

MiniMax「M3.1 Flash」企業導入の知財・セキュリティ影響評価

(調査基準日：2026年10月20日)

「無条件の本番採用は不可。契約・データ統制を伴う限定導入が妥当。」

強力な破壊的ポテンシャル

- ✓ 100万トークンコンテキスト
- ✓ エージェント・コーディング特化
- ✓ 圧倒的低コスト

エンタープライズ保護の空白

- ⚠ ZDR (Zero Data Retention) 未確認
- ⚠ 権利処理のグレーゾーン
- ⚠ IP補償の不確実性

圧倒的な処理スケール

- 1,000,000 tokens (入力+出力の合計)
- 200+ TPS (通常条件), 170+ TPS (P50)



エージェント・実行能力

- 単なるテキスト出力ではなく、ツール利用・Computer Useをサポート。
- OSWorld V2: 61.7 / DeepSWE v1.1: 73.7% / CyberGym: 82%

デュアルユースの脅威

- 脆弱性修正、ペネトレーションテスト、マルウェア解析に強み。

従来の「人間がコピペするAI」から、「AIが直接ファイルを読み書きし、自律実行する」時代へのシフト。権限分離が必須。

THE PRICE

入力: \$0.15 / 1M tokens

(キャッシュ入力: \$0.015 / 1M)

出力: \$0.60 / 1M tokens

THE HIDDEN ENTERPRISE COSTS

Alert List

- ✓  • [未確認] M3.1専用の明示的なZDR (Zero Data Retention)
- ✓  • [未確認] 日本国内でのデータレジデンス (Data Residency)
- ✓  • [未確認] 企業向けの明示的な第三者IP補償 (IP Indemnity)
- ✓  • [未確認] M3.1に特化したSOC 2 / ISO 27001 保証

インサイト：圧倒的なコスト削減分の一部は、社内統制・法的確認コストとして見積もる必要がある。

事前学習コーパス：100兆トークン超 / 画像10億枚超 / 動画100万時間超
(EU向け概要 10月19日更新)

公開ウェブ

クローラ「MINIMAX_UA」(2025年4月～12月収集)。オプトアウト(robots.txt)尊重。

パートナー/非公開データ

private databases等からの取得。
警告: 個別の権利処理・許諾範囲は非公開。

合成データ

M2.7や自社内部モデル、第三者モデルによる合成データ。

M3.1 基盤モデル

User Data Note: API入力には訓練に使用しないと明示する一方、「他のサービス・製品」のユーザー対話データは基盤モデル改善に使い得ると記載。

インサイト：透明性（訓練データ概要の開示）は、企業が「全データが権利クリアである」と見なす免罪符にはならない。

知財・法務リスク・ヒートマップ

[高リスク] 営業秘密・未公開発明の送信

ZDRや国内データレジデンシーの不在により、契約確認前のソースコードや特許草稿投入は極めて危険。

[中～高リスク] 出力の著作権・OSSライセンス / 契約・補償

生成コードの類似性・依拠性の検証必須。公開資料上のIP保護・責任上限が不明確。
別製品(Hailuo AI)における著作権訴訟（2026年5月管轄申立て却下）の係争リスクあり。

