合も、単一性、サポート要件、分割要件、第一国出願制限、共同発明者、優先権、輸出管理との整合を確認する。[12,16]

5.3 BIP/FIP の厳格な区分と事前客観証拠化

政府資金を導入する前に「BIP インベントリ」を確定し、既存特許、ノウハウ、ソースコード、データセット、モデル、設計図、試験方法、開発ツール、第三者ライセンスを記録する。研究ノート、Git コミット、電子タイムスタンプ、仕様書、設計審査記録、費用負担記録等を組み合わせ、開発時点と資金源を客観的に説明できる状態にする。[18,20,21]

- **契約交渉目標①：**政府利用権の対象を、契約資金で直接創出され、かつ納入対象として合意した FIP・データ・ソフトウェアへ明確化する。
- **契約交渉目標②：**FIP の利用に BIP が必要な場合、目的、利用者、期間、第三者提供、改変、製造、再許諾、セキュリティ条件を限定した BIP ライセンスを提案する。

- **契約交渉目標③：**民生利用、海外利用、アップデート、派生モデル、学習済みモデル、運用データ、改良発明の帰属と利用を明記する。
- **証拠化：**資金源を最低実務単位で紐付け、開発前・開発中・納入時の三時点で BIP/FIP 表を更新する。

5.4　第一国出願制限・輸出管理・情報管理を統合した発明クリアランス

発明提案の段階で、①発明地・共同発明者、②特定技術分野・付加要件、③外国出願の予定、④外為法・ITAR・EAR、⑤政府契約・CUI、⑥第三者秘密情報、⑦クラウド・海外拠点アクセスを一体で審査する。必要に応じて法 79 条の確認請求を利用し、外国出願禁止の該当性に関する回答を得る。[12,16,25,26,27]

知財部、法務、輸出管理、情報セキュリティ、研究開発、政府営業を横断する「安全保障知財レビュー」を設置し、発明届、論文、学会発表、データ共有、ソースコード移転、海外クラウド利用、外国人研究者アクセスを同じゲートで管理することが望ましい。

5.5　政府調達契約における個別ライセンス設計

国内：防衛装備庁・DISTI 等

日本版バイ・ドール規定による受託者帰属を出発点としつつ、政府利用権の対象、目的、期間、対象機関、第三者開示、改変、再委託、納入物、ソースコード預託、脆弱性対応、アップデート、終了時の取扱いを個別契約で明確化する。民生市場の排他権や第三者ライセンス権、アルゴリズム更新権限を企業側に留保することは交渉目標であり、法令上当然に保証されるものではない。[17,18]

米国：FAR/DFARS 契約および OT

米国案件では、技術データとソフトウェアを分け、開発資金、納入義務、政府権利、保護期間、表示、第三者権利、SBIR/STTR 該当性を Data Rights Matrix へ落とし込む。OT では、柔軟性を利用して BIP、FIP、政府目的利用、フォローオン生産、民生利用、ソフトウェア更新、終了時のライセンスを具体的に交渉する。[19,20,21,22,24]

5.6　経営・取締役会向けの知財 KPI

防衛デュアルユース事業では、特許件数だけではリスクと価値を把握できない。経営・取締役会には、①BIP 特定率、②納入物の権利区分確定率、③制限表示の適正率、④保全審査・輸出管理の事前判定率、⑤営業秘密アクセス権の棚卸率、⑥CUI 対象システムの適合状況、⑦民生転用可能モジュール比率、⑧政府契約終了後の利用可能性を定期報告することが有効である。

管理領域	主要 KPI 例	経営上の意味
BIP/FIP 管理	研究開始前 BIP 登録率、資金源紐付率、開発履歴証拠化率	政府利用権の過剰拡張と紛争を予防
データ・ソフトウェア	納入物権利区分確定率、適正 legend 率、第三者ライセンス確認率	DFARS・国内契約上の権利喪失を予防
出願・秘匿	判定マトリクス実施率、営業秘密管理監査、侵害立証可能性評価	公開・秘匿の誤選択を削減
安全保障コンプライアンス	第一国出願・輸出管理・CUI 統合審査率、例外・承認の記録率	罰則・契約違反・市場排除リスクを低減
事業成長	民生共通モジュール比率、外部ライセンス可能資産、継続収益比率	防衛 R&D を民生成長へ転換

6.　結論：知財戦略を軸とした民生・防衛連携エコシステム

防衛デュアルユース分野における企業知財戦略は、従来の「特許で自社技術を守る」または「法務リスクを避ける」という受動的枠組みを超え、企業の成長と国家の安全保障基盤を同時に支える経営戦略の中核となる。特許、営業秘密、データ、ソフトウェア、契約、輸出管理、サイバーセキュリティを別々に扱うのではなく、研究開始前から一体設計することが必要である。

