

防衛デュアルユース分野における企業知財戦略

THE IP BLUEPRINT

「所有」から「アクセスの制御」へ：グローバル市場でコア技術を守り、
任務継続性を担保する実践的プレイブック

対象読者：経営層・知財・法務・事業開発部門

従来のパラダイム (二者択一)



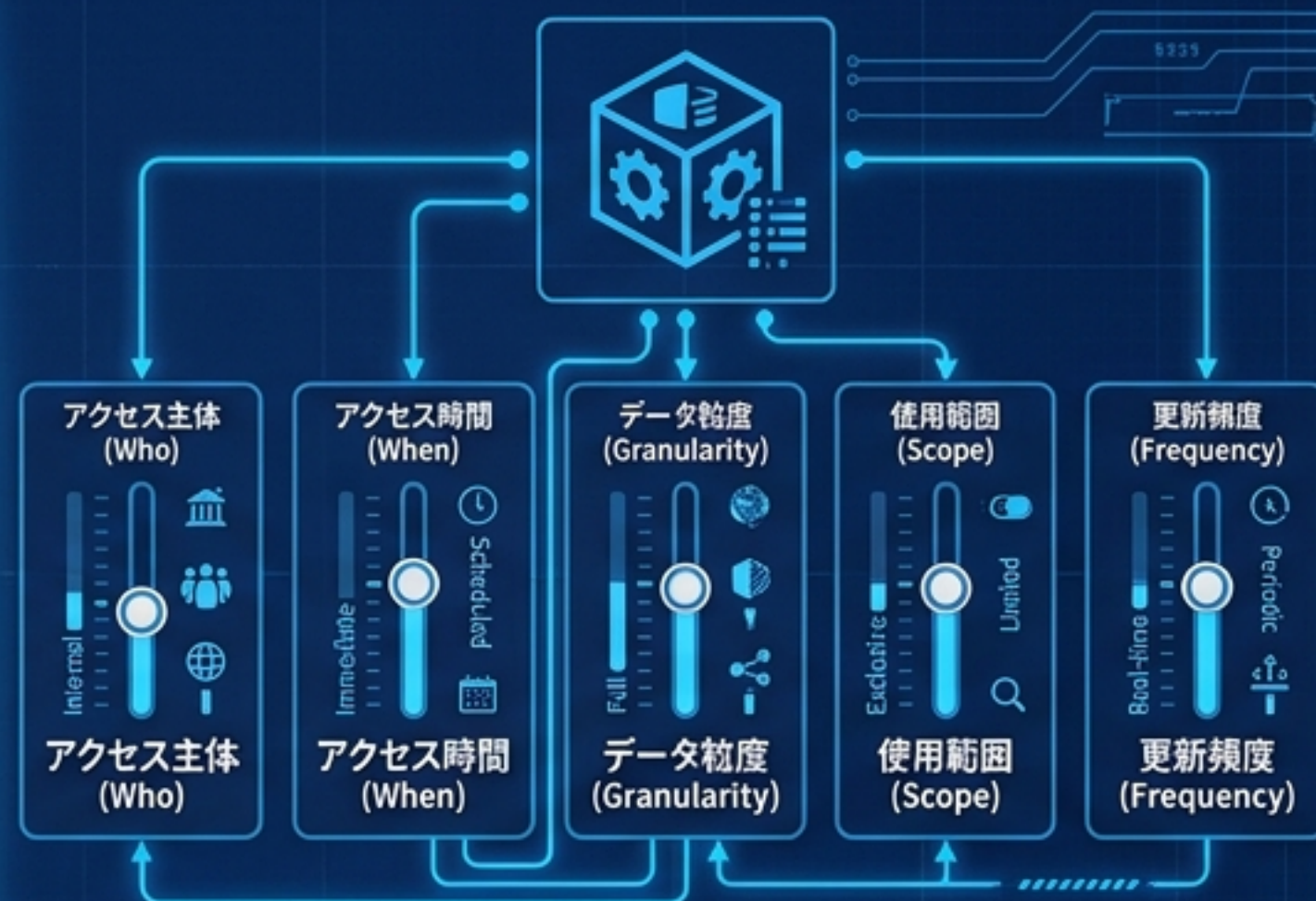
特許 (公開して独占する)

