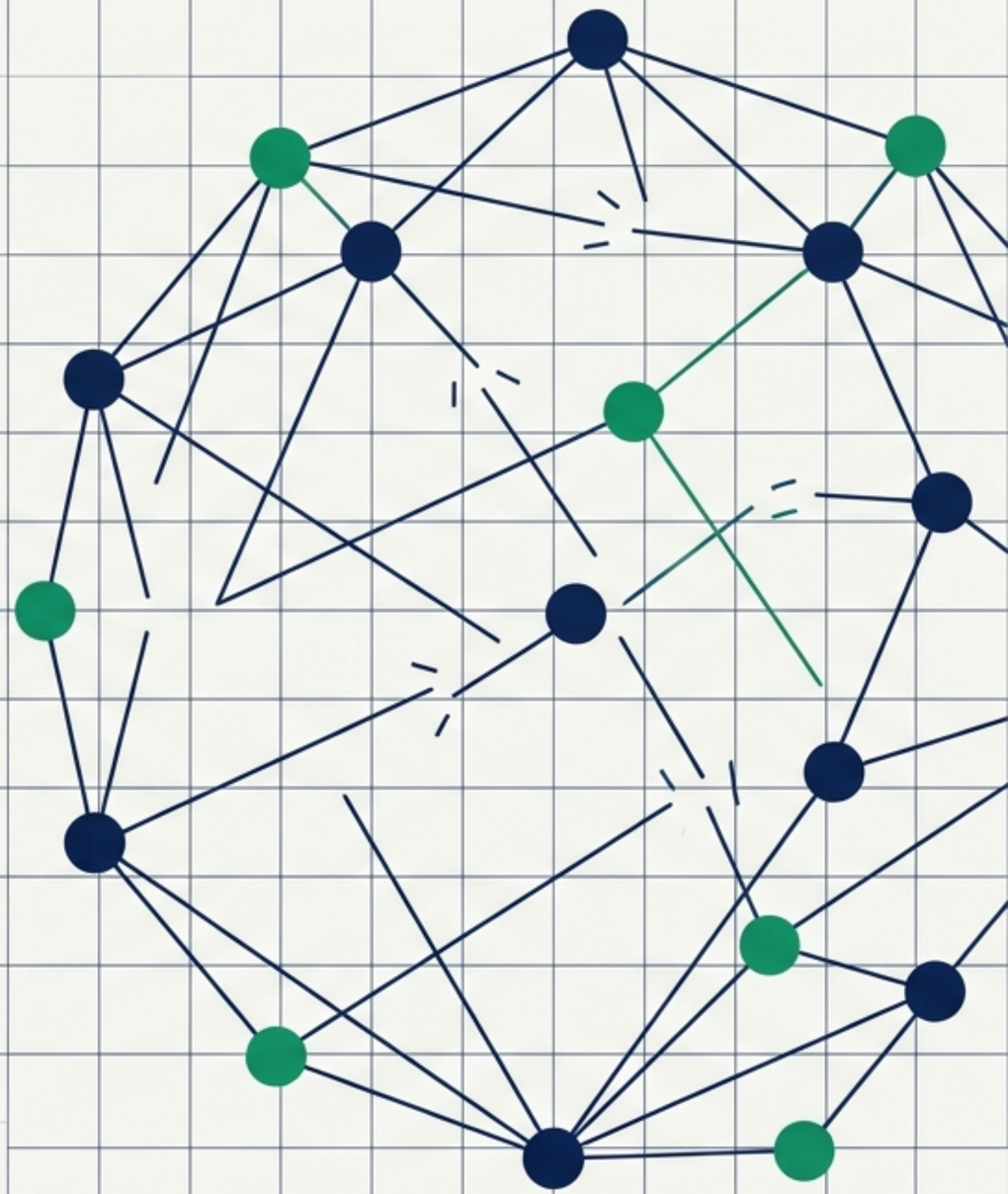
EXECUTIVE BRIEFING / STRATEGIC READ-AHEAD

