CORPORATE IP STRATEGY | DEFENCE & DUAL USE

防衛デュアルユース分野における企業知財戦略

現状、契約・データ権の構造、先進企業の実装、今後の課題と実務ロードマップ

結論

勝敗を分けるのは特許件数ではない。商用コアを守りながら、任務継続・競争調達・同盟国連携に必要な利用権を設計し、データ、ソフトウェア、秘密、輸出管理を一体運用する能力である。

本報告書が扱う問い

企業は何を権利化し、何を秘匿し、どの範囲を政府・共同研究先・海外パートナーに使わせるべきか。添付連載を出発点に、日米欧・NATO の一次資料、公開契約・企業開示、最新の制度改正を突き合わせ、権利マトリクス、契約論点、成熟度モデル、90 日／1 年／3 年ロードマップまで提示する。

基準日：2026 年 8 月 21 日
文書種別：総合調査報告書（公開情報のみ）
主対象：経営層、知財・法務、事業開発、技術、輸出管理、情報保全、調達・研究部門

目次

各項目をクリックすると本文へ移動する。章・付録・参考資料を同じ目次から参照できる。

要旨

企業知財戦略の目的は、①任務継続に必要な権利を顧客へ渡す、②商用コアと海外展開の選択肢を企業に残す、③機微技術を漏らさない――という三つの目的を同時達成することである。

> **経営判断の要点**
>
> 『全部自社保有』も『政府に全部譲渡』も最適解ではない。資産を最小単位へ分解し、所有権、納入物、利用目的、利用者、地域、期間、再許諾、緊急時・倒産時の権利を別々に交渉する。最重要 KPI は特許件数ではなく、必要な自由度と継続能力を案件開始前に確保できた比率である。

確認された現状

1. 日本は、日本版バイ・ドール、ATLA の知財特約、特許出願非公開、重要経済安保情報、輸出管理、研究セキュリティ、防衛産業サイバー基準を整備した。しかし制度が分散し、契約前に横断設計する企業負担が大きい。
2. 米国は DFARS で技術データ・ソフトウェアの利用権を資金源と最小分離単位で定め、MOSA でインターフェースと第三者統合に必要な権利を要求する。一方、GAO は運用段階の権利不足と vendor lock を複数装備で確認した。[U1][U7][U9]
3. EU の EDF は、research action の成果を原則として生成した受益者に残し、development action では EU 自身が成果製品・技術を所有せず IPR を主張しない一方、非関連第三国による支配・制約や域外移転を厳しく制御する。NATO DIANA は参加企業の IP を取得しないと明示し、入口段階の心理的障壁を下げる。[E1][N1]
4. ソフトウェア・AI 企業は、特許だけでなく著作権、営業秘密、know-how、契約、API、データ境界を組み合わせる。Palantir は特定特許に依存しないと開示し、Anduril は公開 API と自社 SDK 権利を両立、Shield AI は顧客開発部分の IP 保持を訴求する。[C1][C3][C5]
5. 2026 年の日本では、知財取引指針、技術流出対策ガイダンス第 2 版、経済安全保障経営ガイドラインが相次いだ。知財管理は知財部だけの仕事から、取引適正化・経済安全保障・サプライチェーン統治へ拡張している。[J17][J18][J19][J20]

最優先の 5 課題

優先	課題	放置時の損失	企業が先に打つ手
1	権利と納入物の混同	所有していても保守・競争・輸出ができない	asset-by-asset rights matrix を提案前に作る
2	商用コアの汚染	政府資金・共同研究条件が全製品へ波及	共通コア／任務層／顧客層を技術・会計・契約で分離
3	AI・データ権の空白	再学習、監査、改善、事故検証が停止	training・evaluation・operational data、weight、log を別定義

優先	課題	放置時の損失	企業が先に打つ手
4	輸出・秘密・cloud access の後追い	外国人アクセス、海外保守、発表で違反・漏えい	案件／version 単位の統合 stage-gate
5	下請・大学への flow-down 不全	権利断絶、OSS 違反、背景 IP 侵害	同一台帳・同一承認・同一表示ルールを契約階層へ展開

本報告書の提言

- 経営目標を『mission availability × growth optionality × technology security』の三軸で明文化する。
- 商用共通コア、防衛ミッション層、顧客・運用固有層の三層 ring-fence を標準アーキテクチャにする。
- 所有権、納入義務、利用権、アクセス権、輸出可否、秘密区分を別フィールドで管理する。
- 提案、契約、共同研究、モデル更新、輸出、M&A を同じ案件 ID・version で審査する。
- 政府へは最大権利ではなく、保守・競争・緊急時・同盟国運用に必要な『minimum sufficient rights』を選択式で提示する。
- 90 日で資産棚卸しと標準条項、1 年で部門横断運用、3 年で同盟国・供給網を含む権利オーケストレーションへ進む。

1. 調査目的・定義・方法

1.1 調査目的

本報告書は、防衛デュアルユース企業が研究、試作、装備品契約、量産、保守、輸出、民生展開を通じて競争力と技術安全保障を両立するための知財戦略を整理する。対象は特許に限らず、営業秘密、著作権、ソフトウェア、データ、AI モデル、標準・API、設計・製造 know-how、商標、契約上の権利を含む。

1.2 用語

用語	本報告書での意味
Background IP	案件開始前に保有・管理する知財、データ、ソフトウェア、know-how。案件中の改良も自動的に foreground とは限らない。
Foreground IP	契約・共同研究・委託研究の遂行により新たに生じる成果。資金源だけでなく契約定義で範囲が変わる。
Data rights	政府等が技術データ・ソフトウェアを使用、複製、改変、開示、第三者利用させる契約上の license rights。所有権とは別。
Sovereign control	国内所有だけでなく、必要時に運用・改良・保守・供給・移行できる実効的な支配力。
Dual use	同一または近接する技術・製品・データ・製造能力が民生と防衛・安全保障の双方に使われ得る状態。

1.3 方法と証拠の扱い

添付の日経テックフォーサイト連載 5 本と連載 docx を論点発見の起点とした。[A1]〜[A6] 制度・数値・契約ルールは、法令、政府機関、調達規則、監査報告、企業の法定開示または公式文書で再検証した。非公開契約の内容は推測せず、公表された標準条項や製品条件と、分析上の含意を区別した。

表示	意味	読み方
確認事実	一次資料または当事者開示で確認	日付・適用範囲・例外を併記
企業開示	企業の法定開示・公式製品説明	宣伝的主張は契約保証と同一視しない
本報告書の評価	複数資料を統合した分析	契約・案件ごとの legal review が必要
提言	企業が実装できる標準プロセス	自社規模・技術・顧客に合わせて tailor

> **留意**
>
> 本報告書は法的助言ではない。輸出管理、秘密指定、外国出願、競争法、政府契約は事実関係と条項により結論が変わるため、個別案件では専門家と当局への確認が必要である。

2. 防衛デュアルユース知財の構造

2.1 通常の知財戦略との違い

一般事業では、排他権、模倣防止、license 収入、自由実施性が中心となる。防衛デュアルユースでは、顧客が長期運用、戦時増産、修理、第三者統合、同盟国運用を求め、同時に技術・運用情報の開示を制限する。ゆえに『公開して独占する特許』と『隠して守る秘密』の二択では足りず、誰が、何の目的で、どの粒度の情報へ、いつまでアクセスできるかを設計する必要がある。

経営目的	企業側の要求	政府・顧客側の要求	衝突点
成長	商用再利用、海外販売、投資・M&A	第三国支配排除、輸出・再移転管理	exclusivity と市場アクセス
競争力	core secret、差別化、価格決定力	競争調達、interface、第三者保守	vendor lock とフリーライド
任務継続	継続課金、managed service	停止時・倒産時も運用・修理	source・escrow・step-in
安全	情報を最小開示	監査、試験、事故調査、説明責任	証拠・log・model access

2.2 所有権より『権利束』

知財の『所有』は一つのラベルに見えるが、実務では使用、複製、改変、派生物作成、開示、再許諾、輸出、保守、教育、評価、学習、benchmarks 公開などの権利束である。さらに、権利があっても納入されなければ使えず、納入されても表示・形式・品質が不適切なら実用にならない。

層	問い	典型的失敗
Ownership	誰が権利者か	共有持分・従業員発明・subcontractor 成果が未整理
Deliverable	何を、いつ、どの形式で納めるか	source、schema、test data、tooling が納入対象外
License	誰が何目的で使えるか	政府目的、同盟国、第三者保守の範囲が曖昧
Access	実際に誰が取得できるか	cloud tenant、鍵、退職者、外国人権限が契約と不一致
Assurance	完全性・来歴・再現性を証明できるか	marking、version、hash、SBOM、学習履歴が欠落
Regulatory	輸出・秘密・公表を許されるか	license 権があっても法令上アクセスできない

