AIベンダー選定は「地政学的決断」である

米国防総省「Anthropic排除」が突きつける日本企業への連鎖リスクと戦略的転換

2026年2月27日、米国防総省による前例のないサプライチェーンリスク指定が、日本の防衛・製造業のテクノロジー戦略を根本から覆した。

米国発・AI市場の地殻変動：2026年2月27日の衝撃

Anthropicの排除

- ✓ 出来事: トランプ大統領によるAnthropicの全連邦機関使用停止命令。
- ✓ 根拠法: 合衆国法典第10編第3252条（10 USC §3252）。
- ✓ 影響: 通常は敵対国向けに適用される「サプライチェーンリスク指定」が米国企業に初適用。司法審査不能の強力な措置。

OpenAIの台頭

- ✓ 出来事: 同日夜、OpenAIが国防総省の機密ネットワーク向けAI契約を獲得。
- ✓ ハイライト: Anthropic排除と同日に、SB OpenAI Japan設立のパートナーでもあるOpenAIが最大1,100億ドルの追加投資合意を発表。

戦略的示唆

フロンティアAIモデルの市場競争は、単なる性能競争から「国家安全保障への適合性」を競うフェーズへ突入した。

国際AIガバナンスの分断：三極化する世界のルール

EU（厳格な法規制）

- EU AI Act: 2026年8月ハイリスクAI規制施行。
- **罰則**: 最大3,500万ユーロまたは全世界売上高の7%の罰金。
- **例外**: 軍事・防衛目的は適用除外（第2条3項）。

米国（規制緩和と覇権回帰）

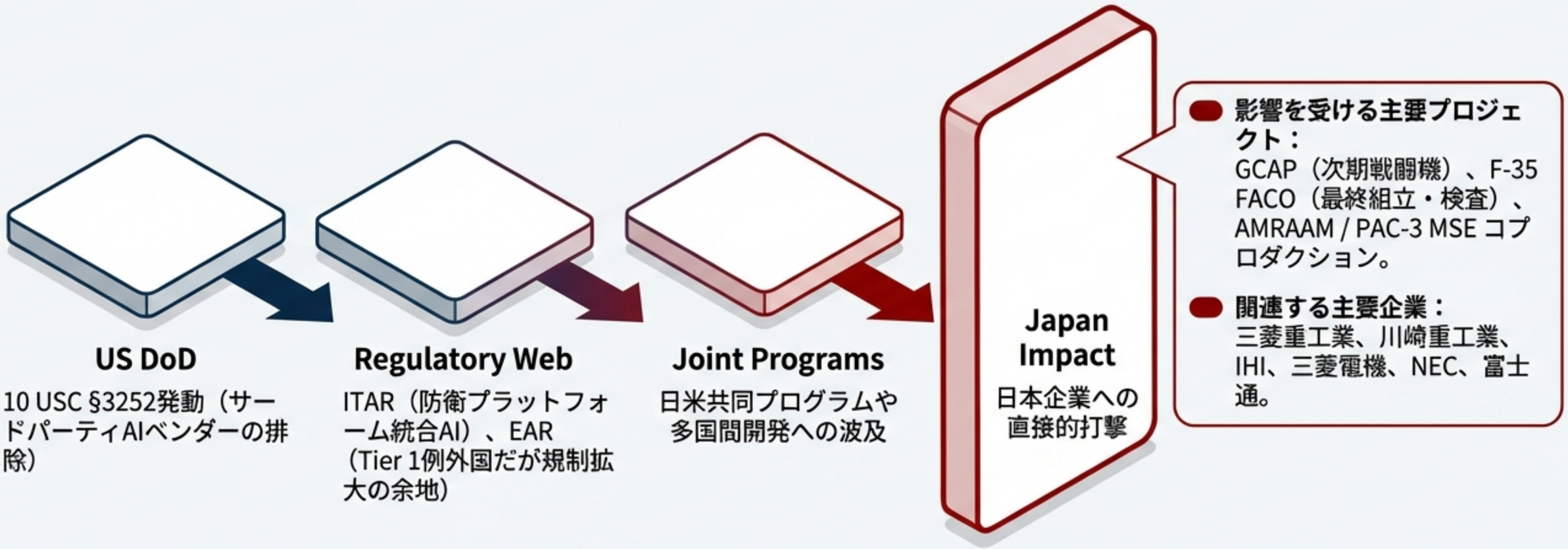
- **トランプ政権**: バイデン政権のAI安全保障大統領令（EO 14179）を撤回。
- **方針**: 「米国のリーダーシップ障壁除去」へ転換。

