ChatGPT

米国国防総省がAnthropicを「サプライチェーンリスク」に指定し、請負業者に取引中止を求める可能性の分析レポート

エグゼクティブサマリ

Gigazine（2026-02-17）は、米国国防総省がAnthropicを「サプライチェーンリスク（supply chain risk）」として扱い、国防総省と取引する請負業者に対し、Anthropic（Claude）との取引停止や「使用していない」ことの証明（certification）を求め得る、という報道（主にAxios等）を起点に、当該措置の“検討”を伝えています。 [1]

一次資料ベースで確認できる確度の高い事実は、(1) 国防総省の公式AI組織である Chief Digital and Artificial Intelligence Office [2] が2025-07-14にAnthropic、OpenAI、Google、xAIへ「各最大2億ドル上限」の契約（Award）を公表していること、(2) Anthropicは「Claude Gov」など国家安全保障顧客向けモデルが“機密環境”で運用されていると自社発表していること、(3) 2026-02中旬以降、国防総省とAnthropicの間で「合法である限り全用途（all lawful purposes）」を求める国防総省側と、「国内大規模監視」「完全自律兵器」などを線引きするAnthropic側の対立が複数の主要メディアで継続的に報じられ、国防総省側が「supply chain risk」指定を“脅し/選択肢”として示唆していること、です。 [3]

一方で、ユーザーが前提として「不明」とした点（国防総省の“正式指定文書”の有無、請負業者リスト、契約影響範囲の確定）は、現時点の公開一次資料からは確定できず、本レポートでも「不明」とします。特に「『サプライチェーンリスク指定』が、(A) 国防総省固有のICTサプライチェーン権限（10 U.S.C. §3252・DFARS）に基づく“調達上の排除/制限”なのか、(B) FASCSA（Federal Acquisition Supply Chain Security Act）に基づく“FASCSA order（除外・撤去命令）”なのか、(C) それ以外（契約条項・運用ガイダンス・事実上の取引停止要請）なのか」は、報道上は混在的で、公式文書の提示がないため断定できません。 [4]

結論として、「国防総省が“何らかの形”で請負業者に対しAnthropicの技術利用制限を求める」可能性は、(i) 国防総省自身が“供給網リスク管理”を制度化しており、(ii) さらに近年はFASCSA条項により「特定ソース/特定技術の排除」を契約上実装できる枠組みが整っていることから、制度面では成立し得ます。 [5]
ただし、報道が示すように本件が“サイバー/改ざん/敵性支配”ではなく「用途制限（契約上のガードレール）をめぐる対立」を主因とする場合、法目的（サボタージュ等の排除）との整合性や「二次的ボイコット（政府取引先に民間サービスの不使用を強要する形）」の正当性が争点化し得る、という指摘もあり、実施には高い政治・法的コストが伴うとみられます。 [6]

事実確認と一次資料検証

以下はGigazine（2026-02-17）の主要主張を抽出し、可能な限り一次資料（国防総省公式、法令、当事者公式声明）または一次情報に近い発言（当局報道官コメント、企業スポークスパーソン声明）で検証したものです。 [7]
（注）国防総省の“正式指定文書”や請負業者向け“通知文書”は、公開一次資料としては確認できず「不明」。 [8]

Gigazineの主張には、少なくとも以下が含まれます。[7]

- 主張：国防総省がAnthropicを「サプライチェーンリスク」に指定することを検討している。
  検証：**“検討/脅し”としての言及は複数報道で確認できるが、公式指定文書の存在は不明。** GigazineはAxios報道を根拠に「検討」と記載。[1]
  参考一次情報（報道官コメントとして流通）：

  > “The Department of War’s relationship with Anthropic is being reviewed.”
  > 日本語訳：「（いわゆる）戦争省（国防総省）のAnthropicとの関係は見直し中だ。」
  > 出典（Axiosに対する Sean Parnell [9] のコメントとして掲載）：[10]
  > 追加の裏取り：少なくとも「supply chain risk」という語を用いた“脅し”が存在する旨は、2026-02-23のAxios続報でも記述。[11]

- 主張：指定されると、国防総省と取引する企業（請負業者）がClaude等を使っていないことを証明する必要が生じ得る（実質的排除）。
  検証：**報道としては複数に出るが、制度上はFASCSA条項（FAR 52.204-30）が“類似の結果”を契約で実装し得る。** Gigazineは「証明」と表現。[12]
  制度面の一次資料（FASCSA条項）では、契約者は「適用されるFASCSA order」に該当する“source”や“covered article”を「提供・使用してはならない」旨が明記され、かつSAM検索・定期確認・報告義務が規定されています。[13]

