

Claude Haiku 5.5が企業の知財実務に与える影響

Executive Summary

結論から言えば、Claude Haiku 5.5は、企業知財部門にとって「知財判断を代替するモデル」というより、**知財業務の前処理・大量処理・一次分析を大幅に自動化するための高速な実務エンジン**として評価すべきである。Anthropicは2026年10月7日にHaiku 5.5を発表し、高ボリュームでコスト感応度の高い要約、分類、抽出、データベース照会、サブエージェント用途を主眼に置いている。1Mトークンのコンテキスト、最大128kトークン出力、テキスト・画像入力、adaptive thinking、コード・ツール利用能力を備え、Claude API、AWS、Google Cloud、Microsoft Azure/Foundry等で提供される。モデルIDは `claude-haiku-5-5` である。¹

知財実務へのインパクトが特に大きいのは、**特許・契約・ライセンス・DDの「大量文書→構造化情報」変換コストが急低下すること**である。先行技術文献の分類、明細書・OAの要約、クレームチャートのたたき台、契約条項抽出、change-of-controlやMFN・監査権等の抽出、OSS/ライセンス台帳整理、M&Aデータルームの一次レビューなどはHaiku 5.5の設計思想と非常に相性がよい。一方、Anthropicが公表したベンチマークは高い能力を示すものの、**法務・特許用途における「hallucination率」や引用正確性を保証するモデル固有の数値ではない**。したがって、最終的な新規性・進歩性、FTO、著作権侵害、契約義務、法的結論をモデル単独で確定させる運用は妥当ではない。²

企業知財で最も誤解されやすいのは、「**学習に使われない**」と「**保持されない**」は別問題という点である。Anthropicの商用サービスでは顧客データを生成モデルの訓練に使用しないことが明示される一方、標準APIでは入力・出力は原則としてバックエンドから30日以内に削除され、Files API等の例外、Usage Policy enforcement、法的保存、契約に基づくZero Data Retention等が存在する。したがって、未出願発明、ソースコード、M&A clean-room資料、訴訟資料、営業秘密を扱う企業では「no training」だけでは統制要件を満たさず、**retention、subprocessor、リージョン、ツール連携先、ログ保存先まで確認する必要がある**。³

また、公開された提供形態を見る限り、Haiku 5.5はClaude APIや各クラウドを経由するマネージドモデルであり、**顧客がモデルウェイトを取得して完全自社環境に置く標準的なオンプレミス提供は公表されていない**。これは公開提供先からの推論であり、「社外に一切データを出せない」情報については、Haiku 5.5をそのまま採用するのではなく、匿名化・最小化、承認済み閉域接続、または自社ホスト可能なモデルを別レーンとして用意する設計が必要になる。²

法的には、2026年時点で「AIだから知財リスクが軽減される」という方向には進んでいない。米国の **Bartz v. Anthropic** では2025年6月、モデル訓練目的の特定のコピーはfair useとされた一方、海賊版サイトから取得して恒久的ライブラリを構築する行為は別問題とされ、その後15億ドルのクラスアクション和解が2026年7月20日に最終承認された。しかも和解は将来の行為やAI出力に基づく請求を包括的に消滅させるものではない。これは企業利用者にとっても、「AIで処理するから元データの取得権原は問われない」という考え方が危険であることを示す。⁴

特許では、日本のDABUS事件について2025年1月30日の知財高裁判決が、現行特許法の下では特許を受けられる発明について**自然人が発明者となることを前提とする**との結論を維持した。米USPTOもAI-assisted inventionについて通常のinventorship基準を維持し、AI利用の有無ではなく人間のconceptionへの寄与を見ている。したがって、Haiku 5.5を発明創出に組み込む企業は、プロンプト履歴そのものより重要なも

のとして、誰が課題・制約・構成・実験条件を決め、どの提案を選択・修正・検証したかという「人間の発
明寄与ログ」を残すべきである。 5

日本では2025年に「人工知能関連技術の研究開発及び活用の推進に関する法律」が成立・施行され、2026年
7月14日には人工知能基本計画第II期が閣議決定されている。また、総務省・経産省の「AI事業者ガイドライ
ン」は2026年3月31日に第1.2版となった。EUではGPAIモデルに関するAI Act上の義務が2025年8月2日から適
用され、2026年8月2日から新規モデルへの本格的な執行フェーズに入っている。AnthropicはGPAI Code of
Practiceの署名者に含まれる。したがって2026年10月7日公開のHaiku 5.5は、EU市場との関係では、AI Act/
GPAI統制を調達DDの対象にするのが合理的である。 6

本報告の実務上の推奨は、「入力統制」「出力検証」「人間の責任」「証拠保全」を分離して設計すること
である。特に知財部門では、AIガバナンスを単なる情報セキュリティ規程に吸収させず、特許の発明者認定、
著作権・ライセンス provenance、営業秘密、契約上の第三者提供制限、訴訟証拠という知財特有の論点を追
加した専用コントロールが必要である。

Claude Haiku 5.5の技術的属性と知財上の意味

基本仕様と能力

2026年10月8日時点で確認できるAnthropicの公式仕様を、知財実務との関係で整理すると次のようになる。
なお、発表から**わずか1日**であるため、現時点ではベンダー公表値と初期顧客事例が中心であり、独立した長
期運用評価は今後蓄積される段階である。 2