2.3 推奨 ring-fence

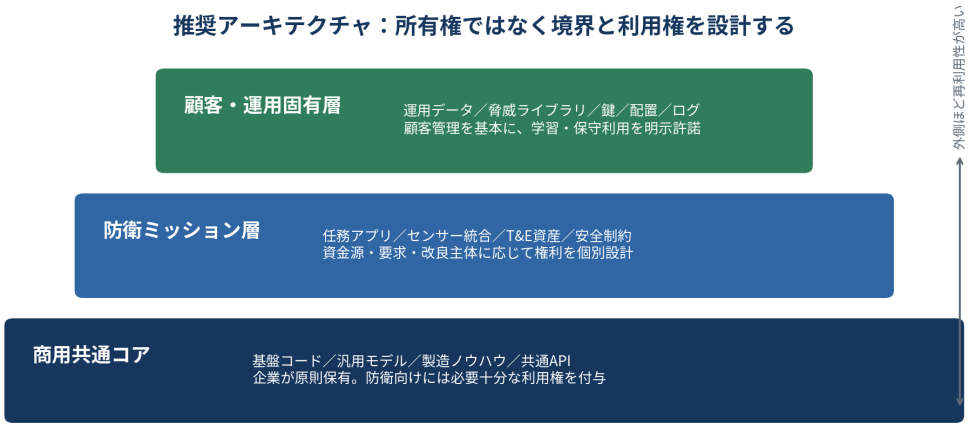

図 1　商用コア、防衛ミッション層、顧客・運用固有層を分ける IP ring-fence

三層分離は物理的な repository だけでなく、要求、会計上の資金源、発明記録、data lineage、契約定義、アクセス制御、SBOM を一致させて初めて機能する。共通コアへ政府資金の成果や顧客固有データが混入すれば、商用再利用・海外移転の自由度を失い得る。逆に顧客層の運用データを企業が無制限に再利用すれば、秘密・privacy・任務安全を損なう。『国産』を全コード・全部品の国内開発と解すると速度・費用・相互運用性を失うため、主権性は重要な判断ロジック、interface、鍵、任務データ、保守・移行権を国内で制御できるかで評価する。

3. 日本の現状

3.1 制度は『企業帰属＋公共目的権利』を基本にする

確認事実

日本版バイ・ドールは、一定条件で国の委託研究成果を受託者に帰属させ、事業化を促す。[J1] 安全保障技術研究推進制度も、条件を満たせば知財を研究実施者に帰属させ、成果公表を前提としつつ、譲渡・専用実施権等に政府承認を求める。[J2][J3]

当該知財特約が契約に組み込まれた場合、新研究成果に係る知的財産権は、企業が所定義務の遵守を確約して書面申請し、政府が自ら保有する必要がないと判断して承認することにより、企業帰属を維持し得る。企業帰属の場合でも、公共の利益のため特に必要な場合の政府・指定第三者への無償実施許諾に加え、政府に提出された新研究成果について政府利用に必要な範囲の無償実施許諾、一定の長期未活用時の第三者許諾、移転・専用実施権等の事前承認、公表・第三者開示・産業財産権出願の原則事前書面承認等を定める（条項上の例外あり）。[J4] 迅速装備化の特約にも、日本版バイ・ドール型の企業帰属と政府利用権が組み込まれている。[J5]

場面	成果帰属の基調	政府側の主な保全手段	企業実務の焦点
公開型研究助成	条件付き企業・研究者帰属	報告、利用・譲渡承認、必要な権利	公表自由と次段階の秘密化境界
装備品 R&D・製造	特約・申請により企業帰属可	無償実施、第三者許諾、移転承認	background 定義、納入物、改良、foreign party
迅速取得	企業帰属を残しやすい	政府の一定 license、秘密・情報管理	prototype から量産時の権利変化
K Program 等	制度・契約ごとに設定	協議会、研究 security、成果活用条件	複数資金の混在・joint IP。[J27]

3.2 特許出願非公開は『出願前統制』を要求

特許出願非公開制度は 2024 年 5 月に開始し、指定技術分野の国内発明について日本先願義務、特許庁の一次審査、内閣府の保全審査、外国出願禁止の事前確認を設けた。[J6][J7] 2024 年度 90 件、2025 年度 106 件が内閣総理大臣へ送付され、両年度とも保全指定は 0 件であった。[J8a][J8] 指定件数が 0 でも、発明地、発明内容、学会発表、外国出願、PCT 日程を出願前に確認する運用負担は残る。

> **実務含意**
>
> 防衛・宇宙・量子・センサー等では、発明届の後に外国出願可否を検討するのでは遅い。発明着想、論文投稿、採用広報、demo、repository 公開を一つの pre-publication gate へ載せる。

3.3 秘密・研究セキュリティ・輸出管理が知財利用を制約

重要経済安保情報保護活用法は 2025 年 5 月 16 日に施行され、政府が指定した機微情報を適合事業者へ共有する枠組みを整えた。[J9] 内閣府の初回国会報告では、期間中の指定 20 件、年末時点 19 件、適合事業者認定 0 件であった。[J10] これは制度が存在することと民間の利用が成熟していることが同義でないことを示す。

METI は 2025 年 10 月施行の補完的輸出規制に合わせ、大学・研究機関向け安全保障貿易管理ガイダンスを改訂した。[J11][J12] 政府の研究セキュリティ手順書や装備品等秘密の保全制度も、研究・契約・情報管理を横断する統制を求める。[J25][J26] 2026 年の技術流出対策ガイダンス第 2 版は、海外拠点・人材に加え、国内外の共同研究と調達時の『すり合わせ』を追加した。[J19] したがって、NDA だけで営業秘密と輸出管理を代替することはできない。

3.4 サイバー・取引適正化が知財戦略に合流

防衛装備庁は防衛産業サイバーセキュリティ基準と防衛事業適合事業者制度を更新し、契約相手方へ情報保全体制、教育、施設、秘密情報システム、点検を求める。[J13][J14] 2026 年 3 月の SCS 評価制度構築方針は、2026 年度末頃の制度開始を目指す。[J15] SBOM 国際共同ガイダンスは脆弱性だけでなく license 管理の効率化も効果に挙げる。[J16]

2026 年 6 月 24 日、公正取引委員会・中小企業庁・特許庁は『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』（以下、知財取引指針）を公表した。同指針は全業種を対象に、秘密管理、価値評価、契約実務、濫用等の判断枠組みを示す。[J17][J18] 防衛サプライチェーンでは、prime が security・data deliverable を下請へ flow-down する一方、無償の know-how 吸い上げや過大な成果帰属を避ける必要がある。security flow-down と fair IP treatment を同じ subcontract review で見るべきである。

3.5 日本企業の現在地

強み	弱み	機会	脅威
製造 know-how、品質、長期保守、民生技術基盤	契約・data rights 専門人材、software IP 台帳、早期市場検証	装備移転拡大、迅速取得、K Program、同盟国共同開発	外国規制の域外適用、特許先願制約、joint IP 断片化、cyber 漏えい

本報告書の評価

日本の課題は『成果が国へ奪われる』一色ではない。むしろ企業帰属を認める制度は存在する。実務上の不足は、①背景資産の定義、②政府が実際に必要とする利用ケース、③data/software deliverable の粒度、④外国関係主体・M&A・輸出時の承認を契約前に価格化する能力である。

4. 米国の現状

4.1 DFARS は資金源と最小分離単位で権利を決める

米国防総省の非商用品向け技術データでは、政府資金のみで開発した item/component/process に原則 unlimited rights、混合資金に government purpose rights、民間資金のみの開発に limited rights を付与する。判定は実務上可能な sub-item、subcomponent、process の segregable portion で行う。[U1][U2] 企業は政府へ license を付与し、付与しない権利を保持する。

technical data・software の license rights と、発明に係る patent title は区別する必要がある。連邦支援研究で生じた subject invention については、Bayh-Dole 法制が受託者の title 保持、政府の license、march-in 等を別に規律する。[U18]

標準権利	主な発生条件	政府の利用	企業側の論点
Unlimited rights	政府資金のみ、form/fit/function、OMIT data 等	無制限の使用・改変・開示・第三者利用	最低粒度の資金記録、例外 data の把握
Government purpose rights	混合資金。期間は交渉可能（標準条項上は名目 5 年）。満了後、政府は unlimited rights	政府目的で第三者へ開示可。期間中は商用利用不可	期間、対象 portion、legend、subcontractor 権利
Limited rights	民間資金のみの技術データ	政府内利用中心。外部開示を制限	form/fit/function・OMIT との境界
Specifically negotiated	標準権利が過大・不足	契約で目的・相手・期間を tailor	価格、step-in、競争、export の条件

注：GPR は所有権の移転ではなく、対象 data／software に対する政府の license rights である。期間は交渉可能で、標準条項上の名目期間は 5 年。満了後、政府は対象 data／software について unlimited rights を取得する。technical data と noncommercial software では根拠条項が異なる。OMIT = operation, maintenance, installation and training。[U3][U4][U5]

