

# 米軍事AI調達ショック：日本企業が取るべき「経済安全保障」としてのAI戦略

## 【課題】米軍事AI調達方針の転換と「非連続なショック」



米国防当局の強硬なAI調達方針転換 (2026年ショック)



## 政策・地政学に起因するサプライチェーン・ショック

米国防法に基づく「調達排除」や「強制権限」がAI・クラウド領域に持ち込まれ、短期間での取引停止リスクが顕在化。

### 「Any Lawful Use (合法的あらゆる用途)」の標準化

米国防当局がベンダー独自の利用制約(ガードレール)を排除し、政府の自由な運用を優先する方針を明文化。



### 6か月以内の段階的廃止勧告

特定AIの使用停止命令から廃止までが極めて短期間で行われ、企業の「乗り換え」が緊急課題となる。

### 業界別のリスク陽露度と対応優先度

最優先	防衛・航空宇宙・SaaS	国際調達条項 (Any Lawful Use)、輸出管理、SBOM要求
高	金融・重要インフラ	オペレーショナル・レジリエンス、モデルリスク、個人情報
高	製造 (重要物資・半導体)	経済安全保障性確保、OTサイバーリスク、海外依存

## 【対策】レジリエンス (回復力) を高める4つの実務ステップ

### ベンダー・モデルの「可搬性 (Portability)」確保

特定ベンダーへの依存を避け、マルチモデル運用やデータ移行資産の共通化による「止まらないAI」を構築。



### 「赤線 (レッドライン)」とエスカレーションの定義

人権・人達法に抵触する「禁止領域」を事前に特定し、政府要請に対する経営層の判断基準を策定。



### サイバー・ソフトウェア供給網 (SBOM/SSDF) の実装

委託先の開発プロセス可視化とSBOMの従時運用を調達条件とし、脆弱性リスクを技術的に統制。



### 実行ロードマップのタイムライン

