ChatGPT

# 日本企業向け報告書：米国の軍事AI調達ショックを踏まえた実務対応

## エグゼクティブサマリー

本報告書は、2026年2月に米国政府がAIベンダーに対して示した「軍事AIは国家が最終決定権を持つ」という強いシグナル（調達排除・供給網リスク指定・強制権限の示唆）を踏まえ、日本企業が取るべき実務対応を、リスクタイプ別に一般化して提示する。米国では、連邦機関に対する特定AIの使用停止命令と段階的廃止（6か月猶予）や、調達プラットフォームからの除外が進み、同時に国防当局は契約条項として「any lawful use（合法なあらゆる用途）」を標準化する方針を明文化した。 1

日本企業にとって重要なのは、今回の事象が「技術事故」ではなく「政策・調達・地政学」に起因する“サプライチェーン型ショック”である点である。供給網リスクを根拠に調達上の措置と情報非開示を可能にする枠組み（米国法）や、優先履行を命じ得る強制権限（国防生産法）といった“例外的権限”が、AI・クラウド・ソフトウェア領域に持ち込まれると、民間企業は短期間で「取引停止」「乗換え」「設計変更」を迫られ得る。 2

結論として、日本企業は「AIガバナンス整備」だけでは不十分であり、①地政学・経済安全保障を含む全社ERMへの統合、②ベンダー／モデルの“可搬性（portability）”確保、③政府・大口顧客からの要請に対する“赤線（レッドライン）”とエスカレーション手順の事前定義、④サイバー／ソフトウェア供給網（SBOM、セキュア開発、委託先管理）の常時運用、をセットで実装する必要がある。これらは、日本の「AI事業者ガイドライン」のリスクベース・アプローチやアジャイル・ガバナンス、国際的なAIリスク管理（NIST AI RMF）、AIマネジメントシステム（ISO/IEC 42001）、人権デューデリジェンス（UNGP、OECD）と整合させることで、経営層・監査・調達先から説明可能な形に落とし込める。 3

本報告書は、現時点ではユーザー企業の業種・米国依存度・AI利用形態が未提示であるため、タイプ別の標準テンプレートとして提示する。追加資料（契約類型、主要顧客、AI利用領域、海外拠点、規制対象データの有無等）が判明し次第、本テンプレートの該当箇所に具体値（優先順位、コストレンジ、体制案）を適用して改訂できる構造とした。 4

## 前提と不明点

本報告書が参照したアップロード資料は、米国における軍事AI利用・政府調達・企業の安全制約（ガードレール）を巡る対立を中心に整理したレポート群である（少なくとも「any lawful use」要求、供給網リスク指定、政府調達からの除外、技術的ガードレールと契約条項の対比、国際人道法・大量監視・自律型兵器の論点を含む）。

ただし、ユーザー企業の固有条件（業種、米国政府・防衛産業基盤との関係、海外売上比率、扱うデータの種類、AIの適用領域、内製比率、主要ベンダー契約、委託先構造等）は未提示であるため、分析は「想定される情報タイプ」ごとに一般化し、業界別影響評価は“典型的な曝露（exposure）”に基づく相対順位として示す。 4

また、軍事・監視・自律兵器に関する議論は、国際人道法や人権に深く関わるため、企業が実務対応を検討する際は、法務・コンプライアンス（国外法を含む）・人権方針・輸出管理・取締役会の監督の下で、適法性と説明責任を担保する設計が前提となる。 5

## アップロード資料が示す論点

米国では、連邦政府調達において「AIの客観性（objectivity）を主要基準にする」「契約条項として　“any lawful use”を標準化する」など、調達側がベンダーの利用制約（AUP等）を“運用上の阻害要因”とみなす設計思想が明文化された。[6]

これと並行して、ベンダー側が「大量監視」「完全自律型致死兵器」等を例外として拒否・制限しようとした場合、政治・調達手段による圧力（政府機関での使用停止、政府調達枠からの除外、供給網リスク指定、強制法の示唆）が短期間で発動され得ることが示された。[7]

