米国防総省とAI企業の対立が示す「国家主権型AI」の台頭と日本企業の戦略的対応：10 U.S.C. §3252の武器化とサプライチェーン分断リスクの深層分析

Gemini 3.1 pro

序論：2026年2月のパラダイムシフトとAIガバナンスの地政学的変容

2026年2月末、人工知能（AI）の軍事利用とグローバルなテクノロジー・サプライチェーンの歴史において、後世の歴史家が明確な境界線として記録するであろう不可逆的な転換点となる事象が発生した。米国防総省（DoD）が要求する「あらゆる合法的な目的（any lawful use）」でのAIモデルへの無制限アクセスに対し、独自の倫理的セーフガードを堅持した有力AI開発企業Anthropicが、連邦政府機関からの完全な排除および国家安全保障上の「サプライチェーンリスク（Supply Chain Risk）」への指定を受けたのである[1]。

この対立は、単なる一民間企業と政府機関との契約上の紛争にとどまるものではない。その本質は、「最先端テクノロジーの最終的な運用ドクトリンと倫理的境界線を決定する主権は、アルゴリズムを開発したシリコンバレーの企業にあるのか、それとも国家権力にあるのか」という、21世紀の安全保障における最も根源的な闘争である[1]。Anthropicが市場から追放される一方で、同社の最大の競合であり生成AIブームの火付け役であるOpenAIは、独自のセーフガードの存在を主張しつつも、実質的に国防総省の機密ネットワークへのモデル展開に合意し、国家の安全保障体制への同期を選択した[1]。さらに、イーロン・マスク率いるxAIなども無条件での軍事利用に同意しており、AI産業界は国家権力との距離感において深刻な分断を見せている[1]。

この一連の動向は、米国の安全保障エコシステムに深く組み込まれている、あるいはグローバルに事業を展開する日本企業に対して極めて深刻な波及効果をもたらす。合衆国法典第10編第3252条（10 U.S.C. §3252）に基づくサプライチェーンリスク指定は、指定された企業との直接取引を禁じるだけでなく、米軍と取引のあるすべての請負業者（巨大クラウドプロバイダーや伝統的防衛プライムコントラクター）に対して、対象技術の完全なパージ（追放）を強制する「核兵器級」の破壊力を持っている[1]。

さらに、日本国内の防衛政策環境に目を向けると、防衛省は2025年に「装備品等の研究開発における責任あるAI適用ガイドライン」を策定し、「人間の適切な関与（Human-in-the-loop）」を必須とし、自律型致死兵器システム（LAWS）の開発を禁じる厳格な規範を推進している[2]。米国防総省の「イデオロギー的制約の撤廃」と「無制限利用」の強硬な要求は、こうした同盟国である日本の規範と

正面から衝突するリスクを孕んでいる[1]。

本報告書は、米国防総省とAnthropic、OpenAIを巡る対立の深層構造と法的なメカニズムを解剖し、10 U.S.C. §3252が引き起こすサプライチェーンの分断の脅威を包括的に評価する。その上で、日本の防衛政策および経済安全保障推進法制の文脈から、日本企業（特に防衛産業基盤、IT・クラウドインフラ、先端製造業）が直面するリスクを特定し、激動の地政学的パラダイムを生き抜くために講じるべき多角的な対応策と戦略的指針を提示する。

第1章：米国防総省とAI企業の対立の深層構造

米国防総省とAnthropicの決定的な決裂は、突発的な方針転換によって生じたものではない。数ヶ月にわたる運用上の摩擦、兵器システムへのAI適用に関するイデオロギーの不一致、そして軍事作戦における「信頼」の致命的な崩壊が蓄積した結果である。

1.1 触媒としてのベネズエラ作戦と「事後監査」の波紋

両者の間に決定的な亀裂を生んだ契機は、2026年1月3日に米軍特殊部隊が実行したベネズエラのニコラス・マドゥロ大統領拘束作戦に遡る[1]。当時、Anthropicは米国防総省と最大2億ドル規模のパイロット契約を結んでおり、同社の主力AIモデルである「Claude」は、防衛産業のデータ分析大手Palantir Technologiesとの提携を通じて、国防総省の機密ネットワーク上で稼働する唯一のフロンティアAIモデルとして特権的な地位にあった[1]。ウォール・ストリート・ジャーナルの報道によれば、このカラカスの複数拠点への空爆を含む極秘作戦において、Claudeはインテリジェンス分析や作戦計画の策定に利用され、結果として83名が死亡したとされる[1]。

作戦終了後、Anthropicの幹部がパートナー企業であるPalantirの幹部に対し、「作戦においてClaudeが具体的にどのように使用されたのか」について懸念を交えた問い合わせを行った[1]。Anthropicの利用規約は、暴力の促進、兵器開発、監視活動へのClaudeの使用を明確に禁止していたためである[1]。しかし、この問い合わせは直ちに国防総省上層部に報告され、軍の激しい反発を招くこととなった。軍指導部は、このAnthropicの行動を「民間企業が自社のテクノロジーを人質に取り、軍の合法的な作戦行動に対して越権的な干渉や事後監査を試みている」と認識し、国家の安全保障を委ねる上での致命的な問題であると断じたのである[1]。