[中～高リスク] 第三者特許のFTO

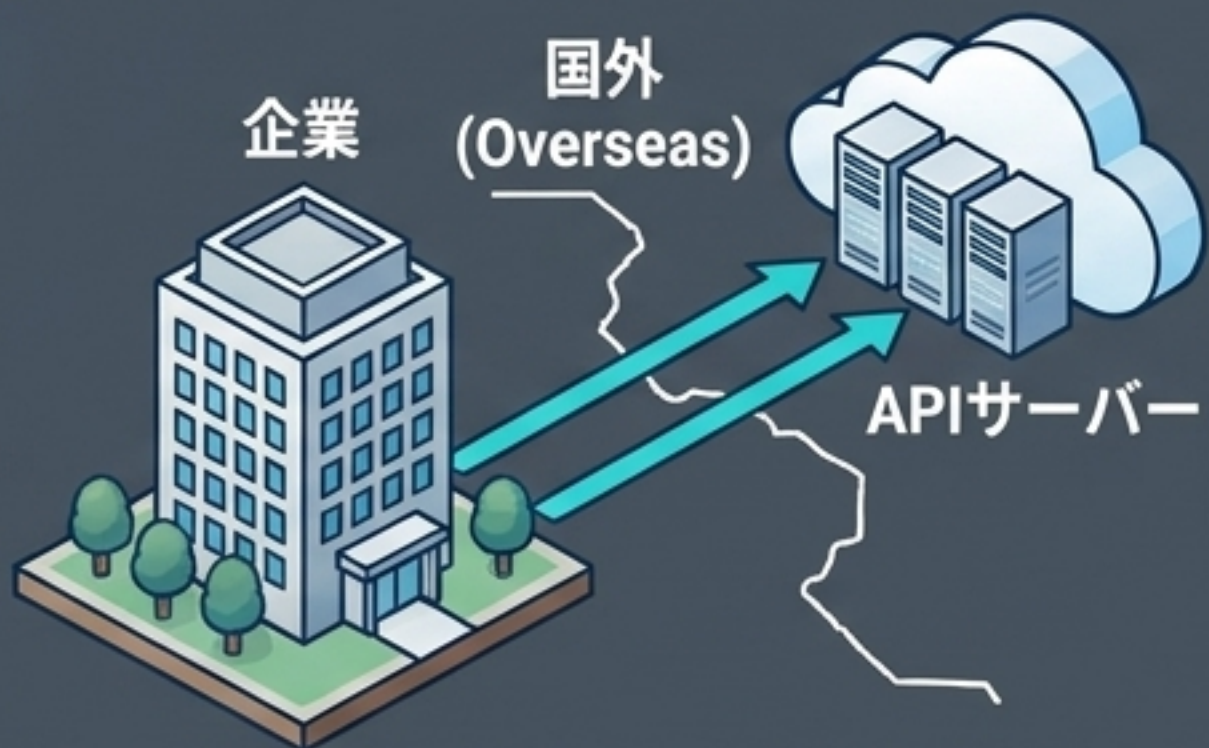
特に将来のセルフホスト時。Sparse AttentionやMoE特許の抵触調査が不可避となる。