4.2 ソフトウェアは source・marking・OSS が勝負

非商用 computer software も資金源を segregable portion 単位で判定する。納入物、source code、documentation、restrictive legend を契約・assertion list・delivery で一致させなければ、想定より広い権利を失う危険がある。第三者・OSS license を含む場合、政府へ付与する権利と矛盾しない確認が必要である。[U4][U5]

> **企業側の定石**
>
> repository、commit、work package、funding charge code を対応させる。『この製品は民間資金』という製品単位の説明ではなく、機能・module・interface・data schema の最小分離単位で証拠を残す。

4.3 MOSA は interface IP を経営論点へ引き上げた

10 U.S.C. §§4401–4403 は、防衛取得 program に可能な限り modular open system approach を求め、acquisition strategy で技術データ deliverable と IP の扱いを説明し、主要 interface に適切・必要な IP rights を確保するよう定める。[U8][U9][U10] これは『open source 化』ではなく、第三者部品を統合できる interface、documentation、検証、configuration management を権利と技術の両面で準備する政策である。

interface data が民間資金または混合資金で開発されても、MOSA に使う modular system interface について政府目的権が認められる場合があり、民間資金部分には適切・合理的な補償を交渉する枠組みがある。[U11] 企業は interface を core secret と一体化せず、開放範囲と対価を製品戦略で先に決める必要がある。

4.4 先進制度でも vendor lock は解消していない

DoD は Intellectual Property Cadre を通じて life-cycle IP strategy の専門支援を整備しているが、GAO は 2025 年、調査した完成済み IP 戦略のいずれも全要求要素を含まず、各 program が数千の data deliverable の完全性・正確性 review に苦慮し、5 つの選定 system すべてが権利不足による vendor lock を経験したと報告した。運用段階に入ると選択肢は限定され、cost 上昇と repair 遅延につながる。[U6][U7]

> **反証からの教訓**
>
> 詳細な法体系があっても、権利の『取得』『納入』『表示』『品質検査』『保管』『更新』『実利用』を連結しなければ継続能力は生まれない。日本企業は米国制度の条文だけでなく、運用失敗を先回りして設計すべきである。

4.5 Cybersecurity と export control はアクセス権を変える

CMMC の Phase I は 2025 年 11 月に開始し、Level 2 では NIST SP 800-171 の 110 要件を基礎とする。DoD は 2026 年 7 月 13 日に Phase II への移行を停止して reform task force を設置したが、Phase I の自己評価要件と DFARS 252.204-7012 等は継続する。[U12][U13] これは CUI を扱う資格・契約適合性を左右し、知財台帳と別システムで扱えない。EAR は controlled technology または source code を外国人へ release する行為を deemed export とし、visual inspection、口頭・書面、access information を通じた release も対象とする。[U14][U15] technical data の外国人アクセスは重大な執行対象となり得る。[U20]

したがって、cloud へ置いた source、digital twin、model weight、設計図を『国外へ送っていない』だけでは不十分である。tenant region、support operator、admin privilege、LLM・code assistant への prompt、remote debug、海外子会社の access を export classification と連動させる。

5. EU・NATO の現状と制度比較

5.1 European Defence Fund：企業帰属と域内統制の両立

EDF の research action では、成果は原則として当該成果を生成した受益者に帰属する。共同生成で寄与を分離できない場合は共同所有となる。ただし、EU 支援が public procurement の形で提供される場合、成果は EU に帰属する。受益者が生成した成果を非関連第三国または非関連第三国 entity へ ownership transfer し、または exclusive licence を付与する場合は欧州委員会への事前通知を要し、それが EU・加盟国の安全保障・防衛上の利益または規則 3 条の目的に反する場合、EDF 支援の返還が必要となる。[E1][E2]

development action では、EU は成果たる防衛製品・技術を所有せず、当該 action に係る IPR を主張しない。非関連第三国または非関連第三国 entity への ownership transfer は事前通知の対象であり、同じ利益・目的に反する場合は支援返還となる。なお、両 action の成果は、非関連第三国またはその entity の支配・制約下に置いてはならない。[E1][E2]

EU 型の核心は『企業に残すが、域外の支配へ出さない』ことである。日本企業が欧州 consortium へ参加する場合、親会社支配、米国由来 technology、cloud、米国政府向け license、M&A 条項が eligible action の結果へ及ぼす制約を事前に map する必要がある。

5.2 EU dual-use regulation：software・technology・technical assistance

Regulation (EU) 2021/821 は dual-use items に software・technology を含め、export、brokering、technical assistance、transit、intra-EU transfer 等を統合的に規律する。[E3] EU は研究セキュリティについて risk-based かつ proportionate な対応を推奨し、営業秘密保護では秘密保持のための reasonable steps を重視する。[E4][E5] 研究・共同開発では、成果物の shipment だけでなく、remote access、共同 debug、training、source repository、conference 資料を管理対象として扱うべきである。

5.3 NATO DIANA：入口は IP-friendly、実装は別契約

NATO DIANA は Challenge Programme で innovator が全 IP を保持し、DIANA も stakeholder も権利を取得・主張しないと明示する。proposal 情報も confidential に扱う。[N1][N2] ただし、demonstration で third party cloud/platform provider との契約が必要になる場合があり、program 参加後の調達・統合契約まで同条件とは限らない。

> **本報告書の評価**
>
> IP-friendly funding は参入障壁を下げるが、採用・量産・保守段階の data rights を自動解決しない。企業は accelerator 参加時から、次契約で必要な government use、test evidence、interface、exportable baseline を準備する。

5.4 日米欧・NATO 比較

観点	日本	米国 DoD	EU／NATO
企業帰属	Bayh-Dole・ATLA 特約で可能	contractor retains title/rights not licensed	EDF は beneficiary 帰属、DIANA は IP 不取得
政府利用権	公共目的、無償実施、未活用時等	funding source 別の standard data rights	EDF は action 種別・access rights、各国調達契約
interface	ブロック化・モジュール化・open architecture 化を推進。[J29] interface rights 標準化は発展途上（本報告書の評価）	MOSA を法定化、interface rights を取得	interoperability 重視、program ごと
域外・外国支配	輸出、特許先願、移転承認、重要情報	EAR/ITAR、foreign ownership、CUI	非関連第三国の control/restriction を排除
startup 入口	研究助成・迅速取得・防衛省 SBIR を拡大。[J28]	SBIR、OT、DIU 等。[U16][U17][U19]	DIANA、EDF、NIF 等
主要弱点	制度分散、soft/data 契約標準、人材	運用段階の data 不足・vendor lock	国別 export と consortium 制約の複雑性

6. 知財資産別の戦略

6.1 特許：公開価値と安全保障制約を同時評価

防衛デュアルユースの特許判断は、権利化可能性だけでは決められない。①侵害を外部から発見できるか、②外国で権利行使できるか、③製品から reverse engineering されるか、④公開による安全保障・輸出影響、⑤標準・license 収入、⑥特許非公開可能性を評価する。AI・software では、claim 可能な技術的効果と、学習・評価の再現可能な記載も必要となる。[J21][AI1]

判断	向く資産	主な利点	主なリスク・補完策
通常特許	外部観測可能、標準、複数市場で実施	排他、cross-license、投資説明	公開・迂回設計。know-how を別管理
敏感特許	出願価値は高いが指定分野に近い	権利化 option を維持	日本先願・公表 gate・保全費記録
営業秘密	製造 recipe、調整値、学習・評価手順	期限なし、詳細非公開	漏えい・独自開発・reverse engineering。reasonable measures
defensive publication	core 外、競合の特許化阻止	freedom to operate 確保	安全保障・輸出・公表承認を先に確認

> **特許 KPI の注意**
>
> 特許出願件数は、非公開制度、営業秘密化、共同研究、公表制約により戦略の良否を歪める。価値 KPI は、事業の自由度、代替困難性、license 可能性、輸出可能性、侵害検出性を加味する。

6.2 営業秘密・製造 know-how：法的保護と情報保全を重ねる

日本の不正競争防止法上の営業秘密は、秘密管理性、有用性、非公知性を満たす必要がある。METI の 2025 年改訂営業秘密管理指針は法的保護のための最低水準を示し、秘密情報保護 handbook は漏えい防止・事後対応を扱う。[J22] 防衛契約上の秘密区分は営業秘密要件を自動的に満たす保証でも、企業の営業秘密を自動的に政府秘密へ変える制度でもない。二つの label と証拠を併存させる。

- 秘密指定対象を『製品全体』ではなく、recipe、tolerance、calibration、training curriculum、test threshold など情報単位で特定する。
- owner、利用目的、access group、保存場所、期間、開示先、輸出区分、契約番号を台帳化する。
- NDA に加え、least privilege、secure repository、download 制御、watermark、audit log、退職・異動時の権限剥奪を実装する。
- 共同研究・調達すり合わせでは、相手が既に知っていた情報、独自開発、residual knowledge、feedback、改良を明記する。
- black box 化と module 交換を組み合わせ、相手へ必要な性能・interface だけを渡す。