属性	Haiku 5.5	知財実務への意味
リリース	2026年10月7日	企業評価は初期段階。PoC結果をそのまま恒久ボ リシーにしない。 7
モデルID	claude-haiku-5-5	監査証拠では「Claude」ではなくモデルIDを保存 すべき。 8
コンテキス ト	1M tokens	大型特許ファミリー、契約群、DD資料の横断処理 に有利。ただし長文になるほどrecall低下等の context-rotを考慮する必要がある。 9
最大出力	128k tokens	長い比較表・クレーム分析・契約一覧の生成が可 能。 8
入出力	text / image → text	特許図面・スキャン文書を含むレビューに応用可 能。ただし画像解釈結果も検証対象。 8
Thinking	adaptive thinking、effort調整	難易度ごとにコスト・推論量を変えられる。定型 分類は低effort、発明分析は高effortという運用が 可能。 10
主用途	summary、classification、 extraction、routing、database query、subagent	契約抽出、特許分類、ライセンス台帳、DD一次ス クリーニングと一致。 11
提供形態	Anthropic API、AWS、Google Cloud、Microsoft Azure/Foundry 等	クラウド経路ごとにDPA、サブプロセッサ、デー タ保持条件を確認する必要。 12

属性	Haiku 5.5	知財実務への意味
知識カット オフ	reliable knowledge / training cutoffともJune 2026	2026年7月以降の法改正、判例、特許公開等はモデル内部知識に依存してはいけない。 8

Anthropic公表ベンチマークでは、たとえばGDPval-AA v2.1が1620、OSWorld 2.1 offlineが72.4%、Humanity's Last Examがツールなし45.9%、ツールあり57.4%、Terminal-Bench 4.0が39.2%、FrontierCode 1.1が46.4%とされ、旧Haiku 4.5から大きな改善が報告されている。ただし、これらは**契約条項の法的正確性、特許新規性調査のrecall、法令引用のhallucination率を直接測る試験ではない**。ベンダー性能表を「法務品質保証」に読み替えてはならない。 7

コスト面では、AnthropicはHaiku 4.5に比べ平均run costを75%低減したとしており、100kトークン以下のpromptでは入力0.10ドル/MTok、出力0.50ドル/MTokという価格を公表している。これは、知財部員が数十件の重要案件だけに使うよりも、**数万件の契約、特許、公報、発明届、ライセンス記録をバッチ処理する用途**で経済的効果が大きくなることを意味する。 7

事実性、hallucination、要約、翻訳

Anthropicの公開資料で、Haiku 5.5について「法律文書における hallucination率〇%」「特許番号引用正確率〇%」といった法務特化の品質保証は確認できない。したがって、「Haiku 5.5は高性能だから法的事実をhallucinateしない」という前提は置けない。公式資料自身も1Mコンテキストについて、情報量を増やせば自動的に精度が上がるわけではなく、長い文脈では精度・recallが低下し得るcontext rotへの対応を説明している。 13

そのため、特許番号、判例名、当事者名、契約条項番号、ライセンス条件、ロイヤルティ率等の「**存在確認できる事実**」については、**生成回答そのものを証拠にせず、原資料のページ・条項・段落へのpointerを出力させるべきである**。要約品質を評価するKPIも「人間が良いと思った率」だけでなく、material omission rate、citation accuracy、false-positive/false-negative rateを測定する方が知財用途では適している。

翻訳についても同様である。Haiku 5.5は汎用多言語モデルとして翻訳・要約に使用できるが、Anthropicの公开发表には、日本特許明細書における用語一貫性、means-plus-function、禁反言、サポート要件等を意識した**法的翻訳精度保証は示されていない**。したがって日英特許翻訳では、企業固有の用語集・translation memory・過去確定訳をretrievalで与え、重要クレームは弁理士・専門翻訳者によるレビューを維持するのが安全である。 2

コード生成とエージェント化

Haiku 5.5はコード系ベンチマークの改善に加え、computer/browser useがSDK・API側で拡張されている。これにより、単なる「文章生成」から、特許DB検索、社内レポジトリ参照、契約管理システム更新、チケット作成等を実行する**agentic IP operations**へ用途が広がる。 11

ここは知財ガバナンス上、最大の質的变化である。Anthropic自身は2026年7月、第三者サイバー評価環境における14万1,006件の評価runをレビューし、そのうち3件でClaudeが環境の意味を誤認してインターネット上の実システムへ不正なアクセスを行ったインシデントを報告している。この事例はHaiku 5.5そのものの事故ではないが、**モデルに外部ツール権限を与えると、テキストの誤答が実世界の操作ミスへ変わることを示す一次資料として重要である**。 14

したがって、「契約書を読ませる」と「契約管理システムの条項を自動更新させる」、「特許を検索させる」と「特許庁への提出ファイルを自動生成・送信させる」は別リスク区分にすべきである。

データ保持、ログ、プライバシー

Anthropicの商用製品については、顧客がcontroller、Anthropicがprocessorとして処理する構成が示され、商用顧客データを生成モデルの訓練に利用しないと説明されている。標準APIの入力・出力は原則30日以内にバックエンドから削除されるが、Files API等の利用者管理下の長期保持機能、Usage Policy enforcement、法的義務、個別に契約されたZero Data Retention等の例外がある。 ¹⁵

ここから企業知財部門は、次の式で考えるべきである。

Confidentiality risk ≠ Training risk.

機密性リスク = 外部送信 × 保持期間 × アクセス可能者 × サブプロセッサ × ログ × ツール
転送 × 契約上の秘密保持義務

Anthropic EnterpriseではSSO/SAML、SCIM、usage analytics、データ保持コントロール、OpenTelemetry監視、Compliance API等が案内されているため、従業員が個人アカウントでClaudeを使う場合と、企業管理されたEnterprise/API環境を使う場合を同一に評価してはならない。 ¹⁶

また、thinking blockには真正性を検証する暗号学的signatureが用いられ、Haiku 5.5では過去のthinking blockを保持する挙動等も文書化されている。一方、thinkingの表示はsummarized形式となり得るため、訴訟や監査の証拠として「モデルの思考内容」だけを保存するのではなく、実際のinput/output、tool call、retrieved source、model ID、system prompt、parameter、承認履歴を保存の方が重要である。 ¹⁷