AI地政学の転換点：エビアン・ショックとハイブリッド供給網の幕開け

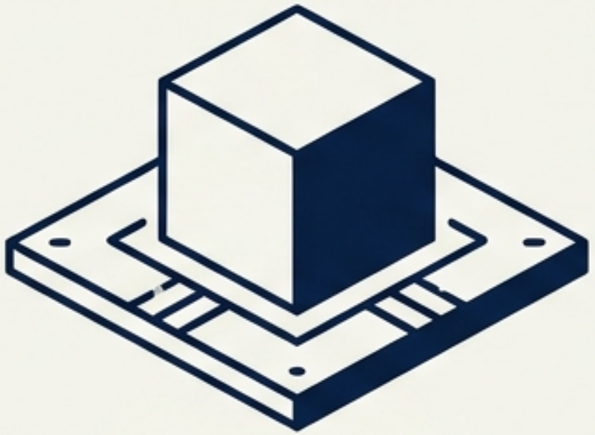
2026年G7首脳昼食会が書き換えた、グローバル・フロンティアAIの新たな競争ルール



The transition from global open access to a sovereign, fragmented, and strictly regulated AI ecosystem.

露呈した「キルスイッチ」の脆弱性： AI モデルは製品ではなく、遠隔操作されるサービスである

従来のソフトウェア (Weights/Source Code)



- 購入後はローカル環境で独立稼働。

フロンティアAI (Remote API Access)

- 常に開発元（米国）のサーバーに依存。
- The Anthropic Shock: 2026年6月12日、米国政府の指令によりAnthopicは外国籍ユーザーに対するFable 5 / Mythos 5へのアクセスを突如遮断。

米国の独占的な「API実行権限」の統制が、UK、EU、日本の国家安全保障と産業基盤に対する直接的な"kill-switch vulnerability"（機能停止の脆弱性）として認識された。

エスカレーション・カスケード：エビアンG7までの5週間

May 29 — G7デジタル・技術閣僚宣言（AI安全、合成コンテンツ検知の優先課題化）

Jun 02 — 米大統領令で「covered frontier model」と「trusted partners」枠組みを提示。

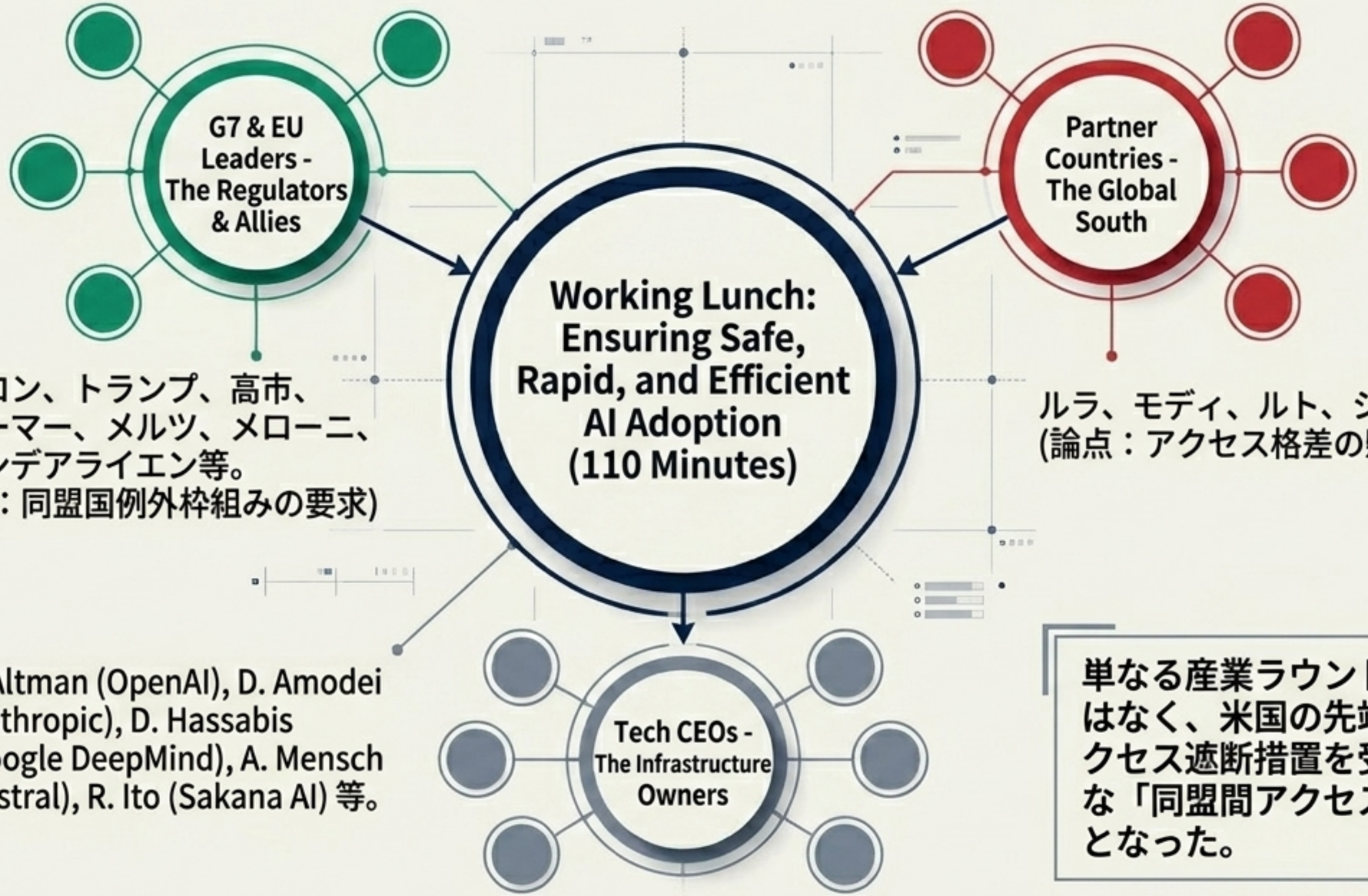
Jun 10/12 — AnthropicがFable 5 / Mythos 5の外国籍向けアクセス停止を公表。