ここで日本企業が学ぶべき核心は、「AIの安全原則（何をさせないか）」を、契約条項で固定するのか、技術的な制御（セーフティスタック、ログ監査、運用統制）で担保するのか、あるいは両方で多層化するのかによって、政府・規制当局・顧客との交渉力とリスク分布が変わる点である。実際、国防当局は“民間企業が運用意思決定を縛ること”自体への反発を示しつつ、他方で安全性配慮を前面に出した提供形態（政府クラウド内・用途限定・ガードレール実装）も受け入れている。[8]

主要アクターを、企業実務に関係する「圧力レバー（lever）」で整理すると以下の通りである。[9]

| 区分 | アクター | 企業にとっての示唆（圧力レバー） |
|---|---|---|
| 行政トップ | ドナルド・トランプ[10] | 行政命令・調達方針で“許容されるAI”の定義を動かし得る（政治要件の調達組込み）。[11] |
| 国防当局 | 米国防総省[12] | 契約条項の標準化（any lawful use）と調達要件（客観性等）を通じ、産業側の設計・運用を規定。[13] |
| 調達当局 | 米国一般調達局[14] | 政府横断の調達枠・評価基盤（サンドボックス）からの除外が市場アクセスに直結。[15] |
| 予算・ガバナンス | 米国行政管理予算局[16] | 政府全体のAI利用・調達ガイダンス（公的信頼、プライバシー等）を通じた統制。[17] |
| AIベンダー | Anthropic[18]／OpenAI[19] | 「拒否線（赤線）」をどう実装するか（契約条項 vs 技術統制）で、政府との合意可能性と反発リスクが変化。[20] |
| 周辺ベンダー | Palantir Technologies[21]／Google[22]／xAI[23] | 防衛プラットフォームやクラウド経由で波及（一次契約者でなくても“巻き込まれ”が起きる）。[24] |

## 情報タイプ別のリスクと対応方針

以下では、ユーザー指定の情報タイプ（規制変更、サイバーインシデント、技術革新、サプライチェーン問題、ESG/気候リスク等）ごとに、必須項目を“実務で使える粒度”に圧縮して整理する。ここでいう「関連規制・ガイドライン」は、原則として官公庁・規制当局・標準化団体等の一次情報を優先する。[25]

| 情報タイプ | 主要ポイントと潜在リスク | 関連規制・ガイドライン（国内／国際） | 業界別影響と優先度（高→低） | 類似事例とベストプラクティス | 対応オプション（短期／中期／長期）と実行可能性 |
|---|---|---|---|---|---|
| 規制・政策変更（AI・調達・国防・輸出管理） | 「調達要件が政治・安全保障要因で急変」し、契約条項（any lawful use等）・評価基準（客観性等）がベンダー設計を規定。違反・不一致は調達排除・指定等の“非連続ショック”になり得る。 26 | 日本：AI事業者ガイドライン（リスクベース、アジャイル更新）。 27 日本：経済安全保障推進法（重要物資、基幹インフラ、重要技術等）。 28 日本：防衛分野の責任あるAI適用（法的・政策的要件、完全自律型致死兵器を否定）。 29 米国：供給網リスク調達措置（10 U.S.C. §3252）、調達排除枠（FAR 9.4 等）、大統領令・AI政策。 30 EU：AI法（AI Act）。 31 | 防衛・航空宇宙／重要インフラ／クラウド・ソフトウェア／半導体・電子部品／金融（規制対応が重い）／一般サービス。 32 | 「政策変化をリスクシナリオに組み込み、契約・技術・運用の3層で耐性を作る」が基本。NIST AI RMFやISO/IEC 42001を“説明可能な管理体系”として採用。 33 | 短期：契約条項レビュー、政府・大口顧客要請の対応プロトコル整備（低〜中コスト、即効性）。 34 中期：調達・輸出管理・人権DDを統合したAIガバナンス委員会、審査ワークフロー実装（中コスト）。 35 長期：重要領域の内製・自立化／多元化（高コスト、競争力も強化）。 36 |
| サイバーインシデント（AI/クラウド/委託先起点） | 生成AI・エージェント導入で「権限過多」「機密漏えい」「プロンプト注入」「サプライチェーン脆弱性」が拡大。政府・重要インフラ向けでは監査・証跡の欠如が致命傷になり得る。 37 | 日本：サイバーセキュリティ経営ガイドライン（重要10項目等）。 38 金融：金融分野サイバーガイドライン。 39 国際：NIST SSDF（SP 800-218）、NIST C-SCRM（SP 800-161r1）、SBOM（NTIA/CISA）。 40 | 金融／重要インフラ／SaaS・IT運用／製造（OT含む）／サプライチェーン（物流）／一般サービス。 41 | SSDF・SBOMを調達条件とし、委託先・OSS依存を可視化。経営ガイドラインの成熟度可視化で投資とKPIを連動。 42 | 短期：AI利用のデータ分類／ログ・監査／権限制御、緊急停止スイッチ（中コスト）。 43 中期：SBOM/SSDFの契約実装、委託先監査、レッドチーム（中〜高）。 44 長期：ゼロトラスト＋AIガードレールの標準アーキテクチャ化（高）。 45 |