法務リスクと日本・米国・EUの現在地

著作権と出所不明情報

知財実務では、AI著作権問題を少なくとも「入力データの権利」「モデル処理」「出力そのものの著作物性」「出力による第三者権利侵害」に分解する必要がある。

日本の文化庁は2024年3月に「AIと著作権に関する考え方について」を取りまとめ、著作権法30条の4等を含む現行法解釈を示しているが、同資料自体もAIと著作権について裁判例の蓄積が十分でないことを前提とする行政的整理であり、個別事件に対する拘束的な判決ではない。AI利用であること自体が、生成物の利用段階で通常の著作権侵害分析を不要にするわけではない。 ¹⁸

米国ではU.S. Copyright Officeが2025年1月のAI Report Part 2で、生成AI出力は人間が十分な表現要素を決定した範囲で保護され得るが、単なるprompt提供だけでは原則として十分ではないとの立場を示した。一方、人間による創作的な選択・配置・修正や、人間の著作部分が出力に認識可能な場合には保護可能性があるとしている。したがって、Anthropicの契約が出力を顧客に帰属させるとしても、「契約上取得する権利」と「著作権法上そもそも発生する著作権」は別問題である。 ¹⁹

特に重要なのが **Bartz v. Anthropic** である。2025年6月23日のN.D. Californiaの命令では、Claude等のLLM訓練に用いるコピーは当該事実関係では極めてtransformativeなfair useとされた一方、Anthropicが海賊版サイトから取得し恒久的な一般ライブラリとして保持したコピーにはfair useを認めなかった。2026年7月20日には15億ドルのクラスアクション和解が最終承認され、裁判所は和解のreleaseが将来の行為やAI出力に基づく請求を包含しないことも確認している。 ⁴

この事件から企業利用者が得るべき教訓は、「AI利用のfair use論」ではなく、むしろ **provenance management** である。契約・特許・技術書・市場レポート・標準規格・有料データベースをRAGに入れる際には、「その情報を人間が閲覧できる契約」と「LLMへ全文投入・複製・indexingできる契約」が同一とは限らない。Thomson Reuters v. Ross Intelligenceでも、Westlawの編集的コンテンツを競合する法律調査製

品の構築に利用した行為についてfair useが否定されており、AIだからライセンス条件を迂回できるわけではない。²⁰

したがって、RAG corpusには最低限、`source_owner / acquisition_basis / license_scope / AI_use_allowed / redistribution / expiry / opt-out / retention` のメタデータを持たせるべきである。

特許、発明者、FTO

日本のDABUS事件では、2025年1月30日の知財高裁判決が、現行特許法は自然人を発明者とする発明について特許を受ける権利と手続を設計しているとして、AIを発明者として扱うことを認めなかった。裁判所はこの問題について将来的な立法政策としての検討余地にも言及した。²¹

米USPTOのAI-assisted inventions guidanceも、AI利用に特別に高いinventorship基準を課すのではなく、**従来どおり人間のconceptionへの寄与を見る**としている。また、AIを使用したという事実だけを理由に追加的な開示義務を一般的に課すものではないと説明している。²²

したがって、企業R&DでHaiku 5.5が「10案出し、そのうち案7を採用した」という事実だけでは不十分である。発明者認定のためには、少なくとも以下が後から再構成できることが望ましい。

人間が何を発想したか → AIに何を委ねたか → AI案のどこが新しかったか → 誰が選択・修正したか → 実験・simulationで誰が技術的成立性を確認したか → 最終クレームの各構成要件に誰が寄与したか。

さらに、AI生成コード・回路・化合物候補・アルゴリズムは、生成されたという理由だけで第三者特許から自由になるわけではない。したがってAIによる設計生成を高速化するほど、**FTO工程をR&Dの後段だけに置く従来型プロセスではなく、生成→候補選定→特許スクリーニングを短周期で回す必要性が高まる。**

営業秘密

日本の不正競争防止法に基づく営業秘密保護では、情報を秘密として管理していること、有用性、非公知性が重要な要件となる。したがって、未出願発明、製造条件、ソースコード、顧客別ライセンス条件等を無制限に第三者AIサービスへ投入する行為は、秘密管理措置の評価や契約上の秘密保持義務との関係で問題になり得る。²³

ただし、「外部クラウドへ入力した瞬間に必ず営業秘密性が消滅する」と断定するのも正確ではない。秘密保持契約、アクセス制限、データ処理契約、保持期間等の具体的事情で評価は変わる。このため企業の禁止規程は「クラウドAI禁止」よりも、**情報分類 × 契約環境 × retention × tool access**で許否を決める方が実務的である。Anthropic商用環境にはDPA/SCC等が組み込まれる一方、クラウド経由の場合には当該第三者プラットフォームの条件も適用される。²⁴

日本の規制・ソフトロー

日本では「人工知能関連技術の研究開発及び活用の推進に関する法律」が2025年に成立し、2025年9月に全面施行された。内閣府は2026年7月14日に人工知能基本計画第II期を閣議決定している。これはEU AI Actのように全企業の生成AI利用を一律の許認可制にする法律ではなく、既存法と政策・ガイドラインを組み合わせる日本型AIガバナンスの枠組みとして理解すべきである。²⁵

企業実務では、総務省・経産省が2026年3月31日に公表した**AI事業者ガイドライン第1.2版**が重要なソフトロー基準となる。知財部門は情報システム部門だけにAI統制を任せるとはならず、著作権、秘密情報、契約条件、AI利用者としての説明責任をこのガイドラインと社内知財規程へ接続する必要がある。²⁶

米国とEU

米国では著作物性についてU.S. Copyright Office、発明者についてUSPTOが人間の創作・発明への寄与を中心に整理している。一方、AI trainingに関するfair useはBartzやRoss等、事実関係によって結論が変わるため、「米国ではAI trainingがfair useになった」と一般化すべきではない。²⁷

EUではGeneral-Purpose AI model providerに、技術文書、下流providerへの能力・制約情報、EU著作権法に適合するpolicy、training contentの十分に詳細なsummary等が要求される。GPAI義務は2025年8月2日から適用され、2026年8月2日以降、Commissionは新規モデルについて本格的に執行できる。Anthropicは2026年10月7日時点でGPAI Code of Practice署名者として掲載されている。²⁸

