ChatGPT

Gemini 3.5 Flash の Computer Use 統合が知財業務に与える影響

エグゼクティブサマリ

Google は 2026年5月に Gemini 3.5 Flash を一般提供し、2026年6月24日には **Computer use が Gemini 3.5 Flash の組み込みツールになった**と公式発表しました。Google の公式モデル文書では Gemini 3.5 Flash は「強いエージェント能力」を持つ高速・低コストモデルとして位置付けられており、Google 公式ブログは Computer use によりエージェントが「プラットフォーム横断で」画面を見て操作できると説明しています。もっとも、筆者が確認できた公開文書のうち、**Computer Use の詳細な評価値・アクション空間・保存ポリシー・承認モデルまで体系的に示した公開モデルカードは 3.5 向けでは未だ限定的**で、定量的ベースラインは主として 2025年公開の Gemini 2.5 Computer Use モデルカードに依拠します。そこでは、入力が「テキスト＋スクリーンショット＋直近の行動履歴」、出力が「次の UI 操作の関数呼び出し」であり、主にブラウザ相互作用に最適化されていること、Online-Mind2Web・WebVoyager・Android World で高性能を示す一方、OSWorld では「OS control not yet supported」とされていました。したがって、**3.5 の統合は“より実務投入しやすい”方向の更新だが、法務・知財上は 2.5 で見えていた制約と責任配分をほぼ引き継ぐ**と見るのが慎重です。 [1]

知財業務への最大の影響は、生成 AI が「文案を書く道具」から、**人間の権限で実際に SaaS、DMS、特許庁サイト、契約管理システム、訴訟支援基盤を横断して閲覧・入力・提出・取得する“実行主体”に近づく**ことです。これにより、先行技術調査、権利化補助、著作権侵害モニタリング、秘密情報の棚卸し、契約条項の比較、証拠収集、社内ワークフロー実行の効率は大きく上がりますが、同時に、**侵害行為・不正アクセス・営業秘密持出し・個人データ越境移転・勝手な「同意」や「送信」**のリスクが、単なるチャット利用よりもはるかに現実化します。日本の個人情報保護委員会は、生成AI利用時に個人情報が二次利用される場合の法違反可能性を明示し、文化庁は AI 生成物・利用段階の著作権侵害が類似性・依拠性で判断され、一定の場合には事業者側にも責任が及び得ると整理しています。さらに、米国では AI が発明者にも著作者にもなれないという線が維持され、EU では GDPR と AI Act がログ、セキュリティ、DPIA、人間監督を強く要求します。 [2]

実務上の結論は明快です。**Computer Use は知財部門にとって強力な“RPA の上位互換”になり得るが、無制限に個人端末や本番アカウントへ接続してよい技術ではない**ということです。導入初期は、①専用実行環境、②最小権限、③ドメイン許可リスト、④人的承認ポイント、⑤完全ログ、⑥証拠保全設計、⑦契約上の再委託・責任・学習不使用条項、⑧訴訟ホールド対応、を最初から組み込む必要があります。Google Cloud 側には Cloud Audit Logs と Agent Observability がある一方、**Data Access ログは明示的有効化が必要**であり、これを忘れると証拠性評価は一段落ちます。結局のところ、知財実務での価値は「どこまで自動化するか」よりも、**“何を自動化しないか”を制度化できるか**で決まります。 [3]

事実認定と評価の前提

まず、ユーザー提示の前提である **「Gemini 3.5 Flash に Computer Use が統合された」点自体は、2026年6月24日の Google 公式ブログで確認できます**。また Google AI for Developers のモデル文書では、Gemini 3.5 Flash は持続的なフロンティア級知能を高速・低コストで提供し、サブエージェント展開、長めのワークフロー、多段タスクに強いと説明されています。Google の changelog でも、2026年5月19日に `gemini-3.5-flash` が GA 化されたことが確認できます。したがって、本件は仮説ではなく、**最新の Google 公式プロダクト変更に基づく検討課題**です。 [4]

