ChatGPT

生成AIの知財業務活用における人間関与モード設計

Executive Summary

本報告書の結論は明確である。知財業務において採るべき方針は、生成AIを「使うか、使わないか」ではなく、業務単位で **HITL**、**HOTL**、**HOOTL** を切り分けることである。権利範囲、法的主張、外部提出文書、秘密情報の開示可否のように、誤りのコストが高く非可逆な工程は **HITL** を基本とし、先行技術調査の一次整理、検索式の拡張、条項抽出、要約、ナレッジ検索のように大量処理が必要で、かつ人間が例外監督しやすい工程は **HOTL** を中心に設計するのが実務的である。**HOOTL** は、メタデータ付与、定型通知、期限監視、文書の重複排除、ルールベースのラベリングや保持制御など、低リスクで可逆的な処理に限定するのが妥当である。 [1]

その理由は、近年の研究が、特許クレーム生成や審査対応ドラフトにおけるLLMの有用性を示しつつも、厳格な知財実務に耐えるには依然として専門家の検証・修正が必要だと示しているからである。特に、特許クレーム生成研究は、説明書ベースの生成が要約ベースより適切であること、GPT-4級モデルでも一貫性や法的堅牢性の確保には追加修正が必要であることを示している。また、審査対応では、知識グラフやRAGを組み合わせた特化型システムが忠実性を大幅に改善し得る一方で、最終判断の人間責任までは代替しない。 [2]

日本法を前提とする実務では、生成AIの導入判断は、著作権、営業秘密、個人情報、契約責任、説明責任を横断する必要がある。実務基盤としては、AI事業者ガイドライン、AIと著作権に関する整理とチェックリスト、営業秘密管理指針・秘密情報保護ハンドブック、個人情報保護委員会の注意喚起、AIの利用・開発に関する契約チェックリスト、特許庁のAIモデル契約書群が重要である。したがって、知財部門の本当の設計課題は「どこまで自動化できるか」ではなく、**どこまでを、あとから根拠付きで説明・検証できる形で自動化するか** にある。 [3]

分析の前提

本報告書は、主として 日本 [4] の知財実務を前提に、経済産業省 [5] と 総務省 [6] のAI事業者ガイドライン、文化庁 [7] のAIと著作権に関する整理、個人情報保護委員会 [8] の注意喚起、特許庁 [9] のモデル契約書、さらに WIPO [10]、OECD [11]、欧州委員会 [12]、NIST [13]、ISO [14] の国際的なガバナンス枠組みを横断して、知財業務に必要な運用モードを再構成したものである。なお、ここでいうモードは「モデルの能力差」を指すのではなく、**組織としての統制様式** を指す。つまり、同じモデルでも、クレームドラフトではHITL、文献アラートではHOTL、メタデータ整形ではHOOTLというように、工程ごとに異なる運用が成立する。 [15]

知財業務でモードを分ける際の判断軸は、生成AI一般論よりも厳しい。特許・契約・侵害判断は、単なる情報処理ではなく、将来の権利範囲、紛争ポジション、秘密管理の適法性に直結するからである。文化庁は、著作権法第30条の4等の解釈とともに、AIと著作権に関するチェックリスト＆ガイダンスを整備し、学習データや生成物に関するリスク低減と情報提供の重要性を示している。経済産業省は、営業秘密管理指針と秘密情報の保護ハンドブックの改訂で、生成AIへの不用意な入力による漏えいリスクを明示した。個人情報保護委員会も、生成AIサービス利用に関する注意喚起を公表している。したがって、知財部の導入判断は「性能が良いか」より先に、「**未公開発明、営業秘密、対外主張、個人情報を、どの境界で処理するか**」から始める必要がある。 [16]

判断軸	実務で問うべきこと	モードを重くすべき条件
法的影響度	その出力が権利範囲、侵害判断、契約責任を左右するか	外部提出、法的主張、ライセンス条件、権利行使に直結する
非可逆性	誤りが出た後に簡単に取り消せるか	出願・中間対応・警告書・契約締結後に回収困難
機密性	未公開発明、営業秘密、相手方秘密、個人情報を含むか	外部モデル投入や第三者連携の影響が大きい
検証容易性	参照根拠、検索式、モデル版、承認者を追跡できるか	根拠が残らない、再現できない、ログが取れない
変化頻度	モデル・RAG・ツール連携が頻繁に変わるか	変更管理が追いつかず、評価結果が陳腐化しやすい