  > “Contractors shall not provide or use … any covered article … if … prohibited by an applicable FASCSA orders …”
  > 日本語訳：「請負業者は、適用されるFASCSA命令で禁じられた対象物（covered article）等を、契約履行の一部として提供または使用してはならない。」
  > 出典（FAR 52.204-30）：[13]
  > ただし、報道が言う“certify（証明）”が、(A) FAR条項上の表明・開示（representation/disclosure）、(B) 10 U.S.C. § 3252系の国防総省手続、(C) 個別契約条項、のどれを指すかは**不明**。[14]

- 主張：対立の発端は、国防総省が「合法ならあらゆる用途」での利用を求める一方、Anthropicが監視・兵器用途などに線引きを求めたこと。
  検証：**複数の独立報道・当事者声明で概ね一致。**[15]

  > “all lawful purposes”
  > 日本語訳：「合法である限り、あらゆる目的」
  > 出典（Reuters：国防総省がAI各社に求めると記述）：[16]
  > またAnthropicのスポークスパーソンは、議論が「完全自律兵器」「大規模国内監視」といった“線引き”に関するものだった旨を述べています。[17]
  > “hard limits around fully autonomous weapons and mass domestic surveillance”
  > 日本語訳：「完全自律兵器と大規模国内監視に関する厳しい上限（線引き）」
  > 出典（Reuters掲載のAnthropic声明）：[18]

- 主張：Claudeが「機密（classified）」環境で使われている／（報道上）唯一のモデルである。
  検証：**“機密環境での運用”は当事者公式発表と複数報道で確認可能だが、“唯一”は報道依存であり厳密には不明。**
  Anthropicは「Claude Govモデルは国家安全保障最高レベルの機関で既に配備され、アクセスは機密環境に限定」と明記。[19]
  また、Palantir Technologies [20] と Amazon Web Services [21] を介して、Claude 3/3.5が“classified environments”へ提供される旨が、Business Wire系の一次情報（Nasdaq掲載）で説明され、「最初

にclassifiedに持ち込む産業パートナー」との表現もあります。[22]
ただし、Reutersは「classified settingsで利用可能なのはAnthropicのみ（through third parties）」と述べる一方、これは“その時点の運用/承認状況”に関する報道であり、国防総省側の公式認定一覧の公開はなく、**完全な検証は不明**です。[23]

- 主張：国防総省とAnthropicの関係には、最大2億ドル規模の契約がある。
  検証：**国防総省公式と当事者公式の双方で確認。**[24]
  国防総省公式（Chief Digital and Artificial Intelligence Office[2]）は、Anthropic等4社に各2億ドル上限のAwardを発表しています。[25]
  Anthropic公式も同趣旨（2年・上限2億ドルのOTA）を公表し、政府導入の一部がPalantir Technologies[20]経由で“classified networks”に統合されていると説明しています。[26]

- 主張：ベネズエラ作戦（Maduro拘束）でClaudeが使われたと報じられ、摩擦が激化した。
  検証：**WSJ起点の報道で、Reutersは「直ちに検証できない」と明記。**[27]
  Reutersは「WSJが関係者を引用してClaude使用を報じた」としつつ、Reuters自身では検証できない旨を明示しています。[28]

  > “Reuters could not immediately verify the report.”
  > 日本語訳：「Reutersは当該報道を直ちに検証できなかった。」
  > 出典（Reuters）：[28]
  > この点はGigazineも“報道ベース”であり、一次資料（作戦報告書・議会記録・公式発表）は**不明**です。[29]

- 主張：Anthropicのポリシーは、暴力支援・武器設計・監視などを禁じる（国防総省の要求と齟齬）。
  検証：**Anthropicの利用規約（Usage Policy）で明文確認可能。**[30]

  > “Do Not Develop or Design Weapons”
  > 日本語訳：「武器を開発または設計してはならない。」
  > 出典（Anthropic Usage Policy）：[30]
  > さらに同ポリシーは「政府顧客と契約する際、目的・法的権限に合わせて制限を調整し得る」とも記載しており、全面禁止ではなく“条件付き調整”の余地を示しています。[30]

