ChatGPT-5.6が知財業務に与える影響と実装戦略

高性能化とガバナンス統制を両立する戦略的プレイブック

Executive Summary: 現状認識と中核となるテーゼ

パラダイムシフト

知財部門の役割の根本的変化

「自ら書く部門」から、生成物の「品質保証・権利整理・証拠化・説明責任を担う部門」への完全なシフト。

法的現在地とリスク

法的安定性の不均一

AI法はソフトロー中心だが、特許法（発明者は自然人のみ）や著作権の侵害判断は個別事案依存。統制なき導入は知財リスクを増幅させる。

戦略的最適解

承認済みの統制環境への収斂

短期は「Enterprise/API」での限定導入による下書き自動化。中長期は「ログ保全・監査制度」を前提としたエージェント型への接続。

GPT-5.6: 技術的能力と実務上の評価マトリクス

	公式確認 (Official Facts)	実務評価・注意点 (Practical Reality & Risks)
データ学習利用	Business/Enterprise/APIは既定で学習不使用。	高機密用途における「第一候補」環境として確定。
権利と出力補償	出力は法令許容範囲で利用者に帰属。API/Enterpriseに出力補償あり。	第三者の権利侵害免責ではない。商標、入力権利欠缺、Beta機能は補償から「除外」される。⚠
ログと監査証跡	Compliance Logsの標準保持期間は30日。Programmatic Tool CallingはZDR互換。	発明者認定・訴訟対応のための「長期保全」には、自社での別環境への退避設計が必須。⚠
未指定領域	多言語法務ベンチマーク、説明可能性の標準メタデータ。	PoC（概念実証）を通じた自社環境での厳密な精度検証が不可避。