上表の含意は単純で、**法的影響度が高いほどHITLへ、可逆性が高く定型性が高いほどHOTL/HOOTLへ寄せる**べきだということである。これは、欧州委員会の信頼できるAI指針が「人間の監督が弱いほど、より広範なテストと厳格なガバナンスが必要」と述べる点と、NIST AI RMFが人間監督のプロセスを定義・評価・文書化せよと求める点、さらにAI事業者ガイドラインがトレーサビリティとアカウンタビリティを重視する点と整合する。[17]

HITL、HOTL、HOOTLの定義と運用フロー

なお、欧州委員会の指針は **HIC** を用いており、**HOOTL** を直接の用語としては採らない。一方で、OECDの自動化分類は human-out-of-the-loop に相当する高自治度の状態を区別している。本報告書では、知財実務の統制設計を明快にするため、**HITL = 事前承認必須**、**HOTL = 例外監督中心**、**HOOTL = 境界設定と事後監査中心** という実務モードとして定義する。[18]

モード	定義	技術的特徴	運用フロー	知財実務での主な用途
HITL	人間が案件ごとの重要出力を確認し、承認しなければ外部利用・対外提出・非可逆処理に進めない運用	公式ソース/RAG、引用必須、低温度設定、差分表示、承認ワークフロー、権限分離	AI下書き → 根拠提示 → 専門家レビュー → 修正/承認 → 提出	クレーム案、審査対応主張、侵害判断、個別ライセンス条項、秘密情報例外承認
HOTL	AIが通常処理を進めるが、人間が監視し、閾値超過・例外・サンプリング結果に応じて介入する運用	信頼度閾値、ポリシーエンジン、例外キュー、サンプリング監査、ルール付き自動化	AI実行 → 閾値/ポリシー判定 → 例外のみ人手 → 継続監視	先行技術調査の一次整理、検索式拡張、契約レビュー一次抽出、審査対応の証拠集約、社内説明資料作成
HOOTL	人間は案件単位の意思決定ループに入らず、事前に境界条件を設定し、事後的に監査・停止権限を持つ運用	制限付きツール実行、固定テンプレート、サンドボックス、改ざん困難ログ、キルスイッチ	トリガー → 自動実行 → 監査ログ保存 → 定期監査 → 異常時停止	メタデータ付与、重複排除、期限通知、定型ラベリング、DLP・保持制御、アラート配信

```
flowchart LR
    A[案件受付] --> B{法的影響度・機密性・可逆性}
    B -->|高い| C[HITL]
    B -->|中程度| D[HOTL]
    B -->|低く可逆| E[HOOTL]

    C --> F[根拠付き下書き]
    F --> G[専門家レビュー]
    G --> H[承認後に利用]

    D --> I[自動実行]
    I --> J{閾値・例外判定}
    J -->|例外あり| G
    J -->|例外なし| K[利用]

    E --> L[制限付き自動実行]
    L --> M[監査ログ]
    K --> M
    H --> M
```

この区分で最も重要なのは、**HITL を名目だけで置かない** ことである。自動化バイアスの研究は、人間が最終承認者として置かれていても、時間不足、UI設計、組織プレッシャー、根拠表示不足があると、実質的にはAIの推薦を追認しやすいことを示している。つまり、「人が最後に見る」だけでは統制にならない。人間が介入できるだけでなく、**介入に必要な情報、時間、権限、教育** が与えられて初めてHITLは機能する。[19]

知財実務では、この含意は大きい。たとえばクレーム案レビューに1件3分しか割けない体制は、運用名がHITLでも実質はHOTL未満である。逆に、先行技術調査の一次整理で、AIが検索式展開・クラスター分け・要約を行い、人間が偽陰性の多いパターンだけを重点監督する設計は、実質的には良質なHOTLになり得る。したがって、重要なのはラベル名ではなく、**人間がどこで、何を見て、どの閾値で止められるか** を定義することにある。[20]

知財業務プロセス別の適用比較

プロセス	HITL	HOTL	HOOTL	推奨デフォルト
特許出願	**例** 発明メモからのクレーム・明細書案作成。 **利点** 法的主張と記載要件を人が直接管理しやすい。 **主リスク** ボトルネック、レビュー工数増。	**例** 背景技術、実施形態整理、図面説明、用語統一の一次生成。 **利点** 下書き速度と整合性が向上。 **主リスク** 権利範囲の過広/過狭、サポート要件ズレ。	**例** 書式整形、分類候補、定型欄補完のみ。 **利点** 事務負荷軽減。 **主リスク** 未公開発明の外部投入、誤分類の放置。	**クレームと対外提出文言は HITL、周辺記述はHOTL、事務整形のみ HOOTL**