（総括）Gigazineが述べる「指定の検討」「請負業者への波及」「用途制限をめぐる対立」は、複数の主要報道と当事者・政府組織の公表で概ね整合します。[31]
ただし「国防総省が実際に“指定”を発令したか」「指定の法形式（10 U.S.C. § 3252なのかFASCSA orderなのか）」「請負業者通知文書・対象者リスト」は公開一次資料では確認できず、**不明**です。[32]

背景と比較

Anthropicの事業・政府向け展開（一次資料中心）として、少なくとも以下が確認できます。
Anthropicは2025-07-14、国防総省（Chief Digital and Artificial Intelligence Office[2]）から2年・上限2億ドルのOTAを受けたと公表し、Thiyagu Ramasamy[33]が「国家安全保障支援の新章」と述べています。[34]
またAnthropicは2025-06-06に「Claude Gov models」を発表し、「機密環境で運用され、国家安全保障上位レベルの機関で既に配備」と明記しました。[19]
インフラ面では、Palantir Technologies[20]とAmazon Web Services[21]を介して、Claude 3/3.5が政府の“classified environments”で運用される構成が、Business Wire系の一次情報で説明されています。[22]
この文脈で、Defense Information Systems Agency[35]のImpact Level 6（IL6）認定に言及しており、少なくとも“高保証の防衛向けクラウド基盤での提供”がパートナー発表の中心要素です。[22]

「サプライチェーンリスク」の定義は、民間一般用語としての広義（供給網の途絶・品質問題）と、米国政府調達文脈での狭義（改ざん・サボタージュ・不正機能混入等）が混線しやすい点が重要です。NISTのC-SCRM（Cybersecurity Supply Chain Risk Management）では、ICT/OT供給網が多様な主体から成り、オープンソースや外部サービス提供者も含まれ、そこでのサイバーリスクを組織的に管理する枠組みとして説明されます。 36
また国防総省の調達文脈で「サプライチェーンリスク」が法的に典型想定するのは、10 U.S.C. §3252が列挙する「sabotage」「malicious introduction of unwanted function」「subversion」等の“敵対的行為”です。 37

過去の類似事例（比較表）は、(A) “政府が特定ベンダーを排除・禁止したケース”と、(B) “供給網攻撃やリスク事案が政策化したケース”を分けて見ると整理しやすいです（ユーザー要件によりOpenAI/Microsoft/Huawei等を含む）。 38

事例	問題の性質	政府側の主要メカニズム	対象範囲	“Anthropic指定”との類似点/相違点
Huawei（例示）	対中安全保障・通信機器リスク（政府調達）	NDAA §889 → FAR条項（例：FAR 52.204-25）	調達・契約に広く影響（機器/サービス）	“供給網リスク”ラベルが対外脅威に用いられやすい点は類似。主因が“国籍・敵対国”である点は相違。 39
Kaspersky（例示）	対露安全保障・ソフトウェア利用禁止	NDAA（実装条項：FAR Subpart 4.20等）	連邦政府契約に影響	対外脅威想定の典型。用途制限ではなく“製品そのものの排除”が焦点。 40
Acronis（FASCSA実例）	供給網リスクとしての排除・撤去命令（公開情報は限定）	FASCSA order（DNI系）→ FAR 52.204-30等で運用	IC/SCI等（報道・分析ベース）	「FASCSA orderが現実に発動した」点で類似枠組み。ただし法目的は“敵対的リスク”で、国内企業の“契約上ガードレール”とは異なると論評される。 41
OpenAI（例示）	政府導入・契約（排除ではない）	2億ドル上限のDoD契約、政策整合（“usage policies”）	DoDの特定領域	“AI供給網の一部として政府導入”は類似。排除・制裁ではなく調達促進が中心で相違。 42
Microsoft（例示：SolarWinds等）	供給網攻撃・クラウド/ソフトの連鎖リスク	政府のインシデント対応・指針（GAO/CISA等）	連邦政府全体の対策強化	“供給網リスク”が政策化した点は類似。ただし特定ベンダーの排除指定ではなく、横断的対策強化が中心。 43