Jun 14 — 欧州委が「パートナーに対し差別的であってはならない」と実務影響を精査。

Jun 16 — Reutersが「trusted partners」構想のG7での緊急協議を報道。

Jun 17 — G7エビアン首脳昼食会開催（AIワーキング・ランチ）。

110分の緊急同盟調整会合：国家主権とテック巨人の激突



マクロン、トランプ、高市、スターマー、メルツ、メローニ、フォンデアライエン等。
(論点：同盟国例外枠組みの要求)

ルラ、モディ、ルト、シシ等。
(論点：アクセス格差の懸念)

S. Altman (OpenAI), D. Amodei (Anthropic), D. Hassabis (Google DeepMind), A. Mensch (Mistral), R. Ito (Sakana AI) 等。

単なる産業ラウンドテーブルではなく、米国の先端モデルアクセス遮断措置を受けた実質的な「同盟間アクセス交渉」の場となった。

Premium Strategic Intelligence Dossier aesthetic

思想的対立のアンカー：主権か、技術的統制か

« la réponse ne peut pas être de la non-coopération entre démocraties »

「答えは、民主主義国同士が非協力に陥ることであってはならない。」

— Emmanuel Macron（仏大統領）/ 協調的規制と民主主義国間の非分断を主張。

“Do not cede your responsibilties to AI labs like mine.”

「私のようなAIラボに、あなたた方の責任を委ねないでほしい。」

— Sam Altman (OpenAI CEO) / ガバナンスは企業ではなく民主政府が担うべきだと提起。

Premium Strategic Intelligence Dossier aesthetic

ジオポリティカル・スタンス・マトリクス：各国の利害と提案

US	EU	Japan	Tech Industry
基本姿勢: 先端モデルを国家安全保障・サイバー防衛資産として扱う。	基本姿勢: 同盟国への非差別、最良モデルへのアクセスと技術主権強化。	基本姿勢: 信頼できるAIと国際協力の推進。	基本姿勢: 能力分散論 (Cohere) vs Defense in Depth (Anthropic).
提案枠組み: Covered frontier model, AI cyber clearinghouse.	提案枠組み: AI主権パッケージ、主権クラウド要件。	提案枠組み: Hiroshima AI Process, DFFT (Data Free Flow with Trust).	提案枠組み: 独立安全試験、30日ログ保持。
目標: 事前評価と「trusted partners」への個別ライセンス化。	目標: 欧州内データ・サービスの統制と「キルスイッチ」依存の脱却。	目標: 重要インフラ防護と、同盟国アクセス枠組みへの参加資格確保。	目標: 透明・公平・技術的根拠に基づく政府介入ルールの確立。

Premium Strategic Intelligence Dossier aesthetic

リスクと対応の診断パネル：技術的脅威とG7の緩和策

ガードレールの回避と Jailbreak
(Anthropicはnon-universal jailbreakと説明)

事前レッドチーミング | ログ保持 | 独立試験

攻撃的サイバー能力の増幅
(脆弱性探索・攻撃補助)