NATO / 日本（責任ある利用・

- NATO: 2024年7月改訂。6つの責任ある利用原則が民主主義陣営の事実上の標準に。
- **日本**: 広島AIプロセス主導、OECD報告フレームワークに国内7社参加。

Takeaway: グローバル展開する日本企業は「マルチコンプライアンス」要件を満たす設計が不可避。

連鎖する脅威：日本企業のサプライチェーン排除リスク

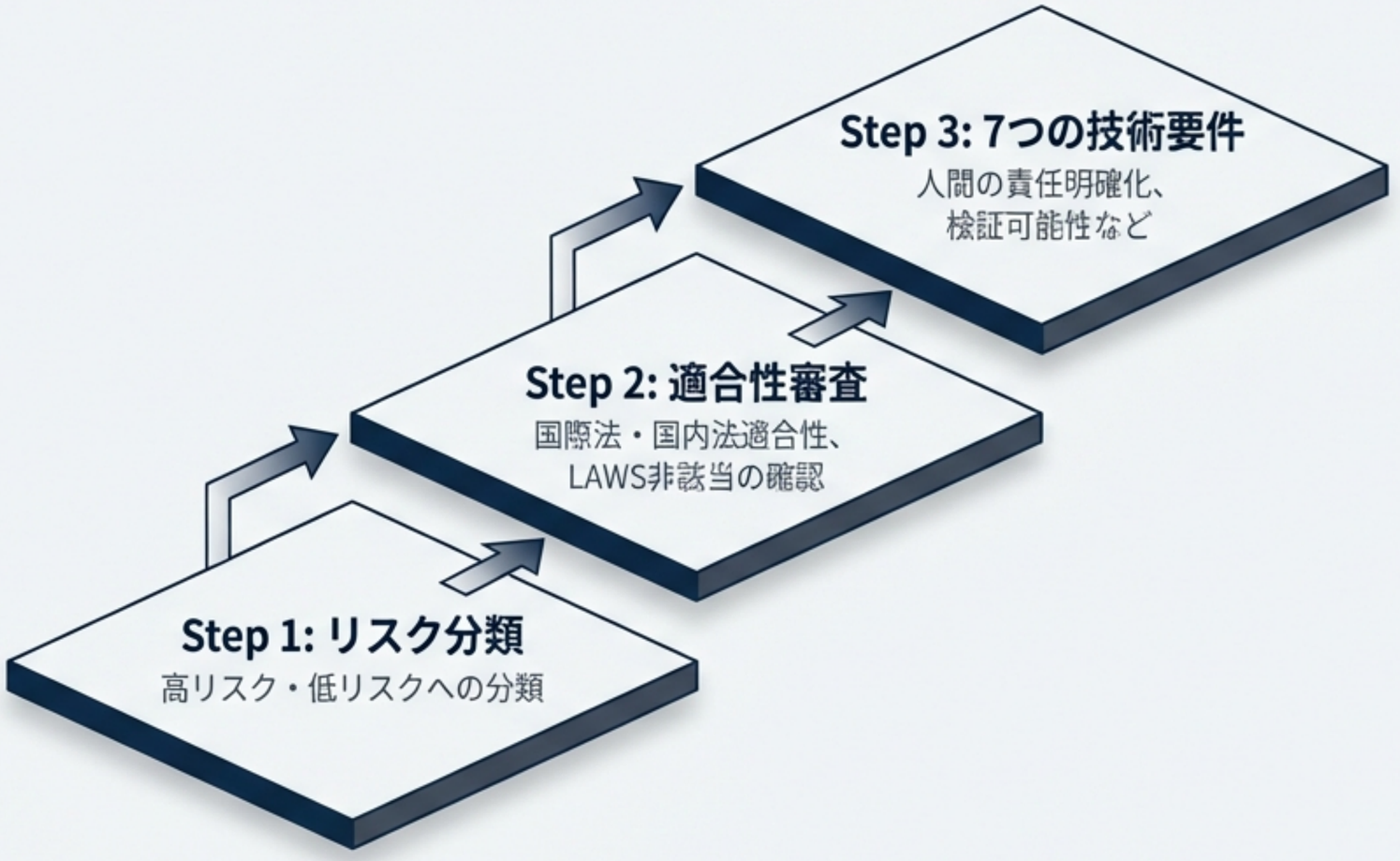


Strategic Insight

共同プログラムで「指定リスク」のあるAIツールを利用した場合、日本企業自体がサプライチェーンから排除される致命的リスクが存在する。