ただし、**公開情報の粒度には段差**があります。3.5 Flash の一般モデル文書と Computer use 統合発表は新しい一方、筆者が確認できた Google の公開 Computer Use モデルカードは 2025年10月版の **Gemini 2.5 Computer Use** です。この 2.5 モデルカードでは、ブラウザ中心最適化、入力構造、UI アクション出力、ベンチマーク、限界がかなり具体的に説明されています。特に、Web ベンチマークでは高性能でも、**OSWorld では OS-level control は未対応**と明示されていました。したがって 3.5 Flash の Computer Use を評価する際には、**「3.5 により agentic 性能は改善したが、法務評価に必要な詳細仕様の一部は 2.5 文書からの連続性で保守的に読む」**のが適切です。これは本レポートの重要な留保です。 [5]

2.5 モデルカードが示す構造は、知財実務との関係で非常に重要です。モデルは **テキスト、環境状態のスクリーンショット、最近の行動履歴**を受け取り、**次に行う UI 操作の function call** を返します。つまり、Computer Use は API 連携の代替ではなく、**「人間が見て操作する GUI を、視覚的に読み取り、操作案を返す制御ループ」**です。この構成は、特許庁・裁判所・商用データベース・契約管理 SaaS のように API が弱い、又は監査上 API 利用より GUI 利用のほうが現実的なシステムで強い一方、GUI 上に表示された秘密情報・個人情報・著作物が、そのままスクリーンショット入力としてモデル処理対象になることを意味します。ここが、通常の LLM API よりも知財・法務リスクが高くなる根本原因です。 [6]

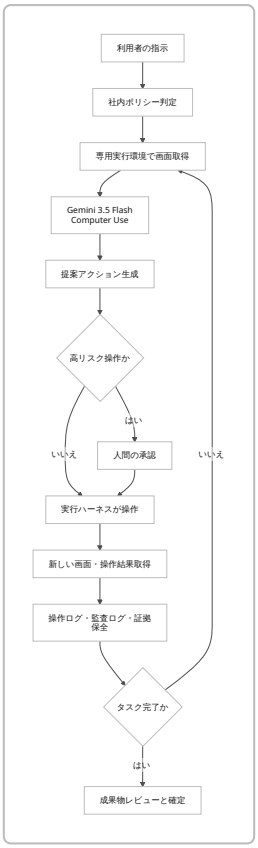
技術的成熟度の裏付けとして、Google は研究面でも ScreenAI を公開しており、UI とインフォグラフィックス理解に特化した VLM として、画面要素の注釈、UI ナビゲーション、QA、要約などを扱うことを示しました。また GUI エージェント研究の標準ベンチマークである Mind2Web、WebVoyager、OSWorld は、いずれも **「現実の Web/OS をまたぐタスクで、視覚理解と行動選択を評価する」**方向へ進んでいます。したがって Gemini 3.5 Flash の Computer Use は、突発的な機能追加ではなく、**Google の ScreenAI 系研究と GUI-agent 評価潮流の商用実装**とみるのが妥当です。 [7]

技術的評価と知財業務フローへの組込み

Computer Use の実態は、知財部門の既存プロセスに「画面認識を伴う agentic RPA」を差し込むことです。現在の知財業務では、特許実務だけでも発明提案入力、先行技術検索、FI/Fターム付与、出願ソフト入力、OA 管理、IDS/情報提供、競合ウォッチ、年金処理、社内承認、外部事務所送付など、**GUI に依存する繰り返し作業が大量に存在**します。Gemini 3.5 Flash の Computer Use が本格稼働すると、これらは「画面→判断→クリック/入力→次画面」の反復として自動化しやすくなります。Google が 3.5 Flash を強い agentic ワークフロー向けに位置づける理由は、まさにここにあります。 [8]

一方で、**知財実務と相性がよいのは、“正解が一意で、かつ最終送信前に人が止められる”仕事**です。たとえば、公開公報の収集、出願番号や年金期限の照合、特許庁ポータルからの定型ダウンロード、契約台帳への入力、侵害モニタリング用の証拠保全画面のキャプチャなどは相性がよいです。反対に、請求項の補正方針、侵害論の最終結論、フェアユース評価、秘密情報該当性、訴訟上の証拠採否見込みのような**高裁量判断**は、Computer Use が“周辺作業を支援する”のは有用でも、最終判断の自動化は推奨しにくいです。Google の 2.5 モデルカードでも、環境やシステム指示に評価が敏感であることが示されており、GUI タスクは見た目の似た要素や予期しない画面遷移で失敗しやすいことが読み取れます。 [9]