[中リスク] 商標・表示の侵害

生成されるUIや製品名に対するクリアランスが必要。

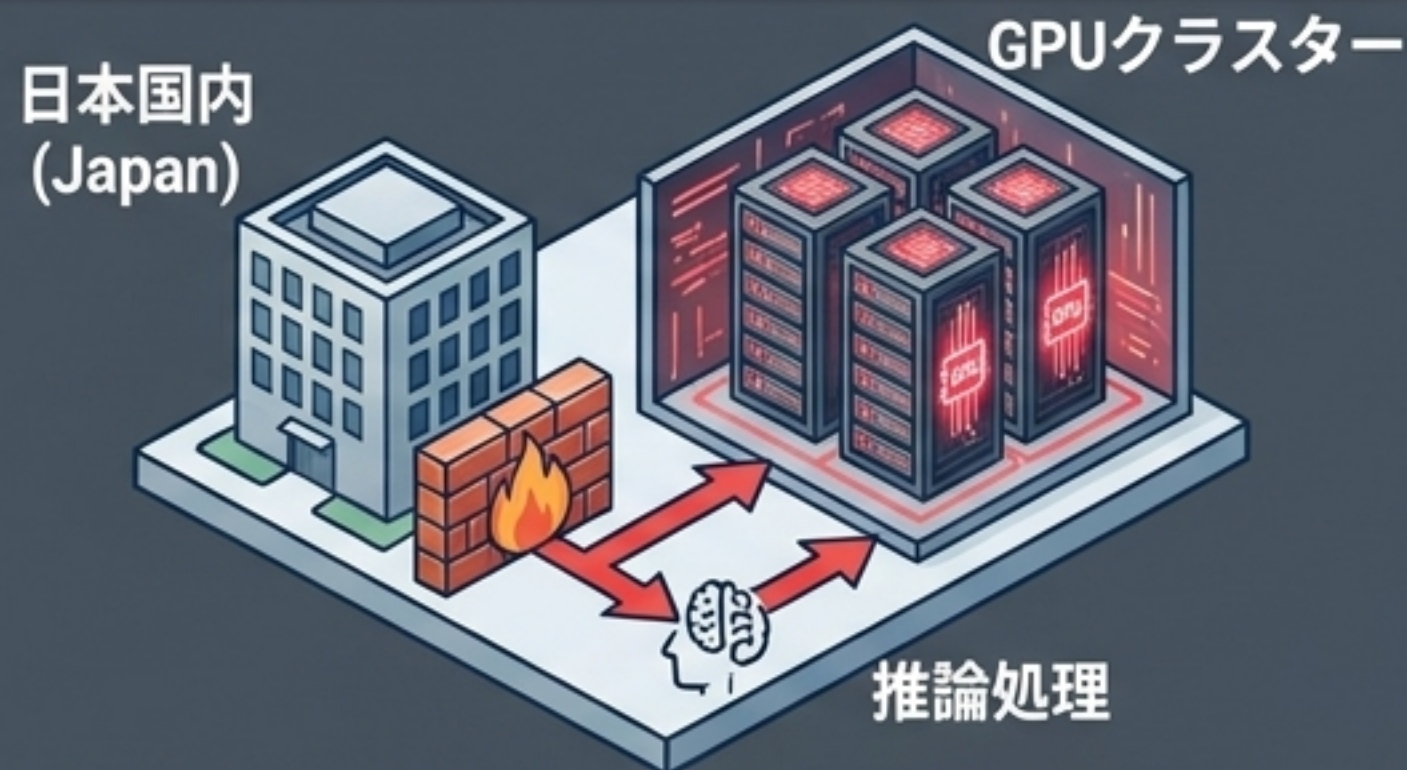
特許(FTO)侵害リスクの構造的理解

シナリオ A: API利用 (現状)



侵害主体は主にサーバ側（国外）。
ユーザーの直接侵害リスクは相対的に低い。

シナリオ B: 国内セルフホスト (将来のウェイト公開時)



⚠ ユーザー企業自身が日本国内で推論処理を
「直接実施」する。FTOリスクが跳ね上がる。



Key Patent Hotspots: Sparse Attention, MoE routing, 長文脈推論
(e.g., Baidu JP2026516535A family等、特許密集領域のFTO調査が必須)。
アーキテクチャの確定仕様(428B/23B等)は正式版で未確認のため注視が必要。

著作権・OSSコード生成に関する罣



Legal Context

特許

2025年1月30日の知財高裁判断を踏まえ、
発明者は自然人に限られる。
発明届に「AI使用有無」と「人間の創作的貢
献」の記録が必須。

コード生成

学習データにソースコードが含まれる。
長いコード片の製品採用時は、必ず SCA
(ソフトウェアコンポジション解析) による
OSSライセンスと依拠性の確認を通すこと。

利用規約とSLAの死角

Warning: M Planの罠 - MiniMax自身が「M Plan」は個人・対話型向けとし、本番 (Production)には推奨していない。Dynamic rate limiting (ピーク時制限) のリスクあり。

契約交渉における必須確認事項 (Checklist)

- ⚠ 1. 入力データの権利保持と学習利用の完全禁止 (ZDR相当)
- ⚠ 2. 第三者IPクレームに対する防御・補償 (Defense/Indemnity) と責任上限
- ⚠ 3. SLA (単なるAPI接続可否ではなく、可用性保証とサービスクレジット)
- ⚠ 4. 秘密保持義務・データ削除義務・データ所在地 (Residency)