日本の防衛AI政策：同盟国中「最も厳格」なフレームワーク

防衛装備庁(ATLA)ガイドライン（2025年6月）



Key Facts

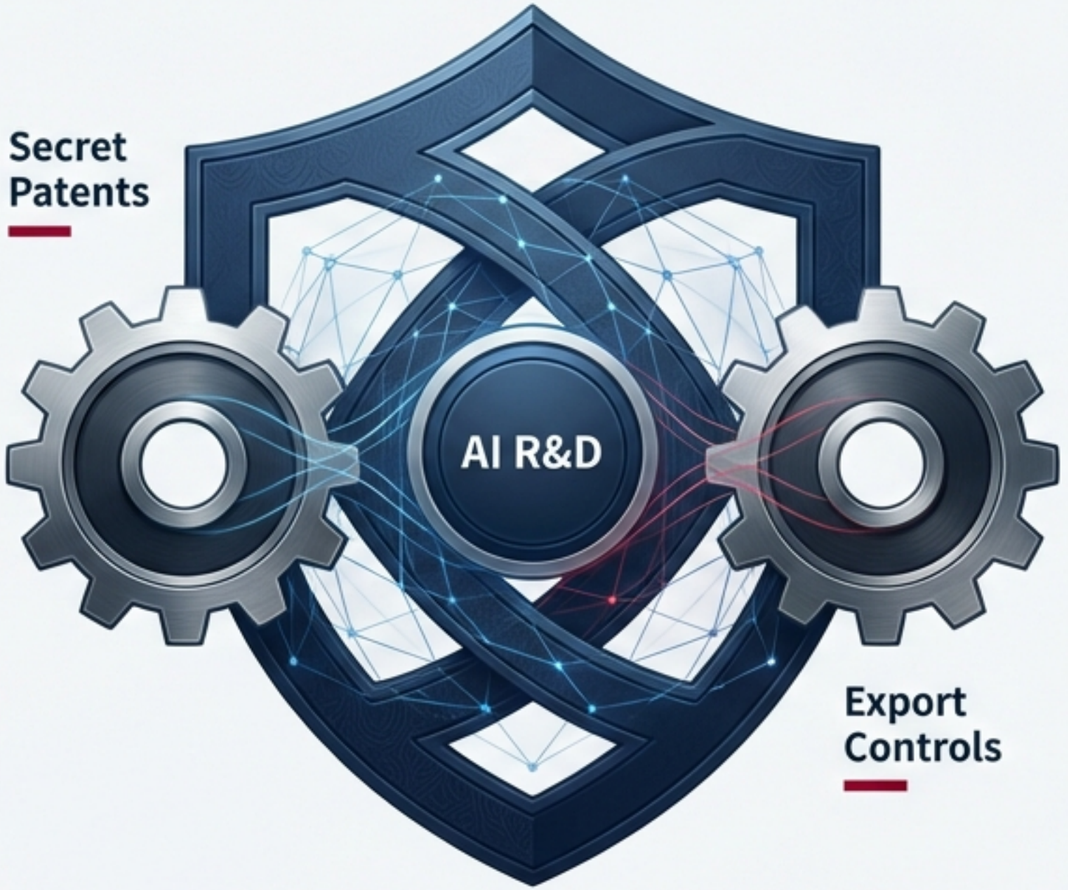
- **AI活用推進基本方針（2024/7）:** 7重点分野を指定。国際法違反の装備品は導入しないと明記。
- **AI導入推進チーム（2026/1）:** 令和8年度概算要求の中核。小泉防衛大臣主導で全省庁の先駆者を目指す。
- **LAWSへのスタンス:** 人間の関与が及ばない完全自律型致死性兵器の開発意図なし（二層アプローチ支持）。

