米国AI軍事利用紛争と日本企業の対応戦略：国家安全保障時代のAIガバナンス

突きつけられた構造的リスク

AI基盤モデルの「軍事コンポーネント」化

AIの最終制御権が開発企業ではなく
国家権力に帰属する新時代に突入した。

6万社に及ぶサプライチェーンリスクの連鎖

60,000社

米軍関連企業との取引がある場合、特定の
AIモデル排除が日本企業にも波及する。

Anthropic（拒絶） vs OpenAI（柔軟な実装）

法的保証を求め排除された前者

不可侵の「レッドライン」固守
＋
契約条項（法的拘束力）

契約縮小・サプライチェーンリスク指定

技術的防御で合意した後者

原則共有
＋
柔軟な技術実装
技術的セーフガード

合経継続・市場拡大

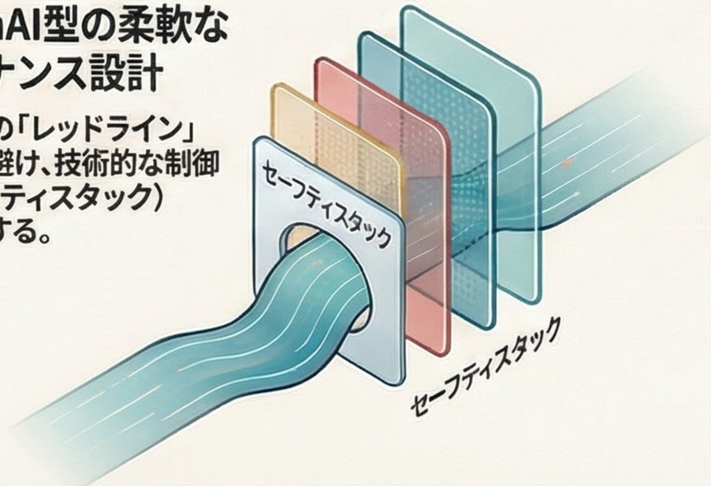
日本企業がとるべき戦略的対応

マルチベンダー化による「ロックイン」の回避

特定モデルへの依存を
避け、国産LLMを含む
代替可能な構成を
構築する。

OpenAI型の柔軟なガバナンス設計

契約上の「レッドライン」
固執を避け、技術的な制御
（セーフティスタック）
で対応する。



AIサプライチェーンの可視化と経済安保対応

自社AIスタックの提供元
と米国防産業との関係を
把握し、スクリーニング
を強化する。