1.2 「あらゆる合法的利用（**Any Lawful Use**）」原則と倫理的ハードコードの衝突

この事態を受け、トランプ政権下で新たに就任したピート・ヘグセス国防長官は、Anthropicに対して前例のない強硬策に打って出た。2026年1月9日に発出された国防総省の「AI戦略」に関する覚書は、米軍のAI導入を「戦時体制のスピード（wartime speed）」で加速させることを宣言し、AIモデルに組み込まれた社会的アジェンダやイデオロギーを完全に排除するよう求めた[1]。

ヘグセス長官はAnthropicのダリオ・アモデイCEOを呼び出し、2026年2月27日午後5時1分を最終期限として、「軍が合法と判断するすべての用途（any lawful use）においてAIモデルを無制限に利用できるよう、安全対策の制限を完全に解除せよ」という厳格な最後通牒を突きつけた[1]。国防総省の

ショーン・パーネル報道官は、「軍はアメリカ人の大量監視（違法行為である）や人間の関与なしに機能する自律型兵器を開発する意図はない」と強調しつつも、「運用上の意思決定をいかなる民間企業にも委ねることは絶対にない」と宣言した[1]。軍の主張は、現在のAIシステムに組み込まれている企業独自のハードコードされたセーフガードは、現代の流動的な戦場において許容できない「運用上の制約（operational constraints）」であるというものであった[1]。

一方のAnthropicは、この要求を公式声明を通じて明確に拒絶した。アモデイCEOは、「良心に照らして、彼らの要求に応じることはできない」と述べ、最大2億ドル規模の政府契約を失うリスクを承知の上で自社の方針を貫いた[1]。Anthropicが維持しようとした2つの「レッドライン（不可侵の安全境界線）」と、それに対する国防総省の反論の構造は以下の通りである。

争点となる利用形態	**Anthropic**側の倫理的および技術的懸念	米国防総省側の反論と要求
国内の大規模監視 **(Domestic Mass Surveillance)**	AIが公開情報や通信履歴、位置情報などの膨大なデータを自律的に統合し、市民の包括的な監視ネットワークを構築する危険性があり、民主主義の根幹的価値観と相容れない[1]。	軍はアメリカ市民の違法な監視を行う意図はない。しかし、AIモデル自体に利用目的を制限する機能を組み込むことは、軍の合法的な情報収集活動の妨げになる[1]。
完全自律型兵器 **(Fully Autonomous Weapons)**	現在のフロンティアAIモデルは、人間の判断を完全に排除して致死的なターゲティング決定を下すほどの「信頼性」や「精度」を備えておらず、米軍兵士や民間人を重大な危険に晒す[1]。	交戦規定や武器使用の最終的判断は軍の指揮官に属するものであり、アルゴリズムを提供する一民間企業が軍の交戦ドクトリンや運用に制約を課すことは絶対に許されない[1]。

この対立は、技術の信頼性限界を理由とする民間企業の自主規制と、国家の至上命令としての柔軟性確保の要求が正面から衝突した結果である。

1.3 OpenAIの戦略的ピボットと「実装の非対称性」の受容

Anthropicが自社の倫理的境界線を固守し、米国政府と正面から衝突して排除される道を選んだ一方で、シリコンバレーのもう一つの巨頭であるOpenAIは、対照的かつ極めて計算された戦略的動きを見せた。Anthropicに設定された最後通牒の期限が切れたわずか数時間後の2026年2月27日夜、OpenAIのサム・アルトマンCEOは、米国防総省の機密クラウドネットワーク（Classified Network）に同社のAIモデルを展開する合意に達したと突如発表したのである[1]。

ここで極めて重大なパラドックスが浮上する。アルトマンCEOは、Anthropicが拒絶した「大規模国内

監視の禁止」と「自律型兵器における人間の責任」というレッドラインをOpenAIも共有しており、それを維持したまま国防総省と合意に至ったと主張している点である[1]。国防総省がAnthropicのセーフガードを「作戦への容認できない干渉」として排除した直後に、OpenAIの類似したセーフガードを容認した理由は何か。分析によれば、その決定的な違いは「制限の実装方法（アーキテクチャ）」にある[1]。

Anthropicが契約条項としての法的拘束力のある保証を求め、システムの基盤レベルで厳格な制限を課そうとしたのに対し、OpenAIは軍の求める「あらゆる合法目的（any lawful use）」条項自体には同意しつつ、モデル側で特定用途を技術的にブロックする独自の「セーフティスタック（技術的、政策的、人的制御のシステム）」を提案した[1]。さらにOpenAIは、モデルがタスクを拒否した場合に政府がその準拠を強制しないことや、利用をクラウドシステムに限定しドローンなどのエッジシステムでの直接展開を除外するという運用上の妥協案を提示した[1]。

