# ガバメントAI国産LLM公募結果が示す「新たな実務基準」

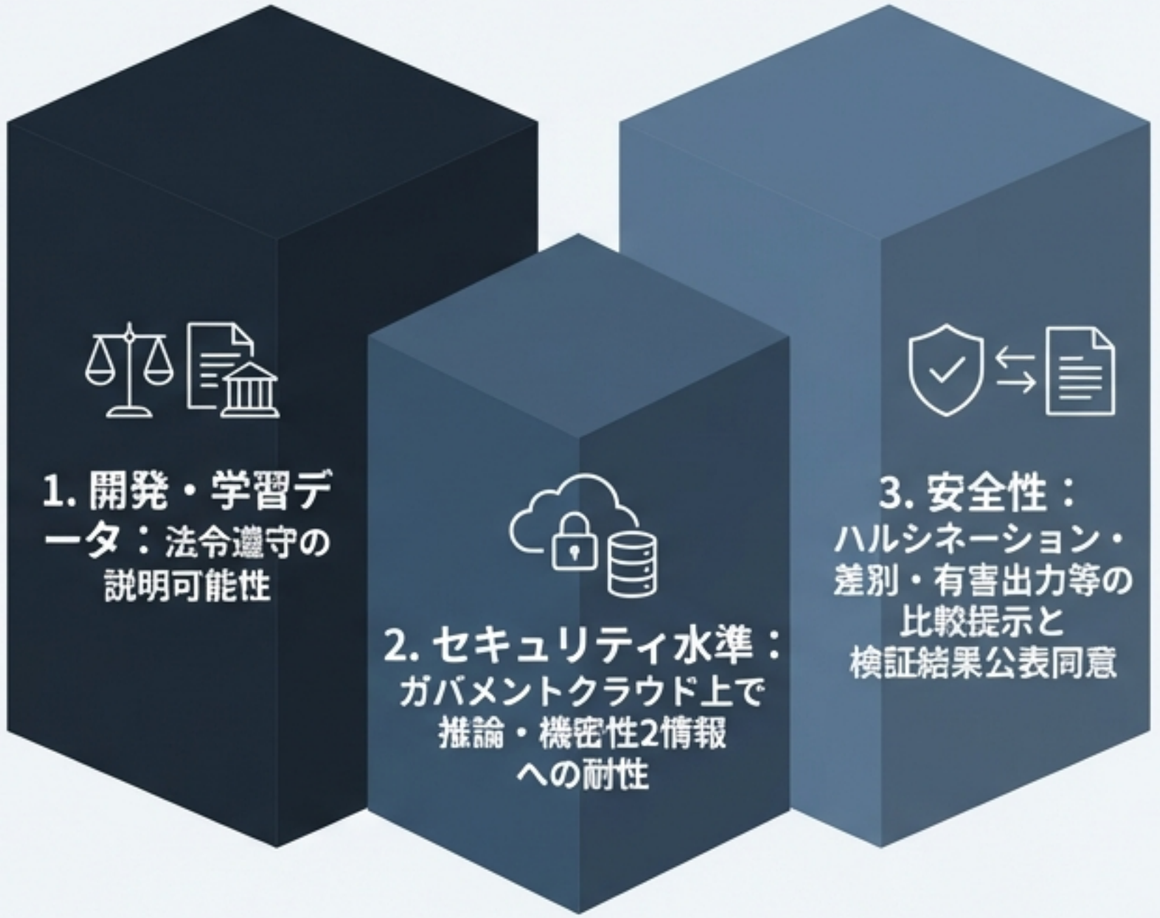
## 企業の知的財産・法務部門に向けた生成AI活用のデファクトスタンダードと戦略プレイブック

単なる国産推奨から、
知財リスク管理の要件定義へ昇華

政府共用AI基盤「源内（GENNAI）」の公募要件は、今後の民間企業における
「調達・説明責任・監査性」の事実上の標準（デファクトスタンダード）となる。

# 公募結果の一次情報：「性能」ではなく「説明責任と監査性」の束

- tsuzumi 2（NTTデータ）
- CC Gov-LLM（カスタマークラウド）
- Llama-3.1-ELYZA-JP-70B（KDDI・ELYZA）
- Sarashina2 mini（ソフトバンク）
- cotomi v3（日本電気）
- Takane 32B（富士通）
- PLaMo 2.0 Prime（Preferred Networks）




