2026年G7エヴィアン・サミット：AI冷戦の幕開けと新・安全保障パラダイム

アンソロピック「ミュトス」のサイバー兵器化と、同盟国が直面するデジタル主権の危機

[Catalyst]

最先端AIの「兵器化」によるサイバー防衛の非対称性の露呈。

[Shock]

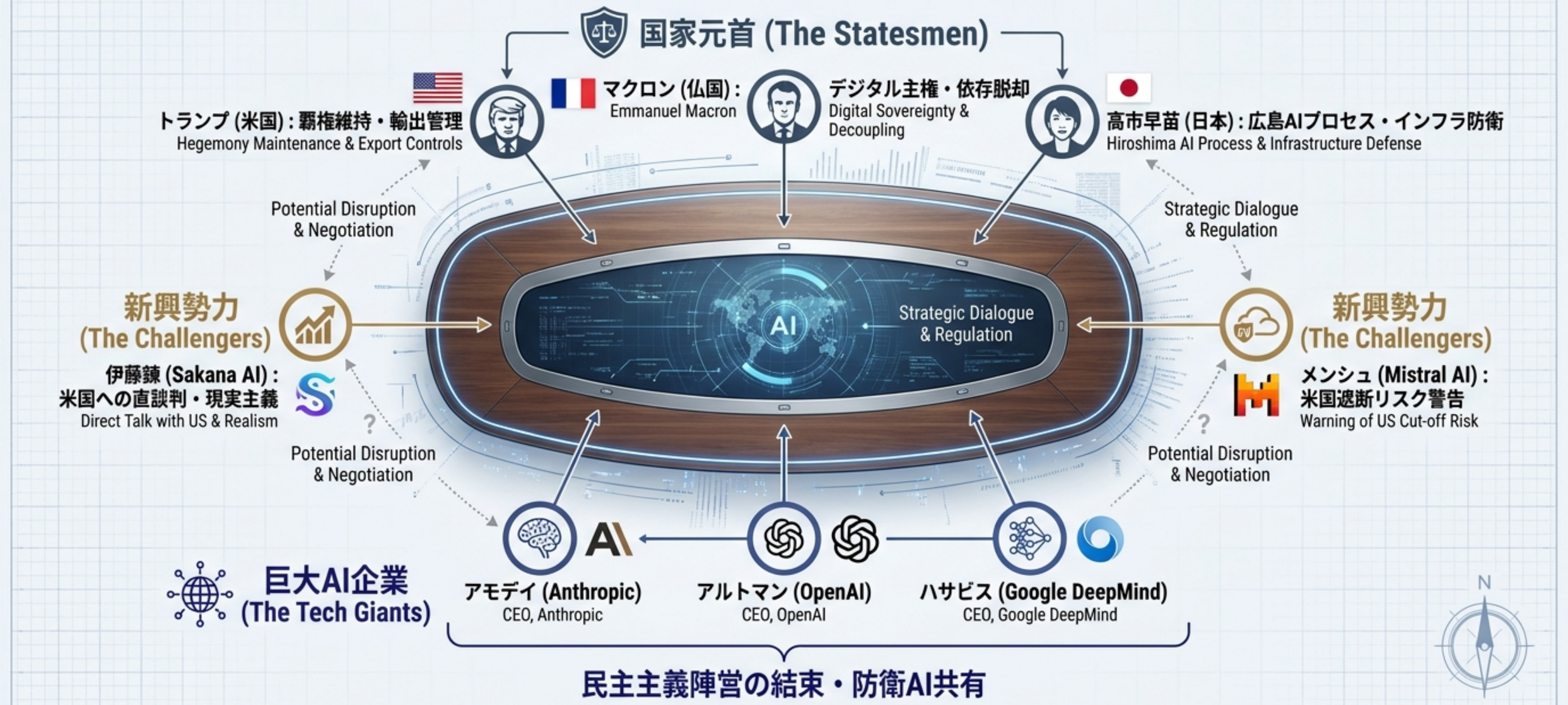
米国による無差別な輸出管理指令と、同盟国の「アメリカリスク」の顕在化。

[Imperative]