プロセス	HITL	HOTL	HOOTL	推奨デフォルト
先行技術調査	**例** 検索戦略、ノイズ除去、最終引用文献決定。 **利点** 防御可能性と再現性を確保しやすい。 **主リスク** 時間がかかる。	**例** 検索式拡張、類義語生成、クラスタリング、一次要約。 **利点** 網羅性と速度が上がる。 **主リスク** 偽陰性、英語偏重、サイレントミス。	**例** 重複排除、翻訳前処理、アラート配信。 **利点** 高スループット。 **主リスク** 欠落文献の見逃しに気づきにくい。	**HOTL中心、最終サーチメモはHITL**
特許審査対応	**例** 引用文献との差異主張、補正方針、補正文言。 **利点** 法的・技術的整合を維持。 **主リスク** 速度低下。	**例** OA要点抽出、証拠箇所抽出、応答案骨子の生成。 **利点** 準備時間短縮、忠実性向上余地。 **主リスク** もっともらしい誤論理、誤引用。	**例** 期限管理、方式指摘への定型応答案。 **利点** 事務の自動化。 **主リスク** 実体審査案件の誤分類。	**実体判断はHITL、証拠集約と骨子づくりはHOTL**
権利行使・侵害調査	**例** クレームチャート、均等論補助論点、無効化反論。 **利点** 紛争耐性が高い。 **主リスク** 高コスト。	**例** 証拠候補抽出、製品仕様からの要素対応一次マッピング。 **利点** 初動迅速化。 **主リスク** マッピング幻覚、証拠管理不備。	**例** 監視アラート、公開情報クロール、文書整理。 **利点** 大量監視に向く。 **主リスク** 誤警報/見逃し、説明責任不足。	**HITLを原則、HOTLは一次トリアージに限定**
契約・ライセンス	**例** 権利帰属、利用範囲、非保証、補償、監査条項のレビュー。 **利点** 責任配分を人が明確化。 **主リスク** スピード低下。	**例** 条項抽出、プレイブック照合、逸脱箇所検知。 **利点** 標準化と見落とし低減。 **主リスク** 背景事情を無視した誤警告/過小警告。	**例** 標準雛形へのメタデータ差し込み。 **利点** 定型契約の大量処理。 **主リスク** 非定型案件への誤適用。	**個別交渉はHITL、標準契約運用はHOTL、定型差込のみHOOTL**
機密管理	**例** 社外モデル投入の例外承認、越境移転判断。 **利点** 漏えい時の責任線が明確。 **主リスク** 業務摩擦。	**例** DLPアラート、外部共有審査、ラベル異常検知。 **利点** 継続監視が可能。 **主リスク** 過剰ブロック、例外処理滞留。	**例** 自動ラベリング、保持期間経過による削除、アクセス剥奪。 **利点** スケーラブルで監査しやすい。 **主リスク** 誤分類・誤削除。	**ルール化できる統制はHOOTL/HOTL、例外はHITL**

上表のうち、**特許出願** と **審査対応** については、学術研究が最も明確な示唆を与えている。クレーム生成研究は、特許クレームが通常の要約よりも高い構造性、精密な語法、論理的連結を必要とすると指摘し、現行モデルでも厳格な専門家修正が必要だとする。さらに、特許クレーム評価の研究は、クレームの良し悪しが「それらしく書けるか」ではなく、特徴網羅性、概念明確性、技術的一貫性、法的精密性で評価されることを示している。審査対応でも、RAGと知識グラフを組み合わせた特化システムが不忠実性を減らせる一方、最終的な補正・主張の適法性は人間が負うべきである。したがって、これらの工程をHOTLやHOOTLへ拙速に移すべきではない。 21

一方で、**先行技術調査** は生成AIの価値が比較的大きい。日本語の研究でも、シソーラスとLLMを組み合わせた検索語拡張が、従来資源と共起しにくい新語彙を補完し得ることが示されている。また、RAG型の特許類似検索は、専門家の初期負荷を下げる可能性が示されている。もっとも、偽陰性のコストは依然大きいた

め、検索式の最終決定、引用文献の採否、サーチメモの対外利用は人間が担うべきである。ここでは **HOTLが最も費用対効果が高い**。[22]