（注）表中の“対象範囲”のうちAcronisの具体範囲は、公開一次資料が限定されるため、主に専門家分析・解説に依存し、詳細は不明が残ります。 44

法的・政策的枠組み

国防総省が企業を「サプライチェーンリスク」とみなし、請負業者に取引停止（または利用排除）を求め得る“法的経路”は、大きく二系統あります。

第一に、国防総省固有のICTサプライチェーン権限（10 U.S.C. §3252 → DFARS Subpart 239.73）です。10 U.S.C. §3252は、国防総省が「covered procurement action」を取り得る枠組みとして、調達における排除・制限（例：特定サプライヤーとの取引拒否、下請け同意の拒否、特定ソースの排除指示等）を規定し、供給網リスクの例として「sabotage」「malicious introduction of unwanted function」「subversion」などを明示しています。 45
さらにこの枠組みは、判断根拠の秘匿やレビュー制限（GAOや裁判所での争訟制限）を含むため、実務上は“公表されない形での排除”も理論上は起こり得ます。 46
ただし、DFARS実装の解説（最終ルール）では「目的はサプライチェーンリスク軽減で、原則として“最小限介入（less intrusive measures）”を優先し、特定ソースの排除を“ケースバイケース”で行う」こと、また実質的なデバー（de facto debarment）にならぬよう内部手続きを整備する旨が示唆されています。 47
加えて国防総省の“信頼できるシステム/ネットワーク”政策（例：DoDI 5200.44）は、ミッションクリティカル機能保護や信頼性確保を目的とし、供給網を含むリスク管理の枠組みを提示します。 48

第二に、政府横断のFASCSA（Federal Acquisition Supply Chain Security Act）系です。FAR 52.204-30は、契約者が「適用されるFASCSA order」に該当する“source”や“covered article”を契約履行に用いることを禁じ、さらにSAM上で“FASCSA order”を検索する義務、少なくとも3か月に一度のSAM確認、該当時の報告（3営業日以内の一次報告等）を規定しています。 13
この条項上、「covered article」には“cloud computing services of all types”を含む情報技術が含まれ得るため、クラウド経由で提供されるAIサービス（モデルAPI等）が「covered article」概念に接続され得る点は、今回の“AIモデル=供給網部品”という主張と整合します。 49
またFAR 4.2304は、(a) SAMに掲出されたFASCSA ordersを参照すること、(c) 追加のFASCSA orderは契約変更等で適用されること、(d) SAMに載らないFASCSA orderの実装では当局手続に従うことを規定しており、“公開されない命令”の余地も条文上は排除されません（ただし実態把握は不明）。 50
FASCSAの原法（Public Law 115-390）上も、連邦政府が供給網リスクに対応する制度基盤を整備したことが確認できます。 51

以上を踏まえると、「国防総省が請負業者に取引停止を求める法的効力」は、**“どの経路で実装されるか”に依存**します。
- FASCSA order＋FAR条項で契約に流れれば、請負業者・下請けは“契約条項違反”のリスクとして従わざるを得ません。 52
- 10 U.S.C. §3252/DFARS系で、調達行為（下請け同意拒否・ソース排除）として実装されれば、個別案件での排除・移行が実務的に強制され得ます（ただし、当該権限は本来“サボタージュ等”の想定であることが条文上明確で、用途制限を理由に適用する妥当性は争点化し得る）。 53

この“法目的との整合性”については、専門家論評として「関連法は外国の敵対者による防衛技術の破壊・改ざん等を念頭にしており、国内企業の契約上の用途制限に適用するのは法的に不透明」という指摘が出ています。 54
もっとも、これ自体は論評であり、実際に国防総省がどう法解釈し、どの手続きを取るかは**不明**です。 55

技術的懸念と緩和策

本件は政治・契約条件の対立として報じられていますが、国防総省が「サプライチェーンリスク」という語を持ち出す場合、技術的には「AIモデル（とその提供経路）が防衛システムの供給網の一部であり、そこに改ざん・漏洩・依存・可視性不足が存在する」という構図に接続されます。 56
以下、Anthropic固有の実装詳細は公開されていないため多くが**不明**ですが、一次資料に基づく「AIサービスが供給網として持つ典型的リスク」を、クラウド依存・第三者統合・モデル供給という前提で具体化します。 57