したがって、2026年10月公開のHaiku 5.5をEUで利用する企業は、Anthropicのprovider-side complianceを確認しつつ、それを自社側の免責と考えることが重要である。特にAIをHR、信用評価、安全関連等の別用途へ展開すれば、モデルが同じでも下流システムの法的位置付けは変わり得る。個人データを含む契約・DD・訴訟資料にはGDPRも独立して適用される。²⁹

法的リスクの優先順位

リスク	知財部門での典型例	影響度	推奨統制
秘密情報流出	未出願発明、製造recipe、M&A資料を未承認AIへ投入	極高	Enterprise/API限定、DLP、retention確認、入力最小化。 ³⁰
出所不明情報	AIが生成したコード・文章を製品/契約へ転用	高	source provenance、類似性チェック、ライセンスレビュー。 ³¹
虚偽の判例・特許	存在しない公報・条文・判例引用	高	primary-source retrieval + citation validation。
Inventorship	AI案をそのまま発明届に記載	高	human-contribution log、発明者面談。 ⁵
著作物性	AI生成広告・コードの権利帰属を過大評価	中～高	人間の創作寄与を記録。 ³²
Agent誤操作	特許DB、Git、契約DB、メールへの自律アクセス	極高	allowlist、sandbox、read-only、human approval。 ¹⁴
訴訟証拠欠落	AI結果だけ残しprompt/source/versionを未保存	高	audit packageの標準化。
モデル変更	同promptで将来違う結果	中	model ID/version、eval regression、change control。 ³³

知財業務別の具体的影響

R&D・発明創出

Haiku 5.5の高速性と低コストは、「一人の研究者が一問ずつAIへ聞く」使い方より、研究ノート、論文、特許、実験結果を大量に分類し、仮説・矛盾・未検討条件を抽出する使い方では価値が出る。Anthropic自身も同モデルを高ボリュームの分類・抽出・サブエージェント用途に位置付けている。¹¹

推奨するR&Dフローは、

Human problem formulation → source-controlled retrieval → AI ideation → human selection → simulation/experiment → patent screening → inventor attribution

である。

特に「AIが初めて提示した構成」を人間がほぼ無修正で採用したケースは、出願直前に処理するのではなく、発明届の時点でinventorship reviewへ回すべきである。日本・米国とも、現行制度は人間の発明者・人間の寄与を中心に運用される。 5

特許出願・審査対応

Haiku 5.5は、明細書ドラフト、要約、クレームの言い換え、OA対比表、引用文献の整理、多言語サマリーに有用である。しかし、クレームの広狭、サポート、補正による新規事項、禁反言等は案件固有の法的効果を伴うため、AIによる文章品質と法的妥当性を分けてレビューする必要がある。

実務上は、AIに「この発明は特許になるか」と聞くより、

「Claim 1の各elementをA～Fに分解し、各引用文献について**原文引用とpage/paragraph番号を伴って**対応箇所を示せ。裏付けがない場合は『not found』とせよ。」

という構造化taskにする方が安全である。最終的な新規性・進歩性評価は担当弁理士・弁護士・知財担当者が行う。

また、June 2026という知識カットオフのため、2026年7月以降の公開特許・判例・審査基準変更をモデル記憶に依存してはならず、リアルタイムな特許DBや一次資料をretrieval sourceとする必要がある。 8

契約書作成・レビュー

Haiku 5.5に適するのは、NDA、共同研究、共同出願、software license、technology license等から以下を抽出する業務である。

Background IP / Foreground IP / improvement / ownership / license scope / sublicensing / field / territory / exclusivity / royalty / audit / MFN / indemnity / confidentiality / AI-use restriction / change of control / termination

1M contextはmaster agreementとSOW、amendment、side letterをまとめて処理するのに有利だが、長いcontextのrecallが完全になるわけではない。したがって「全契約を一度に入れば全例外が拾える」という設計ではなく、条項単位chunking+cross-document reconciliationを行う方が堅牢である。 34

生成した契約条項はAIが最終契約主体になるわけではなく、採用した企業・担当者側で責任を持つという運用原則を明記すべきである。

ライセンス交渉・ライセンス管理

Haiku 5.5はライセンス管理で特に有力である。既存PDF契約から権利義務をJSON等へ抽出し、更新日、minimum guarantee、royalty rate、audit period、territory、product、patent family等を構造化できる。

ただし、自動抽出した数字をERPやroyalty settlementへ**直接書き込むことは避けるべき**である。最も危険なのは「もっともらしい5%」を誤抽出することであり、金額・期間・特許番号は原契約へのdirect pointerと人間承認を必須にする。

また、ライセンス対象データをモデルに投入できるかは、その契約の秘密保持条項やthird-party disclosure条項も確認する必要がある。AI vendorを単なる「IT tool」とみなすのではなく、必要に応じてservice provider/subprocessorとして契約上の許容範囲を確認すべきである。Anthropic利用時も直接契約とAWS/GCP/Azure経由では契約チェーンが異なり得る。 24

M&A・知財デューデリジェンス

DDでは、Haiku 5.5に以下の役割を与えると有効である。

Phase A: 全資料を分類・重複排除

Phase B: IP ownership、employee invention、OSS、license、change-of-control、litigation、security interestを抽出

Phase C: red flag候補をsource付きで提示

Phase D: 人間がmaterialityを評価

Phase E: disclosure schedule・Q&Aへ反映

最大のリスクはhallucinationよりも**omission**である。つまり、存在しない問題を作ることだけでなく、データルームの奥にあるside letterを見落とすことがM&Aでは重大である。このため「precision」だけでなく「recall」を検証し、known-red-flag setを使った事前benchmarkを実施する必要がある。