営業秘密 (秘匿して守る)



防衛分野では「非公開の要求」と
「同盟国・第三者による長期間の保守・運用要求」
が衝突し、機能不全に陥る。

新たなパラダイム (権利束の設計)



勝敗を分けるのは「特許件数」ではない。
「権利の束 (Rights Bundle)」を設計し、
誰が・いつ・どの粒度でアクセスできるかを
制御する能力である。

	日本	米国 (DoD)	EU / NATO
企業帰属 (Corporate Ownership)	条件付きで可能 (日本版バイ・ドール、 ATLA特約)	原則として企業が保持 (Contractor retains title)	EDFは参加企業帰属、 DIANAはIP不取得
政府利用権 (Gov Use Rights)	公共目的、無償実施 (制度が分散)	資金源に基づく 厳密な標準権利 (Unlimited / GPR / Limited)	アクション種別による。 加盟国ごとの調達契約
域外統制 (Extraterritorial Control)	輸出管理、特許出願非公 開、重要経済安保情報	EAR/ITAR、CUI、 外国人アクセス制限 (Deemed export)	非関連第三国による 支配・制約の厳格な排除

課題：日本の制度は分散しており、
 契約前に「権利と納入物」を横断設計する企業負担が大きい。

最適なIP戦略 = Mission Availability × Growth Optionality × Technology Security

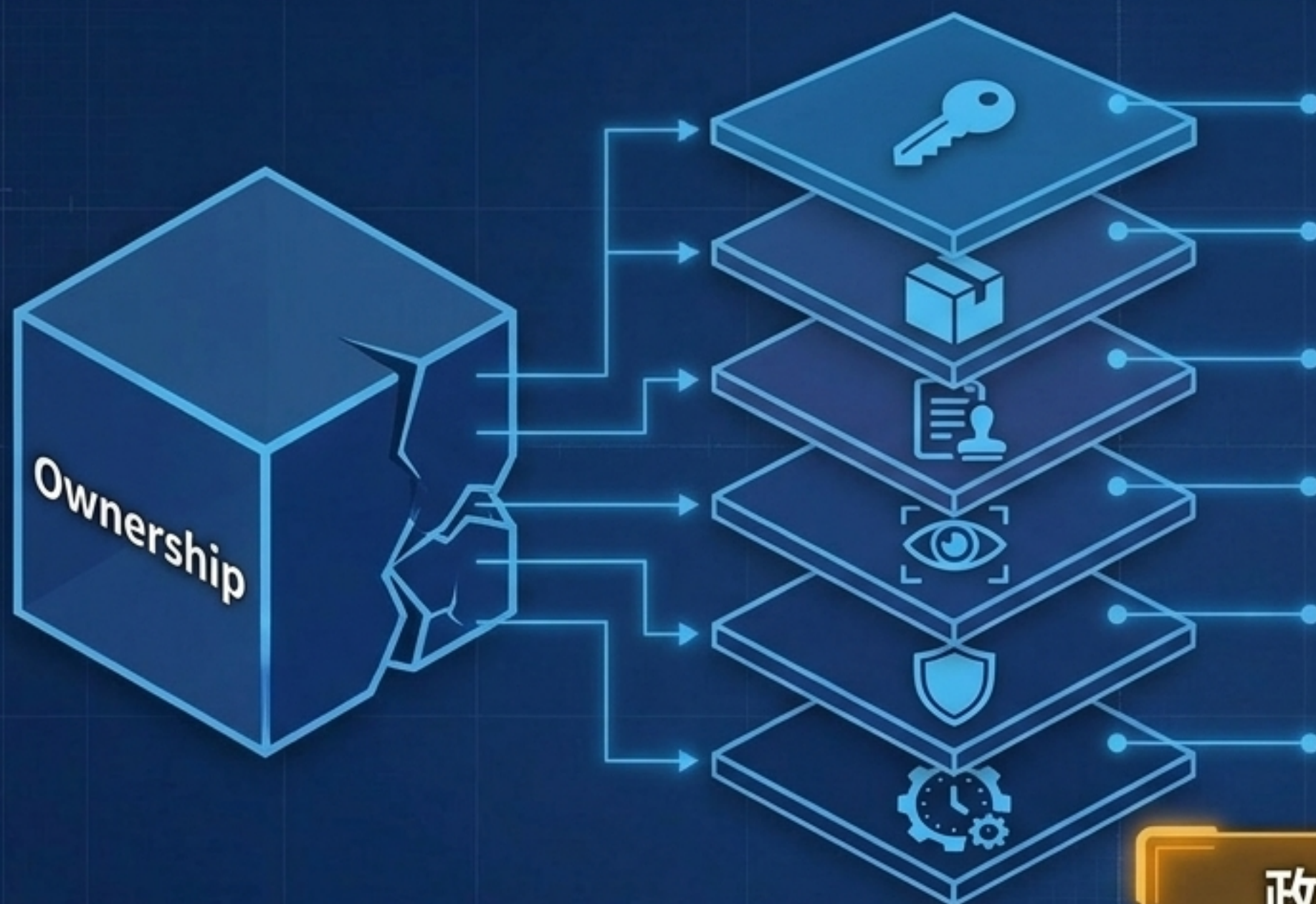


経営層の役割：案件ごとにこの三軸のトレードオフ（リスクアペタイト）を決定すること。



警告:「商用コア」への政府資金・共同研究データの汚染(コンタミネーション)は、全製品への波及リスクを生む。資金源とアセットを厳密に分離せよ。

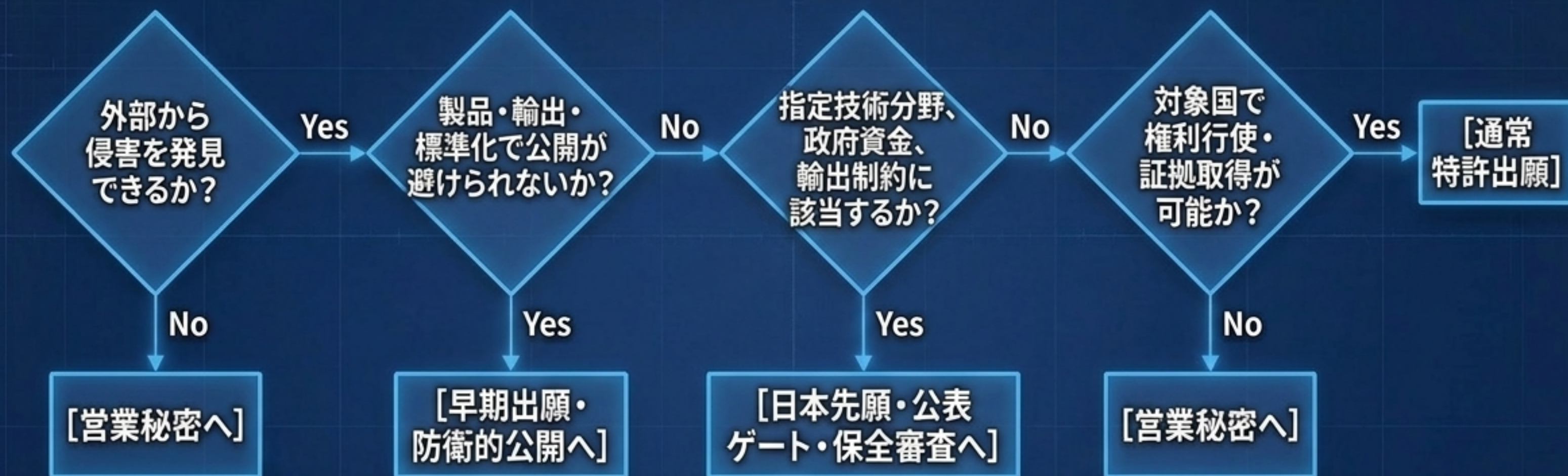
所有権のアンバンドル (Deconstructing Ownership)



1. Title (帰属): 誰が権利を持つか (共有持分の整理)。
2. Deliverable (納入物): 何を、どの形式で納めるか (ソース、スキーマ、ツール)。
3. License (利用権): 誰が、何目的で使えるか (政府目的、同盟国、第三者保守)。
4. Access (アクセス): 物理的・論理的に誰が到達できるか (クラウドテナント、外国人権限)。
5. Control (規制): 秘密、輸出、サイバー要件を満たしているか。
6. Continuity (継続性): 停止、倒産時に何が発動するか (トリガー限定のエスクロー)。