3つの導入シナリオと必須要件

限定利用シナリオ

Enterprise / API

対象業務

社内文書の要約、OA応答案の下書き、先行技術調査メモ。

必須要件

学習不使用、権限制御、ログ取得。

業務接続シナリオ

ChatGPT Work / Workspace agents

対象業務

案件管理・Office・文書管理システムとの直接接続、チーム横断の文脈取得。

必須要件

社内ツール横断でのアクセス権限（RBAC）の厳格な同期。

高機密シナリオ

API（厳格構成）

対象業務

未公開発明の詳細、M&Aデューデリジェンス、訴訟戦略。

必須要件

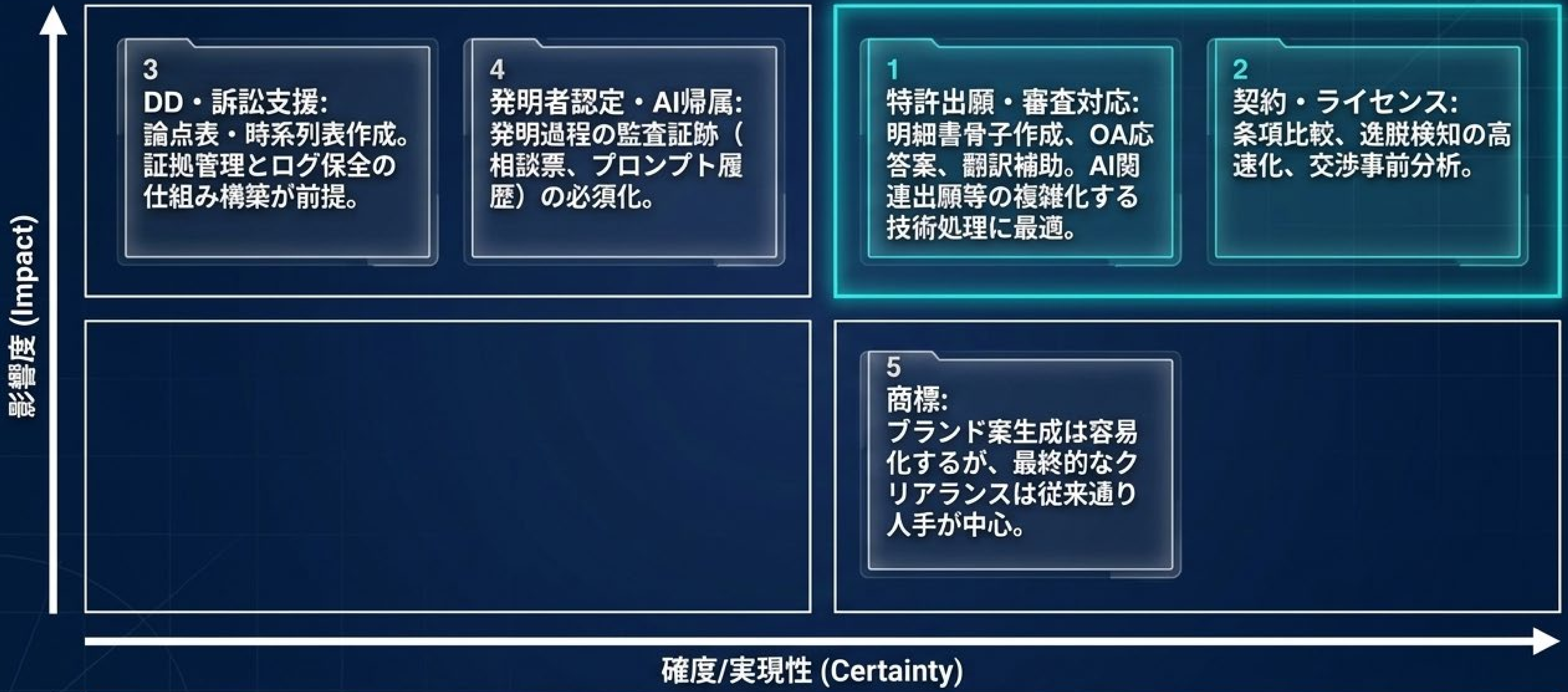
ZDR（ゼロデータ保持）、データレジデンシーの確保、厳格な契約統制。

知財業務プロセスの変革：作成から「検証」へのシフト

最大の制約「もっともらしい誤り（幻覚）」

OpenAI公式（System Card）でも捏造リスクが明示されている。出力本文の品質評価よりも、「根拠資料と照合できるプロセスの設計」が絶対条件となる。

領域別インパクトと導入の確度



要注意領域：著作権・営業秘密領域では、生成物の類似性確認や機密区分の入力制御といった「定常的な権利処理・説明責任」の業務負荷が新たに発生する。

日本法における中心論点と絶対的制約

著作権（Copyright）

文化庁の見解

- 原則: 学習（非享受）と生成（類似性・依拠性）の分離。

⚠ **レッドライン**: 既存著作物と類似する生成物を出力させる目的や、追加学習での意図的出力は「享受目的」とみなされる危険性大。

✓ **対策**: 「入力してよい資料」と「引用・生成根拠としてよい資料」の厳格な分離。

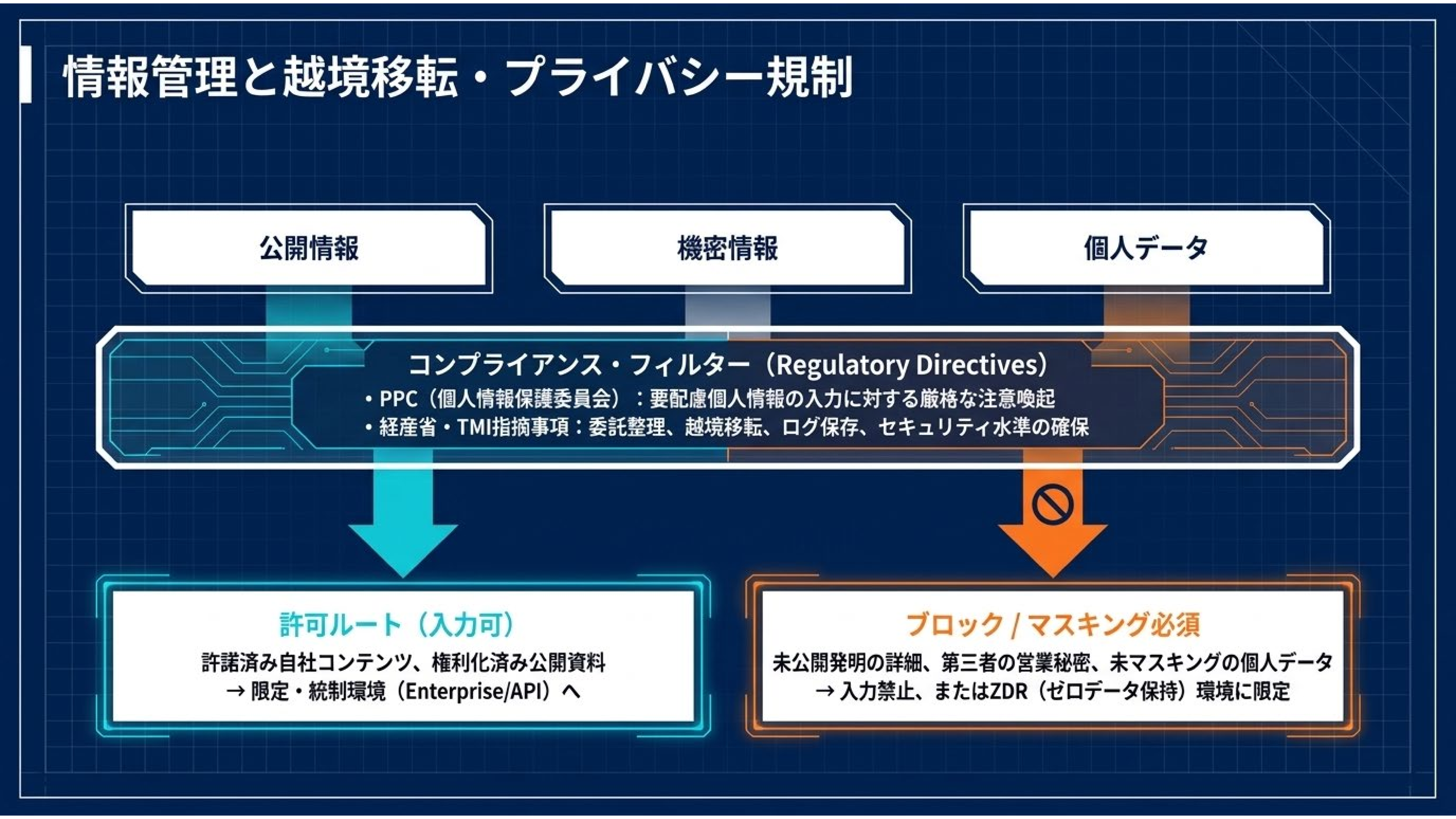
特許法・発明者認定（Patent Law）

知財高裁判決（2025年1月30日）

- 原則: 「発明者は自然人に限る」。AI自体を発明者とすることは現行法上不可。

⚠ **レッドライン**: AIが着想を支援しても、人間の「実質的寄与」が証明できなければ権利化リスクが生じる。

✓ **対策**: 発明相談票、プロンプト履歴、採否判断メモの長期保存（監査証跡）が必須。


情報管理と越境移転・プライバシー規制
公開情報
機密情報
個人データ
コンプライアンス・フィルター（Regulatory Directives）
・PPC（個人情報保護委員会）：要配慮個人情報の入力に対する厳格な注意喚起
・経産省・TMI指摘事項：委託整理、越境移転、ログ保存、セキュリティ水準の確保
許可ルート（入力可）
許諾済み自社コンテンツ、権利化済み公開資料
→ 限定・統制環境（Enterprise/API）へ
ブロック / マスキング必須
未公開発明の詳細、第三者の営業秘密、未マスキングの個人データ
→ 入力禁止、またはZDR（ゼロデータ保持）環境に限定

ガバナンス体制と責任分界点（誰が何を担うか）