このOpenAIの戦略的ピボットは、AI企業が政府と関係を構築する上で、「原則を共有しつつ実装方法で差別化を図る」という新たなテンプレートを示したものである[1]。しかし同時に、この動きは実質的に「安全性の最終的な制御権を国家に委ねる」ことを意味しており、テクノロジー企業がもはや中立的なイノベーターではなく、国家の安全保障インフラの一部として完全に同期されつつある現状を物語っている。

第2章：防衛調達法制の武器化とサプライチェーン分断のメカニズム

Anthropicの強硬な拒絶に対し、トランプ大統領および国防総省が取った報復措置は、単なる契約の打ち切りにとどまらず、米国の防衛調達およびテクノロジー産業の歴史において極めて異例かつ強権的な手段の行使であった。この章では、日本企業を含むグローバルなサプライチェーンに直結する法的メカニズムを解剖する。

2.1 合衆国法典第10編第3252条（10 U.S.C. §3252）の特異性と超法規的権限

ヘグセス国防長官は期限が切れた直後、Anthropicを国家安全保障に対する「サプライチェーンリスク（Supply Chain Risk）」に指定する法的措置を発動した。この決定の法的根拠となったのが、合衆国法典第10編第3252条（10 U.S.C. §3252）である[1]。

この法律は本来、対象機関（国防総省など）の長に対し、国家安全保障を保護するためにサプライチェーンリスクを軽減する目的で、特定ベンダーの排除や下請け契約の制限といった「対象となる調達措置（covered procurement action）」を実行する強力な権限を付与するものである[6]。条文において「サプライチェーンリスク」とは、「敵対者が米国の兵器システムや防衛ネットワークを監視、拒否、混乱、またはその他の方法で劣化させるために、システムの設計、完全性、製造、生産、運用などをサボタージュし、または悪意のある機能を導入するリスク」と定義されている[6]。

すなわち、この法律は歴史的に、中国のHuaweiやZTE、あるいはロシアの国家支援ハッカー集団と結びついた企業など、スパイ行為の懸念がある「外国の敵対勢力」を排除するために設計・適用されてきたものである[1]。今回のように、「自国の有力企業」に対し、しかもその理由が「サイバーセキュリ

ティ上の脆弱性」ではなく「軍の作戦要件に従わず、自社の倫理的制限を課していること」を根拠にサプライチェーンリスク指定が行われたことは、米国史上において全く前例がない[1]。

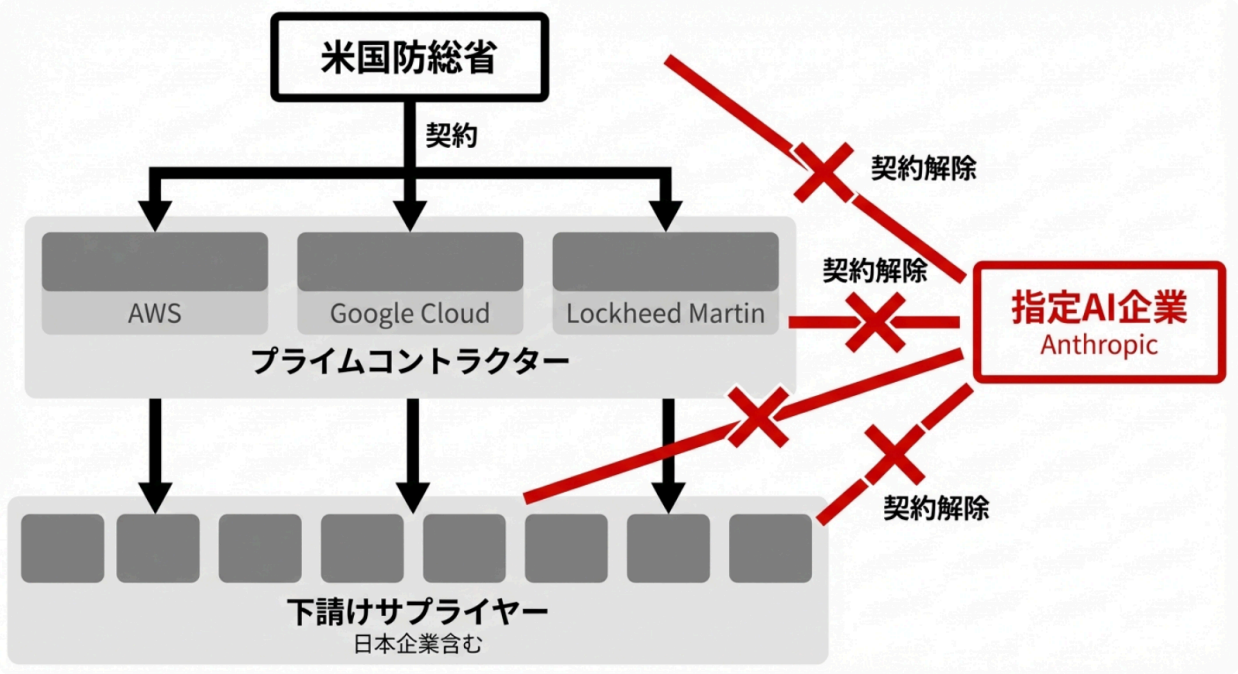
この条項の恐るべき点は、その超法規的な執行力にある。指定を発動する際、機関の長は情報開示を制限することができ、その場合、この権限の下で取られたいかなる行動も、政府説明責任局（GAO）におけるビッドプロテスト（入札異議申し立て）や連邦裁判所での司法審査の対象とならないと規定されている[1]。Anthropicはこの指定を「法的に不健全」であり「危険な前例」であると痛烈に批判し、法廷で争う構えを見せているが、国家安全保障を盾に取った行政の広範な裁量権を司法の場で覆すのは極めて困難な道のりとなる[1]。