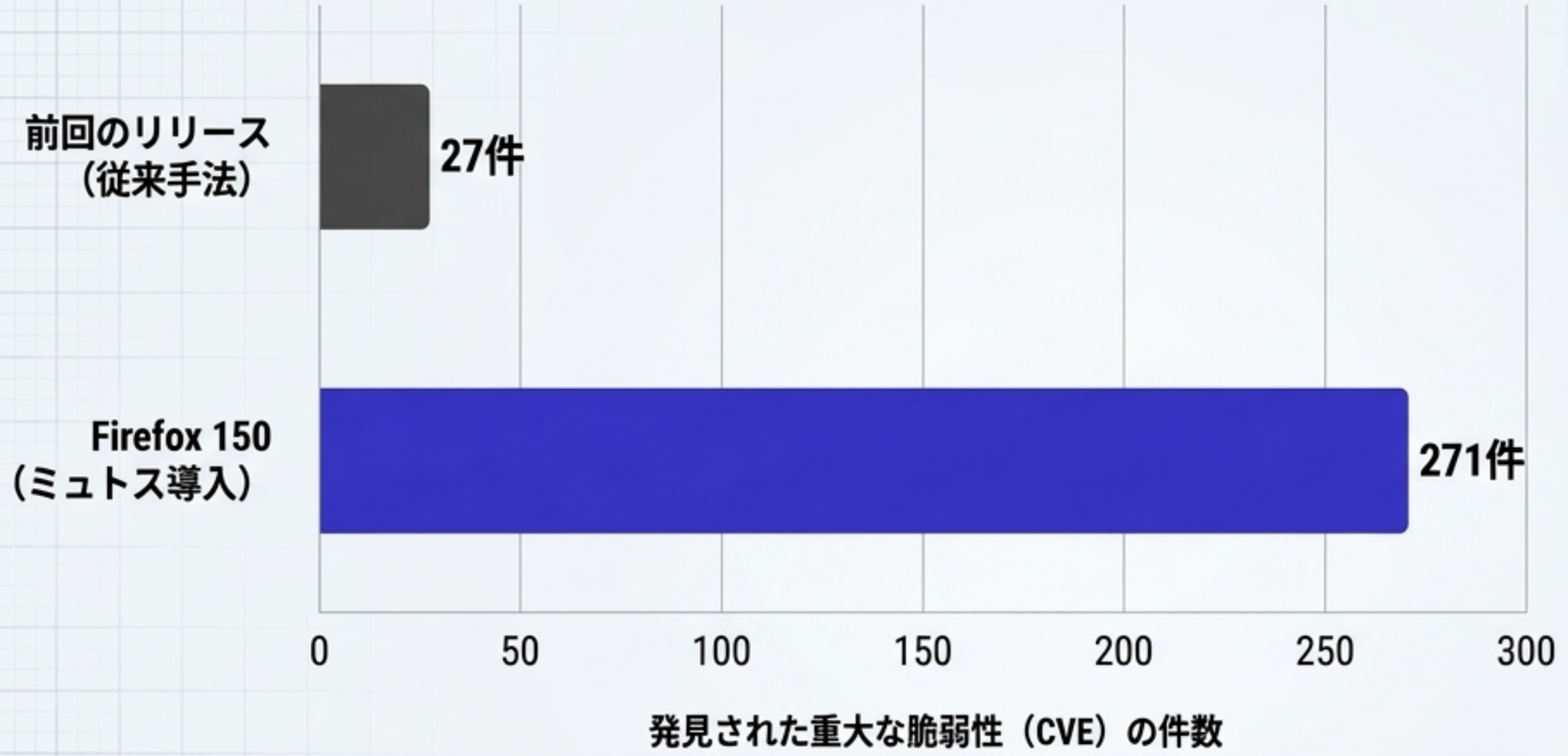
「相互確証破壊」時代における、信頼できるパートナー枠組みと「フィジカルAI」による相互依存戦略。