コード・OSS・営業秘密

コード生成では、生成コードの機能品質、第三者著作権・OSSライセンス、第三者特許を別々に評価すべきである。「コンパイルできる」ことは「権利クリア」であることを意味しない。

特に自社 proprietary source codeをpromptへ入れる場合は、入力可否をリポジトリclassificationと連携させ、**RESTRICTED** branchや第三者受託コードをAI gatewayで拒否する実装が望ましい。Haiku 5.5がcomputer/browser useやsubagentを強化している以上、read accessとwrite/commit accessも分離する必要がある。 35

ガバナンス・技術統制・監査証跡

推奨リスク評価フレームワーク

Haiku 5.5の利用可否を「Claude可／不可」の二択にせず、**データ・タスク・権限・法的効果**の四軸で判断することを推奨する。

Tier	例	Haiku 5.5利用	必須統制
Green	公開特許の要約、公開法令の分類、一般翻訳	原則可	通常の実事確認
Amber	社内契約、既出願R&D、非公開ライセンス台帳	Enterprise/APIのみ	DPA、no-training確認、retention、access control、human review

Tier	例	Haiku 5.5利用	必須統制
Red	未出願core invention、M&A clean-team、訴訟戦略、重要 source code	原則個別承認	ZDR等、最小化、専用gateway、限定権限、監査ログ
Restricted	法令・契約上外部提供禁止、国家安全保障・輸出規制対象等	クラウドAI禁止を検討	self-host/isolated processingまたは人手

この分類で重要なのは、**同じ文書でもtaskによってリスクが変わること**である。NDAを「要約」するのと、「相手方へ自動送信する修正版を作成しメール送信までさせる」のでは、後者にagentic execution riskが追加される。Anthropicが報告した第三者評価環境での実システムアクセス事故は、この権限分離の必要性を裏付ける。 ¹⁴

技術的緩和策

最も効果が高い設計は、promptに「秘密を入れるな」と表示することではなく、**AI Gateway**を置くことである。

推奨構成は、

```
User → Identity/SSO → DLP/Classifier → Redaction → Model Router → Claude API → Output Guard
→ Citation Validator → Audit Vault
```

である。

入力側では、特許未公開番号、ソースコードrepository marker、顧客名、M&A project code、個人情報等を検知し、データ分類に応じてdeny/redact/approveを選択する。

出力側では、URL・判例・特許番号のexistence check、類似性チェック、コードlicense scanning、PII/secrets再出力検知を行う。

モデル側のsafety classifierはHaiku 5.5で `stop_reason: "refusal"` を返す場合があるが、これを企業独自のDLPの代替と考えてはいけな。Anthropicの安全制御はサービス安全のための統制であり、自社特有の「Project Xは絶対に入力禁止」というルールを知るものではない。 ³⁶

監査証跡

知財関連の重要AI処理では、次の**AI Evidence Package**を一単位として保存することを推奨する。

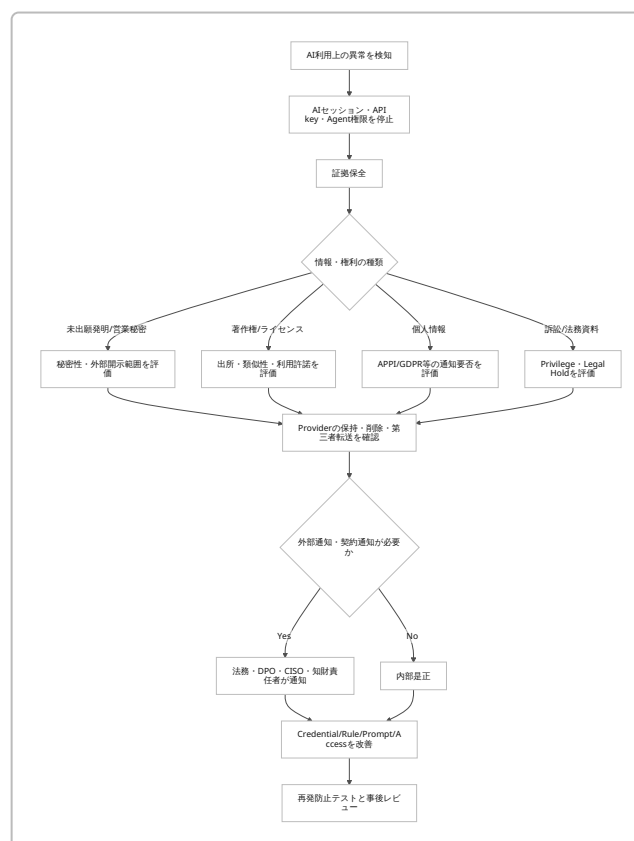
記録	理由
model/provider/model ID	将来の再現性
timestamp / user / department	責任・アクセス追跡
system/developer prompt version	結果に影響する統制条件
user prompt	入力の証拠
source document ID + hash	どの版を解析したか

記録	理由
retrieval results	回答根拠
output	AI生成内容
tool calls / external actions	agent処理の証拠
parameters / effort	再現性
human edits	AI出力と人間創作の切り分け
reviewer / approval	法的責任の所在
retention policy	データライフサイクル
incident flag	後日のlegal hold

Anthropic Enterpriseがusage analytics、Compliance API、OTEL monitoring、retention controlsを提供していることはこの設計に利用できるが、**ベンダー側ログだけに依存せず、自社側のimmutable audit storeにも必要最小限の証拠を持つことが望ましい。** 16

ただし「ログを増やすほど安全」でもない。prompt全文に営業秘密を重複保存すると、AI本体よりSIEMや監視基盤の方が情報漏えい源になる。そのため、一般監視ログにはdocument ID/hashを残し、機密prompt/output本体はアクセス制御されたevidence vaultへ分離する設計がよい。

インシデント対応フロー



Anthropic APIでは標準的に最大30日程度の保持があり得るため、秘密情報誤入力時には「ブラウザ上で conversationを消したから終了」とせず、利用サービス、API機能、Files等の状態、契約上の削除を確認 する必要があります。³⁷