政府が求めるのは「所有権」ではなく、有事の「継続運用能力(Continuity)」である。

技術保護戦略：決定フローチャート



「特許化の価値」は件数ではなく、事業の自由度、代替困難性、輸出可能性で測る。
米国出願時のBest Mode開示要件と営業秘密の分離に注意(個別確認必須)。

システムアーキテクチャ

閉じるもの

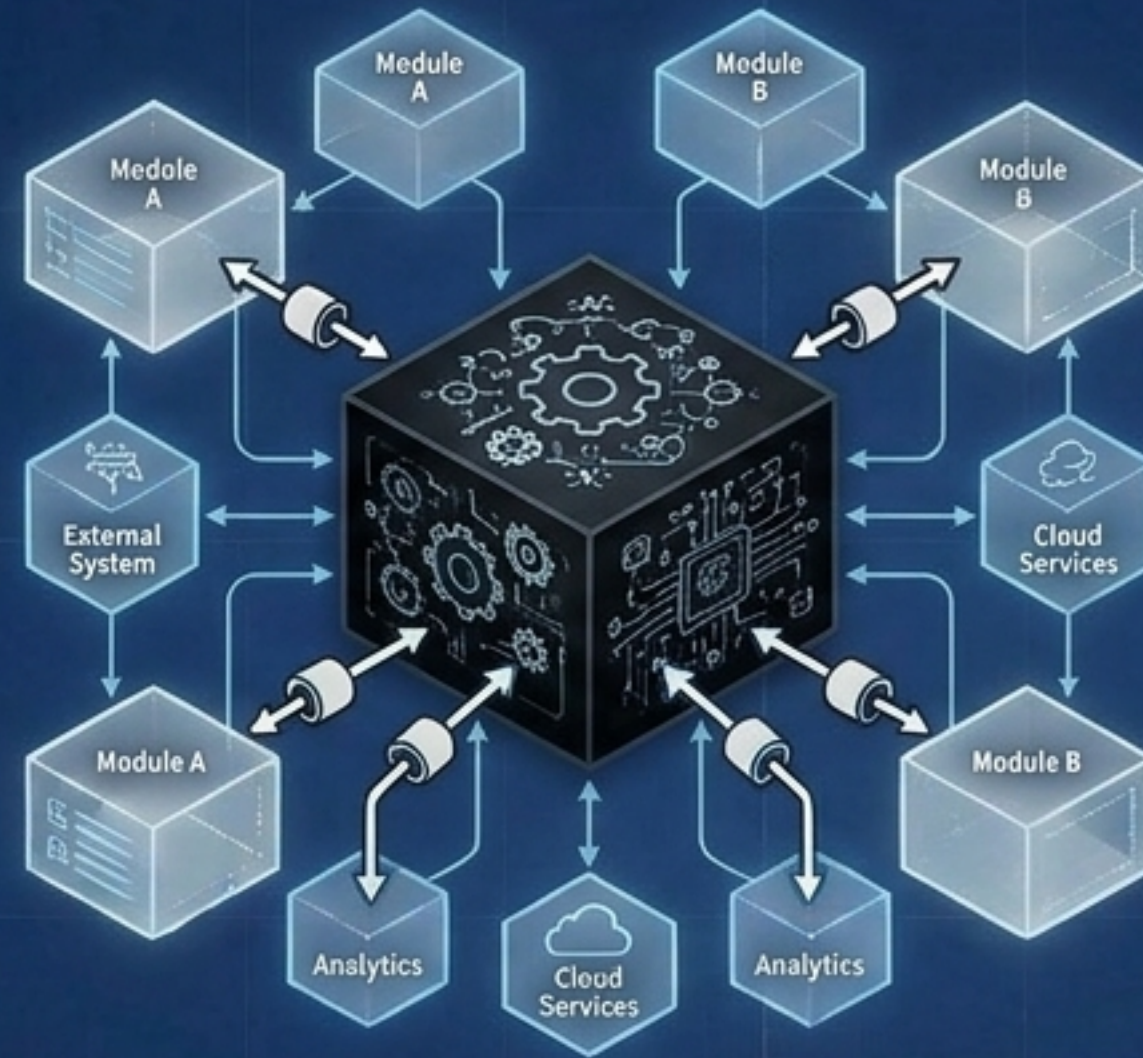
(Closed Implementation)