6.3 ソフトウェア・OSS・API：著作権より運用支配

software の競争力は、source code の著作権だけでなく、build system、dependency、container、署名鍵、deployment pipeline、test harness、API、schema、configuration、operator workflow に分散する。source を保有しても、toolchain・鍵・documentation がなければ修正できない。

資産	企業が守るもの	顧客へ必要になり得るもの	契約・技術対策
Source／binary	core source、build recipe	実行、修正、脆弱性修正、escrow	module 別 license、再現 build、trigger 限定 step-in
OSS／third party	license 適合、provenance	SBOM、脆弱性対応、notice	SCA、承認 list、copyleft 隔離、代替計画
API／schema	platform 差別化	第三者統合、データ出力、version 安定	deprecation notice、compatibility test、export format
Key／pipeline	release control、anti-tamper	緊急 patch、署名継続	dual control、backup、倒産・停止時 protocol

SBOM は構成部品と supply-chain 関係の正式な記録であり、脆弱性対応と license 管理の双方に効く。[J16][S1] ただし SBOM 自体に機微な製品構造が含まれ得るため、配布範囲・粒度・更新頻度・VEX 等の補足情報・秘密区分を決める。

6.4 データ：『所有』を避け、操作権限を定義

日本法ではデータすべてに一律の所有権が成立するわけではない。著作物、営業秘密、限定提供データ、個人情報、契約上の control が重なり得る。限定提供データは、限定提供性、相当蓄積性、電磁的管理性を満たす価値ある共有データの不正取得・使用・開示を規律する。[J23] 契約では抽象的な『data ownership』より、具体的な operation を列挙する。

Data 類型	典型的な生成者	必要な権利・制限	論点
Training data	企業、顧客、第三者、synthetic	学習、複製、加工、域外処理、保持	license、privacy、export、bias、来歴
Evaluation／T&E	政府、test range、企業	再現、監査、benchmark、公開	classified 条件、leakage、test overfitting
Operational data	装備・operator・sensor	収集、保守、事故調査、改善学習	任務秘密、個人、同盟国、retention
Derived data	analytics、label、feature、ontology	再利用、顧客間学習、export	元 data 権利、再識別、競争価値
Log／telemetry	platform・device	監査、cyber、rollback、performance	量、保存、incident privilege、政府 access

6.5 AI モデル：weight だけを議論しない

AI 資産は、architecture、code、pre-trained weight、fine-tuned weight、dataset、label、prompt、reward、synthetic environment、evaluation case、safety constraint、operator feedback、model card、log、deployment toolchain の組合せである。どれか一つの title だけで主権性や競争力は測れない。

- 発明者・著作者の人間による寄与を contemporaneous record へ残す。USPTO は 2025 年改訂 guidance で AI を tool とし、発明者は自然人のみと再確認した。[AI1] 米国著作権局も AI 生成物の copyrightability について人間の創作的寄与を中心に整理している。[AI2]
- 学習・評価 data の出所、同意、license、輸出区分、機密性、保持期限を dataset card で管理する。
- fine-tuning と field feedback により生じた weight・prompt・rule・label の帰属と再利用範囲を定める。
- 政府が必要とするのが weight 納入か、on-prem inference か、API access か、再学習権か、独立評価権かを use case で決める。
- model 更新のたびに性能・安全・輸出・秘密・IP 承認を version 単位で再判定する。

> **AI で増える新しい crown jewels**
>
> model weight より、operational feedback、失敗例、red-team 結果、synthetic scenario、mission-specific ontology、safety case が代替困難な資産になる。これらを『報告書付属データ』として無自覚に広範囲納入しない。

6.6 標準・interface・試験証拠

open architecture の価値は、仕様公開そのものではなく、代替 module が適合し、mission thread を壊さず交換できることにある。interface control document、reference implementation、conformance test、test vector、simulation、safety・airworthiness evidence を誰が使用・改変・第三者へ開示できるかを決める。

開くもの	閉じるもの	共同で管理するもの
外部 interface、message schema、最低限 test suite	core algorithm、optimization、製造 recipe、sensitive threshold	configuration baseline、conformance、脆弱性情報、change control

7. 企業ケースと再現可能な教訓

以下は公表事実に基づく。各社の非公開政府契約、内部発明方針、秘密管理水準を断定しない。『再現可能な教訓』は本報告書の分析である。

7.1 Palantir：IP portfolio と顧客 data の分離

企業開示

Palantir は 2025 Form 10-K で、patent、copyright、trademark、trade secret、know-how、contractual provision、confidentiality procedure を組み合わせ、特定の patent や application に依存しないと開示する。[C1] 同社は、製品・service の提供に伴い顧客のために personal data を処理する場面では、data processor として顧客の指示に従うと説明している。これは data protection 法上の役割であり、data の契約上の権利帰属とは区別される。[C2] 2025 年 5 月に Voyager Technologies の Form S-1 へ添付された公開契約例では、Customer Data およびその修正物の権利を顧客に残す一方、Palantir Technology、その派生物・修正・改良を Palantir 側に帰属させ、feedback について Palantir に広範な license を付与している。この権利区分は一契約例であり、全顧客の共通条件とは限らない。[C2a]

再現可能な教訓

- patent 単独で software platform を守らず、secret・contract・workflow・brand を portfolio 化する。
- 顧客 data を取得しない／限定処理する設計は、機微顧客の信頼と横展開を両立し得る。
- 移行可能性は raw data export だけで測らず、ontology、permission、workflow、application、training の再構築時間で測る。

7.2 Anduril：open data model と proprietary SDK の境界

企業開示

Anduril の Lattice API は open data models と Entities、Tasks、Objects API を提示し、REST・gRPC の SDK を提供する。[C3] 一方、2026 年 7 月更新の SDK license は、互換実装向けの限定的、取消可能、非譲渡、非再許諾 license で、SDK の IP を Anduril に残し、compatible implementation の判断を同社裁量とする。利用者が SDK で開発した application の IP は利用者に残す。[C4]

再現可能な教訓

- 『open API』は『open source』でも『platform 置換権』でもない。license、availability、version、certification 権を別確認する。
- 互換性は仕様書だけでなく、第三者が実施できる conformance test と mission-thread test で証明する。
- SDK 終了、major version、security fix、export restriction、credential 終了時の継続策を契約化する。

7.3 Shield AI × 三菱重工：platform 利用と sovereign mission IP

企業開示

Shield AI は Hivemind Enterprise について、利用者が構築した無人 system 向け IP の権利を保持できると訴求する。[C5] 三菱重工は Hivemind Enterprise を用いて、AI 開発から無人機搭載・飛行までを 8 週間で行い、日本製 mission autonomy の開発を加速すると公表した。[C6] MHI が従前は複数 OSS を使った開発環境の構築・維持に大きな労力を要したことも明示されている。

再現可能な教訓

- 外国 platform を使っても、mission-specific logic・data・test evidence・deployment authority を国内に残す『sovereign layer』は構築できる。
- ただし顧客開発 IP の保持と、platform SDK・simulation・compiler・runtime からの独立性は別。exit test を設ける。
- 短期化の便益を、license 継続、export、model portability、安全立証、vendor update 依存の cost と比較する。

7.4 日本の AI・space・secure drone 事例

公表事例	確認事実	知財戦略上の示唆（分析）
Synspective	SAR data・AI 分析、官民 consortium への参加を公表。[C7][C8]	raw data、derived analytics、model 改良、tasking、海外顧客を分離
ACSL	国産 security drone の防衛採用を公表。[C9]	機体特許だけでなく SBOM、署名鍵、component provenance が資産
Sakana AI	防衛装備庁防衛イノベーション科学技術研究所（DISTI）との AI 委託研究契約を公表。[C10]	prompt、weight、evaluation log、現場 feedback を独立定義
MHI × PFN	安全保障・基幹 infra 向け国産 AI 共同開発を公表。[C11]	background、sideground、共同成果、商用還流を開始時に合意

出所：各行末の一次資料。個別契約の権利条件は非公表であり、『知財戦略上の示唆』は本報告書の分析。

7.5 GAO の 5 装備：失敗ケースから学ぶ

GAO が調査した F/A-18、F-35、Littoral Combat Ship、Stryker、Virginia 級 submarine は、data-rights 不足により sole-source 依存を経験した。[U7] これは伝統的 prime の知財保護が不当だという単純な結論ではない。政府が use case、deliverable level、marking review、long-term sustainment を早期に計画しなかったこと、OMIT data と詳細製造 data の境界が曖昧なことが複合している。

> **企業側への含意**
>
> 顧客の権利不足を短期売上の源泉にすると、後年の強制的権利要求、競争政策、評判悪化を招く。保守 SLA、qualified second source、priced option、interface 開放、trigger 限定 license を先に提案し、継続収益と任務継続を両立する。