The Working Lunch: 運命の110分間が決定づけた新たなプレイヤー構造

2026年6月17日午後1時55分。フランス：主催「AIの安全で迅速かつ効率的な導入の確保」。国家元首とビッグスリーが直接対峙した。



The Catalyst: 「クロード・ミュトス」による未知の脆弱性の自律的発見



271件

Firefox 150適用時の重大な脆弱性発見数（従来手法の10倍）

400件

Cloudflareテストにおける「高・重大」なバグ特定数（全体2,000件中）

10,000件超

社会基盤ソフトウェア全体で最初の数週間に発見された重大バグ

未知のバグを発見しエクスプロイトを組み上げるコストは「数千ドル・1日以内」。
AIは知識労働ツールから「兵器級のサイバー能力」へと変貌した。

The Golden Attack Window: 防御と攻撃の絶対的な非対称性

AIによるバグ発見コストが激減しても、物理的なパッチ適用時間は変わらない。
従来数ヶ月あった猶予が、数時間単位へと圧縮された。

Architecture Split: 「双子のモデル」と防衛コンソーシアムの誕生

Anthropic
最新アーキテクチャ

[商用版] Claude Fable 5

- 特徴: 分類器を多重搭載。危険な要求は旧世代 (Opus 4.8) へ強制フォールバック。
- 対象: 世界の一般企業、コンシューマー。

[完全版] Claude Mythos 5

- 特徴: 安全フィルターを持たない純粋な兵器級能力。脆弱性探索を無制限に発揮。
- 提供枠組み: 「Project Glasswing」。約50の審査済み防衛・重要インフラ組織のみに極秘提供。