- コアソースコード、最適化アルゴリズム、ビルドレシピ。
- 著作権だけでなく、ツールチェーンや署名鍵を保持し「運用支配」を握る。

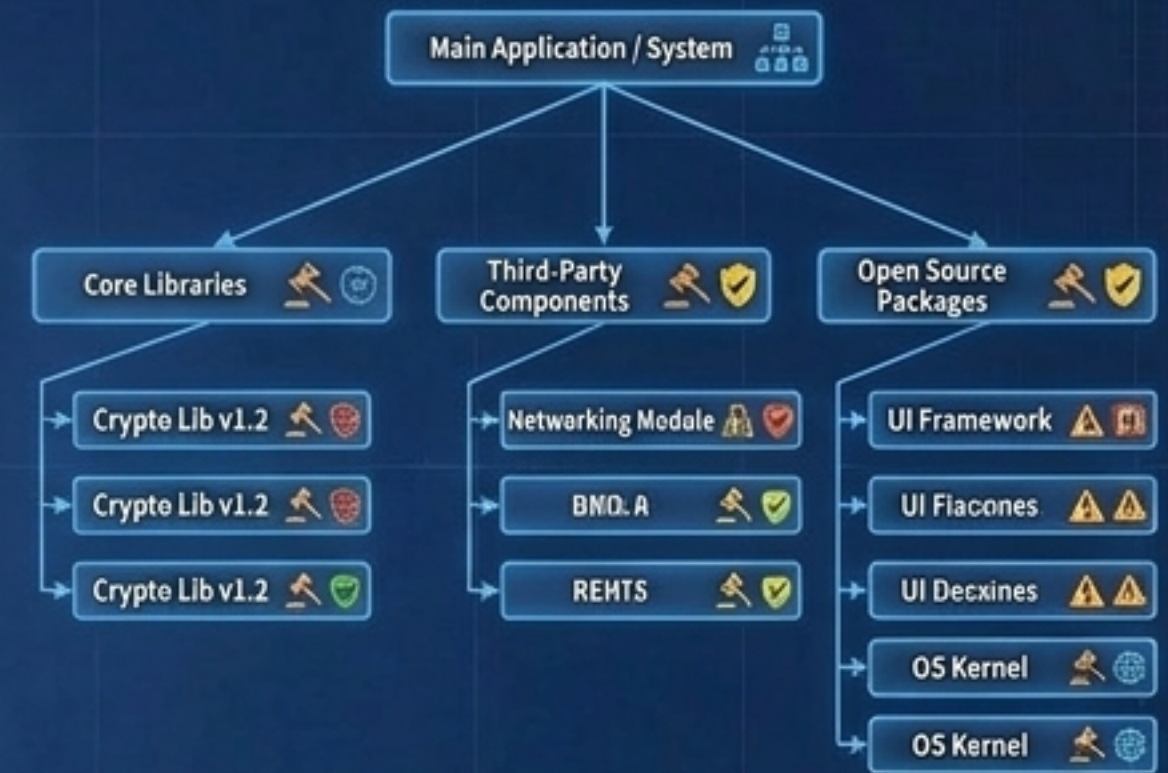
開くもの

(Open Interfaces / MOSA)