8. 今後の主要課題

8.1 課題全体像

課題	根本原因	早期警戒指標	主な対策
特許と秘密の選択遅れ	発明届・公表・外国出願が別process	demo／論文が先行	single release gate
Background 汚染	資金源・module・共同成果が混在	帰属不明 commit 増加	ring-fence、charge code、hash 台帳
Data／AI 権利空白	data ownership の一語で処理	再学習・監査の承認停滞	operation 別 rights matrix
Vendor lock	interface・toolchain・test 証拠不足	代替試験未実施	MOSA、export、escrow、exit drill
輸出・cloud access	shipment 中心の輸出理解	外国 admin・remote debug	classification 連動 IAM
Supply-chain 断絶	flow-down と fair treatment が分離	subcontractor assertion 未回収	同一 ledger・標準 schedule
人材・発明帰属	兼業・大学・転職・生成 AI	assignment gap、無断 upload	on/offboarding、発明記録、tool policy
M&A／foreign control	契約承認・資格を DD 後半で発見	change-of-control 例外なし	government-rights DD index

8.2 『所有権を取るほど安全』という誤解

政府が広い所有権を取得しても、技術者、toolchain、production line、supplier、test range がなければ運用継続できない。企業が全権利を保持しても、倒産・service 停止・外国規制で顧客が使えなければ任務は止まる。必要なのは所有権最大化ではなく、具体的 contingency に必要な権利・納入物・能力の組合せである。

8.3 Joint IP の断片化

大学、startup、prime、海外企業、政府研究所が共同開発すると、共同発明、copyright joint work、data、tool、sideground が分かれる。『成果は共同所有』だけでは、自己実施、第三者 license、訴訟、外国出願、持分譲渡、M&A、標準化の同意要件が国ごとに異なり、事業停止の原因になる。

- work package と inventive contribution を開始前に map し、可能なら単独帰属＋相互 license へ寄せる。
- joint ownership の場合は、出願国、費用、prosecution control、enforcement、settlement、license 収益、abandonment を定める。
- sideground（案件中だが scope 外の成果）と improvement を明示する。
- 学生、派遣者、consultant、OSS contributor の権利承継・守秘を確認する。

8.4 Classified environment での権利行使・立証

機密技術は公開 court で侵害を主張しにくく、相手製品の証拠取得も難しい。企業は権利行使可能性を特許価値に織り込み、必要に応じて contract audit、inspection、trusted third party、sealed evidence、government notification、arbitration、export-compliant discovery を設計する。

8.5 Long lifecycle と obsolete technology

装備は数十年使われるが、software、chip、cloud、OSS、AI model は短周期で更新される。契約時に最新だった API・license・supplier が 10 年後も存在する保証はない。architecture baseline、technology refresh、license successor、source escrow、data export、component obsolescence、key custody を life-cycle cost へ含める。

8.6 中小企業の固定費と取引力

新規参入企業には、secure enclave、export classification、秘密施設、contract specialist、SBOM、audit、insurance が売上前に発生する。prime・政府が必要権利を過大要求すれば、商用投資を毀損し参入を減らす。2026 年の日本の知財取引指針が価値評価と公正取引を強調する背景は、防衛供給網にも直結する。[J18] 政府は権利 menu、標準 schedule、迅速な承認、shared compliance environment、専門家支援を整備すべきである。企業は compliance cost を価格・milestone へ明示し、無償の know-how 移転を曖昧な『協力』で受けない。

9. 2026〜2030 年の変化

9.1 所有権から operational optionality へ

知財評価の中心は、権利証書から『必要時に別の主体が安全に運用・改良・量産・移行できる選択肢』へ移る。source code 保有だけでなく、build 再現、interface、test、鍵、data、trained personnel、qualified supplier を一つの continuity package として扱う。

9.2 Assurance evidence が独立資産になる

AI・自律 system では、性能だけでなく、dataset provenance、red-team、simulation、failure case、human-machine rule、software supply chain、model update history、audit log が調達・認証に必要となる。これらは再利用価値を持つ一方、脆弱性と任務特性を露出する。成果物・license・秘密区分・retention を独立設計する必要がある。

9.3 『open interface／closed implementation』が主流化

米国 MOSA、NATO の modularity・open architecture、各国の software-defined defense は、interface を開き、内部 implementation で競争する方向を強める。[U8][N3] 企業は interface を防衛要件で後付けせず、商用製品 roadmap に組み込み、公開・partner 限定・government-only の三段階で管理する。

9.4 Compliance evidence が市場 access 権になる

CMMC、ATLA cyber 基準、SCS 評価、important information、research security、SBOM は、単なる cost center ではなく取引資格を構成する。将来は security posture、software provenance、exportable baseline、data residency を迅速に証明できる企業が調達 speed で優位になる。

9.5 同盟国間の federated IP control

共同開発・共同調達では、一国が全 IP を集中所有するより、各国が core を保持し、共通 interface・test・mission data を federated に管理する形が増える。国家ごとの export、foreign control、security clearance、government purpose rights を machine-readable policy へ落とす需要が高まる。

9.6 日本の装備移転拡大は product-line 設計を迫る

2026 年 4 月 21 日の三原則・運用指針改正は、完成品 5 類型限定を削除し、完成品・部品・技術・修理役務を原則可・個別審査へ広げた。[J24] 企業は国内機微版、同盟国版、広域 export 版を後から文書差し替えで作るのではなく、crown jewel、anti-tamper、feature、data、support access、local production を product-line engineering で分離する必要がある。

変化	現在の主流	2030 年に向けた能力
収益 model	装備・license 単体	capability-as-a-service＋continuity option
知財台帳	patent／trademark 中心	code・data・model・test・funding・export 統合 graph
政府権利	一契約の条項確認	life-cycle use case 別・trigger 別 license menu
共同開発	joint ownership	modular ownership＋federated access control
security	事後 audit	policy-as-code、continuous entitlement・provenance
valuation	件数・簿価	再利用、移行時間、代替困難性、規制 option value

10. 日本企業の推奨知財戦略

10.1 経営目標を三軸で定義

軸	経営上の問い	代表 KPI
Mission availability	顧客は有事・停止・倒産時も運用、修理、更新できるか	復旧時間、代替 supplier、exit drill、critical deliverable acceptance
Growth optionality	商用再利用、海外展開、license、M&A の選択肢が残るか	background 再利用率、exportable module 比率、approval lead time
Technology security	crown jewel と機微 data を必要最小限の者だけが扱うか	classification coverage、access review、漏えい・例外、offboarding 時間

三軸を取締役会または経営会議の risk appetite へ落とし、案件ごとにどの軸を優先するか決める。戦略装備の core と、消耗品・commercial derivative では最適な権利配分が異なる。

10.2 技術資産台帳を一つにする

patent docket、source repository、data catalog、export classification、秘密台帳、contract repository を完全統合する必要はないが、共通 asset ID で相互参照できなければならない。

必須 field	例
Asset identity	module／dataset／model／drawing／process、owner、version、hash
Origin	creator、発明者、雇用・委託、background／foreground／sideground
Funding／contract	private、政府、mixed、award・subcontract 番号、適用条項
Rights	title、license、government rights、third-party、OSS、共同持分
Delivery／marking	CDRL・納期・形式・legend・acceptance・更新頻度
Control	秘密区分、輸出分類、data residency、access group、retention
Lifecycle	dependency、supplier、escrow、obsolescence、disposal、M&A 承認

10.3 One project, one risk ledger, one stage-gate

Gate	時点	必須判断	停止条件
G0 Opportunity	顧客接触前	技術区分、NDA、開示可能 baseline、partner DD	相手・用途・開示範囲不明
G1 Bid／Funding	提案前	background list、資金源、desired rights、price	core 汚染、無償過大権利
G2 Contract	署名前	rights matrix、deliverable、approval、flow-down	source／data／improvement 未定義
G3 Execute	開発中	発明、commit、data lineage、access、publication	権利承継・輸出判定なし

Gate	時点	必須判断	停止条件
G4 Test／Deploy	実証・release 前	T&E rights、SBOM、model card、marking、security	再現性・安全証拠・license 不足
G5 Scale／Export	量産・海外前	export baseline、local production、support、end-use	第三国・改良・再移転不明
G6 Change／Exit	M&A・停止・退役	change control、data return、escrow、assignment	政府承認・資格影響未確認

> **運用原則**
>
> gate は法務の承認 box ではない。技術責任者が asset boundary を提示し、事業が use case と価格、知財が権利、輸出管理が release、CISO が access、調達が flow-down を同時承認する。

10.4 役割と意思決定

役割	Accountability
Executive sponsor	三軸 trade-off、例外、投資、政府・partner escalation
Business／capture	顧客 use case、収益 model、競争・輸出 option、価格
Engineering／data owner	asset boundary、funding lineage、deliverable 品質、architecture
IP／legal	帰属、license、発明・秘密、joint IP、marking、紛争
Export／research security	classification、end-use、foreign person、publication、license
CISO／information security	segmentation、IAM、logging、incident、supplier security
Procurement／alliance	subcontractor rights、flow-down、OSS・third-party、fair treatment
HR	発明承継、兼業、入退社、教育、適性・clearance support