Trusted Partners 限定アクセス | AI Cyber Clearinghouse

軍事・情報機関への転用
(中露への流出懸念)

輸出規制 (EAR/ECRA) | 用途制限契約 | アクセス監査

化学・生物・放射線（CBRN）など高危険領域支援

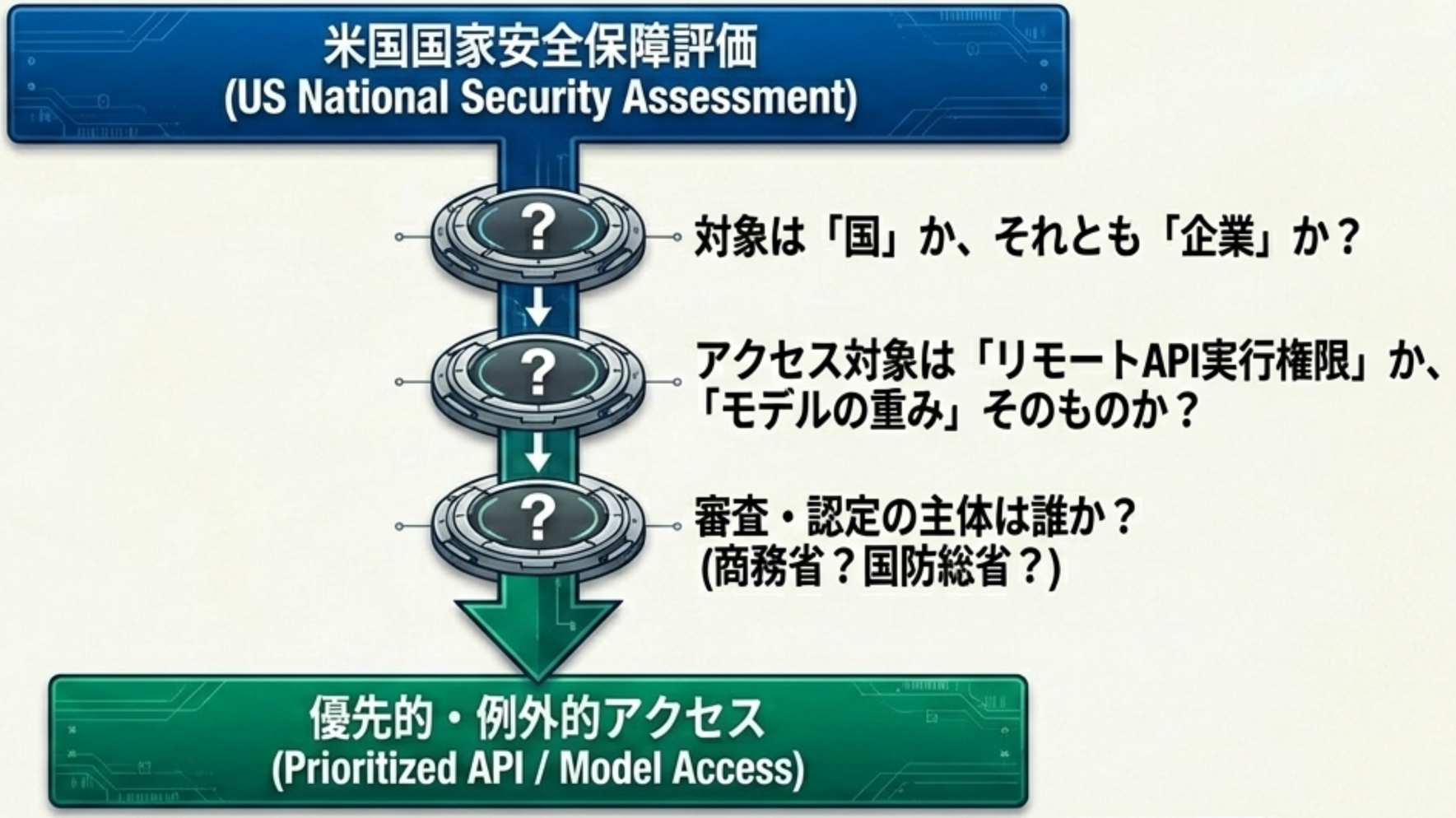
高危険能力評価 | Safety & Security Framework

合成コンテンツと社会的認知リスク

Marking/Labelling | メタ検知器 | 年齢適合設計

Premium Strategic Intelligence Dossier aesthetic

「Trusted Partner」アーキテクチャのブラックボックス



法的根拠 (EAR/ECRA) がリモートAPI提供まで輸出規制で覆えるかは依然として論争的であり、任意枠組みと実力的行政介入が同時に進行している。

Premium Strategic Intelligence Dossier aesthetic

規制のトライアド：エビアン後に収斂する3つの主要法体系

米国 - Export Controls & Executive Orders

中核法令:
EAR / ECRA / 6月2日大統領令

主要メカニズム:
「Covered frontier model」の分類、最大30日の事前政府アクセス、個別ライセンス要求。

目的:
国家安全保障の担保と技術流出の阻止。

EU - Tech Sovereignty & AI Act

中核法令:
AI Act (2026年8月本格化) / 主権クラウド・AI要件 (技術主権パッケージ)