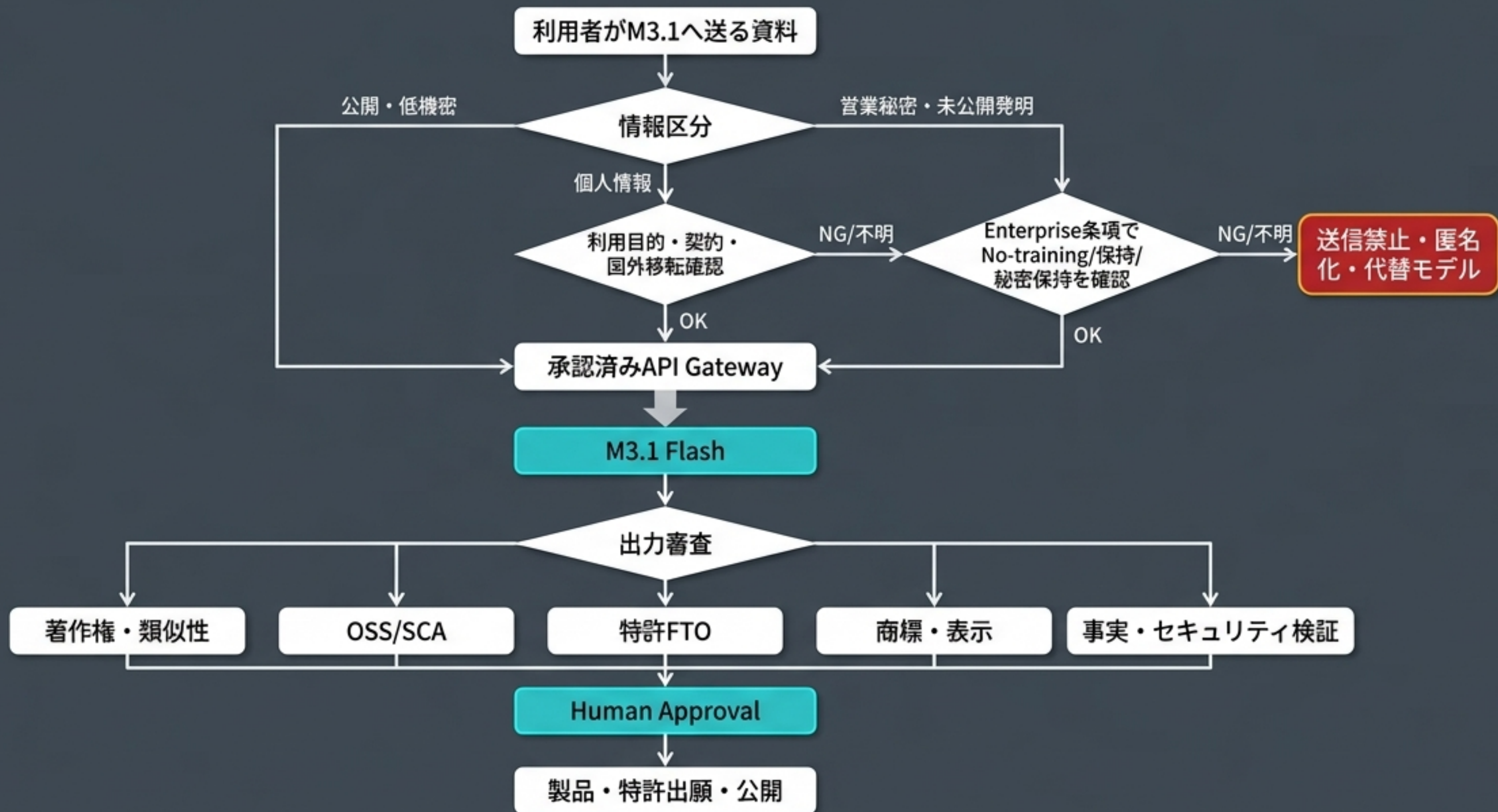
インサイト： Web上の一般App規約とAPI Open Platform Termsを混同しないこと。
本番採用時は版管理された契約書での条項精査が必須。