契約・ライセンス と **機密管理** では、日本の公式資料が重要である。経済産業省の契約チェックリストは、AI利活用契約における利益とリスクの適切な配分を目的にしており、特許庁のAIモデル契約書群も、権利帰属、利用権、精度保証、知財非侵害、追加学習、秘密情報範囲のような論点を具体化している。また、営業秘密・個人情報・著作権の観点からは、何を入力してよいか、どのログを保存すべきか、どの説明をベンダーから受けるべきかが導入判断の中心になる。したがって、契約と機密領域では、**AIの生成能力そのものより、境界設定と証跡設計が先に来る**。[23]

ガバナンス、コンプライアンス、説明責任の実装指針

知財部門のAIガバナンスは、少なくとも三層で設計すべきである。第一に **モデルガバナンス**。どのモデル、どの接続先、どのデータ領域が許可されるのか。第二に **案件ガバナンス**。どの案件をHITL/HOTL/HOOTLに配分し、誰が承認者になるのか。第三に **証拠ガバナンス**。どの出力が、どの入力、どの根拠文書、どのモデル版、どの承認者に基づいて生成されたかを後から検証できるのか。この三層がそろって初めて、AI事業者ガイドラインが求めるトレーサビリティとアカウンタビリティ、NISTが求める文書化・監査・人間監督、文化庁のチェックリストが求める記録保存・説明可能性が知財実務に落ちる。[24]

テーマ	最低限の実装	実務上の要点
業務分類	業務ごとにHITL/HOTL/HOOTLを指定	「特許は全部HITL」のような粗い設計ではなく、クレーム、検索、契約、秘密管理を分ける
データ境界	公知情報、社内限定、未公開発明、相手方秘密、個人情報を区分	未公開発明や相手方秘密は、消費者向けAIや保持設定不明の環境へ入力しない
ベンダー審査	学習利用有無、保持期間、地域、サブプロセッサ、濫用監視、監査ログを確認	「No training」だけでは不十分で、保持・監視・ログ連携まで確認する
プロンプト統制	承認済みテンプレートと禁止パターンを版管理	検索、クレーム、契約レビューは自由入力よりテンプレート運用が再現性を高める
検証設計	ゴールドセット、サンプリング監査、ドリフト確認、レッドチーミング	モデル変更時だけでなく、RAGコーパス更新時にも再評価する
監査ログ	入力、出力、モデル版、参照ソース、承認者、エクスポート、共有イベントを保存	後日の無効審判、係争、監査、インシデント対応に耐える粒度で残す
説明責任	RACIを明確化し、運用者・承認者・責任者を分離	「誰が最終判断したか」を案件単位で追えるようにする
例外処理	キルスイッチ、即時停止、再承認、証拠保全手順	HOTL/HOOTLでは例外キューが実質的な安全弁になる
契約管理	削除、終了後処理、知財非侵害、学習利用、監査協力、越境移転を条項化	とくにファイルアップロードや追加学習機能の権利・保持条件を見落とさない

実務上、**verifiability** は「AIが説明できること」では足りない。必要なのは、**出力を事後に再構成できること**である。最低限、案件ID、入力テンプレート版、モデル名・版、システムプロンプト版、参照コーパスのスナップショット、引用ソース、信頼度閾値、例外判定、承認者、共有/保存先を保存するべきである。文化庁のチェックリストは、学習データや意思決定過程の文書化・保存が事後確認に有益だと示しているし、AI事

業者ガイドラインも、データの出所と意思決定過程の追跡可能性を強調している。知財実務ではこの考え方をさらに強め、**「再現不能な出力は、権利を動かす工程に使わない」** を運用原則にすべきである。[25]

国際的な観点では、欧州委員会のAI Act Q&Aが、提供者・利用者にAI literacyを求めること、そして人間監督・透明性と結びつけて理解すべきことを示している。知財部門に置き換えれば、出願担当者、調査担当者、法務、セキュリティ、IT管理者は、それぞれ異なるAIリテラシーを要する。知財部のAI導入は、単なるツール導入ではなく、**役割別能力要件の設計** を伴う。[26]

導入時の評価基準と段階的移行ロードマップ

導入評価では、精度だけを見ると失敗する。知財実務で必要なのは、**精度・再現性・コスト・スループット・人的レビュー負荷・リスク許容度** を同時に測ることである。NISTやISOの文脈でも、AIリスク管理は単一KPIではなく、文書化、監視、インシデント対応、組織責任まで含む継続運用として扱われる。したがって、PoCの評価表には、少なくとも次の項目を含めるべきである。[27]