| 情報タイプ | 主要ポイントと潜在リスク | 関連規制・ガイドライン（国内／国際） | 業界別影響と優先度（高→低） | 類似事例とベストプラクティス | 対応オプション（短期／中期／長期）と実行可能性 |
|---|---|---|---|---|---|
| 技術革新（モデル更新・自律化・エージェント化） | 能力向上は生産性を上げる一方、「説明不能性」「幻覚」「自動化バイアス」「責任分界の曖昧化」を増幅。高リスク用途では人間関与と検証可能性が必須になる。 46 | 日本：AI事業者ガイドライン（リスクに応じた取組・継続的改善）。 47 国際：NIST AI RMF、ISO/IEC 42001、OECD AI Principles。 48 | 製造（品質・保安）／金融（モデルリスク）／医療・ヘルスケア（規制）／IT（プロダクト責任）／サービス（顧客対応）。 49 | モデルリスク管理（金融庁の原則等）や、NIST AI RMFのマップ（Govern-Map-Measure-Manage）で“運用の仕組み化”を優先。 50 | 短期：重要ユースケースの棚卸し・禁止領域定義（低〜中）。 51 中期：MLOps/LLMOpsの変更管理（モデル更新審査、評価、ロールバック）整備（中）。 52 長期：標準化（ISO/IEC 42001準拠）と第三者保証（高）。 53 |
| サプライチェーン問題（地政学・ブラックリスト・依存） | “供給網リスク指定”“政府調達枠からの除外”が実質的に市場アクセス遮断となり、関連企業へ波及。単一ベンダー依存は事業継続リスクに直結。 54 | 日本：経済安全保障推進法（重要物資・基幹インフラ等）、経済安全保障経営ガイドライン。 55 日本：外為法に基づく安全保障貿易管理（技術移転含む）。 56 米国：10 U.S.C. §3252、DPA（優先履行）。 57 | 防衛・航空宇宙／半導体・電子部品／クラウド・ソフトウェア／製造（重要物資）／物流（重要物資）／その他。 58 | C-SCRM（NIST SP 800-161r1）の多層管理と、契約での可搬性（代替調達、データ移行、エスカレーション）確保。 59 | 短期：ベンダー依存度の見える化、代替候補の評価・PoC（中）。 60 中期：マルチモデル運用、データ・プロンプト・評価資産の移植可能化（中〜高）。 52 長期：重要領域の内製・共同調達・国内外分散（高）。 61 |