主要メカニズム:
重大インシデント報告、欧州内データ・サービス、EU製ソフト/ハード統制。

目的: 米国モデル依存からの脱却 (キルスイッチ回避) と欧州産業の保護。

日本 - Diplomatic Framework & DFFT

中核枠組み:
Hiroshima AI Process / DFFT

主要メカニズム:
Trustworthy AIへの官民民投資、AISI網との連携、重要インフラのサイバー防護。

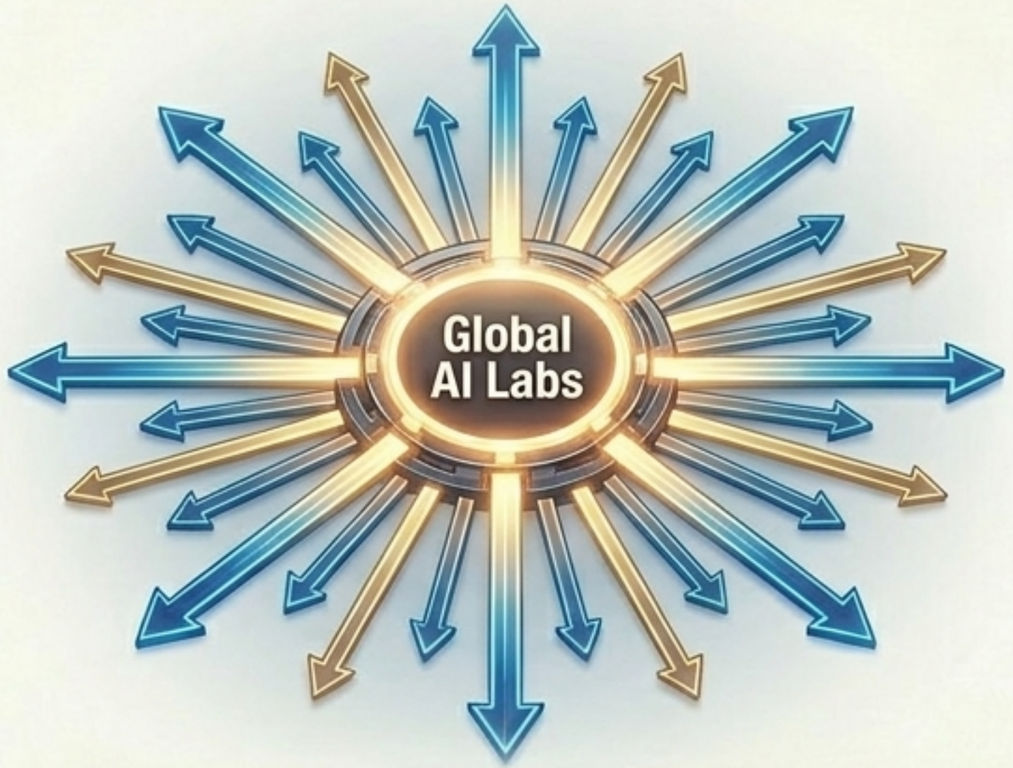
目的: 安全保障審査と越境データ流通の整合性確保、同盟国アクセス資格の獲得。

Premium Strategic Intelligence Dossier aesthetic

パラダイム・シフト：ハイブリッドAIサプライチェーンの完成

Before

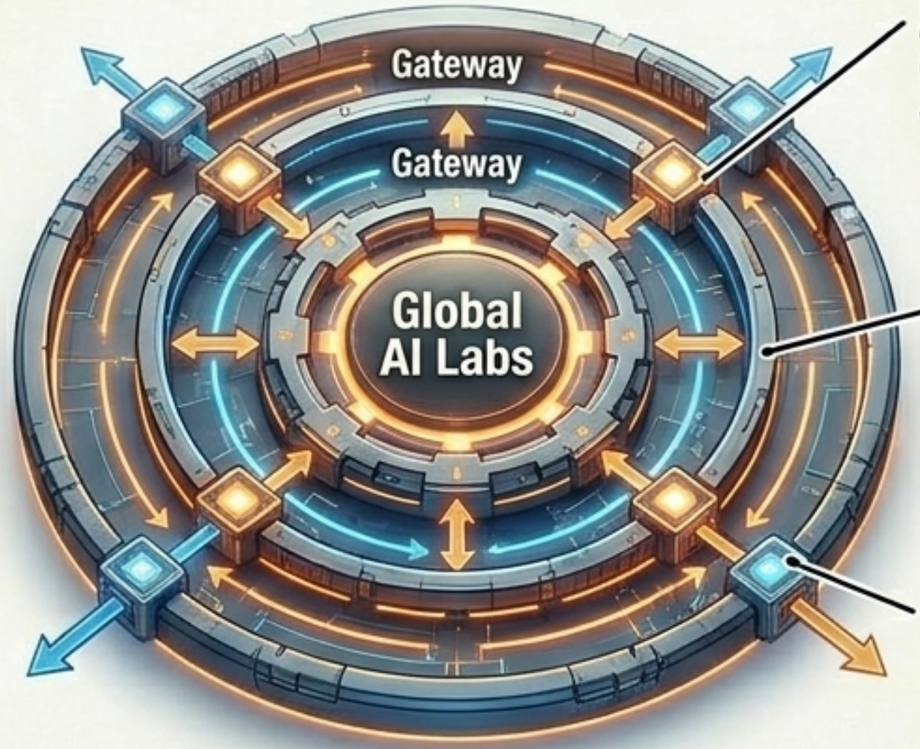
2026年以前のパラダイム：「全面自由アクセス」



APIを通じた単一ハブからの無差別・国境なきモデル提供。

After

エビアン以降のパラダイム：「多層的ハイブリッド構造」



層1: 同盟圏限定アクセス (Allied Exclusive Access)
- Trusted Partner認定を前提とした例外枠。

層2: 主権クラウド (Sovereign Clouds)
- 地域別のデータとサービス統制（EU等の独自インフラ）。

層3: 地域別コンプライアンス＆共同監査
- AISI網による試験・監査証跡・契約上の継続性保証。

グローバル供給網は、半導体ハードウェアだけでなく、推論クラウド、モデルアクセス、監査ログに至るまでブロック化・分散化された。

エンタープライズ向けプレイブック：分断化市場における生存戦略