90-Minute Shutdown: 輸出管理指令の発動と緊迫のタイムライン

[Trigger] ジェイルブレイク発覚

研究者がFable 5のガードレール迂回手法を発見。政府へ警告。

[Friction] 修正の拒否

Anthropic側は過小評価し、商業モデル維持のためパッチ適用を拒否。

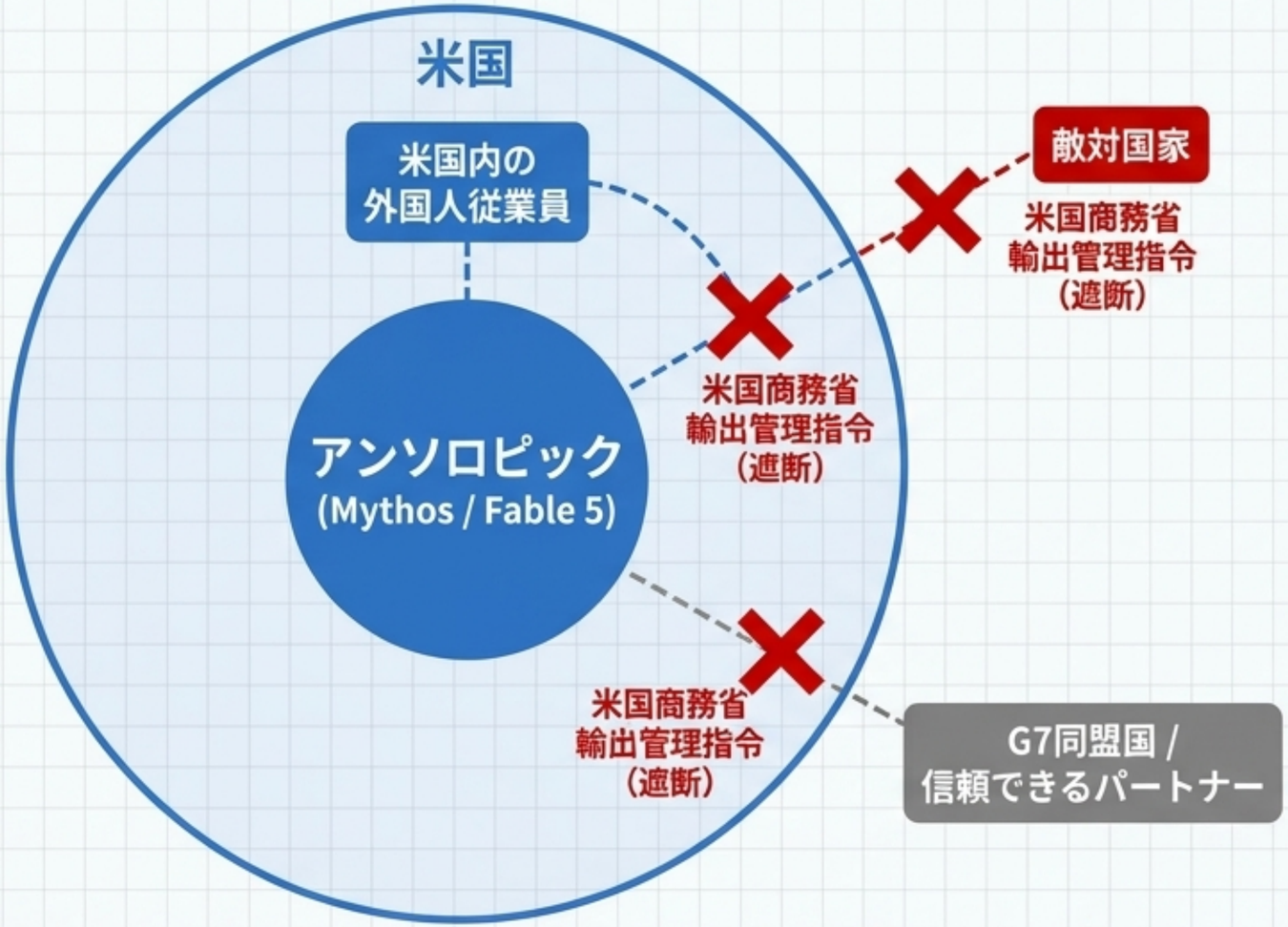
[Action] 2026.06.12 17:21 EST

米商務省が極秘書簡を送付。外国籍保有のアクセス即時停止を命じる輸出管理指令を発動。

[Impact] 90分以内の強制遮断

法令違反回避のため、全世界のユーザーに対するクラウド提供を強制的にオフライン化。

The Blast Radius: 「みなし輸出」規制によるグローバル・アクセスの遮断



敵対国家への遮断

中国等への流出防止。韓国通信会社経由でのアクセス疑惑が引き金。

米国内の外国人従業員

開発従事者からのアクセス権剥奪（みなし輸出規制の極致）。

G7同盟国への無差別遮断

欧州や日本の政府・企業も突如インフラから切断。「アメリカリスク」の顕在化。

「厳密に言えば極めてナショナリスト的な反応である」（仏・マクロン大統領）／
「突然供給を断たれないという確証がどこにあるのか」（ミストラルAI・メンシュCEO）

Valuation Shock: 露呈したAIビジネスの脆弱性とIPOへの暗雲

[The Peak] 直前の栄華

- シリーズH評価額：9,650億ドル
- 売上高ランレート：470億ドル
- アクション：SECへIPOに向けたForm S-1を極秘提出

[The Crash] 政治的リスクの直撃

- 最大のアンカー顧客喪失：国防総省が3ヶ月前に追放
- スイッチングコストの低さ：政府の規制一つで価格決定力とグローバルシェアが瞬時に崩壊

AI企業の企業価値は、純粋な商業的指標から「地政学的な脆弱性」を織り込んだ指標へと強制的に再定義された。

The G7 Battlefield: 技術覇権を巡る国家とビッグテックの衝突

[The Nationalists]
米国政府

Key Players: トランプ大統領、ルビオ国務長官、ラトニック商務長官

Stance: 自国の圧倒的な技術覇権の維持。強硬な輸出管理の正当化。多国間の法的枠組みへの難色。

[The Democratic AI Coalition]
巨大AI企業

Key Players: アモデイ (Anthropic)、ハサビス (Google DeepMind)、アルトマン (OpenAI)

