デジタル安全保障の新秩序：ソブリンAI確立に向けた戦略的ロードマップ

地政学ショックと法規制強化に伴う「海外依存AIの停止リスク」を明らかにし、自立的な事業継続性を確保するためのAI主権確立アプローチを提示する。

2026年に直面した「AI停止リスク」と法制ショック



米国AIの突如アクセス停止
輸出管理指令により最新AI停止。



中国のAI技術輸出規制
重みや技術23項目を規制対象化。



国内サイバー防衛法の施行
基幹インフラに監査報告義務化。

実践アプローチ：3階層ハイブリッド主権ポートフォリオ



Tier 3：定型大量処理領域

国内管理の低コストオープンモデル

主な対象業務：
定型構築処理・
非機密データ

低コストモデルで効率化を推進。

Tier 2：一般社内・顧客対応領域

ソブリンクラウド / 機密保護環境＋主要モデル

主な対象業務：
社内文書・
業務自動化

ソブリンクラウドで安全に活用。

Tier 1：基幹・極秘データ領域

国産オンプレミス / 国産LLM (cotomi・Takane等)

主な対象業務：
基幹インフラ・
極秘・OT制御

国産AIとオンプレで完全統制。