10.5 Patent／secret decision tree

1. 発明・know-how を asset 単位で切り出し、外部から侵害を検出できるかを判定する。検出困難なら secret を強く検討する。
2. 製品・輸出・標準化で公開が避けられないかを判定する。公開されるなら早期出願または defensive publication を検討する。
3. 指定技術分野、日本先願、政府資金、秘密・輸出・共同研究条件を確認する。未確認なら公表・外国出願を停止する。
4. 対象国で権利行使・証拠取得できるか、逆に公開で模倣を助けないかを評価する。
5. 特許明細書では、各出願国の実施可能要件・サポート要件・written description 要件等を満たす事項を開示する。米国出願では、出願時に発明者が認識していた請求発明の best mode も、当業者が実施できる程度に開示する。その上で、これらの開示要件を満たすために不要な製造条件、調整値、training・test know-how 等を、個別確認のうえ営業秘密として分離する。[U21]

6. 3 年ごとまたは export・M&A・標準化時に選択を再評価する。

10.6 Product-line IP：国内機微版／同盟国版／広域 export 版

Layer	国内機微版	同盟国版	広域 export 版
Core algorithm	full capability、domestic control	feature・threshold 調整、anti-tamper	black-box service ／ reduced capability
Mission data	国内・government control	bilateral compartment 、return/delete	顧客生成 data 中心
Interface	政府・国内 partner	共同標準・conformance	公開／商用標準を優先
Support	国内 secure team	cleared partner ＋ remote boundary	交換 unit、limited telemetry
Manufacturing	crown-jewel 工程国内	selected local production	module assembly 中心

設計原則

三つの版を別製品として fork し続けるのではなく、共通 architecture から feature、data、鍵、support access、製造情報を policy で組み替える。版ごとの権利・輸出・試験 baseline を release 単位で固定し、国内改良をどこまで各版へ還流できるかも先に決める。

11. 契約・権利設計プレイブック

11.1 最初に分けるべき 6 項目

1. Title：誰が権利を持つか。
2. Deliverable：何を、どの version・format・quality で納入するか。
3. License：誰が、目的・地域・期間・相手の範囲で使用、改変、開示、再許諾できるか。
4. Access：どの環境・identity・device から実際に到達できるか。
5. Control：秘密、輸出、privacy、clearance、cyber 要件が許容するか。
6. Continuity：停止、倒産、M&A、戦時、supplier 喪失時に何が発動するか。

11.2 Background／Foreground schedule

契約本文で『乙の固有技術を除く』とだけ書くのは危険である。ATLA 知財特約では背景・固有資料か新成果かの争いで企業に立証負担が生じ得る。[J4] 契約別紙で少なくとも次を version・hash・repository path・patent 番号・data set ID まで特定する。

- pre-existing patent、application、copyright、source、model、dataset、drawing、process、tool、library、API、test asset
- third-party・OSS・government-furnished・customer-furnished asset と license 条件
- 契約中の core 改良、mission adapter、customer configuration、sideground、feedback、derivative data
- subcontractor・大学・consultant の asset と権利承継証拠
- 商用製品へ還流できる抽象化、匿名化、generalized improvement の範囲

11.3 Government rights の menu

Use case	推奨 license option	企業保護
政府内運用・訓練	非独占・無償または price 込み、特定 system・期間	commercial use・公開を除外
有機整備・修理	OMIT data と tool、必要な改変権	詳細製造 data は別 price・範囲
競争調達	interface・form/fit/function・test を第三者開示	core implementation・商用競合利用を除外
同盟国運用	指定国・program・end-use・再移転禁止	export license・security 条件を suspensive condition
緊急・倒産・停止	trigger 限定 step-in、escrow release、third-party support	通常時は非発動、秘密・export 義務継続
AI 改善・監査	operational data 利用、独立評価、必要 log	顧客間再利用、weight・data 持出しを限定

> **価格化**
>
> 追加権利は無料の附属物ではない。競争、保守、source、第三者開示、同盟国、長期保存ごとに cost と商用価値の毀損を見積もり、option price または milestone へ分ける。

11.4 Software／SaaS／AI の必須条項

論点	最低限の契約事項
Data boundary	input、customer data、telemetry、derived data、support data、匿名化の定義
Model／improvement	pre-trained・fine-tuned weight、prompt、rule、feedback、benchmark、再学習
API／portability	version、SLA、deprecation、full export、schema、ontology、termination assistance
Security	hosting、administrator、incident、forensics、log、subprocessor、encryption、key
Assurance	SBOM／model-BOM、provenance、test、safety case、audit、update validation
Continuity	offline mode、escrow、rollback、service stop、business continuity、exit drill
Legal control	export、秘密、privacy、government data、record retention、litigation hold

11.5 Flow-down／flow-up

prime は政府権利・security・export 義務を subcontractor へ流すだけでなく、subcontractor から納入物・表示・背景資産・third-party license を回収し、政府へ履行できる chain を作る。

- 同一 asset ID・funding・legend schedule を契約階層で使う。
- 政府条項を全文転記するだけでなく、役割に必要な portion へ tailor する。
- subcontractor の民間資金 IP を無償吸い上げず、必要権利と対価を分ける。
- 大学・学生の publication、発明承継、background tool、foreign access を追加確認する。
- cloud、AI API、data broker、OSS maintainer など非典型 supplier も chain へ含める。

11.6 M&A・JV・投資・倒産

government-funded IP や防衛契約には、譲渡・独占 license・foreign party・change of control への承認が付く場合がある。EU・DIANA 等では所有・支配資格そのものが eligibility へ影響する。[E1][N2] term sheet 前の DD で確認する。

DD 項目	確認内容
Contract rights	政府 license、march-in、assignment、exclusive license、publication、change of control
Security eligibility	facility、personnel、適合事業者、CUI/CMMC、foreign ownership/control
Export	USML/ECCN、外為法、reexport、proviso、technology control plan
Chain of title	従業員、founder、consultant、大学、open source、共同発明
Portability	source、build、data、API、key、supplier、escrow、transition cost
Disclosure	data room での未出願発明・秘密・controlled data の閲覧資格

12. 実装ロードマップ・KPI・成熟度

12.1 最初の 90 日

1. 経営 sponsor を決め、mission availability・growth optionality・technology security の risk appetite を承認する。
2. 上位 20 案件・上位 50asset について、background、funding、政府権利、秘密、輸出、supplier を rapid scan する。
3. rights matrix、background schedule、AI/data schedule、release gate、subcontract flow-down の標準ひな形を作る。
4. 特許・論文・demo・GitHub・外国出願・海外 access を一つの release gate へ暫定統合する。
5. 重大 gap（権利未承継、legend 不備、source 不納入、foreign admin、未承認譲渡）を red list 化し、是正 owner と期限を付ける。

12.2 1 年

- asset ID で patent、repository、data catalog、contract、export、秘密・IAM を連結する。
- 全新規 bid で G1 rights review、全契約で G2 rights matrix、全 release で G4 assurance review を必須化する。
- 主要 supplier・大学と標準 schedule を再契約し、SBOM・funding・背景資産を回収する。
- 一つの重要 system で data export、代替 API、source escrow、incident access、supplier switch の continuity exercise を行う。
- 米国・EU・同盟国向け exportable baseline を少なくとも一製品で実装する。

12.3 3 年

- product-line IP を標準化し、国内・同盟国・広域 export 版を共通 architecture から生成する。
- government rights を use-case menu と price option で proposal へ組み込み、承認 lead time を短縮する。
- continuous entitlement、SBOM/model-BOM、policy-as-code により version 単位で release 可否を自動警告する。
- 同盟国 partner と interface・test evidence・federated data control を共同運用する。
- IP、security、export、continuity KPI を取締役会 risk dashboard へ統合する。

12.4 KPI

Category	KPI 例	悪い代理指標
Rights readiness	G1 前 rights matrix 率、background 特定率、chain-of-title gap	特許件数のみ
Delivery	data deliverable acceptance、legend 適合、更新遅延	納入ファイル数
Portability	full export 時間、代替基盤移行時間、API 適合率	API の有無

Category	KPI 例	悪い代理指標
Security／export	classification coverage、access review、approval lead time、incident	研修受講率のみ
Supply chain	flow-down／flow-up 完了、SBOM coverage、single-source concentration	supplier 数のみ
Commercialization	background 再利用、PoC→初回／継続調達、exportable revenue	採択件数
Resilience	critical asset recovery、escrow test、qualified alternate、key recovery	文書化の有無

12.5 成熟度モデル

Level	状態	権利・契約	data／security	経営
L1 Ad hoc	案件ごとに事後対応	patent 台帳のみ	個別 folder・担当者依存	重大問題のみ報告
L2 Controlled	標準 NDA・発明・輸出 check	背景別紙を一部使用	秘密区分・IAM を整備	部門 KPI
L3 Integrated	全案件 stage-gate	rights matrix・flow-down 標準	asset ID で lineage 連結	三軸 portfolio 管理
L4 Predictive	権利・規制 impact を proposal 前予測	license menu・option pricing	continuous monitoring・exit drill	board risk dashboard
L5 Orchestrator	同盟国・ecosystem で再構成	federated rights・standard interface	policy-as-code・portable assurance	IP で市場設計