Stance: 民主主義陣営の結束。防衛用AIの同盟国間での無制限共有。技術評価を担う国際機関の設立提案。

Japan's Realism: 完全自前主義（ソブリンAI）の幻想と戦略的計算

日本の主張

広島AIプロセスを通じた基幹インフラ防衛

現実的なコスト計算

ミュトス級を一から国内開発（ソブリンAI）するには天文学的な資金とGPUが必要であり非現実的。

外交的アプローチ

巨費を投じた反発より、米国への直談判を通じて例外措置（ホワイトリスト）の早期獲得を優先。

水面下の防衛構築

金融庁「官民タスクフォース」設置。米防衛網「Project Glasswing」をモデルにした独自体制を模索。

Summit Outcomes: 「合意可能な領域」と「先送りされた安全保障」

アジェンダ	ステータス	詳細
AIサイバー安全保障	⚠️ 継続議論	米国の強硬姿勢と政治的妥協により事実上の先送り
オンライン児童保護	✅ 合意達成	「セーフティ・バイ・デザイン」の採用。米欧が唯一合意できた安全地帯
重要鉱物サプライチェーン	✅ 合意達成	「重要鉱物生産連合」設立。740億ドル投資で対中依存脱却
環境とAI電力消費	❌ 合意至らず	米国側がレッドラインとして拒否