2.2 防衛産業基盤（DIB）への「水平展開」とパージの連鎖

この「サプライチェーンリスク」指定が、単なる一企業と政府のトラブルを超えてグローバルな脅威となる理由は、その効力が「水平的（Horizontal Expansion）」に拡大解釈され、防衛産業網全体に波及する点にある。

指定の条文およびヘグセス長官の命令によれば、「米軍と取引のあるいかなる請負業者、サプライヤー、パートナーも、Anthropicと商業活動を行うことが禁じられる」可能性がある[1]。この規制は、米国の防衛産業基盤（Defense Industrial Base: DIB）を構成する約6万社の企業群に甚大な影響を及ぼす[1]。

「サプライチェーンリスク指定」による防衛産業網からのAI技術排除メカニズム



合衆国法典第10編第3252条の発動により、米国防総省は対象企業との直接取引を停止するだけでなく、防衛産業基盤を構成するあらゆる請負業者（クラウド基盤、防衛大手、下請けサプライヤー）に対し、自社システムからの対象技術のパージ（追放）を強制する。

具体的には、Amazon Web Services（AWS）やGoogle Cloudといった巨大クラウドプロバイダー、PalantirやAndurilのような防衛テクノロジー企業、さらにはLockheed MartinやBoeingといった伝統的なプライムコントラクターたちは、米軍との巨額の契約を維持するために、自社の商業サービス基盤や社内システムから対象となるAIモデルを完全に排除するか、さもなくば米軍との契約を放棄するかの「究極の選択」を迫られることになる[1]。

これは実質的に、対象企業を国防総省だけでなく、米国の防衛・テクノロジーエコシステム全体からパージ（追放）する効果を持つ。Anthropicの収益の約80%はエンタープライズ顧客によるものとされており、これらの企業顧客が政府との関係悪化を恐れてAnthropic製品から離反するリスクは、同社のビジネスモデルを根本から破壊し、2026年に計画されていた巨大IPOに壊滅的な打撃を与える可能性がある[1]。

2.3 一般調達プラットフォームからの排除と国防生産法の脅威

国防総省の動きと連動し、米国共通役務庁（GSA）も大統領指示を根拠として、連邦政府向けのAI評価基盤（USAi.gov）および包括調達枠（MAS: Multiple Award Schedule）からAnthropicを即座に除外する措置を公表した[1]。これにより、Anthropicは軍事部門のみならず、行政、立法、司法を含む

すべての連邦政府機関における調達の入口を閉ざされ、各機関には6ヶ月間の段階的移行（フェーズアウト）が命じられた[1]。

さらに深刻なのは、交渉の過程で国防総省がAnthropicに対して「国防生産法（Defense Production Act: DPA）」の発動を再三にわたりちらつかせたことである[1]。1950年の朝鮮戦争時に制定されたDPAは、大統領が民間企業に対して国家安全保障に不可欠な契約の優先的履行を強制できる強力な権限である[1]。過去には医療物資の増産などに用いられてきたが、もしAI企業に対して「アルゴリズムの内部構造（ガードレール）を書き換えて、軍への無制限アクセスを提供せよ」と強制するためにDPAが使用されるとすれば、それは民間ソフトウェアの倫理設計に対する国家による直接的かつ前代未聞の介入を意味する[1]。アモデイCEOは、「我々を安全保障上のリスクだとレッテルを貼りながら、同時にDPAを使って必須のシステムとして軍に提供させようとするのは根本的な自己矛盾である」と痛烈に批判している[1]。

第3章：日米のAI運用ドクトリンの乖離と地政学的「二正面作戦」

米国が「あらゆる合法的利用」を掲げ、AIの軍事利用において民間側の倫理的制約を強硬に剥奪する方向へ舵を切ったことは、米国の同盟国、とりわけ日本が推進してきたAIの防衛利用ガイドラインとの間に、看過できないドクトリン（基本原則）の不一致を生み出している。