想定リスクの具体像（供給網観点）
- データ漏洩・越権アクセス：機密環境であっても、モデル統合にはデータフロー（入力・出力・ログ・監

査）が生じます。NISTは外部サービス提供者や統合者を含めた供給網リスク管理の必要を明示しており、可視性不足は構造的課題です。 58
- バックドア/不正機能混入：10 U.S.C. §3252が想定する“malicious introduction of unwanted function”や“sabotage”は、ソフトウェア供給網（ビルド、配布、署名、更新）における典型リスクです。AIモデルの場合、モデル重み・推論サービング基盤・更新配布が同型の攻撃面になります。 59
- 依存性（単一ベンダーロックイン）：ReutersやAxiosは「機密システムでClaudeが深く組み込まれており、代替が容易でない」と描写しています。これは技術面では、モデル性能だけでなく、認証・監査・運用・データ統合まで含む依存の問題です。 60
- ガードレール（用途制限）とミッション要件の摩擦：AnthropicのUsage Policyは“検知・監視によりポリシーを執行する”としており、政府向けには“法的権限とミッションに合わせた制限調整”の余地も示します。ここは“安全性（制約）”と“作戦柔軟性（無制約）”の衝突点で、技術というより統治（governance）の問題ですが、監視・兵器用途はリスク領域として明文化されています。 61

攻撃（失敗）シナリオ例（推定）
- サプライチェーン改ざん（モデル/推論基盤）：第三者統合（例：クラウド＋統合プラットフォーム＋モデルAPI）のいずれかが侵害され、機密入力が外部へ流出、または特定トリガーで誤誘導するふるまいが混入する。NISTが指摘する「供給網は多主体で、オープンソースや外部サービスも含む」特性が攻撃面を広げる。 62
- “誤り/幻覚”の高リスク領域流入：Reutersは、AIがもっともらしい誤情報を生成し得て、機密環境での誤りが致命的結果を生む恐れを研究者が警告している、と報じています。用途制限交渉の背景には、こうした“安全性”をどこまで制度で担保するかという問題がある。 63
（注）Anthropic固有の誤り率・評価結果は本レポートでは**不明**（公開評価への直接アクセスは未確認）。 64

緩和策（制度・技術の両輪）
- 供給網の可視化と監査設計：NISTのC-SCRMが示すように、供給網を構成する主体（供給者、統合者、外部サービス提供者等）を前提に、リスクを“Frame→Assess→Respond→Monitor”の反復で管理する。 65
- 契約条項での“排除・代替・報告”の仕組み化：FAR 52.204-30は、SAMの定期確認（少なくとも3か月ごと）や、該当時の迅速報告（3営業日以内）を要求しており、サプライチェーン上の変化を“継続監視”で扱う設計になっている。 13
- ガードレール交渉の透明化：NIST AI RMFは、GOVERN/MAP/MEASURE/MANAGEとしてリスク管理機能を提示しており、軍事転用領域の“どのリスクを誰が引き受けるか”を合意可能な形で文書化・測定・更新する枠組みが必要です。 66
（注）現状の交渉がどの程度文書化されているかは**不明**。 67

影響分析

本件の影響は「国防総省の契約（最大2億ドル）」という直接額よりも、「供給網リスク指定」というラベルが、請負業者の契約適格性・使用技術の棚卸し・下請け連鎖に波及し得る点にあります。 68
加えて、Anthropic側は“商用の大企業顧客の広がり”を示す発表をしており、仮に「政府取引先はClaude不使用」を求められると、民間大企業やスタートアップの調達・コンプライアンスにも連鎖し得ます。 69

定量材料（公開一次/準一次）としては、少なくとも以下が確認できます。
- 国防総省（CDAO）によるAI企業4社へのAward：各2億ドル上限。 24
- Reuters：国防総省は“classifed networks”への展開を求め、OpenAIは“genai.mil”という非機密ネットワークで300万人超に展開された、と報じる。 70
- Anthropic：年換算収益ランレート（annualized revenue run-rate）約140億ドル、Fortune 10のうち8社が顧客、合計で米国人口の3分の1にリーチするシステムで使用されている、等の主張を自社発表。 71
（注）“Fortune 10の8社”の具体社名・契約形態は当該発表からは特定できず**不明**。 72

ステークホルダー別影響（短期/中期/長期の代表例）は次の通りです（数値は上記の公開材料に限定し、未確認は不明）。 [73]