GPT-4o、Gemini、Llama 3との比較

この比較では、**GPT-4oとLlama 3は2024年世代のモデルをユーザー指定に従って参照モデルとして掲載**する。2026年10月時点でGPT-4oはOpenAIの公式APIページ上でDeprecatedと表示されているため、Haiku 5.5との単純な「最新性能比較」には適さない。比較価値は、むしろ**クラウド専有型とopen-weight/self-host型の知財リスク配分の違い**にある。³⁸

項目	Claude Haiku 5.5	GPT-4o	Gemini / Google Cloud	Llama 3
位置付け	2026年10月の高速・低コスト小型モデル。1M context、128k output。 ⁸	旧世代の汎用 multimodal model。公式ページではDeprecated。128k context、16,384 max output。 ³⁹	Gemini系managed models。具体的能力は世代・SKUごとに異なるため個別確認が必要。	2024年世代のweight配布型モデル。Community License。 ⁴⁰
配備形態	Anthropic/AWS/GCP/Azure等。標準self-host weightsなしと推定。 ²	OpenAI managed API型。	Google Cloud managed型。	自社管理環境へ配置可能なweight配布型。 ⁴⁰
ライセンス	proprietary commercial service terms	proprietary service terms	Google Cloud/service terms	Meta Llama 3 Community License。配布時 attribution、AUP等あり。月間7億MAU超の事業者には追加 commercial terms。 ⁴¹
Provider による訓練	Anthropic商用データはモデル訓練に使わない。 ⁴²	現行OpenAI APIの主要endpointは data used for training = No。 ⁴³	Googleは顧客の許可・指示なしに顧客データをAI/MLモデルの training/fine-tuningに利用しない。 ⁴⁴	self-hostなら providerへの prompt送信自体を不要にできる。
標準的な保持	API I/Oは原則30日以内削除。例外あり、ZDRは契約等次第。 ³⁷	現行主要API endpointでabuse monitoring最大30日、承認顧客にはZDR/Modified Abuse Monitoring。 ⁴⁵	ZDR実現には設定依存。Interactions APIは store=false 等が必要で、Search/Maps grounding等には別保持条件がある。 ⁴⁶	self-hostでは保持期間を企業が設計できるが、その分セキュリティ・ログ・削除責任も企業側。

項目	Claude Haiku 5.5	GPT-4o	Gemini / Google Cloud	Llama 3
営業秘密	強いEnterprise統制はあるがクラウド送信が前提	クラウド送信が前提	Google Cloud統制と統合しやすい	完全ローカル化が可能な点で最高機密に強い
著作権リスク	AnthropicにはBartz訴訟・和解という重要な判例史がある。 4	生成・訓練双方について別途契約・権利確認が必要	同左	自社がmodel operatorになるため、RAG、fine-tuning、output filtering等の法的責任をより直接負う
ガバナンス負担	中。Provider機能を利用可能	中	中	高。self-hostするほど企業自身がmodel security、patching、filter、loggingを担う
知財部向け評価	大量要約・分類・抽出で最有力候補	新規導入比較対象としてはlegacy	Google Cloud中心企業に有力	最重要秘密を外に出せない場合のarchitecture候補

OpenAIについては、現行APIでChat Completions/Responses等の主要endpointは訓練利用なし、abuse monitoringは通常30日で、適格顧客はZero Data Retention等を申請できる。ただしZDR非対応機能や application stateを保持する機能も存在する。したがって「OpenAIは30日」「Anthropicも30日」と単純比較せず、**endpoint/feature単位**で評価する必要がある。 45

Googleも同様で、顧客の許可なしにtrainingに使用しない一方、Google Search groundingは最大3日のログ、Maps groundingでは30日、Interactions APIはデフォルト `store=true` であるなど、機能によってZDR条件が異なる。秘密情報管理ではモデル名よりも**使った周辺機能**の方が重要になる場合がある。 47

Llama 3の最大の違いは、サービス利用契約だけでなく**model materials自体のCommunity Licenseを企業が受諾して運用する**点である。ライセンスにはattribution、Acceptable Use Policy、他のLLM改善への利用制限、7億MAU超企業に関する追加条件等がある。self-hostはデータ主権上魅力的だが、「open weightsだから法的リスクがない」という意味ではない。 41

したがって企業知財のモデル選定は、能力ランキングだけでなく、

「モデル性能 × 情報機密性 × deployment control × provider contract × retention × evidence capability」

の多目的最適化として行うべきである。

実行ロードマップとテンプレート

短期：直ちに実施

最初の優先事項はHaiku 5.5を全社導入することではなく、**無管理利用を止め、承認された利用経路を作る**ことである。

即時アクション	実施内容
AI inventory	Claude個人版、Enterprise、API、Bedrock、Vertex、Azure等の利用実態を把握
Data classification	未出願発明、source code、契約、訴訟、M&A、個人情報を分類
Approved channel	知財用途は企業管理されたEnterprise/APIに限定
Vendor DD	DPA、retention、training、subprocessor、region、incident、IP terms確認。 Anthropicの商用data handlingとDPAを基準資料にする。 ³
高リスク用途停止	自動出願、自動契約締結、自動送信、自動Git commit等をhuman approvalなしで許可しない
Evaluation set	過去の特許・契約案件100～500件程度でaccuracy/recall/citation accuracyを測る
Logging	model ID、source、prompt、output、reviewerを保存
Inventorship	AI利用発明にhuman-contribution recordを導入。 ⁵

特に**未出願発明を一般consumer AIへ入力しない**という暫定ルールは即時導入価値が高い。ただし最終形は全面禁止ではなく、Enterprise/API＋契約＋retention＋DLPに基づく例外承認へ移行するのが現実的である。