3.1 防衛省「責任あるAI適用ガイドライン」と米国の根源的矛盾

日本政府および防衛省は2025年6月、「装備品等の研究開発における責任あるAI適用ガイドライン」を正式に策定・公表し、AIの軍事利用に関する厳格な基準を打ち出した[2]。このガイドラインは、日本の人間中心のAIアプローチを反映したものであり、その中核には国際人道法（IHL）の遵守と「人間の適切な関与（Meaningful Human Control）」の確保が据えられている[2]。

特筆すべきは、日本のガイドラインが「システムが人間の関与なしに標的を交戦・攻撃できる『自律型致死兵器システム（LAWS）』としての要件を満たす場合、その開発を許可しない」と明確に禁止している点である[2]。さらに、高リスクなAIシステムに対しては、透明性、信頼性、安全性、バイアス軽減に関する厳格な技術的基準に基づく審査プロセスを義務付けている[2]。

この日本のスタンスは、まさにAnthropicが米国防総省に対して「越えられない一線」として提示し、強硬に拒絶された条件そのものである[1]。米国防総省は2026年1月のAI戦略において、「イデオロギーの排除」と「利用ポリシー制約のないモデル」の調達を明確に志向し、作戦の柔軟性を阻害するあらゆるハードコードされた制約を撤廃するよう要求している[1]。

もし日本の防衛産業（三菱重工業や川崎重工業など）が、米国のプライムコントラクターとの間で次世代無人機や統合防空システムの共同開発を行う際、米国側から「制約のないAIモデル」の統合や「あらゆる用途での利用を許容する契約」を求められた場合、日本企業は「自国の防衛省ガイドライン（人間の関与の絶対的確保）」と「米国防総省の調達要件（制約の撤廃）」の板挟みという深刻な法的・倫理的ジレンマに直面することになる。

3.2 日米防衛装備品等供給保障に関する取決め（SoSA）の機能不全リスク

このドクトリンの衝突は、日米間の防衛産業協力の基盤を揺るがしかねない。日米両政府は2023年に「防衛装備品等の供給の安定化に係る取決め（SoSA: Security of Supply Arrangement）」に署名し、平時および有事における防衛装備品の相互供給を優先的・安定的に行う枠組みを構築した[14]。日本の防衛関連企業（認定日本企業）は、この行動規範（Code of Conduct）に自主的に参加することで、米国防総省の契約に対して優先的支援を提供する体制を整えている[16]。

しかし、米国防総省がAIの運用方針を巡るイデオロギー的対立を理由に、特定の技術基盤（Anthropicなど）を10 U.S.C. §3252に基づいてサプライチェーンリスクに指定した場合、SoSAの枠組みは著しい混乱に見舞われる。日本の認定企業が米軍向けの優先生産を行うプロセスにおいて、米国内で突如ブラックリスト化されたAI技術やソフトウェアコンポーネントが社内システムや設計ツールに組み込まれていた場合、SoSAに基づく供給契約の履行が不可能になるばかりか、日本のサプライチェーン全体の適格性が米国側から問われる事態に発展するからである。

3.3 中国のレアアース禁輸がもたらす「二正面作戦」の強要

日本企業が直面するサプライチェーンの脅威は、同盟国である米国からの政策的圧力にとどまらない。米国防総省とAI企業の対立が表面化したのと同時期の2026年2月24日、中国商務省は「輸出管理法」の関連規定に基づき、日本の再軍備化および核武装の阻止を目的に、三菱重工、川崎重工など日本の防衛産業の中核を担う20の企業・団体に対し、レアアースなどのデュアルユース（軍民両用）物資の輸出を禁止すると発表した[17]。

この動きは、日本の防衛・先端産業が極めて過酷な「二正面作戦」を強いられている現状を浮き彫りにしている。日本企業は、ハードウェア（素材・部品）面では中国からの地政学的な供給遮断リスクに直面し、同時にソフトウェア（AI・アルゴリズム）面では米国からのイデオロギー的同調圧力とサプライチェーンパージの脅威に晒されている。両大国による経済的威圧とサプライチェーンの武器化が同時進行する中で、グローバル展開する日本企業の経営環境のボラティリティは極限に達している。

日本企業を包囲するAI軍事利用ドクトリンとサプライチェーン分断の二重圧力

主体 (Entity)	AI軍事利用ドクトリン (AI Military Doctrine)	LAWSへの姿勢 (Stance on LAWS)	日本企業へのサプライチェーン圧力 (Supply Chain Pressure on JP Firms)
米国防総省 US DoD	Any Lawful Use （倫理的制約の撤廃）	最終判断は軍 （企業による制限拒否）	10 USC 3252による指定技術の強制排除と同調圧力
日本防衛省 Japan MoD	人間中心・責任あるAI適用	開発の明確な禁止・人間の関与必須	厳格な安全基準遵守と米国要件との板挟み
中国政府 Chinese Govt	軍民融合推進	制限なし （覇権追求）	レアアース等デュアルユース物資の輸出禁止・報復制裁