ステークホルダー	短期影響（数週〜数か月）	中期影響（〜1年）	長期影響（1年〜）
国防総省（調達・作戦部門）	交渉決裂/継続、代替検討、ガードレール運用負荷。 [74]	“機密環境での代替モデル承認”や統合再設計が必要（不明だが報道上は困難と示唆）。 [75]	“AI調達のルール形成”が制度化されれば、単一企業交渉から脱却。 [76]
主要請負業者（prime）	供給網棚卸し・利用停止の可否判断。FASCSA条項型ならSAM検索・報告などの手続負担。 [13]	“Claude依存”が深い場合、代替コスト・遅延・品質低下。 [77]	供給網リスク管理が常態化し、AIベンダー選定が“政治/規制リスク”を含む。 [78]
下請け・SaaS/ツール提供者	“二次的排除”の恐れ：上位契約に引きずられ、利用ツール変更を迫られる可能性。 [79]	契約条項のフローダウン（下請け条項流し込み）による監査・報告要件増。 [13]	国防市場参入障壁が上がり、寡占化・政府向け“専用モデル”の潮流が強化。 [80]
民間大企業（政府取引あり）	報道通り“証明”が求められると、ワークフロー再設計・コンプラ対応。 [81]	ツール標準化が進むほど切替コスト増（ベンダーロックイン問題）。 [82]	“政府向け利用可否”が商用AI選定要件化し、AI市場の分断（gov/commercial）を促進。 [83]
AI産業（競合含む）	“軍事用途ガードレール”の業界標準が揺れ、各社が姿勢を迫られる。 [84]	国防総省が求める“all lawful purposes”に合わせた製品設計・契約が増える可能性。 [85]	“安全性 vs 国家安全保障”的緊張が国際的に制度化され、輸出規制や同盟国調達にも影響。 [86]

反応と見解・シナリオ分析・推奨

当事者・主要関係者の反応（一次/準一次中心）
- 国防総省側：Axiosによれば、Sean Parnell [9] が関係見直しを述べたとされ、さらに2026-02-23のAxiosでは“supply chain risk”指定をちらつかせたうえで、請負業者に「Claude不使用の証明」を迫り得る、と明記されています。 [87]
- Anthropic側：Reutersは、議論が特定作戦ではなく「Usage Policy上の論点（完全自律兵器・大規模国内監視）」に集中しているとのスポークスパーソンコメントを掲載。 [88]
またAnthropic公式は、国防総省との協業を“責任あるAI導入”として位置づけ、Palantir Technologies [20] を含むパートナー経由で“classified networks”に統合されていること、Usage Policyを含むガバナンスを強調しています。 [89]
- 主要請負業者（Palantir）側：Nasdaq掲載の一次情報（Business Wire）では、Shyam Sankar [90] が「Claudeをclassified environmentsに持ち込む最初の産業パートナー」等の文脈で安全な展開を述べています。 [22]
一方で、今回の“指定検討”に対するPalantir公式の直接コメントは、公開一次資料では**不明**（報道上は“沈黙/コメントなし”として扱われがち）。 [91]

信頼度評価（簡易）
- 高：国防総省公式（CDAO発表）、Anthropic公式発表、FAR/DFARS条文、NIST文書（供給網リスクの定義）。 [92]

- 中：Reuters（複数ソース・匿名当局者を含むが、検証不能を明示する場合あり）、Axios/WaPo（当局者コメント流通、ただし公式文書提示なし）。 [93]
-　低〜中：二次まとめ記事（切り取りや推測混入の可能性）。ただし“何が一次にあるか”の導線としては有用。 [94]

シナリオ分析（推定）
以下は公開情報に基づく推定であり、確率は筆者推定です（根拠となるトリガーは報道・条文の示す実装可能性）。 [95]

シナリオ	トリガー（起点）	確率（推定）	影響度	推奨対応（要旨）
最良	2026-02-23の高官会合で合意し、Usage Policyの“政府向け調整”を枠内で拡張。指定は見送り。 [96]	40%	中	契約条件・監査ログ・用途レビュー手順を文書化し、“all lawful purposes”の範囲を実装上限定。 [97]
中間	“正式指定”ではなく、個別プログラム単位での利用制限・代替モデル併用へ（事実上のリスク扱い）。 [16]	45%	中〜高	請負業者は用途別にモデル分離、代替経路を確保。供給網台帳と監査を強化。 [78]
最悪	10 U.S.C. §3252/DFARSまたはFASCSA orderで“排除・撤去”が契約上実装され、請負業者に不使用証明が波及。 [98]	15%	高	契約適格性維持のため迅速オフボーディング計画、代替AIの認可取得、法的救済（可能性は不明）を同時進行。 [99]