知財部（IP Department） Owner	利用対象業務の選定、出力された根拠資料のレビュー、人間の寄与の証明（発明者認定）。
法務・コンプライアンス（Legal & Compliance） Co-owner	利用規程の策定、AI利活用契約の精査、越境移転対応、秘密管理水準の定義。
情報システム / CISO（IT / CISO） Enabler（必須）	SSO/RBAC（アクセス権限）の管理、API/Enterpriseログの自社退避（30日以上の長期保全設計）、接続アプリ審査。
事業部 / 研究開発（Business / R&D） User / Verifier	入力データの機密区分判定、AI成果物の事実確認・採否判断。

The “Four-Piece” Core Strategy: 日本企業向けの最適解

1
承認済み環境への限定導入
消費者向け無料版を排除し、学習不使用・統制可能なEnterprise/API環境へ全社利用を収斂させる。

2
厳格な入力統制の規程化
利用禁止データ、機密区分、個人データの取り扱いルールを策定し、システム的にブロックする

3
生成過程の自社証跡化
標準の30日ログに依存せず、プロンプト履歴や発明者認定メモを案件台帳と紐付けて自社退避・長期保存する。

4
人間の最終判断の必須化
AIを「文章作成ツール」ではなく「ワークフローの一次処理」と位置づけ、対外提出前の人手レビューと根拠紐付けを絶対条件とする。

実装ロードマップ：GPT-5.6対応のタイムライン

短期（即時着手）

- 承認済み環境（Enterprise/API）の選定と一本化
- 利用規程と入力禁止情報の定義
- ユースケース限定のPoC開始（調査・OA・要約）

中期（プロセス統合）

- Compliance/APIログの自社退避システム構築と監査設計
- 特許・契約・DD業務のテンプレート化
- 社内教育の定期化

中長期（全社スケール）

- Work/Agents機能の段階的接続
- 発明者認定・証拠保全の完全制度化
- 全社ガバナンスへの拡張

導入前エグゼクティブ・チェックリスト

契約・システム（Contracts & Systems）

- ☐ データ学習利用の有無が明示的にオプトアウトされているか。
- ☐ データ越境移転（データレジデンシー）の要件をクリアしているか。
- ☐ 監査条項とログの長期保存（自社退避）が設計されているか。

情報管理（Information Management）

- ☐ 機密情報の入力区分（未公開発明等のブロック）が定義されているか。
- ☐ 個人データ入力に対する委託整理・本人同意の指針があるか。

業務設計（Workflow Design）

- ☐ 全ての対外文書において、人手による「根拠資料との照合」プロセスが組み込まれているか。
- ☐ AI出力の無審査での提出を禁じる「提出禁止ライン」が設定されているか。

知財管理（IP Management）

- ☐ 著作権法に基づく入力制限（類似生成・意図的学習の禁止）が周知されているか。
- ☐ 特許出願における「自然人による発明」の寄与（プロンプト等）を記録する体制があるか。