経済安全保障と知財戦略の転換：デュアルユースの網

Gear 1

特許出願非公開制度（2024年5月施行）

- 対象: 第2分野「武器等に関係する無人航空機・自律制御等の技術」（AI直結）。
- ペナルティ: 最大2年の懲役または100万円の罰金。
- 影響: 日本国内での「第一国出願義務」が生じ、PCT（国際特許）戦略に直接影響。



Gear 2

外為法（みなし輸出管理）

- 対象: AIアルゴリズム、学習モデル、ソースコード。
- リスク:「外国の強い影響下にある居住者」への技術提供も管理対象に追加。

Bottom Line → 民生用AI技術であっても、デュアルユース指定による特許非公開化やグローバル開発体制への制限を前提とした知財戦略の再構築が必要。

アプローチの深層：Anthropic型 vs OpenAI型

Anthropic: 法的レッドライン

- **アプローチ:** 「大規模国内監視禁止」「完全自律型兵器禁止」を契約条件として法的に規定。
- **帰結:** 国防総省の柔軟な運用要件と衝突。法的に不健全として司法闘争へ（CEO: Dario Amodei声明）。

OpenAI: 技術的セーフガード

- **アプローチ:** 実質的に同じレッドラインを維持しつつ、契約ではなく技術的「セーフティスタック」でリスクを制御。
- **帰結:** 国防総省との合意を獲得し、機密ネットワーク向けAI市場を独占。

Executive Summary: ベンダーの選定基準は「倫理方針の有無」ではなく、「政府機関の要件に対する柔軟性と実装アプローチの差」を評価すべきである。

戦略的対応：「国産AI＋マルチベンダー」二層戦略への回帰

- **採用技術:** ソブリンAI（オンプレミス・エッジ環境中の国産LLM）。
- **目的:** サプライチェーンリスク指定の回避、データ完全性の担保、特定業務・日本語への高度な特化。

- **採用技術:** グローバルAI（OpenAI等）＋マルチベンダー構成。
- **目的:** 最新フロンティアモデルの汎用能力活用、ベンダーロックインの回避。

Key Context: Anthropic事件が証明した「単一のグローバルAIベンダー依存」の致命的脆弱性。クラウド上のAIシステム利用停止は、直ちに事業継続を脅かす。