上記の時間軸（主要マイルストーン）は、少なくとも公開情報上、次のように整理できます。 [100]

```
timeline
  title Anthropic×国防総省（供給網リスク論点）主要イベント
  2024-11 : Palantir＋AWS経由でClaude 3/3.5をclassified環境へ提供（発表）
  2025-06 : AnthropicがClaude Govモデルを発表（機密環境での運用を明記）
  2025-07 : CDAOがAI企業4社へ各$200M上限のAwardを公式発表
  2026-02-12 : Reuters：国防総省がAI各社にclassified展開・制限緩和を要請と報道
  2026-02-13 : Reuters：Maduro作戦でClaude使用（WSJ報道）を「検証不能」と併記
  2026-02-16 : Axios：国防総省が“supply chain risk”指定を検討/示唆と報道
  2026-02-17 : Gigazine：上記を起点に「指定検討」「請負業者への波及」を報道
  2026-02-22 : WaPo：対立の拡大と政治・制度的含意を報道
  2026-02-23 : Axios：国防長官とCEO会合（ultimatum示唆）を報道
```

推奨（政策・技術対応案：短期/中期/長期）
“指定”が形式的に何であれ、契約条項と供給網管理の観点から、関係主体は次の準備が合理的です（不明点は不明のまま、実装可能な一般策に落とし込み）。 [101]

対象	短期（〜3か月）	中期（〜1年）	長期（1年〜）
米国政府（国防総省・調達当局）	“supply chain risk”の法形式を明確化（どの権限/条項か）し、請負業者に必要情報を提示（可能なら）。 102	AI用途の許容範囲を、個社交渉でなく政策（議会/規程）へ寄せる（Lawfareが問題提起）。 76	同盟国も含む“防衛AI供給網標準”を整備（監査、ログ、撤去・代替手順の標準化）。 78
請負業者（prime/sub）	供給網台帳を整備：AIモデル/API/統合基盤を“source”単位で棚卸し。SAM確認・報告の運用手順を準備。 103	“モデル多重化”と“用途分離”（機密/非機密、分析/作戦等）でロックインを低減。 104	供給網リスク訴訟・契約停止に備えたBCP（代替調達・移行計画）を常設化。 103
Anthropic	政府向け例外のガバナンス（何を許す/許さない/監査可能性）を明文化し、Usage Policyの“政府向け調整”条項を具体運用へ。 105	“機密環境向け安全評価”の透明性（可能な範囲で）と、統合先（クラウド/プラットフォーム）に対するC-SCRM要求を契約化。 106	国際的には、同社が掲げる輸出規制・地域制限の論理（国家安全保障）と、国内防衛用途の整合を政策提言として整理。 86
第三者監査機関・標準化主体	NIST等の枠組みに沿った“AI供給網監査”の評価手順を整備（C-SCRMとAI RMFの接続）。 107	監査結果の共有スキーム（機密/非機密の切り分け）を制度化し、撤去・代替の“演習”を組み込む。 103	政府・産業・同盟国で相互承認可能な評価基準を形成し、サプライチェーン分断リスクを抑える。 108

（参考：主要一次ソースURL一覧。引用・根拠は本文のリンク付き引用を参照）

```
DoD（CDAO）公式発表（2025-07-14）: https://www.ai.mil/latest/news-press/pr-view/article/4242822/
Anthropic（DoD契約発表 2025-07-14）: https://www.anthropic.com/news/anthropic-and-the-department-of-defense-to-advance-responsible-ai-in-defense-operations
Anthropic（Claude Gov 2025-06-06）: https://www.anthropic.com/news/claude-gov-models-for-u-s-national-security-customers
Anthropic Usage Policy（2025-09-15施行）: https://www.anthropic.com/legal/aup
FAR 52.204-30（FASCSA条項）: https://www.acquisition.gov/far/52.204-30
DFARS 239.73（Supply Chain Risk Management）: https://www.acquisition.gov/dfars/subpart-239.73-requirements-information-relating-supply-chain-risk
NIST SP 800-161r1（C-SCRM）: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
```

1 4 7 8 12 14 29 31 32 33 55 64 68 94 https://gigazine.net/news/20260217-pentagon-anthropic-supply-chain-risk/
https://gigazine.net/news/20260217-pentagon-anthropic-supply-chain-risk/

2 30 61 105 https://www.anthropic.com/legal/aup
https://www.anthropic.com/legal/aup

3 24 25 80 92 https://www.ai.mil/latest/news-press/pr-view/article/4242822/cdao-announces-partnerships-with-frontier-ai-companies-to-address-national-secu/
https://www.ai.mil/latest/news-press/pr-view/article/4242822/cdao-announces-partnerships-with-frontier-ai-companies-to-address-national-secu/