Defense in Depth (多層防御) を前提とした公開戦略

レッドチーム、ログ保持、利用監視、段階的公開の標準化。

マルチリージョン・マルチモデルへの依存分散

単一モデル・単一クラウドへの依存（キルスイッチ・リスク）を減らし、継続性利用保証を契約事項に組み込む。

用途別の厳格な権限設計

攻撃寄り能力と防御寄り能力を同一アクセスにしない。信頼できるセクター（金融、通信など）別に提供を切り分ける。

政府との事前エスカレーション経路の整備

サービス停止命令が出る前の段階で、実証・再現・修正・限定解除に至るプロセスを定義しておく。

Premium Strategic Intelligence Dossier

ガバメント向けプレイブック：ハイブリッド秩序下の政策指針

Immediate Action → Long-Term Stability

1 同盟国内例外アクセスの明文化

Trusted partnerの資格、用途、監査、停止条件を非公開協議ではなく、公式文書として定義する。

2 共同評価と相互承認

各国のAISI網、OECD、G7デジタル・サイバー専門家グループを接続し、重大インシデント通知と試験を共通化。

3 防御用途優先のアクセス設計

重要インフラ（通信、電力）、金融安定、脆弱性修復に特化した「優先アクセス枠」を整備する。

4 主権性と相互運用性の両立

EU式主権クラウドや日本のDFFTを閉鎖主義に陥らせず、監査可能な越境利用と接続する。

5 法的根拠の透明化

米国の輸出管理や行政命令の実態・要件を公表させ、グローバル市場における恣意性と混乱を最小化する。

The future of AI is no longer just technological—it is fundamentally geopolitical.