ガバメントAI選定結果が示す「企業知財×生成AI」の新基準

2026年3月、デジタル庁による行政用国産LLM選定基準（説明責任・安全性・機密性）は、
民間企業の知財活動における「LLM選定の要件定義」の事実上の標準となることが予測されます。

ガバメントAIが定義した「信頼の基準」

性能よりも「説明責任」と「安全性」を重視

学習データの法令遵守やハルシネーション対策の説明可能性が必須条件となった。

「機密性2情報」に耐えうる運用要件

ガバメントクラウド上での推論など、秘密情報を外部流出させない環境が評価された。

15件中7件の国産LLMを厳選

NTT、ソフトバンク、NEC、富士通 etc。
実務レベルとして認定。

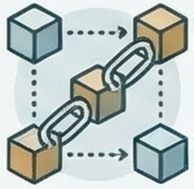
知財実務で今すぐ導入すべき「3つの防御策」

契約による「二次利用禁止」と「ログ監査」の義務化

交渉論点	条項の狙い
学習利用の禁止	発明・契約情報の二次利用による秘密喪失を遮断する
ログの取得・提供	発明者認定、内部監査、訴訟対応時の証拠とする
知財侵害の補償	学習データに起因する第三者からの権利侵害申立てを防御する

知財ユースケース別の入力ポリシー策定

特許ドラフト、契約レビューなど、業務ごとに利用可能なモデルと環境を定義する。



生成プロセスの「証跡（メタデータ）」を保存

出願書類のどの文言がAI由来かを再現できるよう、プロンプトIDやモデル版数を記録。