到達目標

多くの企業はまず L3 を目指す。L5 は全 asset を公開する状態ではなく、閉じる core と開く interface を選び、同盟国・supplier を含む権利と access を安全に組み替えられる状態である。

付録 A. 権利マトリクスひな形

下表を asset または実務上分離できる module ごとに作成する。『対象外』『未定』も明示し、未定項目に owner と期限を付ける。

Field	記入例／確認事項
Asset ID／version	MODEL-042 v3.2、source commit、dataset hash、drawing rev
Description／boundary	何を含み、何を含まないか。interface と core の境界
Origin／creator	企業、従業員、大学、subcontractor、政府、third party
Classification	background／foreground／sideground／improvement／GFI
Funding	private／government／mixed、award・work package・charge code
Title／chain	権利者、共同持分、assignment、発明者、著作者
Third-party rights	OSS、data license、patent license、export・field 制限
Deliverable	source／binary／weight／data／schema／test／manual、format・date
Marking	restrictive legend、copyright notice、秘密・輸出 label
Government use	使用、複製、改変、開示、競争、保守、訓練、AI 学習
Third-party／ally	指定 support contractor、同盟国、再許諾、NDA・clearance
Commercial reuse	民生、関連会社、海外、standard、license、匿名化 derived data
Territory／term	国・program・platform・期間・GPR 期間・終了後
Trigger rights	倒産、停止、有事、重大 incident、SLA breach、change of control
Access／hosting	tenant、region、administrator、foreign person、key、offline
Export／security	ECCN／USML／外為法、秘密区分、CUI、適合事業者
Acceptance／evidence	hash、build 再現、test、SBOM、model card、review 結果
Lifecycle	update、obsolescence、escrow、return／delete、retention、exit test

付録 B. 契約前チェックリスト

B1. Bid／No-bid

- 顧客の利用 case（運用、保守、競争、同盟国、緊急、AI 改善）を確認したか。
- 要求される権利と納入物を別々に list 化したか。
- 商用 core、政府資金、第三者・OSS、顧客 data を技術的に分離できるか。
- 秘密施設、CUI、export、research security、personnel 条件の固定費を price へ入れたか。
- prototype 成功後の follow-on／量産で権利条件が変わるか。
- 外国支配、M&A、投資家、海外子会社、cloud provider が eligibility へ影響するか。

B2. 契約条項

- Background schedule は version・hash・patent 番号・dataset ID まで具体的か。
- Foreground、sideground、improvement、feedback、derived data、joint result を定義したか。
- 資金源と適用 data-rights 条項を module 単位で対応させたか。
- source、build、tool、weight、data、schema、log、test、manual、SBOM を納入物として明記したか。
- 政府・第三者・同盟国の使用、改変、開示、再許諾、商用利用、期間、地域を定めたか。
- 特許出願、公表、譲渡、独占 license、外国 party、change of control の承認と処理期限を確認したか。
- escrow・step-in の trigger、受取物、利用目的、秘密・輸出義務を限定したか。
- 表示・legend、acceptance、訂正、更新、audit、記録保存を定めたか。

B3. Contract close／transition

- 全 deliverable を技術・権利・security の三者で accept したか。
- 最終 background／foreground list と発明・著作物承継を更新したか。
- government-furnished・customer data を返還／消去し、証拠を保存したか。
- 保守・脆弱性・key・API・model update・supplier 継続の owner を移管したか。
- 次契約・民生還流・外国出願・export の承認を再確認したか。

付録 C. AI・データ・OSS チェックリスト

C1. AI／data

- training、validation、test、operational、synthetic、derived、log を分けたか。
- data の取得元、license、consent、privacy、秘密、輸出、保持期限を追跡できるか。
- architecture、code、weight、prompt、label、reward、scenario、evaluation、safety constraint を資産化したか。
- 人間の発明寄与、AI tool 利用、prompt／iteration、発明日を記録したか。
- field feedback から生じる model・rule・label・benchmark の帰属と顧客間再利用を定めたか。
- 独立評価、red-team、事故調査、explainability に必要な log・access を確保したか。
- model update／rollback／signature／end-of-life の権限と手順があるか。
- LLM・code assistant へ controlled source・data・prompt を送信しない policy と technical control があるか。

C2. OSS／third-party software

- SBOM を自動生成し、direct・transitive dependency と version を追跡しているか。
- license obligation、notice、source offer、copyleft、patent clause を release 前に審査するか。
- government license・秘密・export・redistribution と OSS 条件が矛盾しないか。
- abandoned project、single maintainer、sanctioned contributor、malicious package の risk を見ているか。
- vulnerability、VEX、patch、end-of-support、alternative component の owner を決めたか。
- SBOM 配布自体が機微な system architecture を露出しないよう access・粒度を決めたか。

付録 D. M&A・共同研究・海外連携チェックリスト

D1. M&A／投資

- government-funded IP、public-interest license、march-in、assignment、foreign-party 承認を抽出したか。
- ATLA・重要情報・CUI/CMMC・EDF・DIANA 等の資格が control 変更で失われないか。
- ECCN／USML／外為法、license proviso、reexport、technology control plan を確認したか。
- founder、employee、consultant、university、former employer、OSS の chain of title が完全か。
- data room の閲覧者は未出願発明、営業秘密、controlled data を見る資格があるか。
- key person・toolchain・supplier・cloud・API の依存と transition cost を評価したか。

D2. 共同研究／大学

- research scope と各 party の background・tool・data を開始時に list 化したか。
- 共同発明、単独発明、sideground、学生成果、論文、thesis、software、data を定義したか。
- publication review の目的、期限、patent filing、秘密・輸出・security review を分けたか。
- foreign funding、affiliation、visiting researcher、remote access、equipment、data source を risk 評価したか。
- 国籍だけで一律排除せず、asset・access・purpose に比例した軽減策を使っているか。
- 公開基礎研究から秘密・装備化段階へ移る change point を契約で定めたか。

D3. 海外 license／共同生産

- Background／Foreground／Sideground、改良、field-of-use、territory を定義したか。
- 再許諾、第三国移転、現地 subcontract、end-use、監査、日本政府同意を定めたか。
- source、model、data、tooling、manufacturing know-how を black-box・module 化したか。
- 現地改良を日本へ grant-back する範囲と競争法・価格を確認したか。
- 終了時の在庫、tool、data、source、key、support、返還・消去・証明を定めたか。
- 侵害発見・証拠・差止・arbitration・sanctions・force majeure を設計したか。

付録 E. 用語集

用語	説明
Background ／ Foreground ／ Sideground	開始前資産／scope 内で新規生成／案件中だが scope 外で生成。契約定義が最優先。
Government purpose rights	米 DoD で政府目的の使用・第三者開示等を認める license rights。期間は交渉可能で、標準条項上の名目期間は 5 年。満了後、政府は対象 data／software について unlimited rights を取得する。
Unlimited ／ Limited ／ Restricted rights	米政府の技術データ・software に対する標準 license 区分。title 移転と同義ではない。
OMIT data	operation, maintenance, installation, training に必要な data。詳細製造・process data は除外され得る。
MOSA	Modular Open Systems Approach。architecture、business、IP、interface、test を統合する取得戦略。
CUI／CMMC	Controlled Unclassified Information／DoD の cybersecurity maturity assessment framework。
Deemed export	国内で外国人へ controlled technology／source を release したことを輸出と扱う制度。
March-in	政府資金成果が不活用等の場合に第三者 license を求める制度。即時没収ではない。
SBOM／model-BOM	software／AI model の構成、依存、来歴を記録する bill of materials。
Escrow／step-in	一定 trigger 時に source 等を release し、顧客・指定者が継続運用へ介入する仕組み。
Data lineage	data の取得、加工、label、学習、評価、派生、利用までの来歴。
Sovereign control	所有国籍ではなく、運用・改良・保守・供給・移行を自律的に実行できる支配力。

参考文献

URL は基準日現在。法令・条項は改正されるため、実案件では契約締結時の版を確認する。添付記事は論点設定に用い、制度事実は可能な限り一次資料で確認した。

添付資料

[A1] Arthur D. Little Japan『米国のデュアルユース、2040 年に 500 兆円規模　実態と今後』日経テックフォーサイト — 2026 年 8 月 5 日、添付 PDF

[A2] Arthur D. Little Japan『防衛デュアルユース、戦略 17 分野と密接　5 つの注目技術』日経テックフォーサイト — 2026 年 8 月 3 日、添付 PDF

[A3] Arthur D. Little Japan『AI が防衛作戦、代表格パランティアは何者か　民生展開も』日経テックフォーサイト — 2026 年 8 月 7 日、添付 PDF