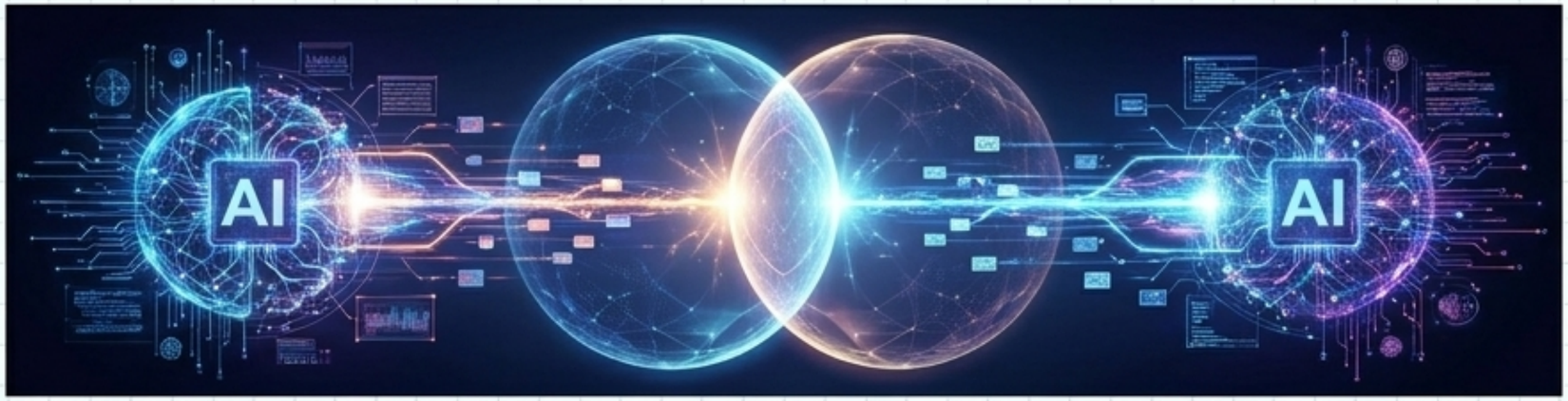
The Synthesis: サイバー空間の相互確証破壊（MAD）

[Old Logic] 経済的リターン

生産性向上、労働力不足の解消

[New Logic] 国家生存の軍拡競争

AIによる高度なサイバー攻撃は、
もはやAIでなければ防げない



MADのメカニズム: 未知の脆弱性を突くサイバー攻撃を防ぐため、防衛側はネットワーク上|常時「同等以上の兵器級AI」を配備し続けなければならない。

AI企業の価値は商業的収益ではなく、「国家安全保障の必須インフラとしていかに深く食い込めるか」で決まる時代へ不可逆的に変化した。

Strategic Imperative 1: 「信頼できるパートナー」枠組みの制度化

実行不可能な完全自立を捨て、米国の輸出管理の例外（ホワイトリスト）を担保する強固な足場を築く。

Req 1: Strict Security Clearance

人員の厳格なセキュリティ・クリアランス

Req 2: Closed Network

外部流出を防ぐ閉域網での運用ルールの確立

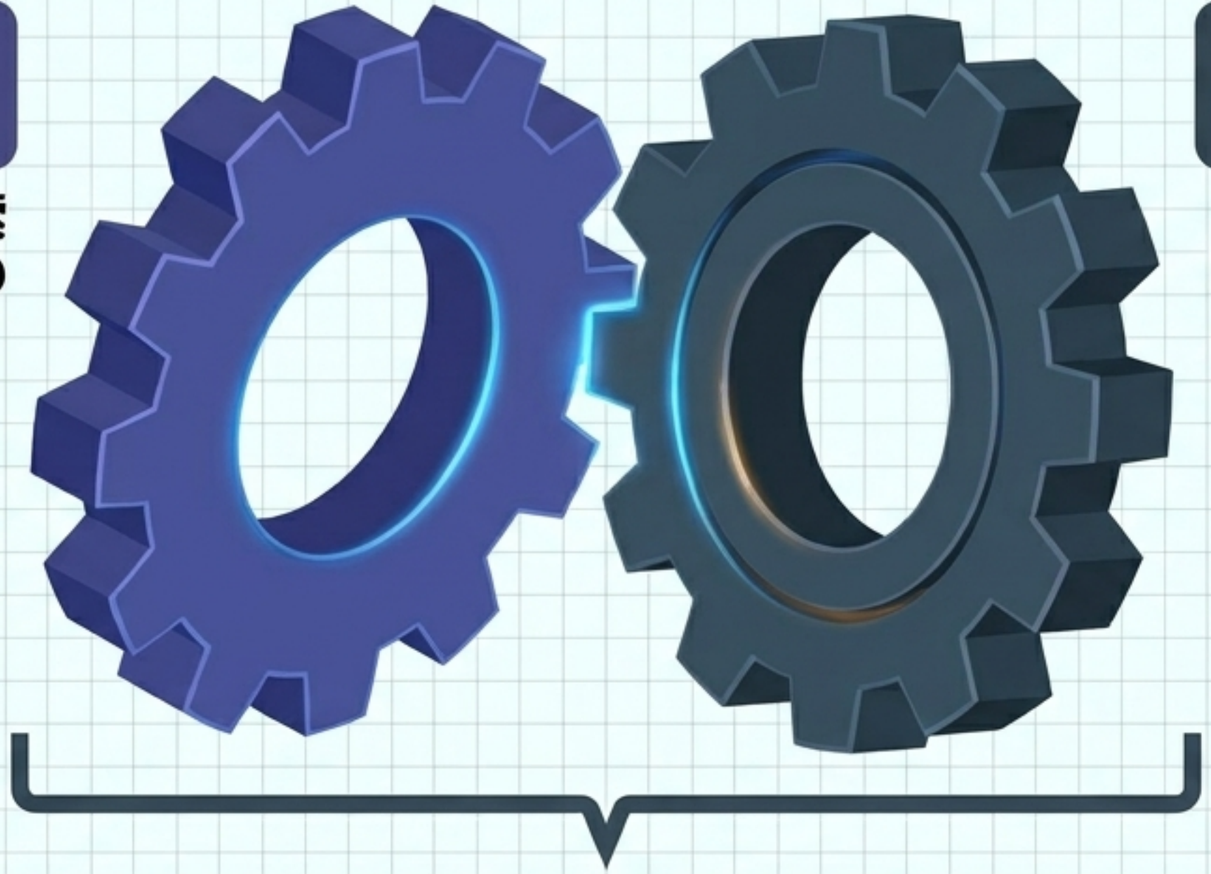