以下のフローは、知財部門における望ましい実装像です。重要なのは、**モデルが直接権限を持つのではなく、企業側ハーネスがスクリーンショットと実行を仲介し、ログと承認を挟む**ことです。これは Google だけでなく、Anthropic や OpenAI の Computer Use 文書でも共通する基本構造です。 [10]



この構造を前提にすると、機能詳細は次のように整理できます。**視覚認識精度**については、Google の 2.5 Computer Use モデルカードで Online-Mind2Web 69.0%、WebVoyager 88.9%、Android World 69.7% などが示され、少なくとも web/mobile UI 認識・操作では強い水準にあります。ただし OSWorld は未対応扱いだったため、Windows Explorer やローカルフォルダ、独自業務アプリを含む “PC 全般” の安定性は、法務部門が想像するよりまだ不均一です。**操作自動化範囲**は、2.5 文書から読む限り、スクリーンショットを見てクリックやキーボード入力を返す形が中心で、ブラウザ作業に最適化されます。3.5 については「platforms across」と公式ブログが言う一方、詳細アクション仕様の公開度はまだ十分ではありません。したがって、**知財部門は “Web-first GUI automation” として導入し、ローカル端末や VDI への拡張は別プロジェクトとして扱うべき**です。 11

API / 権限モデルについては、Google 側の個別公開文書だけでは OpenAI や Anthropic ほど詳細な approval semantics までは見えませんが、Google Cloud 側では Enterprise Agent Platform の IAM、Cloud Audit Logs、Private Logs Viewer などの統制機構が整備されています。実務上は、モデルの能力よりも、**どのサービスアカウントで、どの画面に、どの権限で入るか**の設計が支配的です。少なくとも Google 自身も、Agent Platform に監査ログと observability を備え、データアクセスログは有効化が必要と示しているため、企業側が「ログを取れる設計」を選ばない限り、証拠性は向上しません。 12

法的影響

特許

特許法の観点では、Computer Use の統合は **発明者性のルール自体を変えません**。米国では連邦巡回区が Thaler v. Vidal で、Patent Act 上の “inventor” は自然人だと明言し、USPTO も AI-assisted inventions について、AI が使われても人間の「significant contribution」があれば特許性は否定されないが、AI 自体を発明者にはできないという運用を維持しています。日本でも DABUS 事件について、知財高裁判決要旨および JPO 調査資料は、AI を発明者として記載した出願の却下処分を適法と整理しています。したがって Gemini 3.5

Flash の Computer Use が先行技術調査、実験条件探索、クレームドラフト補助をどれだけ高度化しても、**法的に問われるのは“誰が発明の特徴的部分の完成に創作的に寄与したか”であり、AI の自律行動そのものではありません。** [13]

しかし、だから安全という意味ではありません。むしろ Computer Use によって、モデルが論文・特許・試験結果・社内 wiki・ELN・市場情報を横断し、複数サブタスクを高速反復するほど、**「人間の着想」と「AI による探索・選択・組合せ」の境界が曖昧**になります。このとき企業に必要なのは、AI が関与した発明案件ごとに、①人間が与えた課題設定、②重要パラメータの選定理由、③採否判断、④実験・検索のレビュー履歴、⑤最終的な請求項化判断、をログとして残すことです。将来の発明者紛争や職務発明対価紛争では、**「AI を使ったこと」より「人間がどこで創作的判断をしたか」**の立証が勝負になるからです。 [14]

著作権

著作権の論点は、Computer Use ではむしろ生成 AI 一般より広がります。文化庁の「AI と著作権に関する考え方について」は、AI 生成物・利用が著作権侵害となるかは基本的に **類似性と依拠性**で判断すると整理し、AI 利用者が原則として侵害主体となる一方、一定の場合には事業者が規範的行為主体として責任を負う余地があると述べています。また、AI 生成物が著作物となるかは、創作意図・創作的寄与の有無が焦点です。米国 Copyright Office も、人間著作性要件を維持し、AI 生成物を含む作品では人間の創作部分のみが保護されると整理しています。したがって、Gemini 3.5 Flash が表示中の論文、画像、マニュアル、コード、契約条項を読みながら要約・転記・貼付・再編集する場合、**結果物だけでなく、その過程での複製・送信・表示・抽出**が著作権問題になります。 [15]