| 情報タイプ | 主要ポイントと潜在リスク | 関連規制・ガイドライン（国内／国際） | 業界別影響と優先度（高→低） | 類似事例とベストプラクティス | 対応オプション（短期／中期／長期）と実行可能性 |
|---|---|---|---|---|---|
| ESG・人権・気候リスク（監視・武力行使・開示） | 大量監視や自律兵器への関与は、法令違反だけでなく、レピュテーション・投資家評価・採用に直結。気候・サステナ開示の高度化で、ガバナンス不備は開示リスクにもなる。[62] | 人権：UNGP、OECDデューデリジェンス。[63] 武力行使：自律型兵器の国際議論（UNODA、ICRC）と日本政府方針（LAWS）。[64] 気候・開示：ISSB IFRS S2、SSBJ基準（日本）。[65] | 金融（開示・投資家圧力）／グローバル製造（サプライチェーン人権）／IT（監視用途）／サービス（顧客信頼）。[66] | 人権影響評価（HRIA）と、用途審査（ユースケース・レビュー）を“形式”でなく意思決定権限・KPIで根付かせる。[67] | 短期：禁止ユースケースとエスカレーション設計（低）。[68] 中期：持続的DD（取引先含む）と開示統制（中）。[69] 長期：第三者保証・監査の組込み（中〜高）。[70] |

上表のうち、今回の米国事例から直接引き出せるのは「規制・政策変更」「サプライチェーン問題」「ESG・人権」の結節である。具体的には、調達当局がサンドボックス（評価基盤）と包括調達枠を用いて政府全体への波及を起こし得ること、国防当局が契約条項を標準化することで“個別交渉”を“制度”に変えること、そして指定・排除が民間市場まで波及し得ることが、企業の事業継続設計に直結する。[71]

日本側では、経済安全保障推進法が（重要物資・基幹インフラ・重要技術・特許非公開）を柱に制度化され、官民の経営ガイドラインも整備されているため、AI・クラウド・半導体・重要物資が絡む企業は「規制順守」ではなく「供給網の継続性と技術流出対策」を経営課題として扱うことが求められる。[72]

## 業界別影響評価と優先度

業界別の影響は、①米国政府・防衛産業基盤との接点、②重要データ（個人情報・機密・重要インフラ）取扱い、③AI/クラウド依存度、④越境取引・輸出管理の該当性、で概ね決まる。米国の調達方針変更や供給網指定のようなイベントは、①と③が高いほど短期に顕在化し、②が高いほど復旧コストが増える。[73]

下表は、ユーザー企業の詳細が未提示である前提での“標準的な優先度”である（ユーザー情報が判明次第、再採点する）。[4]

| 業界 | 想定ユースケース例 | 主なリスクドライバー | 優先度ランク |
|---|---|---|---|
| 防衛・航空宇宙・安全保障関連サプライヤー | 解析、設計支援、保全、訓練、情報分析 | 国防調達条項（any lawful use等）、供給網指定・排除、輸出管理、責任あるAI（完全自律兵器否定） | 最優先 |

| 業界 | 想定ユースケース例 | 主なリスクドライバー | 優先度ランク |
|---|---|---|---|
| クラウド・ソフトウェア・AI提供（B2B） | 生成AI API、SaaS、MLOps/LLMOps基盤 | 顧客の規制要件が製品設計に直結、サイバー供給網（SBOM/SSDF）、ガバナンス監査 | 最優先 |
| 金融（銀行・証券・保険・決済） | 審査、AML、マーケ、顧客対応、自動化 | サイバー・オペレーショナルレジリエンス、モデルリスク、個人情報・説明責任、外部委託管理 | 高 |
| 製造（重要物資・半導体・電子部品を含む） | 需給計画、品質、設計、工場DX | 経済安全保障（重要物資）、OT/ITサイバーリスク、海外依存（クラウド・部材） | 高 |
| 重要インフラ・公共性の高いサービス | 運用最適化、保守、客服、監視 | 基幹インフラの安定提供、データ保護、供給網の継続性 | 高 |
| 一般サービス（小売、広告、一般事務） | 問い合わせ対応、文書作成、分析補助 | 個人情報・機密の入力、ベンダーロックイン、レピュテーション | 中 |

金融分野では、サイバーセキュリティに関するガイドライン整備に加え、モデル・リスク管理の高度化も監督上の焦点となっており、AI導入を“モデル管理”として統制する設計が有効である。 74