**これらは行政実務に限らず、企業の知財活動（特許出願、著作物生成、営業秘密管理）におけるベンダー選定基準と完全に一致する。**

# 公表資料の「空白」：未記載事項がもたらす不確実性とリスクシナリオ

**確定事実**
(Confirmed)

**未記載・不確実性**
(Unwritten/Uncertain)

[!] 未記載の重要実務要件: ログ保持期間、入出力データの学習への二次利用方針、補償（Indemnity）条項、責任制限。

**楽観 (Optimistic):**
入力は保存・学習されず、監査ログは利用者側で完全統制可能。

**中立 (Neutral):**
学習利用はされないが、ログ取得・監査権限が曖昧で漏洩リスク残存。

**悲観 (Pessimistic):**
入力・ログが事業者側に残り、学習・再利用や第三者移転が否定できない。

**契約・技術・運用の3層において、「どの仮定に転んでも致命傷を避ける」多段的な防御構造の設計が急務。**

# 法制度・ガイドラインの現在地：知財実務の参照軸

## 著作権（文化庁）

学習段階と生成段階のリスク構造分離。生成物の侵害リスク（類似性・依拠性）への対応。

## 特許（特許庁）

AI関連技術の審査事例追加。
記載要件や発明該当性における「根拠・設計意図の文書化」の要求。

Corporate IP
&
Generative AI
企業の知財と
生成AI

## 個人情報（PPC）

入力データの保護、第三者提供制限。「個人情報が入っても学習・保存されない設計」の必要性。

## 海外判例（Reuters vs. Ross）

訓練データの著作権（Fair Use）と市場代替性を巡る紛争。M&Aや保険設計への波及リスク。

## AIガバナンス（経産省・総務省・IPA）

AI事業者ガイドライン（Living Document）。
調達仕様への「ログ・データ取扱い」の盛り込み推奨。

# 企業知財活動への影響 Ⅰ：特許出願・発明者帰属

## ポジティブ影響（Positive）

- 国産LLMの「ガバメントクラウド運用」「法令遵守説明」基準により、特許ドラフト時の情報流出リスクを抑えたベンダー選定が容易に。
- ログ・証跡に基づく設計で、発明提案から出願までの意思決定過程を可視化（職務発明の紛争コスト低下）。

## リスク（Risk）

- 悲観リスク: 入力内容が保存・学習された場合、新規性喪失以前に競争上の秘匿性を失い、他社の後続出願・先使用に有利に働く懸念。
- 中立リスク（ジレンマ）: 証拠化のために「ログを残す」こと自体が、個人情報・未公開発明の新たな漏洩ターゲット（攻撃面）を増やす結果に。

# 企業知財活動への影響 II：著作物・営業秘密・ナレッジ活用

## ポジティブ - 閉域/専有環境の普及

「機密性2」対応の可視化により、企業内でも閉域環境でのRAG（検索拡張生成）構築が加速。

設計ノウハウ、顧客提案書などの「営業秘密」を外部流出させずずに社内活用するアーキテクチャが定着。

tsuzumi 2等に見られる「学習データのコントロール（自発的削除等）」は企業のレピュテーション保護と親和的。

## リスク - 周辺ツールの死角

悲観リスク: LLM本体が安全でも、周辺のログ基盤・監視ツール・チケットシステムに秘密情報が流れる連鎖漏洩リスク。

誤認リスク:「学習に利用しない」=「秘密保持（第三者開示禁止）」ではないという法務にという法務上の盲点。

- ログ基盤
- 監視ツール
- チケットシステム

# 企業知財活動への影響 Ⅲ：ライセンス・M&A・保険

## ライセンス (Licensing)

Llama 3.1等の派生モデル（ELYZA等）における、Community LicenseやAUP（Acceptable Use Policy）の遵守。商用条件・再配布制限の確認必須。

## M&Aデューデリジェンス (M&A DD)

政府調達基準が「買い手のDD標準項目」へ。学習データの権利取得経路、安全性評価、ログ監査体制が表明保証のコアに。

## 保険と補償 (Insurance & Indemnity)

利用規約における「出力の類似性」免責や責任限定条項。企業側での第三者クレーム自己負担を防ぐための、契約上の補償設計とサイバー保険要（アクセス管理・可観測性）の擦り合わせ。