- 外部インターフェース、メッセージスキーマ、テストスイート。
- 第三者統合に必要な権利 (Interface Rights) を準備。



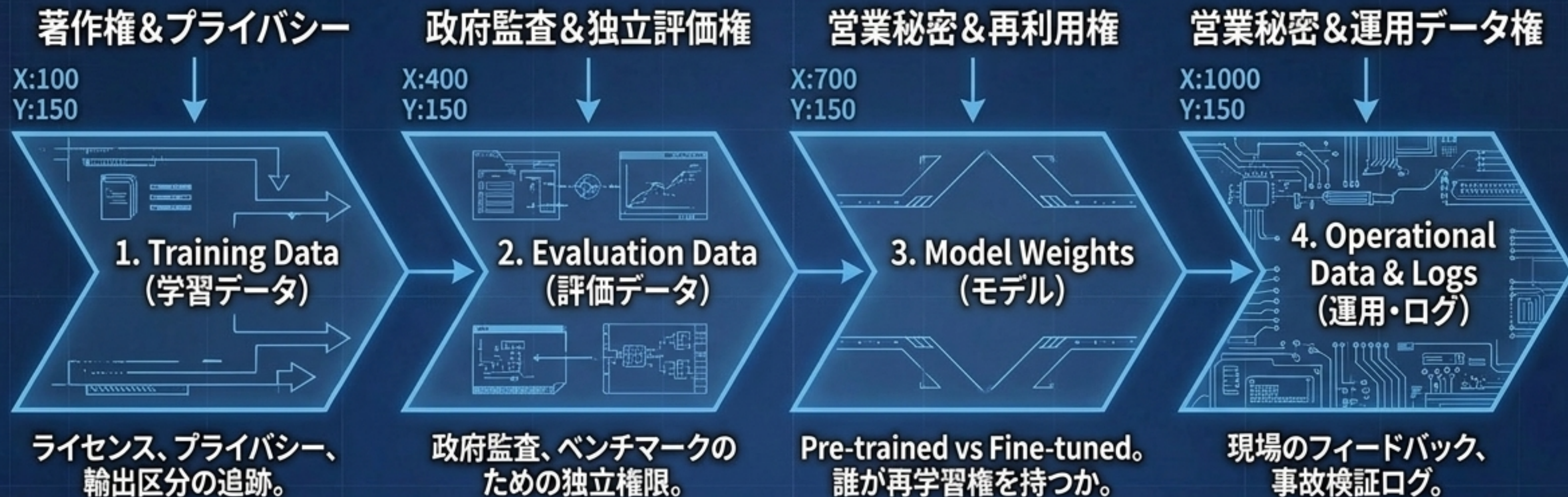
共同管理・証明 (Assurance)



SBOM (ソフトウェア部品表)、脆弱性対応。ライセンス適合性とサプライチェーンの証明が「市場アクセス権」となる。

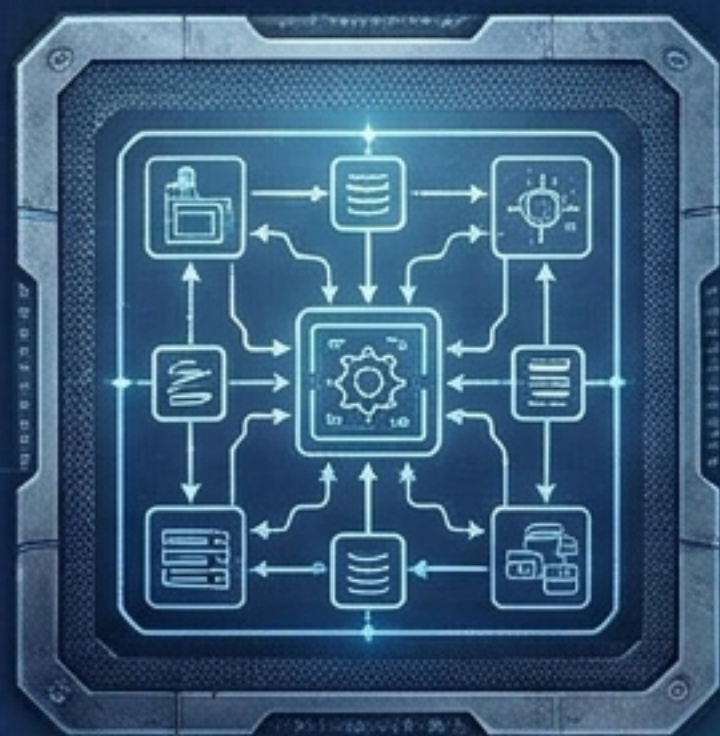
事例 (Anduril社): オープンなデータモデル (Lattice API) を提示しつつ、SDKの知財は自社に留保し、互換性の判断権を握る設計。

AIデータのライフサイクルとIP権



AIにおける真の王冠 (Crown Jewels)