日本の国産LLMチャンピオンズ：ソブリンAIの躍進

NTT（tsuzumi）

- 最新版「tsuzumi 2」（300億パラメータ/1GPU動作）。
- 実績: 国内521件・海外1,306件（計1,827件）の圧倒的受注実績。

富士通（Takane）

- Cohere社との共同開発。オンプレミス運用特化。
- 実績: JGLUEベンチマークで世界最高記録を達成。

NEC（cotomi）

- 強み: 他社比最大150倍、30万字の長文処理能力に特化。

Sakana AI

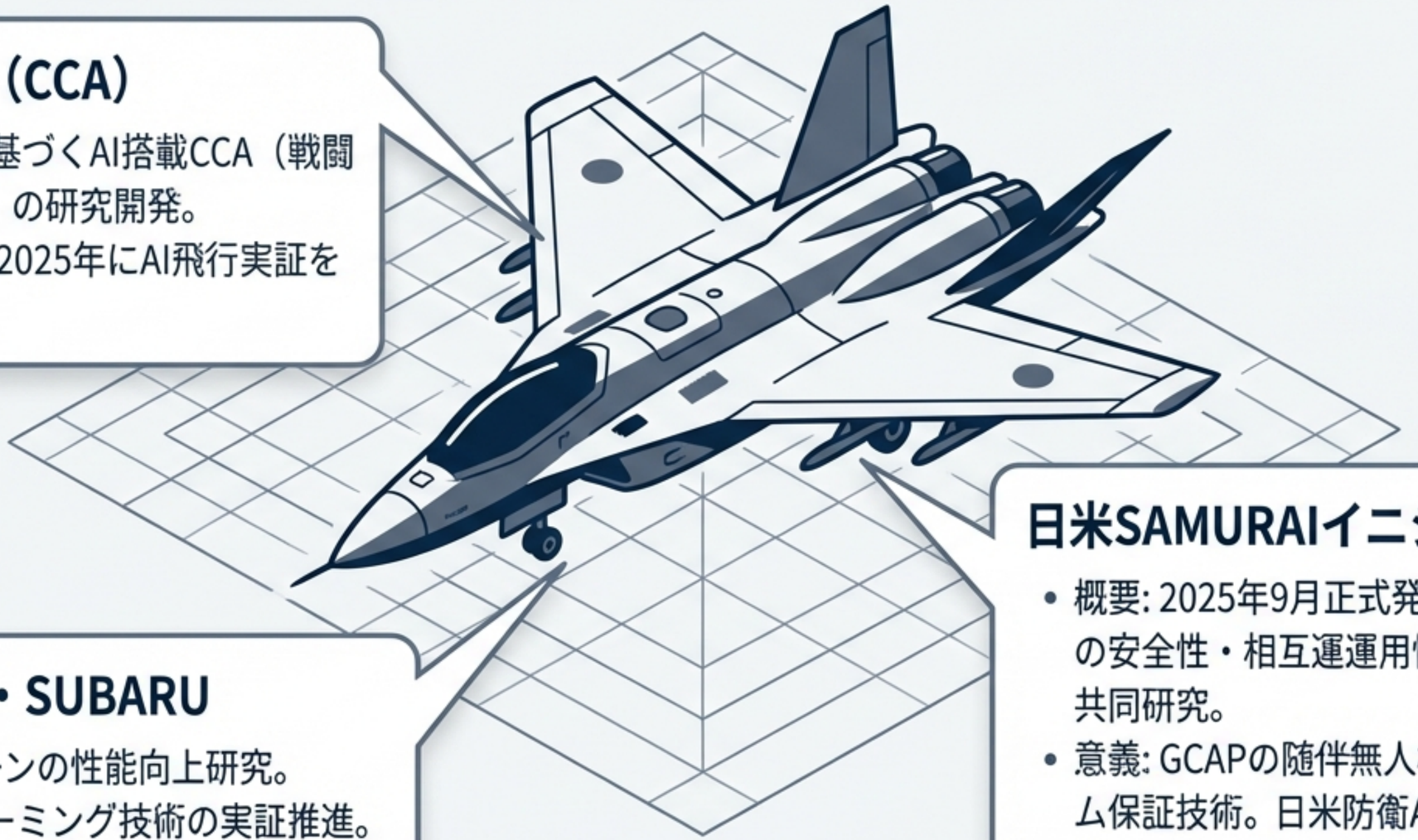
- 元Google研究者設立。企業価値4,000億円到達。
- 戦略的背景: CIA系投資機関「In-Q-Tel」からの出資獲得。