防衛領域では、日本の方針として「人間の関与が及ばない完全自律型致死兵器の開発を意図しない」旨が示され、責任あるAI適用の枠組みも整備されているため、関連企業は最初から“用途の線引き”を契約・設計・運用に織り込むことが不可欠である。 75

## 対応オプションと実施ロードマップ

本章では、（A）取り得る対応オプションを比較し、（B）推奨アクションとロードマップ（責任部署・マイルストーン・KPI）を提示する。設計思想は「AIガバナンス」単体ではなく、「経済安全保障・サイバー供給網・人権DD・調達可搬性」の統合である。 76

### 対応オプション比較

| オプション | 狙い | メリット | コスト・時間・組織影響 | 適用が向く企業 |
|---|---|---|---|---|
| オプション1：現状維持＋最低限統制 | 短期で火消し | 導入が速い | コスト低いが、単一ベンダー依存・政策ショックに脆弱。監査対応で後から高くつく | AI利用が軽微、規制曝露が低い |
| オプション2：レジリエンス型（推奨） | “止まらないAI”を作る | ベンダー乗換え・監査・説明責任に耐性 | 中コスト。調達・法務・CISO・事業部の連携が必要（権限設計が鍵） | グローバル企業、重要データ取り扱い、B2B基盤 |
| オプション3：主権型（部分適用推奨） | 最重要領域の自立化 | 地政学・指定・輸出管理の影響を最小化 | 高コスト・人材投資が必要。判断を誤ると過剰投資 | 防衛・重要インフラ・戦略技術、長期競争力を狙う |

オプション2〜3へ進むほど、NIST AI RMFやISO/IEC 42001のような体系で「設計・運用・監査」を一体運用すると、社内外に説明しやすい。 77

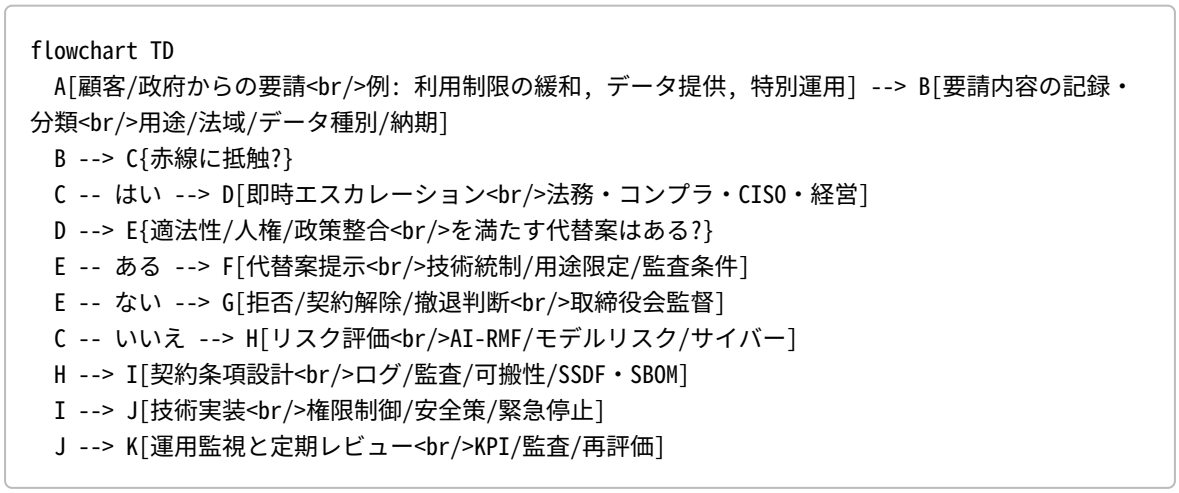
## 推奨アクション

推奨は「オプション2を全社標準にし、最重要領域のみオプション3を部分適用」である。政策ショック（調達排除・指定）とサイバー供給網リスクは、どちらも“依存関係”を突くため、平時に可搬性を作らない限り、発生時の選択肢が消える。 78