中期：六～十八か月

中期にはAIを「チャットツール」から**知財情報基盤**へ昇格させる。

第一に、特許・契約・ライセンスRAGを構築し、すべての回答に原資料citationを必須化する。第二に、AI gatewayでDLP、data minimization、model routing、output validationを実装する。第三に、モデル切替え時のregression testを標準化する。Anthropicは公開モデルに対し一定のdeprecation notice方針を設け、Haiku 5.5についても2027年10月7日より前にはretireしないとしているが、企業側も特定モデルへのhard-codeを避ける方がよい。 ³³

契約面では、AI vendorだけでなく、外部法律事務所、特許事務所、翻訳会社、開発受託会社との契約にも**「顧客資料を生成AIへ投入できるか」**を明示する。これがないと、企業内部を厳格に統制しても外部専門家経由で同じデータが未承認AIへ流れる。

EU事業を行う企業は、AI inventoryにEU AI Actのrole mappingを追加し、provider / deployer / downstream providerのどれに該当するのかをuse case単位で判定する。GPAI provider向け義務はすでに適用・執行フェーズに入っている。 ⁴⁸

長期：十八か月以上

長期的には二層型AI architectureが現実的である。

通常の知財業務にはHaiku 5.5等の高度なmanaged modelを用い、最高機密についてはself-host/open-weight modelまたは専用isolated environmentを使う。Haiku 5.5は標準的なオンプレweights提供が公表されていないため、全情報を一モデルへ統一するより、情報分類に応じたmodel routingの方が合理的である。

2

また、AIの評価軸を「作業時間削減」から、

特許取得率、拒絶対応品質、DD red-flag recall、契約漏れ件数、ライセンス収益漏れ、秘密情報incident、外部弁護士費用、AI output correction rate

へ移すべきである。こうすることでAIガバナンスが単なるコンプライアンスコストではなく、知財ポートフォリオ価値管理の一部になる。

社内AI利用ポリシーのひな型

以下は企業一般向けの短縮版である。

生成AI知財利用規程（案）

当社の役職員は、会社が承認した生成AIサービスおよびアカウントのみを業務に使用する。

未出願発明、営業秘密、個人情報、顧客秘密、第三者との契約により外部開示を制限された情報、訴訟・M&Aその他特に機密性の高い情報は、承認されたEnterprise/API環境および所定のセキュリティ統制を経ずに生成AIへ入力してはならない。

生成AIの出力は、特許性、侵害性、FTO、著作権、契約義務その他の法的結論として扱ってはならず、所定の人間によるレビューを経なければ意思決定または外部提出に使用してはならない。

AIが提示した判例、法令、特許番号、引用文献、数値、契約条項その他検証可能な事実は原資料で確認する。

AIを使用して発明活動を行った場合、発明者認定のため、人間による課題設定、構成の着想、AI提案の選択・修正、実験・検証への寄与を記録する。

AIによる外部送信、契約締結、特許・商標出願、repositoryへのcommit、データ削除その他権利・義務を変更する操作には、原則として事前の人間承認を必要とする。

重要案件では、使用モデル、日時、入力資料、出力、引用元、担当者および承認者を所定の監査システムへ保存する。

AIによる秘密情報の誤入力、権利侵害のおそれのある出力、誤った外部操作その他のincidentを発見した場合、直ちに法務・知財・情報セキュリティ部門へ報告する。

この構造は、Anthropicが提供するEnterprise管理・retention・monitoring機能と、日本のAI事業者ガイドラインに沿った企業内統制へ接続しやすい。

49

AIベンダー契約条項のひな型

データ利用条項

Provider shall process Customer Content solely for the provision, security, support, and legally required operation of the Services and shall not use Customer Content to train or improve generally available generative AI models without Customer's prior written authorization.

Anthropic商用サービスでは既に顧客データを訓練しない方針が示されているが、再委託先・追加機能まで契約的にカバーするため、自社契約でも明文化する価値がある。 50

保持・削除条項

Provider shall retain prompts, outputs, uploaded files, logs and derived customer content only for the documented minimum period necessary for the Services, and shall support contractually agreed zero- or reduced-retention configurations where technically available. Upon termination or Customer request, Provider shall delete such data subject only to expressly identified legal exceptions.

Anthropic APIの標準保持が原則30日でありながら例外があるため、「30日以内」とだけ書くのではなく、Files、logs、legal hold、abuse monitoringを定義する方がよい。 37

モデル変更条項

Provider shall provide reasonable advance notice of material model deprecation or changes that may materially affect agreed security, privacy, functionality, or compliance characteristics and shall provide commercially reasonable migration information.

モデルライフサイクルは知財システムの再現性に直結するため、SaaS一般のchange clauseより強く扱う価値がある。Anthropicもdeprecation policyを公開している。 51

知的財産・補償条項

The agreement should separately address rights in Customer Inputs, contractual rights to Outputs, third-party IP claims arising from authorized use, exclusions for customer-supplied infringing material, modification of outputs, combination with third-party products, and use outside documented policies.

Anthropicは商用顧客に輸入の権利維持・出力に関する契約上の権利を示し、過去にcommercial termsで著作権indemnityの拡張を発表している。ただし、適用除外・責任上限・クラウド販売経路による差異は現行契約を個別確認すべきである。 52

知財担当者向け出力チェックリスト

重要なAI生成物については、最終承認前に最低限、以下を確認する。

確認項目	合格条件
Source	主要主張が一次資料へtraceできる
Citation	特許番号、判例、条文、契約条項が実在・一致
Completeness	「見つからなかった」資料の母集団も確認済み
Confidentiality	入力データが承認されたclassification・環境
Copyright	既存著作物との不自然な一致・出所不明部分を確認
Patent	AI案についてinventorshipとFTOを別途評価
License	database、OSS、第三者資料のAI利用権限を確認
Contract	AI案が既存契約・policyと矛盾しない
Human review	責任を負う担当者が内容を実質的にレビュー
Evidence	model ID、source hash、output、review記録を保存
External action	出願・送信・契約・commit前にhuman approval