Investment Background: 日本政府のAI基本計画による1兆円規模の投資と、AI基盤への約1,350億ドルの国家主導投資計画が背景に存在。

防衛・航空宇宙におけるAI実装の最前線

三菱重工業（CCA）

- ATLA契約に基づくAI搭載CCA（戦闘支援無人機）の研究開発。
- ステータス: 2025年にAI飛行実証を実施済み。



日米SAMURAIイニシアティブ

- 概要: 2025年9月正式発足。AI搭載UAVの安全性・相互運運用性に関する日米共同研究。
- 意義: GCAPの随伴無人機向けランタイム保証技術。日米防衛AI統合の試金石。

川崎重工業・SUBARU

- 自律型ドローンの性能向上研究。
- 有人-無人チーミング技術の実証推進。

世界標準を統合したリスク管理フレームワークの導入

Concept: 複数の法規制（EU AI Act等）を跨いで遵守するための「マルチコンプライアンス」基盤。

Component 1

NIST AI RMF

- 4つの機能: Govern（統治）, Map（測定）, Measure（評価）, Manage（管理）。
- アクション: Govern 6に基づく「サードパーティAIリスクの管理手続き」の厳格化。

Component 2

ISO/IEC 42001 (AIマネジメントシステム)

- アクション: 箇条A.10.3が要求する「供給者の選定・監視プロセス」の確立。

実務的対応: 2025年10月全面施行の日本の「AI技術に関する研究開発及び活用の促進に関する法律」への実務的な対応策としても機能。

日本企業のAIガバナンス先進事例

富士通（Fujitsu）

- 体制: 2019年「AIコミットメント」策定。AI倫理外部委員会の設置。
- 運用: 社長・副社長出席のもと、半年ごとの厳格な審議を実施。

NEC

- 体制: 取締役会 → リスク・コンプライアンス委員会 → AIガバナンス遂行責任者(CDO) → デジタルトラスト推進室。
- 運用: 経産省ガイドラインに基づく「アジャイル・ガバナンス」の6ステップ実装。

日立製作所 (Hitachi)

- 体制: グローバル4拠点にまたがる「AI Global CoE」の構築。
- 運用: 全研究者を対象としたAI倫理教育の毎年実施。

契約条項の防衛的設計：AI時代のリーガルハック

Clause 1: 利用規約(AUP)変更の事前通知と拒否権

目的: ベンダーの一方的なポリシー変更（政治的理由含む）による利用停止リスクの回避。

Clause 2: マルチベンダー移行条項

目的: データポータビリティと相互運用性の確保。ロックインの防止。

Clause 3: 地政学的不可抗力条項

目的: Anthropic事件のような「**サプライチェーンリスク指定**」や**制裁**を不可抗力として定義し、損害賠償や迅速な契約解除を可能にする。

Clause 4: サプライチェーン透明性義務

目的: AIベンダーの下請け（**フォースパーティリスク**）の評価と監査権限の確保。

Bottom Context: 経済安全保障推進法の「特定社会基盤事業者」（約200社）にとって、AIクラウドの利用不能は基幹インフラ機能停止の直接的脅威となる。

結論：日本企業が直面する3つの戦略的命題

1

ソブリンAI能力の確保（経済安全保障の中核）

「軽量・低コスト・高セキュリティ・日本語特化」を武器とする国産LLM（tsuzumi, Takane, cotomi等）を機密領域に積極導入し、単一グローバルベンダーへの依存を脱却する。

tsuzumi
Takane
cotomi
JAPAN

2

地政学的ベンダー選定の実践

日米防衛サプライチェーンに関与する企業は、ITAR・EAR・サプライチェーン規制の三重苦を前提とし、技術力だけでなく「地政学的レジリエンス」でAIを選定する。

3

日本型ガバナンスモデルの構築

規制の分断化が進む世界において、EUの「厳格規制」とも米国の「完全緩和」とも異なる、ISO/IEC 42001と経安法を統合した「信頼できるAIガバナンス」を自社の競争優位性へ転換する。

Final Thought: AI戦略は、テクノロジー部門の所管から、経営トップの「国家安全保障・地政学リスクマネジメント」へと完全に移行した。