評価基準	具体的な測定例	HITL向きの状態	HOTL向きの状態	HOOTL向きの状態
精度	事実誤り率、引用正確性、クレーム要素漏れ率、検索再現率	誤差があっても人手で補正可能	安定して高精度、例外抽出が機能	ルール型で誤りが限定的かつ可逆
再現性	同一入力での出力ばらつき、テンプレート間差	ばらつきを人手で吸収	ばらつきが閾値内に収まる	ほぼ固定的・決定論的
コスト	1案件あたりのAPI費・人件費・監査費	高コストでも許容	人手削減で改善	大量処理で明確に低下
スループット	週次処理件数、期限遵守率	小規模でも可	中〜大規模で改善	大規模・定型で大幅改善
人的リソース	専門家レビュー時間、必要スキル	専門家フルレビュー前提	例外・サンプルレビュー中心	監査担当が定期確認するだけで回る
リスク許容度	誤り時の法的/財務/信用影響	低許容度案件向き	中程度の許容度	低リスク・可逆案件に限定
セキュリティ適合性	保持設定、DLP連携、監査ログ、地域制御	例外承認前提	ログと境界統制が機能	完全なログ、制限付きアクション、停止手段必須

上表を実務で使う場合、判断の実際はこうなる。**HITL** は「精度が低いから使う」のではなく、「誤りのコストが大きいから使う」。**HOTL** は「精度が一定以上で、例外を抽出できるから使う」。**HOOTL** は「タスクが可逆で、操作が限定され、ログが完全で、停止できるから使う」。この順序を逆にして、先に自動化率を決めると失敗しやすい。[28]

以下は、知財部門での段階的導入案である。NIST AI RMFの文書化・評価・監視の循環、ISO 42001/23894の管理システム的な実装、AI事業者ガイドラインの「why / what / how」を知財実務に落とし込むと、いきなりHOTLやHOOTLへ進むのではなく、まず **HITLで計測可能な基準を作り、その後にHOTLを拡張し、最後に限定HOOTLへ進む** 形が最も堅実である。[29]

```
gantt
    title 知財部門向け段階的導入ロードマップ
    dateFormat  YYYY-MM-DD
    axisFormat  %m月
    section 基盤整備
    業務棚卸し・データ分類・禁止入力設定        :a1, 2026-05-01, 45d
    ベンダー審査・監査ログ・保持設定整備        :a2, after a1, 30d
    section HITLパイロット
    出願ドラフト・審査対応のHITL運用            :b1, 2026-07-01, 60d
    ゴールドセット作成・評価基準確定            :b2, after b1, 20d
    section HOTL拡張
    先行技術調査・契約レビュー一次処理のHOTL化   :c1, 2026-09-01, 75d
    例外キュー・サンプリング監査運用             :c2, after c1, 20d
    section HOOTL限定運用
    メタデータ付与・通知・保持/DLP自動化         :d1, 2026-11-15, 60d
    section 定着
    KPI監査・ドリフト再評価・標準化              :e1, 2026-12-15, 75d
```

段階	到達目標	次段階へ進む条件
基盤整備	どの業務をどのモードで回すかを定義し、禁止入力と承認済みツールを明確化	データ境界、保持設定、監査ログ、責任者が確定
HITLパイロット	出願・中間対応で「AIを使っても説明可能」な状態を作る	精度評価、レビュー時間、誤り類型が可視化
HOTL拡張	検索・契約一次処理で例外監督が成立する	例外抽出精度とサンプリング監査が安定
HOOTL限定運用	可逆的な定型処理のみを自動実行	監査ログ完全性、停止手順、障害時巻戻しが確認済み
定着	KPI監査と変更管理を含む運用標準が確立	モデル変更時の再評価手順が制度化

ツール・サービス例と短評

以下の短評は、主として公式資料ベースで整理したものであり、採用可否は自社のゴールドセット評価、セキュリティ質問票、契約条項確認を前提とする。ベンダーの「高精度」「高セキュア」は自己記述であるため、**公式機能の確認** と **自社PoCの成績** は分けて読むべきである。 [30]