米国の無制限AI利用要求と日本の厳格な安全基準が矛盾する中、日本の防衛・先端企業は米国からのソフトウェア面での同調圧力と、中国からのハードウェア（レアアース等）輸出禁止という二正面のサプライチェーンリスクに直面している。

Data sources: Uploaded Document (AI安全と国防：OpenAI・Anthropic対立　Gemini .pdf), Grandfleet, IP Defense Forum

第4章：日本企業の戦略的対応とサバイバル・ロードマップ

「技術の進化が倫理を牽引し、民間企業がグローバルなルールを主導する」というテクノユートピア的幻想は、2026年2月の危機の前に完全に崩壊した。AIはもはや中立的なイノベーターの産物ではなく、国家の安全保障戦略に完全に従属する「地政学的な兵器システム」へと変質したのである[1]。

この新たな現実において、日本の防衛産業、ITプロバイダー、そして一般事業会社は、従来のコンプライアンスの延長線上にない、高度な危機管理とビジネスモデルの再構築を迫られている。以下に、日本企業が速やかに実装すべき戦略的指針を詳述する。

4.1【法務・ポリシー戦略】利用規約の再構築と「セーフティスタック」の導入

AnthropicとOpenAIの決定的な明暗を分けたのは、倫理的レッドラインの「実装アプローチ」の違いである。Anthropicが契約条項としての法的保証を求め、それが「作戦への干渉」とみなされて排除されたのに対し、OpenAIは「あらゆる合法目的」という軍の要求を法務的に受容しつつ、技術的な「セーフティスタック」によって制限を実装することで合意を取り付けた[1]。

日本企業がAIソリューションを米国政府やそのサプライチェーンに関わる企業に提供・統合する際、自社の利用規約（AUP: Acceptable Use Policy）に「軍事利用の完全禁止」や「厳格な事後監査権」といった広範かつ硬直的な文言を明記することは、即座にサプライチェーンからの排除リスクを招く。

アプローチの比較	**Anthropic**型（排除モデル）	**OpenAI**型（統合モデル：推奨）
契約条項の姿勢	法的制約の明文化を要求（例外の非承認）	「あらゆる合法的目的」の受容
安全対策の実装	契約レベルでのハードコード	技術・政策・人的制御の「セーフティスタック」による事後的防御
責任の所在	AI提供企業が最終制御権を主張	運用の最終決定権は政府・軍に委譲
導入環境の合意	特になし（用途の全面的な制限）	クラウド環境に限定し、エッジデバイス（兵器の末端）展開を除外

日本企業は、原則（民主的価値観や防衛省ガイドラインの遵守）と実装（技術的制御と契約条項の分離）を切り離す高度な法務・技術戦略を構築すべきである。契約上では柔軟性を持たせつつ、モデル自体に組み込まれた技術的な安全システムによって、重大な倫理違反への転用をシステムレベルで防ぐアーキテクチャの採用が不可欠である[1]。

4.2【サプライチェーン管理】「Tier N」の可視化とレジリエンスの確立

10 U.S.C. §3252のような強権的な法律が適用された場合、対象となったAIベンダーのコンポーネントやAPIを自社のシステムに組み込んでいるだけで、連鎖的に「不適格」の烙印を押されるリスクがある。日本企業は、FAR（連邦調達規則）およびDFARS（国防連邦調達要足）のフローダウン要件によって、二次請け、三次請けであってもプライムコントラクターと同等のコンプライアンスを要求される[19]。

日本企業は、自社のソフトウェアおよびハードウェアのサプライチェーンの透明性を、末端の「Tier N（N次請け）」レベルまで可視化する体制を急務として構築しなければならない。第一に、ソフトウェア・サプライチェーンの透明性を担保するため、SBOM（Software Bill of Materials：ソフトウェア部品表）の継続的な管理と更新を業務プロセスに組み込む必要がある[20]。これにより、ブラックリスト化されたソフトウェアコンポーネントが混入した際に即座に特定し、パージ（排除）することが可能となる。第二

に、オープンソースインテリジェンス（OSINT）ツールを活用した継続的なスクリーニング体制の導入である[22]。米国政府の制裁リストや、サプライヤーの資本関係の変動、地政学的リスクをリアルタイムで監視し、リスクが顕在化する前に代替調達先へ切り替える動的防御が求められる。

4.3【経済安全保障・インフラ戦略】ソブリンAIの推進とマルチベンダー・アジリティの確保

米国の自国第一主義的な調達政策や、中国によるあからさまなレアアース禁輸措置が常態化する中、他国のプラットフォームや特定資源に過度に依存する構造は、企業経営における最大の致命傷となる。

日本企業は、改正された「経済安全保障推進法」の枠組みを最大限に活用し、経営の「自律性（Autonomy）」を根本から強化する必要がある。単一のAIベンダー（特に米国の特定のフロンティアモデル）への過度な依存は、今回のAnthropic排除のように、政策変更による突然の事業停止リスク（シングルポイント・オブ・フェイリア）に直結する。