以下のロードマップは、全社導入の最短線を示す（ユーザー企業の規模・業界で調整）。 4

| 期間 | 主要マイルストーン | 責任部署（主／協） | KPI例 |
|---|---|---|---|
| 0〜60日 | AI利用の棚卸し（ユースケース・データ分類・ベンダー依存度）、禁止領域（赤線）案の策定、米国向け契約条項の緊急点検 | 経営企画／リスク（主）、法務、CISO、調達、事業部 | 棚卸しカバレッジ（%）、赤線合意（取締役会or経営会議承認） |
| 60〜120日 | ベンダー切替設計（マルチモデル、データ移行、評価資産の共通化）、ログ・監査・緊急停止の標準実装、委託先セキュア開発要求（SSDF/SBOM）を調達条件化 | IT・データ基盤（主）、CISO、調達、法務 | 切替訓練（回/四半期）、SBOM提出率（%）、特権権限制御の適用率（%） |
| 120〜240日 | 人権DD（監視・武力行使・差別等）を用途審査に組込み、内部監査・第三者評価の準備、海外規制（EU AI Act等）に合わせた文書化 | コンプライアンス（主）、法務、監査、サステナ、事業部 | 高リスク案件の審査通過率、監査指摘の是正リードタイム |
| 240日〜24か月 | 重要領域の主権型運用（内製・専用環境・共同調達）、経済安全保障の取引先審査強化、定期的なレッドチームとBCP更新 | 経営層（主）、CISO、調達、R&D、人事 | 重要領域の単一依存解消（件数）、BCP訓練結果（RTO/RPO達成率） |

AIガバナンスの核となる「用途審査→契約→技術統制→監査」の流れを、意思決定フローとして固定する。




このフローは、AI事業者ガイドラインが求めるガバナンス構築と整合し、リスクベースで継続改善する設計に一致する。 25

実施計画のタイムラインは以下のように設計すると、監査・説明責任の観点で“抜け”が生じにくい。

```
gantt
  title 実施ロードマップ（標準テンプレート）
  dateFormat  YYYY-MM-DD
  axisFormat  %Y-%m

  section 体制・方針
  AI利用棚卸しと赤線策定          :a1, 2026-03-01, 45d
  経営会議/取締役会の監督設計      :a2, after a1, 30d

  section 契約・調達
  契約条項レビュー（可搬性/監査）   :b1, 2026-03-15, 60d
  SSDF・SBOMを調達条件に組込み     :b2, after b1, 90d

  section 技術・運用
  ログ/監査/緊急停止の標準実装     :c1, 2026-04-01, 120d
  マルチモデル運用と切替訓練       :c2, after c1, 120d

  section 人権・開示
  人権DDの用途審査組込み           :d1, 2026-06-01, 120d
  第三者評価・保証（必要領域）     :d2, after d1, 180d
```

このロードマップが必要となる背景には、供給網リスク指定等の調達措置が情報非開示も含めて迅速に行われ得る点、また国防生産法のような強制的な優先履行権限が示唆され得る点がある。 2

## チェックリストとテンプレート

以下は、現場で“そのまま使える”ことを重視したチェックリストとテンプレートである。監査・規制対応を見据え、NIST AI RMF（リスク管理）、ISO/IEC 42001（マネジメントシステム）、NIST SSDF/SBOM（供給網セキュリティ）、UNGP/OECD（人権DD）に整合する形で構成した。 79

### リスク緩和チェックリスト

**AI導入・運用の最低限チェック（全社共通）**
- [ ] ユースケース（業務目的、意思決定の影響範囲、失敗時の被害）を文書化したか。 80
- [ ] 入力データを、機密・個人情報・輸出管理対象（技術）に分類し、入力禁止・マスキング・匿名化のルールを決めたか。 81
- [ ] モデル更新（バージョン変更）時の評価手順（精度・安全・バイアス・回帰）とロールバック手順があるか。 33
- [ ] ログ（入出力、権限、重要操作）と監査証跡が取得でき、保全期間が定義されているか。 43
- [ ] 緊急停止（kill switch）と、誤作動時の業務継続手順（代替プロセス）があるか。 82