生成AIプラットフォーム

- OpenAI [31] の ChatGPT Enterprise / API Platform は、業務データについて既定で学習に使わず、保持期間を制御でき、SOC 2 監査済みである。さらに、Enterprise / Edu向けの Compliance Platform は、ワークスペースのログとメタデータを eDiscovery、DLP、SIEM に接続でき、append-only のコンプライアンスログを提供する。**短評**: 幅広い知財文書処理と統合性で有力だが、実務投入時は Compliance API と保持設定を前提にすべきであり、コンシューマ設定の延長で使うべきではない。 [32]

- Microsoft [33] の Azure OpenAI / Foundry は、入出力や埋め込みを他顧客や基盤モデル改善に使わず、Azure環境内で提供される一方、サービス提供と不正使用監視のための処理・保存があり、Azure Monitor でログとメトリクスを扱える。**短評**: Microsoft基盤と統合しやすく、地域・監視設計を取りやすい。知財部門では、機密文書を含むRAG基盤や統合監査に向くが、濫用監視・保存の条件は契約前に精査したい。 [34]

- Google [35] の Gemini for Google Cloud は、プロンプトや応答をモデル訓練に使わず、監査ログの仕組みを持つ。Google自身が、もっともらしいが事実と異なる出力があり得るので利用前に検証すべきだと明示している。**短評**: Google Cloud中心の開発・ドキュメント環境には適合しやすいが、知財用途では引用付きRAGと人間検証を合わせる前提が必要である。 [36]

- Anthropic [37] の Claude Enterprise は、監査ログのエクスポート、Compliance API、カスタム保持期間設定を提供し、監査ログは直近180日分をエクスポートできる。一方で、保持設定を行わない限りデータは既定で無期限保持であり、機能によっては零保持の対象外もある。**短評**: 長文文書や契約レビューには強い選択肢だが、保持設定とファイル機能の例外条件を詰めてから導入すべきである。 [38]

- NTT [39] の tsuzumi 2 は、高性能・高セキュア・低コストな国産LLMとして、公衆環境とクローズ環境を含む複数の業務形態に最適化した導入をうたう。**短評**: 日本語性能と国内運用志向を重視する企業に適する可能性が高い。知財文書の国内保持や日本語の細かな語感を重視する組織でPoC価値がある。 [40]

- NEC [41] の cotomi は、日本語性能、高速性、専用ハードウェア・データセンター・APIなどの柔軟な提供形態を打ち出している。**短評**: 機密性要件に応じて配置を変えたい企業、特に国内大企業・公共寄りの運用に親和的である。 [42]

- 富士通 [43] の Fujitsu Kozuchi は、企業向け生成AIとして機密情報保護機能や独自のハルシネーション検出を訴求している。**短評**: 幻覚検出やプライベート環境志向を重視する場合に検討価値があるが、実際の有効性は自社文書での評価が不可欠である。 [44]

特許検索・分析ツール

- INPIT [45] の J-PlatPat は、日本の特許・実用新案・意匠・商標の基礎情報を扱う公的基盤であり、国内案件の法的状態確認の起点として不可欠である。**短評**: 無料で信頼性が高いが、グローバルFTOやNPL横断には補完ツールが必要である。 [46]

- 欧州特許庁 [47] の Espacenet は、1.6億件超の文献、Patent Translate、AI-based CPC text categorizer を提供する。**短評**: 無料系では非常に強力で、概念探索と多言語検索に向く。日本担当者のグローバル探索能力を底上げしやすい。 [48]

- PATENTSCOPE は、PCT文献に加え、各国データやNPL連携、AI Index などを提供する。**短評**: 国際出願や技術トレンド監視に有用で、WIPO系データの起点として価値が高い。 [49]

- PatSnap [50] の PatSnap / Eureka は、検索、ドラフティング、OA対応、商機分析までをAIネイティブに統合する方向を打ち出している。**短評**: ワークフロー一体化の魅力は大きいが、生成した法的推論部分は必ずHITLに戻すべきである。 [51]

- Clarivate [52] の Derwent Patent Search は、ヒューマンオーサードの要約、40の特許庁で使われるデータ、FTO/有効性検索への強みを訴求する。**短評**: 高リスク案件の検索品質重視に適し、特にFTO・無効資料探索で信頼性が高い。 [53]

- Questel [54] の Orbit Intelligence は、特許・意匠・NPL、実質的な権利者情報、法的ステータス、ライセンス・係争連携を提供する。**短評**: 検索と権利活用分析を横断したい企業に向く。権利者同定と法的状態の信頼性を重視する用途で有力である。 [55]