日本法では、AI 学習などの情報解析は著作権法30条の4の非享受目的に当たり得る一方、文化庁は **複数目的のうち一つでも享受目的があれば要件を欠き得る**と整理しています。この点は Computer Use に特有の示唆があります。たとえば、競合企業の有償データベース画面を AI に読み取らせ、情報解析の名目で大量抽出しつつ、実質的にはユーザーが表示内容を享受し営業利用するなら、30条の4依拠は弱くなります。EU DSM Directive でも、TDM は保護対象行為を伴い得るため、例外がなければ権利者許諾が必要だとされています。米国ではフェアユースがなお重要ですが、17 U.S.C. § 107 は要件衡量型であり、Warhol 判決も用途・市場代替性の重みを再確認しました。結局、**Computer Use によるスクリーンスクレイピングや UI 経由の大量取得は、「AI だから自由」ではなく、通常の著作権・契約・DB 利用条件がそのまま適用される**と考えるべきです。 [16]

営業秘密

営業秘密のリスクは、知財部門にとって最も深刻です。日本の不正競争防止法は、営業秘密の不正取得・使用・開示を禁じ、EU Trade Secrets Directive も、秘密情報の違法取得・利用・開示を禁止しています。Computer Use は API 制限を迂回して「画面に見えているもの」を読めるため、従来の DLP が API やファイル搬出だけを見ていた環境では、**スクリーンショット経由の持出し**が死角になります。特に、M&A データルーム、外部法律事務所ポータル、共同研究サイト、ライセンス交渉資料、侵害鑑定ドラフト等は、GUI 上だけで閲覧可能に設計されていることが多く、Computer Use はここに直接アクセスし得ます。もし競業情報の収集や契約違反の横断取得に使えば、単なる社内不正にとどまらず、営業秘密侵害や不法行為の争点になります。 [17]

この点で重要なのは、**秘密情報の法的保護は、秘密管理性・有用性・非公知性だけでなく、企業がアクセス統制を実際に維持していたか**にも左右されることです。Computer Use を無差別に本番アカウントへ接続し、共有資格情報で複数部門が使い回す運用をすると、「誰がいつ何を見たか」が曖昧になり、秘密管理の立証も弱くなります。逆に、専用 ID、案件別ワークスペース、ダウンロード禁止、貼付禁止、座標クリックより API 優先、監査ログ有効化、外部送信遮断、という運用をすれば、秘密情報利用の必要最小限性と社内統制を説明しやすくなります。 [18]

契約・コンプライアンス・訴訟リスク

Computer Use の導入で見落とされやすいのが、**AI が「同意」「送信」「提出」「支払」など法的効果を生むクリックを代行し得る**点です。OpenAI の Computer use 文書は、ログイン、権限承認、年齢確認、ファイルアップロード、機微情報送信、コード投入などでユーザーの明示承認を要するとし、第三者コンテンツ上の指示は原則として“permission”とみなすべきでないと明示しています。Anthropic も prompt injection により画面上の命令をユーザー指示より優先してしまうリスクを警告しています。Microsoft Copilot Studio も、共有されたエージェントが maker-provided credentials で実行される場合、他ユーザーが元の作者のアクセス権で行為し得ると警告しています。これらは競合の文書ですが、**法務論点は Google の Computer Use でもほぼ同型**です。つまり、AI が UI を操作する限り、クリック権限と権限濫用の問題は避けられません。 19