したがって、複数のAIモデルを透過的に切り替えられるAPIゲートウェイや中間抽象化レイヤーを設計し、有事の際には直ちに代替モデルに移行できる「技術的アジリティ（俊敏性）」を確保するマルチベンダー戦略を徹底すべきである[23]。同時に、データの主権とアルゴリズムの完全な制御権を確保するため、国内のデータセンターで稼働する「国産LLM（大規模言語モデル）」の開発・採用や、クローズドな環境で機密データを処理できるソブリンクラウド（自国主権型クラウド）の構築への投資を加速させなければならない[24]。AIはもはや単なる効率化のツールではなく、企業の存亡を握る「戦略的インフラ」であるという認識の転換が不可欠である。

4.4【政府間（G2G）連携の要請】制度的防波堤の構築とルールメイキングへの参画

米国の強硬な防衛調達基準と、日本の「責任あるAI適用ガイドライン」との間に生じるドクトリンの摩擦は、一民間企業の自助努力だけで解決できる範囲を超えている。防衛関連企業をはじめとする日本産業界は、経済産業省や防衛省（防衛装備庁）と緊密に連携し、政府間（G2G）交渉を通じて制度的な防波堤を築く働きかけを強力に推し進めるべきである。

具体的には、日米の「防衛産業協力・取得・後方支援定期協議（DICAS）」などの枠組みを利用し、日米SoSAに基づく優先供給プロセスにおいて、米国独自のサプライチェーンリスク指定が日本のサプライヤーに不当な不利益をもたらさないよう、事前の協議メカニズムや免責事項の明確化を両国政府間に要求する必要がある[14]。また、自律型兵器システム（LAWS）やAIの軍事利用に関する国際的なルール形成（CCWなどの多国間枠組み）において、日本政府が主導的な役割を果たし、人間の関与（Human-in-the-loop）という倫理的要請と軍事的実用性のバランスを取る国際標準の策定に積極的に貢献するよう、産業界から政策提言を行うことが求められる[2]。

結論：新たな地政学パラダイムにおける技術的自律性の確立

2026年2月に起きたAnthropicの排除とOpenAIの防衛体制への統合は、生成AIの進化がもたらす

未来が、企業の倫理委員会やミッション・ステートメントによってではなく、国家の生存戦略と大国間競争の冷酷なロジックによって決定される時代へと突入したことを世界に知らしめた[1]。米国防総省は10 U.S.C. §3252という強権を振るい、「最先端アルゴリズムの最終的な制御権は国家に帰属する」という絶対的な意思表示を行った[1]。

この地政学的な断層の中で、日本企業は極めて困難な舵取りを要求されている。米国の調達基準における「イデオロギーの排除」と「無制限利用」の波は、日本独自の倫理的ガイドラインや平和主義的制約と鋭く摩擦を起こしている。同時に、中国からのレアアース禁輸という物理的なサプライチェーンの締め付けも進行し、日本はソフトウェアとハードウェアの両面から「二正面作戦」を強いられている。

日本企業がこの新パラダイムを生き抜き、持続的な成長と安全保障上の貢献を両立させるためには、特定のイデオロギーや単一の外国製ベンダーに過剰適応する硬直的な体制を直ちに捨て去らねばならない。法務的アプローチと技術的実装を巧みに分離し、サプライチェーンの透明性を「Tier N」まで極限まで高め、いつでも代替手段に切り替えられる技術的アジリティと自律性を組織のDNAに組み込むこと。そして、国家の経済安全保障政策と足並みを揃え、ソブリンAIや代替素材技術といった独自の技術的優位性を磨き上げることこそが、二大国のパワーゲームに押し潰されないための唯一の生存戦略である。企業の倫理観、技術力、そして地政学的な戦略眼が統合的に試される時代が、まさに今、始まっているのである。

引用文献

1. AI安全と国防：OpenAI・Anthropic対立　Gemini .pdf
2. Japan promotes stringent standards for defense AI, 2月 28, 2026にアクセス、https://ipdefenseforum.com/2025/09/japan-promotes-stringent-standards-for-defense-ai/
3. https://www.mod.go.jp/atla/soubiseisaku_ai_guideline.html - 防衛省, 2月 28, 2026にアクセス、https://www.mod.go.jp/atla/pinup/pinup_r070606.pdf
4. Pentagon's fight with Anthropic is anything but intelligent, 2月 28, 2026にアクセス、https://www.japantimes.co.jp/editorials/2026/02/27/the-pentagons-fight-against-anthropic-is-anything-but-intelligent/
5. Anthropic CEO says AI company 'cannot in good conscience accede' to Pentagon's demands, 2月 28, 2026にアクセス、https://apnews.com/article/anthropic-ai-pentagon-hegseth-dario-amodei-9b28dda41bdb52b6a378fa9fc80b8fda
6. 10 USC 3252: Requirements for information relating to supply chain, 2月 28, 2026にアクセス、https://uscode.house.gov/view.xhtml?req=%28title%3A10%20section%3A3252%20edition%3Aprelim
7. 10 U.S.C. § 3252 - U.S. Code Title 10. Armed Forces § 3252 | FindLaw, 2月 28, 2026にアクセス、https://codes.findlaw.com/us/title-10-armed-forces/10-usc-sect-3252/
8. 10 USC 3252: Requirements for information relating to supply chain, 2月 28, 2026