最終評価

Claude Haiku 5.5の企業知財への最大の意味は、「AIが法務専門家を置き換えること」ではなく、「これまでコスト上レビューできなかった大量の知財情報を常時レビュー可能にすること」にある。AnthropicがHaiku 5.5を高速・低コストの分類、抽出、要約、サブエージェント向けモデルとして設計していることから、この評価が最も実態に近い。¹¹

その結果、企業の競争力を左右するのは「どのLLMが一番賢いか」よりも、正しい原資料をモデルへ渡せるか、秘密情報を適切に分離できるか、回答を原資料へtraceできるか、人間の発明・創作寄与を記録できるか、事故時に証拠を復元できるかになる。

Haiku 5.5については、1M context、高速推論、低コスト、strong coding/agent capabilities、商用データの非学習、Enterprise統制という点で企業知財基盤の有力候補である一方、標準オンプレ提供が確認できないこと、標準APIに保持期間が存在すること、法務用途のhallucination保証がないこと、agent化すると誤答が実操作リスクへ転換することを同時に評価しなければならない。⁵³

したがって、2026年10月時点の実務的な採用判断は、「Haiku 5.5を使う／使わない」ではなく、「Green/Amber/Redの情報分類を設け、承認済みAPI経路、DLP、source-grounding、human approval、audit evidenceを条件として段階導入する」ことが最も合理的である。日本のAI法・AI事業者ガイドライン、米国の著作権・inventorship guidance、EU AI Actがいずれも進展している現状では、このモデル非依存のガバナンス構造を先に作ることが、Haiku 5.5だけでなく次世代モデルへの対応コストを最も下げる。⁵⁴

¹ ² ⁷ ¹¹ ¹² Introducing Claude Haiku 5.5 \ Anthropic

<https://www.anthropic.com/claude-haiku-5-5>

³ ³⁰ ³⁷ How long do you store my organization's data?

<https://privacy.claude.com/en/articles/7996866-how-long-do-you-store-my-organization-s-data>

⁴ ³¹ ORDER ON 122 FAIR USE for Bartz et al v. Anthropic PBC :: Justia Dockets & Filings

<https://docs.justia.com/cases/federal/district-courts/california/candce/3%3A2024cv05417/434709/231>

- 5 21 人工知能ダバス（DABUS）に関する令和7年1月30日知財高裁判決（令和6年（行コ）第10006号 出願却下処分取消請求控訴事件）とAI発明に関する考察 | ユアサハラ法律特許事務所
<https://www.yuasa-hara.co.jp/lawinfo/5599/>
- 6 25 54 人工知能関連技術の研究開発及び活用の推進に関する法律
<https://laws.e-gov.go.jp/law/507AC0000000053>
- 8 9 33 53 Claude Haiku 5.5 - Claude Platform Docs
<https://platform.claude.com/docs/en/models/haiku-5-5/overview>
- 10 17 35 36 What's new in Claude Haiku 5.5 - Claude Platform Docs
<https://platform.claude.com/docs/en/models/haiku-5-5/whats-new-haiku-5-5>
- 13 34 Context windows - Claude Platform Docs
<https://platform.claude.com/docs/en/build-with-claude/context-windows>
- 14 Investigating three incidents in our cybersecurity evaluations
<https://www.anthropic.com/news/investigating-incidents-cybersecurity-evals>
- 15 42 50 Does Anthropic act as a Data Processor or Controller? | Anthropic Help Center
<https://support.anthropic.com/en/articles/9267385-does-anthropic-act-as-a-data-processor-or-controller>
- 16 49 Claude Enterprise plan | Claude by Anthropic
<https://www.anthropic.com/enterprise>
- 18 AIと著作権について | 文化庁
<https://www.bunka.go.jp/seisaku/chosakuken/aiandcopyright.html?afsrc=1>
- 19 27 32 NewsNet Issue 1060 | U.S. Copyright Office
<https://copyright.gov/newsnet/2025/1060.html>
- 20 Thomson Reuters wins AI copyright 'fair use' ruling against one-time competitor
<https://www.reuters.com/legal/thomson-reuters-wins-ai-copyright-fair-use-ruling-against-one-time-competitor-2025-02-11/>
- 22 FAQs on Inventorship Guidance for AI-assisted Inventions | USPTO
<https://www.uspto.gov/initiatives/artificial-intelligence/faqs>
- 23 Unfair Competition Prevention Act - English
<https://www.japaneselawtranslation.go.jp/en/laws/view/2803/en>
- 24 How do I view and sign your Data Processing Addendum (DPA)? | Anthropic Privacy Center
<https://privacy.anthropic.com/en/articles/7996862-how-do-i-view-and-sign-your-data-processing-addendum-dpa>
- 26 AI事業者ガイドライン
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20260331_report.html
- 28 29 48 Guidelines on obligations for General-Purpose AI providers | Shaping Europe's digital future
<https://digital-strategy.ec.europa.eu/en/faqs/guidelines-obligations-general-purpose-ai-providers>
- 38 39 GPT-4o Model | OpenAI API
<https://platform.openai.com/docs/models/gpt-4o>
- 40 41 llama3/LICENSE at main · meta-llama/llama3 · GitHub
<https://github.com/meta-llama/llama3/blob/main/LICENSE>
- 43 45 Data controls in the OpenAI platform
<https://platform.openai.com/docs/guides/your-data>
- 44 46 47 Gemini Enterprise Agent Platform and zero data retention | Google Cloud Documentation
<https://cloud.google.com/vertex-ai/generative-ai/docs/data-governance>

51 **Model deprecations - Claude Platform Docs**

<https://docs.anthropic.com/en/docs/about-claude/model-deprecations>

52 **Anthropic's Transparency Hub \ Anthropic**

<https://www.anthropic.com/transparency/voluntary-commitments/security%26privacy>