ソブリンAIの全貌と企業が取るべき知財・ガバナンス戦略

米国の供給停止リスクやデータ保持義務変更を受け、自社の技術・運用・データを自国または自社で管理する『ソブリンAI』の確保が急務。
単なるオンプレミス回帰ではなく、機密性や業務継続性に総継続性に応じた階層別のハイブリッド構築と厳格な契約・知財管理が重要。

データ分類の再設計



営業秘密の区分に応じて外部AIへの入力可否と環境を紐付け



契約条項の標準化

学習利用の禁止データ保持期間
削除証の取得を期守



暗黙知の権利管理

現場知のオントロジー化時に
独自データの帰属条項を厳守

ソブリンAIを構成する3つの主権階層

技術主権の確保

自国でのモデル・半導体・
計算基盤の製造能力を保持

運用主権の確立

外部遮断時も自社管理下の
鍵と環境で稼働を継続

データ主権の証明

機密情報の管轄権・
アクセス権限・監査証跡を
技術的に担保



2026年 地域別ソブリンクラウドIaaS市場規模予測

中国　474億ドル



技術流出防止籬を強化
し自国基盤を強力推進

北米
164億ドル



ハイパースケーラーを
中心に巨大需要が継続

欧州
126億ドル



法的自律性を重視し
2027年には北米を逆転予測

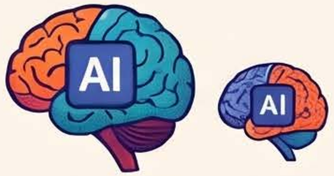
契約書項の標準化



学習利用
不可

削除証明

学習利用の禁止、データ保持期
間、削除証明の取得を明記



代替モデルの常備

主力AIの供給停止に備え
国産LLM等の迂回路を用意



監査ログの自動記録

利用者と入力データの移動履歴
を自動追跡できる体制を整える

Gemini Notebook