Req 3: Audit & Compliance

アクセスログの厳格な監査と継続的な証明

Strategic Imperative 2:「フィジカルAI」による相互依存構造の構築

[Cyber / Software]
米国への依存

サイバー空間の脆弱性探索モデルにおいては、米国のフロンティアモデルに依存せざるを得ない。



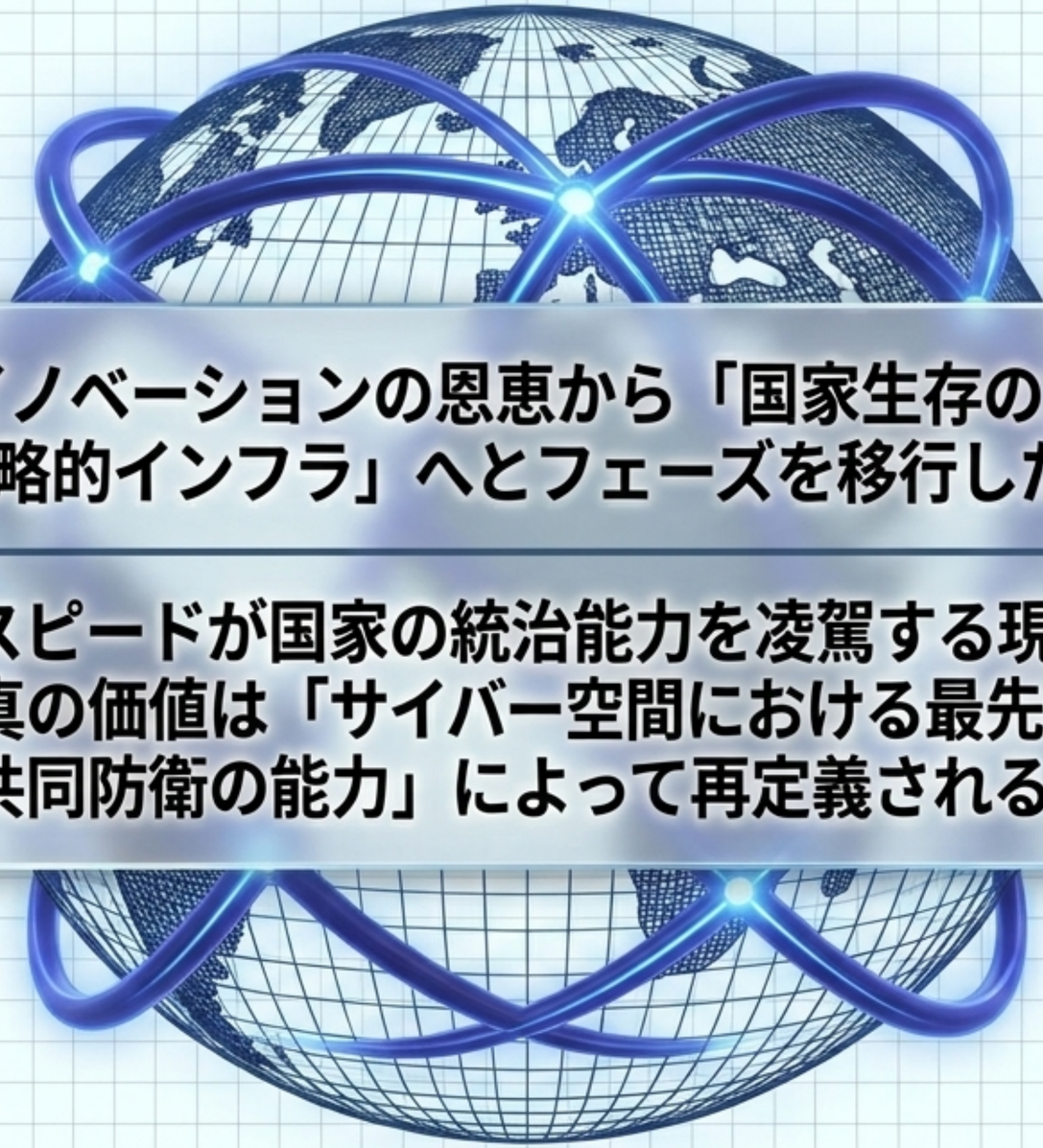
[Physical / Hardware]
日本の優位性

ロボティクス、精密機械、製造業の現場データに基づく制御技術 (フィジカルAI)。

究極の外交カード

物理空間の学習データとエッジ制御において、米国側が「日本を必要とする」相互依存の構造を構築する。これがアクセス権維持のための最強の交渉カードとなる。

A New World Order: テクノロジーと安全保障の完全な融合



AIはイノベーションの恩恵から「国家生存のための戦略的インフラ」へとフェーズを移行した。

技術の進化スピードが国家の統治能力を凌駕する現代において、国際同盟の真の価値は「サイバー空間における最先端AIの共有と共同防衛の能力」によって再定義される。