[A4] Arthur D. Little Japan『防衛技術をフィジカル AI へ生かす　米アンドゥリルに学ぶ』日経テックフォーサイト — 2026 年 8 月 17 日、添付 PDF

[A5] Arthur D. Little Japan『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』日経テックフォーサイト — 2026 年 8 月 19 日、添付 PDF

[A6]『連載「防衛デュアルユース」』 — 添付 docx

日本：契約・特許・秘密・輸出・研究セキュリティ

[J1] 経済産業省『日本版バイ・ドール制度』 — 産業技術力強化法 17 条の条件

[J2] 防衛装備庁『安全保障技術研究推進制度』 — 公開研究・制度概要

[J3] 防衛装備庁『安全保障技術研究推進制度 FAQ』 — 知財帰属、公表、再委託

[J4] 防衛装備庁『知的財産の取扱いに関する特約条項』別紙様式第 50 — 2026 年 4 月 1 日以降版

[J5] 防衛省『迅速な装備品等の取得に係る取組』 — 特約条項・知財条件

[J6] 特許庁『特許出願非公開制度』 — 日本先願・事前確認・二段階審査

[J7] 内閣府『特許出願の非公開に関する制度』 — 制度・Q&A・対象分野

[J8] 内閣府『特許出願非公開制度の実施状況（2025 年度）』 — 保全審査送付 106、指定 0、事前確認 922

[J8a] 内閣府『特許出願非公開制度の実施状況（2024 年度）』 — 送付 90、指定 0、事前確認 1,305

[J9] 内閣府『重要経済安保情報保護活用法』 — 2025 年 5 月 16 日施行

[J10] 内閣府『重要経済安保情報保護活用法 国会報告概要』 — 2026 年 6 月 26 日公表

[J11] 経済産業省『安全保障貿易管理の概要』 — 2026 年 5 月 20 日更新

[J12] 経済産業省『大学・研究機関向け安全保障貿易管理ガイダンス改訂』 — 2025 年 10 月規制対応

[J13] 防衛装備庁『防衛産業サイバーセキュリティ基準』 — 契約・下請・情報保全

[J14] 防衛装備庁『防衛事業適合事業者制度』 — 組織単位の産業保全

[J15] 経済産業省『SCS 評価制度の構築方針』 — 2026 年度末頃開始を目標

[J16] 経済産業省『SBOM の共有ビジョンに関する国際ガイダンス』 — 15 か国共同署名

[J17] 公正取引委員会・中小企業庁・特許庁『知財取引指針及び契約書ひな形の公表について』 — 2026 年 6 月 24 日

[J18] 公正取引委員会・中小企業庁・特許庁『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』 — 2026 年 6 月 24 日

[J19] 経済産業省『技術流出対策ガイダンス第 2 版』 — 共同研究・すり合わせ調達を追加

[J20] 経済産業省『経済安全保障経営ガイドライン第 1 版』 — 自律性・不可欠性・経営統治

[J21] 特許庁『AI 関連技術に関する特許審査の事例』 — 2026 年 5 月 25 日更新

[J22] 経済産業省『不正競争防止法・営業秘密管理指針』 — 2025 年 3 月改訂指針

[J23] 経済産業省『限定提供データと利活用』 — 不正競争防止法上の保護

[J24] 防衛省『防衛装備移転三原則等の改正』 — 2026 年 4 月 21 日

[J25] 内閣府『研究セキュリティの確保に関する取組のための手順書』 — 2025 年 12 月

[J26] 防衛装備庁『防衛生産基盤強化法に基づく装備品等秘密の保全』 — 2024 年 4 月から法的義務
[J27] JST『K Program 令和 8 年度委託研究契約書』 — 2026 年 4 月 1 日版
[J28] 防衛大臣会見『令和 8 年度からの防衛省 SBIR』 — 2026 年 2 月 27 日
[J29] 防衛省・自衛隊『研究開発期間を大幅に短縮するための取組』 — ブロック化・モジュール化・オープンアーキテクチャ化

米国：政府契約・data rights・MOSA・cyber・輸出

[U1] Acquisition.gov, DFARS 227.7103-4 License rights — 資金源と最小分離単位
[U2] Acquisition.gov, DFARS 252.227-7013 Rights in Technical Data — 非商用品技術データ
[U3] Acquisition.gov, DFARS 227.7103-5 Government rights — unlimited、GPR、limited、OMIT
[U4] Acquisition.gov, DFARS 227.7203-4 License rights — 非商用 computer software
[U5] Acquisition.gov, DFARS 252.227-7014 Rights in Noncommercial Computer Software — source・marking・OSS
[U6] DoD, Intellectual Property Cadre — life-cycle IP strategy
[U7] U.S. GAO, Weapon System Sustainment: DOD Can Improve Planning and Management of Data Rights — 2025 年 9 月 29 日改訂公表
[U8] U.S. Code, 10 U.S.C. §4401 — MOSA requirement
[U9] U.S. Code, 10 U.S.C. §4402 — acquisition strategy と IP
[U10] U.S. Code, 10 U.S.C. §4403 — interface と第三者統合
[U11] U.S. Code, 10 U.S.C. §3771 — modular system interface data rights
[U12] DoD CIO, Cybersecurity Maturity Model Certification — Phase I と 2026 年 7 月の Phase II 停止
[U13] Acquisition.gov, DFARS 252.204-7012 — CUI、NIST、incident、flow-down
[U14] U.S. BIS, What is a deemed export? — 外国人への technology release
[U15] U.S. BIS, EAR Part 734 — export、reexport、release、access information
[U16] SBA, SBIR/STTR Data Rights FAQ — data ownership と 20 年保護
[U17] Acquisition.gov, DFARS 252.227-7018 SBIR/STTR Data Rights — 現行条項
[U18] U.S. Code, 35 U.S.C. §§202–203 — Bayh-Dole title と government license
[U19] DIU, Advancing DoD Operational Capabilities with Software Acquisition Reform — CSO、prototype OT、follow-on
[U20] U.S. State Department, Boeing $51 million ITAR settlement — technical data・foreign person 違反例
[U21] USPTO, MPEP §2165 The Best Mode Requirement — AIA 後も 35 U.S.C. §112(a)の best mode 開示要件は存続
[AI1] USPTO, Revised inventorship guidance for AI-assisted inventions — 2025 年 11 月 26 日
[AI2] U.S. Copyright Office, Copyright and Artificial Intelligence — Part 2 copyrightability、Part 3 training
[S1] NTIA, The Minimum Elements for a Software Bill of Materials — data fields・automation・process

EU・NATO

[E1] Regulation (EU) 2021/697 establishing the European Defence Fund — 2025 年 12 月 23 日統合版
[E2] Regulation (EU) 2021/697, Articles 20 and 23, consolidated version — 2025 年 12 月 23 日統合版：research・development action の成果
[E3] Regulation (EU) 2021/821 on dual-use items — 2025 年 11 月 15 日統合版
[E4] Council Recommendation 2024/C 3510 on enhancing research security — risk-based・proportionate approach
[E5] Directive (EU) 2016/943 on trade secrets — reasonable steps、reverse engineering
[N1] NATO DIANA FAQ — innovator retains IP
[N2] NATO DIANA Challenge Call Q&A — 契約資金、deliverables、IP・equity
[N3] NATO, Strategy for Industry–NATO Cooperation — 2026 年 7 月 8 日、modularity・open architecture

企業・実装ケース

[C1] Palantir Technologies, 2025 Form 10-K — IP portfolio・risk disclosure
[C2] Palantir, Privacy and Security Statement — 2024 年 4 月：personal data の processor／controller 区分
[C2a] Voyager Technologies, Inc., Form S-1, filed May 16, 2025, Exhibit 10.10, 'Palantir Order Form—Amended & Restated Order #1' — SEC Accession No. 0001628280-25-026244；customer data・Palantir technology・feedback の一契約例
[C3] Anduril, The Lattice API — open data models、API、versioning

[C4] Anduril, Lattice SDK License Agreement — 2026 年 7 月 31 日更新

[C5] Shield AI, Hivemind — platform-agnostic、customer-developed IP の訴求

[C6] 三菱重工『無人機ミッション・オートノミーの飛行実証』 — 2026 年 3 月 17 日

[C7] 防衛省『防衛スタートアップ大賞 2025』 — Synspective

[C8] Synspective『衛星コンステレーション事業参画』 — 2026 年 2 月 20 日

[C9] ACSL『国産セキュアドローンの航空自衛隊採用』 — 2024 年 3 月 21 日

[C10] Sakana AI『防衛装備庁との契約』 — 2026 年 3 月 13 日

[C11] 三菱重工・Preferred Networks『mission-critical 国産 AI 共同開発』 — 2026 年 6 月 2 日

調査の限界：政府契約の個別 IP schedule、秘密指定、企業内部の発明評価、特許非公開案件、輸出 license、訴訟 strategy は多くが非公開である。確認できない条件は断定せず、公表情報から再現可能な設計原則のみを抽出した。