- LexisNexis [56] の PatentSight+ は、可視化と競合・ポートフォリオ分析に強みを置く。**短評**: 先行技術調査の一次工具というより、経営・IP戦略向けのポートフォリオ評価に向く。 [57]

データ管理・統制ツール

- Microsoft Purview は、統合監査ログ、DLP、秘密度ラベルを提供し、機密データの分類・保護・調査フローを統合できる。**短評**: Microsoft中心の情報基盤では、知財文書のラベリング、監査、DLP運用の中核になりやすい。 [58]

- Box [59] の Box は、法的保持、監査証跡、外部共有制御、DLPを提供する。**短評**: 文書共有と監査証跡を強く保ちたい企業に向く。外部共同研究や契約交渉文書の管理に相性がよい。 [60]

- iManage [61] は、監査証跡と厳格なDMS運用を前面に出す。**短評**: 法務・知財に近い文書文化を持つ組織、特に法律事務所型の運用には適している。 [62]

- NetDocuments [63] の ndMAX / Legal AI Assistant は、監査証跡やガードレールと組み合わせた法務AIを打ち出す。**短評**: 契約・法務ドメイン寄りだが、ライセンスや共同研究契約レビューの知財法務には応用しやすい。 [64]

実務担当者向けチェックリスト

以下のチェックリストは、AI事業者ガイドライン、NIST AI RMF、ISO 42001/23894、WIPOガイド、文化庁チェックリスト、営業秘密・個人情報関連資料を、知財実務向けに再構成したものである。 [65]

導入前は、まず **業務分類、データ境界、契約条件、評価設計** を固めるべきである。 [66]

- [ ] 業務を「権利範囲を動かす工程」「高頻度支援工程」「定型事務工程」に分け、HITL/HOTL/HOOTLを割り当てた。
- [ ] 未公開発明、営業秘密、相手方秘密、個人情報について、入力禁止・要承認・許可済みの三区分を決めた。
- [ ] ベンダーごとに、学習利用、保持期間、監査ログ、DLP/SIEM連携、地域、サブプロセッサを確認した。
- [ ] 出願、調査、契約レビューごとにゴールドセットと評価KPIを定めた。
- [ ] 承認者、運用者、監査担当、インシデント責任者のRACIを定義した。
- [ ] 契約で、削除、終了後処理、学習利用、監査協力、知財リスク配分を確認した。

導入中は、**説明可能な運用** を作ることが重要である。AIを回すこと自体ではなく、どの出力がなぜ採用されたかを残すことが主眼になる。 [67]

- [ ] すべての重要出力に、参照ソースまたは根拠文書を紐づけた。
- [ ] モデル名・版、プロンプト版、RAGコーパス版、承認者、共有ログを保存した。
- [ ] HOTL工程では、閾値超過・例外・サンプリング監査の仕組みを運用した。

- [ ] HITL工程では、レビュー所要時間と差戻し理由を記録した。
- [ ] 監督者に、自動化バイアス、誤引用、秘密情報入力ミスの教育を実施した。
- [ ] モデルまたはコーパス変更時に、即時再評価ルールを適用した。

導入後は、**拡大条件の管理** が重要である。精度が良いから拡大するのではなく、誤り類型が理解され、例外処理が機能し、停止できることを確認してから次段階へ進むべきである。 [68]

- [ ] 月次で、誤り率、差戻し率、レビュー時間、期限遵守率、近接インシデントを監査した。
- [ ] ベンダーの保持ポリシー、機能追加、監査ログ仕様の変更を定期点検した。
- [ ] 対外提出案件について、提出後に根拠パックを保全した。
- [ ] HOOTL工程は、低リスク・可逆・制限付きアクションに限っていることを確認した。
- [ ] 新規業務へ拡張する前に、既存業務での例外処理と停止手順が実際に機能したことを確認した。
- [ ] 係争・監査・説明要求に備え、案件単位で「誰が、どの根拠で、どのAI出力を採用したか」を再現できる状態を維持した。

---

[1] [13] https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/02/oecd-framework-for-the-classification-of-ai-systems_336a8b57/cb6d9eca-en.pdf
https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/02/oecd-framework-for-the-classification-of-ai-systems_336a8b57/cb6d9eca-en.pdf

[2] [12] [21] [35] https://aclanthology.org/2025.findings-naacl.70.pdf
https://aclanthology.org/2025.findings-naacl.70.pdf

[3] [15] [56] https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20260331_1.pdf
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20260331_1.pdf

[4] [26] [39] [63] https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers
https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers

[5] [61] [64] https://www.netdocuments.com/solutions/legal-ai/
https://www.netdocuments.com/solutions/legal-ai/

[6] [16] https://www.bunka.go.jp/seisaku/chosakuken/aiandcopyright.html
https://www.bunka.go.jp/seisaku/chosakuken/aiandcopyright.html

[7] [28] https://airc.nist.gov/airmf-resources/playbook/govern/
https://airc.nist.gov/airmf-resources/playbook/govern/

[8] [30] https://www.wipo.int/publications/en/details.jsp?id=4713
https://www.wipo.int/publications/en/details.jsp?id=4713

[9] [34] https://learn.microsoft.com/ja-jp/azure/foundry/responsible-ai/openai/data-privacy
https://learn.microsoft.com/ja-jp/azure/foundry/responsible-ai/openai/data-privacy

[10] [48] https://www.epo.org/en/searching-for-patents/helpful-resources/patent-knowledge-news/why-switch-current-espacenet-version
https://www.epo.org/en/searching-for-patents/helpful-resources/patent-knowledge-news/why-switch-current-espacenet-version

[11] [23] [31] [37] [66] https://www.meti.go.jp/press/2024/02/20250218003/20250218003.html
https://www.meti.go.jp/press/2024/02/20250218003/20250218003.html

[14] [44] [54] https://documents.research.global.fujitsu.com/chat-gen-ai/
https://documents.research.global.fujitsu.com/chat-gen-ai/

17 18 41 68 https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/1.html
https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/1.html

19 https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/automation-bias-in-the-ai-act-on-the-legal-implications-of-attempting-to-debias-human-oversight-of-ai/C97C85015056C09326944DE55CBC4D2C
https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/automation-bias-in-the-ai-act-on-the-legal-implications-of-attempting-to-debias-human-oversight-of-ai/C97C85015056C09326944DE55CBC4D2C

20 https://airc.nist.gov/airmf-resources/playbook/map/
https://airc.nist.gov/airmf-resources/playbook/map/

22 https://www.jstage.jst.go.jp/article/pjsai/JSAI2024/0/JSAI2024_4A1GS605/_article/-char/en
https://www.jstage.jst.go.jp/article/pjsai/JSAI2024/0/JSAI2024_4A1GS605/_article/-char/en

24 52 65 67 https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20260331_10.pdf
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20260331_10.pdf

25 https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/seisaku/r06_02/pdf/94089701_05.pdf
https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/seisaku/r06_02/pdf/94089701_05.pdf

27 29 https://www.iso.org/standard/42001
https://www.iso.org/standard/42001

32 https://openai.com/enterprise-privacy/
https://openai.com/enterprise-privacy/

33 43 49 https://www.wipo.int/en/web/patentscope
https://www.wipo.int/en/web/patentscope

36 47 https://docs.cloud.google.com/gemini/docs/discover/data-governance
https://docs.cloud.google.com/gemini/docs/discover/data-governance

38 50 https://support.claude.com/en/articles/9970975-access-audit-logs
https://support.claude.com/en/articles/9970975-access-audit-logs

40 https://group.ntt/jp/newsrelease/2025/10/20/251020a.html
https://group.ntt/jp/newsrelease/2025/10/20/251020a.html

42 45 https://jpn.nec.com/LLM/index.html
https://jpn.nec.com/LLM/index.html

46 https://www.inpit.go.jp/j-platpat_info/index.html
https://www.inpit.go.jp/j-platpat_info/index.html

51 https://www.patsnap.com/
https://www.patsnap.com/

53 https://clarivate.com/intellectual-property/derwent/patent-search/
https://clarivate.com/intellectual-property/derwent/patent-search/

55 https://www.questel.com/patent/ip-intelligence-software/orbit-intelligence/
https://www.questel.com/patent/ip-intelligence-software/orbit-intelligence/

57 https://www.lexisnexisip.com/solutions/ip-analytics-and-intelligence/patentsight/
https://www.lexisnexisip.com/solutions/ip-analytics-and-intelligence/patentsight/

58 https://learn.microsoft.com/ja-jp/purview/audit-solutions-overview
https://learn.microsoft.com/ja-jp/purview/audit-solutions-overview

59 62 https://imanage.com/resources/customer-stories/robbins-russell/
https://imanage.com/resources/customer-stories/robbins-russell/

60 https://www.box.com/en-gb/security/governance-and-compliance/self-governance
https://www.box.com/en-gb/security/governance-and-compliance/self-governance