**政府・大口顧客対応の赤線チェック（特に防衛・重要インフラ）**
- [ ] 完全自律型致死兵器・人間の関与なき武力行使に当たる用途を禁止（または契約上・技術上で排除）しているか。 83
- [ ] 国内外の大量監視・個人追跡につながる設計（位置追跡・識別子連結等）の禁止／厳格審査を規定したか。 84

- [ ] 「合法なあらゆる用途」等の包括条項が入る場合、例外（red lines）をどの層で担保するか（契約条項／技術統制／運用監査）を事前に決めたか。 85

**サイバー・ソフトウェア供給網チェック（委託・購入時）**
- [ ] セキュア開発（SSDF）への適合を要求し、開発・運用プロセスの証跡（レビュー、脆弱性管理）を確認しているか。 86
- [ ] SBOMを取得し、脆弱性情報と突合できる運用（継続更新）になっているか。 87
- [ ] サプライチェーン・リスク（C-SCRM）の評価（重要委託先、再委託、国外拠点、制裁・指定リスク）を実施しているか。 88

## テンプレート

**用途審査シート（例）**
- 用途：_____／対象業務：_____／利用者：_____
- 意思決定影響：低・中・高（高の場合は人間の最終判断者：_____） 89
- 取扱データ：公開・社外秘・機密・個人情報・輸出管理対象（該当：_____） 81
- 想定誤りと影響（安全・法務・金銭・人権）：_____ 90
- 必須統制：ログ／監査／権限／人手確認／緊急停止／第三者評価（必要：_____） 91

**契約条項チェック（例：AI/クラウド）**
- データの学習利用禁止（明示）／保持期間／削除要件 92
- 監査権（ログ提示、第三者監査レポート、インシデント通知SLA） 43
- 可搬性（エクスポート形式、移行支援、終了時の移行期間、追加費用上限） 93
- 供給網要件（SBOM提出、SSDF準拠、再委託開示） 94

**経営KPIテンプレート（例）**
- AI利用棚卸し完了率（%）／高リスク案件の事前審査率（%） 95
- ベンダー切替訓練回数（回/四半期）／切替目標RTO（時間） 96
- SBOM取得率（%）／重大脆弱性の是正リードタイム（中央値） 87
- 人権DDの実施率（重要取引先、重要ユースケース） 97
- 監査指摘の是正完了率（%）／再発率（%） 98

最後に、ユーザー企業の追加アップロード（契約、顧客構成、AI利用一覧、海外拠点、データ分類表、委託先一覧等）が得られれば、本テンプレートの「業界別優先度」「ロードマップの工数・費用・体制」を、より具体的な“実行計画（Budget/Headcount含む）”に落とし込める。

---


1 7 9 11 54 Trump directs US agencies to toss Anthropic's AI as Pentagon calls startup a supply risk
https://www.reuters.com/world/us/trump-says-he-is-directing-federal-agencies-cease-use-anthropic-technology-2026-02-27/?utm_source=chatgpt.com

2 23 30 57 78 10 USC 3252: Requirements for information relating to ...
https://uscode.house.gov/view.xhtml?edition=prelim&num=0&req=granuleid%3AUSC-prelim-title10-section3252&utm_source=chatgpt.com

3 4 10 25 27 34 47 51 95 AI 事業者ガイドライン
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20250328_1.pdf?utm_source=chatgpt.com

5 62 63 67 84 90 97 GUIDING PRINCIPLES ON BUSINESS AND HUMAN ...
https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf?utm_source=chatgpt.com

6 13 26 73 85 Artificial Intelligence Strategy for the Department of War
https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF?utm_source=chatgpt.com

8 21 Anthropic CEO says it 'cannot in good conscience accede' to Pentagon's demands for AI use
https://apnews.com/article/9b28dda41bdb52b6a378fa9fc80b8fda?utm_source=chatgpt.com

12 38 41 43 82 サイバーセキュリティ経営ガイドラインと支援ツール
https://www.meti.go.jp/policy/netsecurity/mng_guide.html?utm_source=chatgpt.com