米国では、防衛 R&D や政府調達を通じて高度化されたネットワーク、無人システム、データ統合・AI プラットフォーム等が民生市場へ展開され、デュアルユース産業基盤の形成に寄与してきた。オントロジー技術一般を防衛 R&D 起源と断定するのではなく、政府・防衛現場での実装が、データ統合・意思決定プラットフォームの高度化と民生展開を促したと評価するのが適切である。[2,3,5,6]

日本について引用元が示す 2040 年約 16.8 兆円は、8.6 兆円のベースラインと 8.2 兆円の技術・人材転用効果を組み合わせたシナリオ上の市場ポテンシャルであり、公的統計上の確定値ではない。このポテンシャルを実現するには、政府側の透明で予見可能な制度運用、柔軟かつ均衡の取れた契約設計、適正な損失補償と、企業側の BIP 保護、Data Rights 管理、特許化・秘匿化判定、安全保障コンプライアンスが両輪となる。[4,11,15,18,20]

知財戦略を安全保障と事業成長の双方に最適化し、民生共通技術を広く展開しつつ、防衛固有情報を適切に保全できる企業が、次世代の防衛・民生融合市場で持続的な競争優位を確立する。

参考文献・一次資料

法制度および政府契約に関する記述は、原則として下記の政府・公式資料を優先して確認した。企業事例については各社の公式発表を用い、市場規模・産業波及のシナリオ分析には提示された日経 Tech Foresight 資料を用いた。アクセス日は、特記のない限り 2026 年 8 月 21 日である。

1. 日本成長戦略 — 内閣官房（2026 年 7 月 21 日）
2. 防衛デュアルユース、戦略 17 分野と密接　5 つの注目技術 — NIKKEI Tech Foresight。提示資料
3. 米国のデュアルユース、2040 年に 500 兆円規模　実態と今後 — NIKKEI Tech Foresight。提示資料
4. 日本の防衛デュアルユース、有望 3 分野　R&D 再考で産業へ — NIKKEI Tech Foresight。提示資料
5. Ontology building: Overview — Palantir Technologies
6. Lattice: Command & Control / Mission Autonomy / Mesh / SDK — Anduril Industries。関連ページを含む
7. Mitsubishi Heavy Industries and Preferred Networks Form Business Alliance to Jointly Develop Japan-Made AI Technologies for Mission-Critical Applications — Mitsubishi Heavy Industries / Preferred Networks（2026 年 6 月 2 日）
8. Sakana AI、防衛イノベーション科学技術研究所からの委託研究を開始 — Sakana AI（2026 年 3 月 13 日）
9. 随意契約に係る情報の公表（物品・役務等） — 防衛装備庁 防衛イノベーション科学技術研究所（2026 年）
10. 「宇宙システムにおけるセキュリティ標準ガイドラインの作成」受注発表 — Skygate Technologies
11. 特許出願の非公開に関する制度 — 内閣府
12. 経済安全保障推進法の特許出願の非公開に関する制度の Q&A（第 3 版） — 内閣府（2026 年 3 月 27 日）
13. 特定技術分野および付加要件に関する資料 — 内閣府
14. 特許出願の非公開に関する制度における適正管理措置に関するガイドライン — 内閣府
15. 損失の補償に関する Q&A（第 2 版） — 内閣府
16. 特許出願非公開制度についての Q&A — 特許庁
17. 日本版バイ・ドール制度（産業技術力強化法第 17 条） — 経済産業省
18. 安全保障技術研究推進制度　FAQ（知的財産権等） — 防衛装備庁
19. DFARS Part 227—Patents, Data, and Copyrights — Acquisition.gov
20. DFARS 252.227-7013 Rights in Technical Data—Other Than Commercial Products and Commercial Services — Acquisition.gov（DFARS Change 5/7/2026）
21. DFARS 252.227-7014 Rights in Other Than Commercial Computer Software and Documentation — Acquisition.gov
22. DFARS 252.227-7018 Rights in Other Than Commercial Technical Data and Computer Software—SBIR/STTR — Acquisition.gov
23. DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting — Acquisition.gov
24. Other Transactions for Research / Prototype Projects — Defense Acquisition University
25. 安全保障貿易管理 — 経済産業省
26. International Traffic in Arms Regulations (ITAR), 22 CFR Parts 120–130 — eCFR
27. Export Administration Regulations (EAR) — U.S. Bureau of Industry and Security
28. NIST SP 800-171 Rev.3: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations — NIST（2024 年 5 月）
29. Cybersecurity Maturity Model Certification (CMMC) — U.S. Department of Defense Chief Information Officer（2026 年 8 月時点）。2026 年 7 月 13 日の Phase II 停止および Phase I 継続を確認
30. AI 関連技術に関する事例について — 特許庁
31. 特許・実用新案審査ハンドブック — 特許庁（2026 年 7 月 1 日更新）
32. 営業秘密管理指針・関連資料 — 経済産業省

改訂管理

今後、特許出願非公開制度の Q&A・特定技術分野、DFARS、CMMC、輸出管理規則、政府調達条項に変更が生じた場合は、情報基準日を更新し、制度部分を再検証することが望ましい。