競合モデルとのエンタープライズ比較マトリクス

Model	1M Input Cost	Context/Agent	Enterprise Data Control (ZDR)	IP Indemnity
MiniMax M3.1	\$0.15	1M/Agentic	未確認	個別確認
OpenAI GPT-6.1 Sol	Astraの1/5	Agentic	○ (ZDR公開)	○ (補償あり)
Anthropic Claude 5.5	\$2.00	Agentic	○	○ (商用契約)
DeepSeek V4.1	\$0.15 (off-peak)	Agentic	個別確認	個別確認

インサイト：価格ではM3.1とDeepSeekが圧倒的だが、知財保護・ガバナンスではOpenAI/Anthropic/Googleが優る。機密R&Dでは「価格差の一部を統制コストとして見込む」必要がある。

【核心】 M3.1導入のための安全ゲートウェイ・アーキテクチャ



アクションプラン [フェーズ1: 今後30日]

ターゲット: 全面禁止・解禁の二元論を捨て、「どの情報・用途なら使えるか」を定義する。

📅 Week 1 (Triage)

- ・シャドーAI（ブラウザ、IDEプラグイン、個人API）の棚卸し。
- ・ **暫定ポリシー適用: 未公開特許、ソースコード全体、顧客・個人データのM3.1投入を即時禁止。**

📅 Week 2 (Legal & DD)

- ・ MiniMaxへエンタープライズDD（デューデリジェンス）質問票の送付（Retention, Training, Subprocessor等の確認）。
- ・ 契約差分レビューの開始。

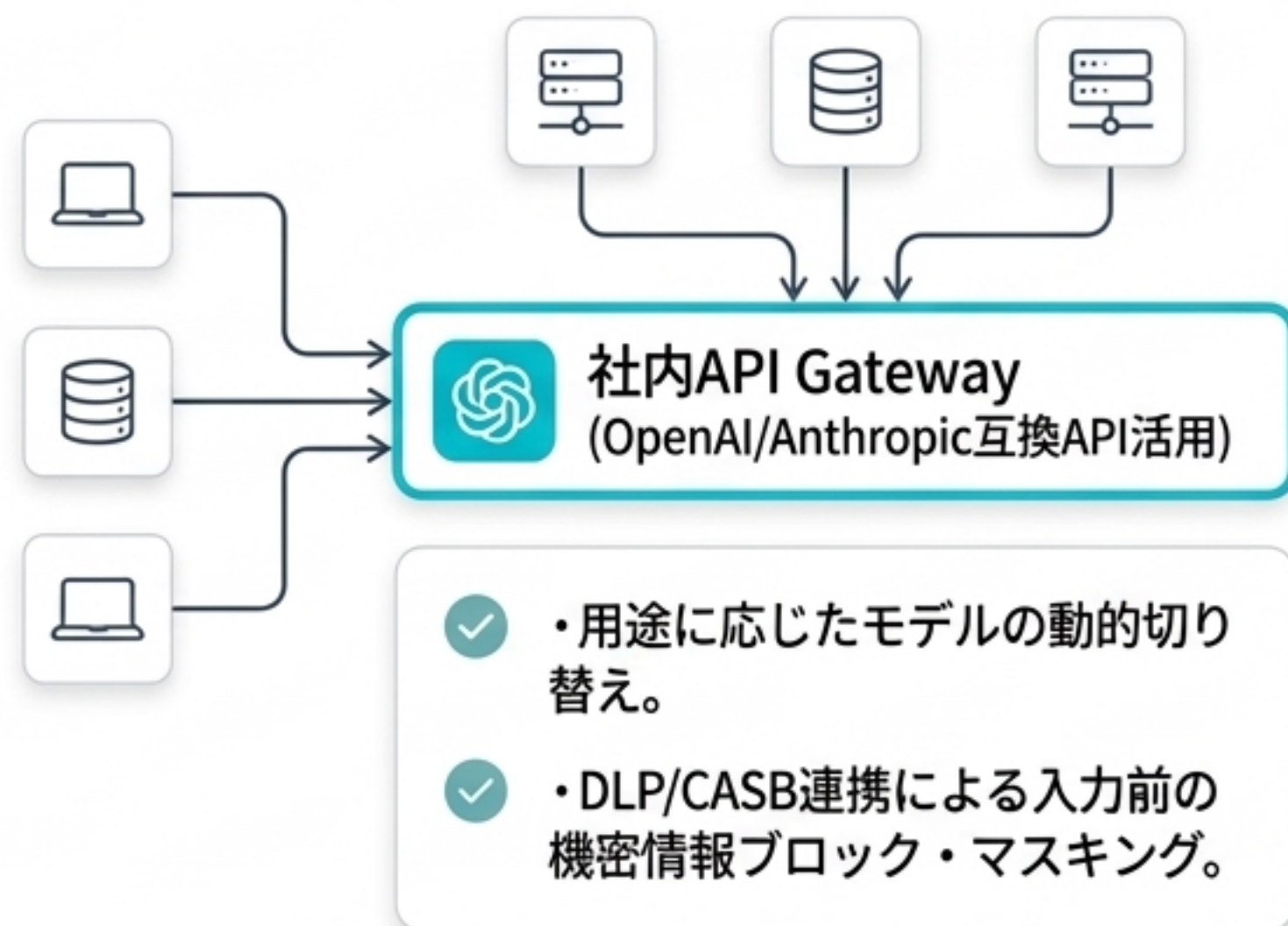
📅 Week 3-4 (Pilot & IP Setup)