14 87 The Minimum Elements For a Software Bill of Materials ...
https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom?utm_source=chatgpt.com

15 18 71 GSA Stands with President Trump on National Security AI ...
https://www.gsa.gov/about-us/newsroom/news-releases/gsa-stands-with-president-trump-on-national-security-ai-directive-02272026?utm_source=chatgpt.com

16 35 52 53 70 91 98 ISO/IEC 42001:2023 - AI management systems
https://www.iso.org/standard/42001?utm_source=chatgpt.com

17 M-25-21 Accelerating Federal Use of AI through Innovation ...
https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf?utm_source=chatgpt.com

19 81 92 生成AIサービスの利用に関する注意喚起等について
https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert?utm_source=chatgpt.com

20 Statement on the comments from Secretary of War Pete Hegseth
https://www.anthropic.com/news/statement-comments-secretary-war?utm_source=chatgpt.com

22 40 42 44 86 94 Secure Software Development Framework (SSDF) Version 1.1
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-218.pdf?utm_source=chatgpt.com

24 The War Department to Expand AI Arsenal on GenAI.mil ...
https://www.war.gov/News/Releases/Release/Article/4366573/the-war-department-to-expand-ai-arsenal-on-genaimil-with-xai/?utm_source=chatgpt.com

28 32 55 72 経済安全保障政策
https://www.meti.go.jp/policy/economy/economic_security/index.html?utm_source=chatgpt.com

29 83 責任あるAI適用ガイドライン策定の意義
https://www.mod.go.jp/atla/soubiseisaku/ai_guideline/ai_guideline_ver.01_ov.pdf?utm_source=chatgpt.com

31 Regulation - EU - 2024/1689 - EN - EUR-Lex - European Union
https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng?utm_source=chatgpt.com

33 46 48 77 79 80 89 Artificial Intelligence Risk Management Framework (AI ...
https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf?utm_source=chatgpt.com

36 61 76 96 経済安全保障経営ガイドライン （第 1 版）
https://www.meti.go.jp/press/2025/01/20260123004/20260123004-1r.pdf?utm_source=chatgpt.com

37 45 59 88 Cybersecurity Supply Chain Risk Management Practices for ...
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf?utm_source=chatgpt.com

39 74 金融分野におけるサイバーセキュリティに関する ガイドライン 令 ...
https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf?utm_source=chatgpt.com

49 50 モデル・リスク管理に関する原則 令和3年 11 月 12 日
https://www.fsa.go.jp/common/law/ginkou/pdf_02.pdf?utm_source=chatgpt.com

56 安全保障貿易管理について
https://www.meti.go.jp/policy/anpo/seminer/shiryo/setsumei_anpokanri.pdf?utm_source=chatgpt.com

58 サプライチェーン強靱化の取組（重要物資の安定的な供給 ...
https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/supply_chain/supply_chain.html?utm_source=chatgpt.com

60 93 Buy AI
https://www.gsa.gov/technology/government-it-initiatives/artificial-intelligence/buy-ai?utm_source=chatgpt.com

64 Lethal Autonomous Weapon Systems
https://disarmament.unoda.org/en/our-work/emerging-challenges/lethal-autonomous-weapon-systems?utm_source=chatgpt.com

65 issb-2023-a-ifrs-s2-climate-related-disclosures. ...
https://www.ifrs.org/content/dam/ifrs/publications/pdf-standards-issb/english/2023/issued/part-a/issb-2023-a-ifrs-s2-climate-related-disclosures.pdf?bypass=on&utm_source=chatgpt.com

66 サステナビリティ開示基準
https://www.ssb-j.jp/jp/ssbj_standards.html?utm_source=chatgpt.com

68 75 自律型致死兵器システム（LAWS）について｜外務省
https://www.mofa.go.jp/mofaj/dns/ca/page24_001191.html?utm_source=chatgpt.com

69 OECD Due Diligence Guidance for Responsible Business ...
https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/02/oecd-due-diligence-guidance-for-responsible-business-conduct_c669bd57/15f5f4b3-en.pdf?utm_source=chatgpt.com