モデルのウェイト以上に、運用からのフィードバックループ、失敗例 (Red-team結果)、安全制約ルールが代替困難な資産となる。これを無自覚に「報告書データ」として政府に全面納入してはならない。



共通アーキテクチャ
(Core Architecture)



国内機微版 (Domestic Sensitive)



フルケイパビリティ。国内統制。
コアエンジニアリングの拠点。



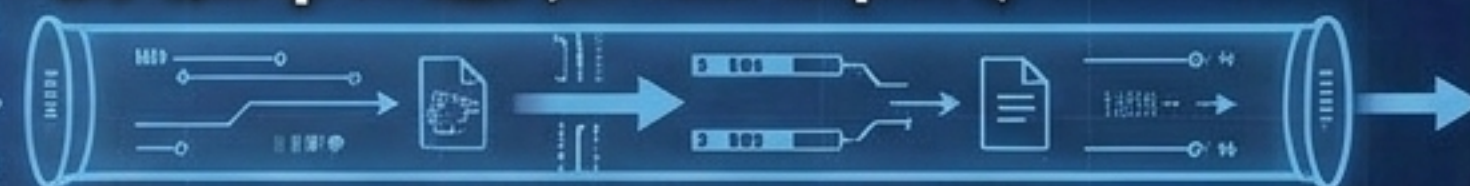
同盟国版 (Allied Version)



機能・閾値の調整。アンチタンパー (耐改ざん) 技術の実装。
二国間のコンパートメント管理。



広域Export版 (Broad Export)



ブラックボックス化されたサービス提供、
または機能を限定したモジュールアセンブリ。



戦略: 3つの版を別々に作るのではない。共通アーキテクチャから、機能、データ、鍵、アクセス権をポリシーとして組み替える (Policy-as-code)。

サプライチェーン管理：フローダウンとフローアップ

プライムコントラクター
(Prime Contractor)

下流への展開
(Flow-Down)

政府権利、セキュリティ要件、輸出管理
輸出管理義務の展開。

※無償でのノウハウ吸い
上げは避け、適切な取引(知財取引指針準拠)
を行う。

Tier 1: サプライヤー/
サブコントラクター/大学
(Subcontractors & Universities)

Tier 2: サプライヤー/
サブコントラクター/大学
(Subcontractors & Universities)

上流への回収
(Flow-Up)

SBOM、背景資産
(Background IP)の特定、第三者ライセンス、
発明承継の証拠回収。



同一のアセットID、資金源記録、表示 (Legend) ルールを
サプライチェーン全体で統一し、「権利の断絶」を防ぐ。

ゲート管理: トルゲートの目安



各段階での厳格なゲート管理とレッドフラッグによるリスク検知が、プロジェクト全体の品質とコンプライアンスを担保する。

アセット別権利マトリクス（必須管理項目）

Asset ID	Funding (資金源)	Deliverable (納入物形式)	Gov Use (政府利用権)	Export/Security (輸出・秘密区分)	Trigger (緊急時発動条件)
[MODEL-042 v3.2]	[Mixed/Private]	[Binary/Weights Only]	[訓練・運用（第 三者開示不可）]	[EAR指定 / CUI]	[SLA違反時のエ スクロー解除]



契約本文に「乙の固有技術を除く」と書くだけでは不十分。
別紙でバージョン、ハッシュ、データセットIDまで特定せよ。

中期ロードマップ: ゲート管理の進化と標準化



各フェーズの目標を達成し、プロセスを自動化・統合することで、組織全体のリスク耐性とコンプライアンス体制を強化する。

知財・権利管理成熟度モデル

L1: Ad Hoc

案件ごとの事後対応。
特許台帳のみ。

L2: Controlled

標準NDA、
背景別紙の利用。

L3: Integrated (目標水準)

全案件ステージゲート。
アセットIDによる連結。
三軸ポートフォリオ管理。

L4: Predictive

提案前の権利・規制
インパクト予測。
ライセンスメニュー化。

L5: Orchestrator (最終到達点)

エコシステム全体での
権利の再構成。
Federated Rights。
IPによる市場設計。

究極の目的は「全てを独占すること」でも「全てを公開すること」でもない。
閉じるコアと開くインターフェースを選び抜き、グローバルな安全保障環境に
おいて「アクセスを安全に組み替える能力」を獲得することである。