5 37 45 46 53 59 https://www.law.cornell.edu/uscode/text/10/3252
https://www.law.cornell.edu/uscode/text/10/3252

6 54 76 https://www.lawfaremedia.org/article/congress-not-the-pentagon-or-anthropic-should-set-military-ai-rules
https://www.lawfaremedia.org/article/congress-not-the-pentagon-or-anthropic-should-set-military-ai-rules

9 36 56 58 62 65 78 82 90 107 108 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

10 87 https://www.law.cornell.edu/cfr/text/41/201-1.303
https://www.law.cornell.edu/cfr/text/41/201-1.303

11 67 74 75 77 81 95 96 https://www.axios.com/2026/02/23/hegseth-dario-pentagon-meeting-antrhopic-claude
https://www.axios.com/2026/02/23/hegseth-dario-pentagon-meeting-antrhopic-claude

13 21 35 41 49 52 73 79 83 98 99 101 102 103 52.204-30 Federal Acquisition Supply Chain Security Act Orders—Prohibition. | Acquisition.GOV
https://www.acquisition.gov/far/52.204-30

15 16 23 60 63 70 84 85 93 104 https://www.reuters.com/business/pentagon-pushing-ai-companies-expand-classified-networks-sources-say-2026-02-12/
https://www.reuters.com/business/pentagon-pushing-ai-companies-expand-classified-networks-sources-say-2026-02-12/

17 18 88 https://www.reuters.com/technology/pentagon-threatens-cut-off-anthropic-ai-safeguards-dispute-axios-reports-2026-02-15/
https://www.reuters.com/technology/pentagon-threatens-cut-off-anthropic-ai-safeguards-dispute-axios-reports-2026-02-15/

19 20 106 https://www.anthropic.com/news/claude-gov-models-for-u-s-national-security-customers
https://www.anthropic.com/news/claude-gov-models-for-u-s-national-security-customers

22 57 100 https://www.nasdaq.com/press-release/anthropic-and-palantir-partner-bring-claude-ai-models-aws-us-government-intelligence
https://www.nasdaq.com/press-release/anthropic-and-palantir-partner-bring-claude-ai-models-aws-us-government-intelligence

26 34 89 https://www.anthropic.com/news/anthropic-and-the-department-of-defense-to-advance-responsible-ai-in-defense-operations
https://www.anthropic.com/news/anthropic-and-the-department-of-defense-to-advance-responsible-ai-in-defense-operations

27 28 91 https://www.reuters.com/world/americas/us-used-anthropics-claude-during-the-venezuela-raid-wsj-reports-2026-02-13/
https://www.reuters.com/world/americas/us-used-anthropics-claude-during-the-venezuela-raid-wsj-reports-2026-02-13/

38 39 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. | Acquisition.GOV
https://www.acquisition.gov/far/52.204-25

40 https://www.ecfr.gov/current/title-48/chapter-1/subchapter-A/part-4/subpart-4.20
https://www.ecfr.gov/current/title-48/chapter-1/subchapter-A/part-4/subpart-4.20

42 https://openai.com/global-affairs/introducing-openai-for-government/
https://openai.com/global-affairs/introducing-openai-for-government/

43 https://www.gao.gov/products/gao-22-104746
https://www.gao.gov/products/gao-22-104746

44 https://www.mayerbrown.com/en/insights/publications/2025/10/dni-issues-first-fascsa-exclusion-and-removal-order-against-acronis-ag
https://www.mayerbrown.com/en/insights/publications/2025/10/dni-issues-first-fascsa-exclusion-and-removal-order-against-acronis-ag

47 https://www.govinfo.gov/content/pkg/FR-2015-10-30/pdf/2015-27463.pdf
https://www.govinfo.gov/content/pkg/FR-2015-10-30/pdf/2015-27463.pdf

48 https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf?ver=2018-11-08-075800-903
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf?ver=2018-11-08-075800-903

50 https://www.govinfo.gov/link/plaw/115/public/390
https://www.govinfo.gov/link/plaw/115/public/390

51 https://www.law.cornell.edu/cfr/text/41/201-1.102
https://www.law.cornell.edu/cfr/text/41/201-1.102

66 97 https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf
https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf

69 71 72 https://www.acquisition.gov/far/4.2304
https://www.acquisition.gov/far/4.2304

86 https://www.anthropic.com/news/updating-restrictions-of-sales-to-unsupported-regions
https://www.anthropic.com/news/updating-restrictions-of-sales-to-unsupported-regions