- ・ 公開データ・ダミーデータに限定した「技術パイロット」開始。
- ・ M3.1関連の特許FTO一次検索（Sparse attention, MoE等）。
- ・ CI/CDに出力IP検査（SCA, License scan）を追加。

アクションプラン [フェーズ2: 今後6ヶ月]

ターゲット：実験的統制をAI調達・開発の標準プロセスへ組み込む。

System Integration（マルチモデル戦略）



Process Engineering（プロセスの改修）

- ✓ 発明届への「AI利用有無」「入力した先行情報」「人間の創造的貢献」記載義務化。
- ✓ 生成AI専用の「調達付属書」の策定（No-training、IP Indemnity等の要求基準の統一）。
- ✓ サイバー保険・知財侵害補償の適用範囲再点検。

アクションコアクションプラン [フェーズ3: 1~3年]

ターゲット: 特定モデルへの依存を**知財リスク**にしないアーキテクチャへの移行。



Self-Hosting & License Assessment

将来のウェイト公開時、安易なオンプレ移行を控える。（過去のM3公開ウェイトのModified-MIT系条件のような商用制限・派生モデル条件を再評価）。

IP Strategy Shift

「モデル」自体ではなく、「自社データ+AIエージェントによる固有のプロセス」の特許化戦略へ。

最終シンセシス：R&D承認のための「7つのコントロール」



1. 秘密情報の流れ: DLP/Gatewayによる入力制御
2. 出力IPの検査: CI/CDでのSBOM/SCA必須化
3. 特許FTO: 将来のオンプレミス実装を見据えた特許監視
4. 人間の発明寄与: ツール実行・出力に対する自然人の介入記録
5. Vendor Indemnity: 明示的な契約上の第三者IP侵害補償
6. データ保持・学習: ZDR相当の確約とログ保持の分離
7. 将来ライセンス: ウェイト公開時の商用利用制限の再評価

結論：「透明性（訓練データ概要の開示）は、契約上の保証や非侵害保証の代替にはならない。これら7つの統制が完了するまで、無制限の本番導入は見送るべきである。」