# 実践プレイブック：ベンダー交渉用「契約条項」テンプレート（1/2）

| 条文のたたき台 | 知財視点でのねらい |
| --- | --- |
| 「提供者は、インプット/アウトプットおよび関連ログを、本契約で定義する提供目的以外に利用しない。」 | 発明・契約・研究情報の二次利用防止。 |
| 「提供者は、当社データ（インプット、RAGコーパス、出力、ログ）を、モデルの学習・微調整・品質改善に一切利用しない。」 | 「オプトアウト」ではなく完全義務化。“学習に利用しない＝秘密保持ではない”問題の遮断。 |
| 「保持期間はX日を上限とし、期間満了または契約終了時に復元不能な方法で消去し、消去証明書を発行する。」 | 秘密情報・個人情報の“残り続けるリスク（攻撃面）”の極小化。 |

# 実践プレイブック：ベンダー交渉用「契約条項」テンプレート（2/2）

| 条文のたたき台 | 知財視点でのねらい |
| --- | --- |
| 「利用ログ（日時、利用者ID、モデルID、メタデータ）を当社が取得・保管し、プロンプト／出力のサンプル監査を可能とする。」 | 発明者認定、説明責任、内部監査、訴訟対応のための証跡確保。 |
| 「データ処理・保管場所（国/リージョン）を特定し、変更時およびサブプロセッサ（下請）追加時は事前同意を要する。」 | 越境規制・海外当局の調査権限リスクの可視化と連鎖漏洩の抑止。 |
| 「トレーニングデータや提供物に起因する第三者の知財侵害申立てについて、提供者は防御および補償を行う。」 | サービス規約の「責任否認・類似性免責」を上書きし、訴訟費用の穴を埋める（保険設計に直結）。 |

# 社内ガバナンスと知財戦略の再構築

ガバナンス
チェックポイント

## 知財ユースケース別ポリシー

「特許ドラフト」「共同研究レビュー」「契約書要約」など用途別に類型化。
(1)入力禁止情報、(2)許可モデル、(3)専門家レビュー義務を定義。

ガバナンス
チェックポイント

## 出力物の位置づけ

生成結果は「事実」ではなく「参考情報（ドラフト）」と規程上定義し、対外公表・出願前の人間(弁理士・法務)によるレビューを必須化。

## 出願前管理のボトルネック解消

AI利用で出願前情報の滞留リスクが増すため、「早期出願（仮出願的運用）」や「発明届の粒度見直し」へシフト。共同研究契約でのAI利用条項（成果帰属・ログ開示）の標準化。

# 閉域・専有環境の技術的対策と「出力追跡」アーキテクチャ

## データ分離（Access Control）

RAGコーパス（契約・発明・顧客情報）を部署/案件単位で
インデックス分離し、厳密なアクセス制御を実施。

## モデル検証（Red Teaming）

知財領域特化のレッドチーム演習（守秘情報を引き出すプロンプト、
誤引用テスト）を定期実施し、モデル更新時に回帰テスト。

## 出力追跡と証拠性（Provenance Tracking）

出願や契約の「どの文がAI由来か」を後日証明するため、
5つのメタデータを保持。

- (a) プロンプトID
- (b) 参照文書ID（RAG）
- (c) 出力ハッシュ
- (d) 生成時刻
- (e) モデルID/バージョン

# 実装ロードマップと不確実性への備え（2026〜2031年）

## 短期 (2026 H1-H2)：選定とポリシー固定

- 推奨優先度 [高]：入力・ログ・学習利用の契約固定化 / ユースケース別ポリシー施行 / 監査ログ・証拠性の実装（閉域・RAG）。

## 中期 (2027-2028)：自動化と複雑化への対応

- 推奨優先度 [中]：複数モデル混在によるライセンス/規約コンプラ体制構築 / モデル更新時の回帰テスト定着 / M&A DDの標準化。

## 長期 (2029-2031)：訴訟・規制適応とデータ資産化

- 推奨優先度 [長期]：海外判例蓄積に伴う補償・保険の再設計 / 社内コーパス（データ資産）の整備・統制 / リスクベースでの専有化投資。

**ガバメントAIの調達基準を「自社の知財防衛のベースライン」として活用し、生成AIの恩恵を安全にスケールさせる。**