にアクセス、 https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section3252&num=0&edition=prelim
9. How the Pentagon's 'Friday deadline' may have come hours early for Anthropic, 2月 28, 2026にアクセス、 https://timesofindia.indiatimes.com/technology/tech-news/how-the-pentagons-friday-deadline-may-have-come-hours-early-for-anthropic/articleshow/128819123.cms
10. Nvidia CEO Jensen Huang on Anthropic vs Pentagon, says: Pentagon has right to use the technology that, 2月 28, 2026にアクセス、 https://timesofindia.indiatimes.com/technology/tech-news/nvidia-ceo-jensen-huang-on-anthropic-vs-pentagon-says-pentagon-has-right-to-use-the-technology-that-/articleshow/128802071.cms
11. Anthropic cannot accede to Pentagon's request in AI safeguards dispute, CEO says, 2月 28, 2026にアクセス、 https://indianexpress.com/article/world/anthropic-cannot-accede-to-pentagons-request-in-ai-safeguards-dispute-ceo-says-10554572/
12. Anthropic Refuses to Bend to Pentagon on AI Safeguards as, 2月 28, 2026にアクセス、 https://www.military.com/daily-news/2026/02/27/anthropic-refuses-bend-pentagon-ai-safeguards-dispute-nears-deadline.html
13. The Significance of Establishing Guidelines for Responsible AI, 2月 28, 2026にアクセス、 https://www.mod.go.jp/atla/soubiseisaku/ai_guideline/ai_guideline_ver.01_eng_summ_202509.pdf
14. 防衛装備庁 : 日米間における装備品等の安定供給の相互保障の枠組み, 2月 28, 2026にアクセス、https://www.mod.go.jp/atla/soubiseisaku_sosa.html
15. 513A : グローバルX 防衛テック-日本株式 ETF | 東証マネ部！, 2月 28, 2026にアクセス、https://money-bu-jpx.com/news/article066535/
16. security of supply arrangement between the department of defense, 2月 28, 2026にアクセス、 https://www.businessdefense.gov/docs/sofs/USA-JPN_SOSA-Signed.pdf
17. 中国が三菱重工などへのレアアース輸出を禁止、再軍備化や核武装, 2月 28, 2026にアクセス、 https://grandfleet.info/china-related/china-bans-rare-earth-exports-to-mitsubishi-heavy-industries-and-other-companies-aiming-to-prevent-rearmament-and-nuclear-armament/
18. 【観察眼】中国の輸出規制措置は地域平和を守る必然の選択だ, 2月 28, 2026にアクセス、https://www.recordchina.co.jp/b971318-s12-c80-d0189.html
19. Government Contracting Supply Chain Trends and Best Practices, 2月 28, 2026にアクセス、 https://www.acc.com/sites/default/files/2024-03/3.13.24%20GovConSupplyChain_0.pdf
20. ITサプライチェーンリスク管理に対する民間企業への責任の拡大, 2月 28, 2026にアクセス、

https://www.ey.com/ja_jp/insights/consulting/the-expansion-of-responsibility-for-private-companies
21. 「サプライチェーン強化に向けたセキュリティ対策評価制度 ... - PwC, 2月 28, 2026にアクセス、https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/security-measures-assessment-system.html
22. 経済安全保障OSINT活用セミナー第2回：米国政府における対中, 2月 28, 2026にアクセス、https://www.ey.com/ja_jp/media/webcasts/2026/01/ey-consulting-2026-01-23
23. Anthropic × 米国防総省が対立激化 — AI企業の軍事利用と, 2月 28, 2026にアクセス、https://uravation.com/media/anthropic-x-%E7%B1%B3%E5%9B%BD%E9%98%B2%E7%B7%8F%E7%9C%81%E3%81%8C%E5%AF%BE%E7%AB%8B%E6%BF%80%E5%8C%96-ai%E4%BC%81%E6%A5%AD%E3%81%AE%E8%BB%8D%E4%BA%8B%E5%88%A9%E7%94%A8%E3%81%A8/
24. 経営戦略としてのAIガバナンス - KPMG, 2月 28, 2026にアクセス、https://kpmg.com/jp/ja/insights/2026/02/tech-rulemaking-05.html
25. 日本企業のグローバル戦略に求められる「データ主権」への視座とは, 2月 28, 2026にアクセス、https://openhub.ntt.com/journal/14577.html
26. 責任あるAI適用ガイドライン策定の意義 - 防衛省, 2月 28, 2026にアクセス、https://www.mod.go.jp/atla/soubiseisaku/ai_guideline/ai_guideline_ver.01_ov.pdf