日本の個人情報保護委員会は、生成AIサービスに個人情報や個人データを含むプロンプトを入力し、それが応答生成以外の目的で扱われる場合、法違反になり得ると注意喚起しています。EU では GDPR が目的限定・データ最小化・安全管理・DPIA・自動化意思決定規制を置き、AI Act は高リスク AI に対し精度、ロバスト性、サイバーセキュリティ、ログ、人間監督を要求します。だから知財部門が Computer Use を使って従業員評価、案件配賦、発明報奨、懲戒判断、アクセス制限などに踏み込むと、**単なる業務自動化ではなく、個人情報・労務・AI 規制の交差点**に一気に入り込みます。特に EU 関連会社を持つ企業では、DPIA とユースケース分類を省略すべきではありません。 20

証拠性と企業ガバナンス

証拠収集の面では、Computer Use は非常に魅力的です。侵害サイトの巡回、競合 UI の表示保存、契約締結画面のキャプチャ、利用規約改定履歴の取得、SNS・EC・アプリ画面の時系列保全など、**“人間が見ていた画面と操作履歴”を一体で残せる**からです。しかし、証拠化の観点で重要なのは、「ログがある」ことではなく、**そのログが真正・完全・時系列一貫・改ざん困難であること**です。NIST は有効なログ管理が必要だとし、米国の証拠法では真正性について、その証拠が主張どおりのものであると支持する証拠が必要になります。したがって、単にモデルの出力テキストやスクリーンショット PNG を残すだけでは、訴訟上の説得力は限定的です。 21

Google Cloud 側には、Gemini Enterprise Agent Platform の Cloud Audit Logs と Observability があり、誰がいつ何をしたかを追うための基盤はあります。Admin Activity と System Event は無効化不可で、Data Access は明示的有効化が必要です。Observability では raw agent logs、severity、timestamps、execution summaries が見られます。これは知財・訴訟実務にとって大きな利点ですが、**これだけでは“改ざん不可能”までは自動的に担保されません**。そのため、知財部門で証拠利用を想定するなら、Cloud Audit Logs に加えて、SIEM への転送、WORM ストレージ、ハッシュ付与、案件 ID 紐付け、担当者電子署名、原本保存期間、ホールド管理を追加する必要があります。要するに、Google のログは「素材」として有用ですが、**証拠能力を高めるには企業側の保全設計が不可欠**です。 22

日本の AI 事業者ガイドラインも、トレーサビリティとアカウンタビリティを重視し、AI の学習プロセス、推論過程、判断根拠等のログ記録・保存、データ出所や意思決定の追跡可能性確保を求めています。この文脈でいうログは、単なる障害調査用メタデータではなく、**後から説明責任を果たせる設計**を意味します。知財業務に置き換えると、最低限、①入力指示、②参照した画面又は URL、③操作提案、④実行結果、⑤人間の承認・修正、⑥成果物の確定版、⑦外部送信有無、を紐づけて保存すべきです。これがないと、後で「AI が勝手に送った」「誰が秘密情報をアップロードしたか不明」「どの時点で著作物を取得したか不明」といった主張への備えが弱くなります。 23

企業ガバナンスの核心は、**“利用規程”と“アクセス制御”と“監査”を別文書にしない**ことです。規程に「使ってよい」と書くだけでは不十分で、IAM ロール、実行環境の分離、Private Logs Viewer の割当て、Secrets 管理、ファイルダウンロード禁止、root/terminal 制限などを実装しなければ統制は成立しません。

Google Cloud は生成 AI ワークロード向けに推奨 IAM グループと役割分離、Workbench での file downloads/root access/terminal 無効化などの統制オプションを示しています。Computer Use を知財部門へ入れるなら、**“知財担当者”の権限で使わせるのではなく、“知財自動化用サービスアカウント”と“レビュー権限者”を分離する**のが基本です。 [24]

競合比較

以下の比較表は、**現時点で公開されている公式仕様に基づく機能比較**と、そこから導かれる法務・実務影響を並べたものです。法的リスク欄の一部は、機能差に基づく実務的推論であり、その点は明示します。 [25]

機能	法的リスク	実務上の影響	推奨対応
Google Gemini 3.5 Flash + built-in Computer use：Google 公式発表では 3.5 Flash に Computer use が組み込まれ、モデル文書では agentic ワークフローや長いタスクに強いとされる。他方、詳細な公開評価の主たる基準点は 2.5 Computer Use モデルカードで、ブラウザ最適化・スクリーンショット＋行動履歴入力・関数呼び出し出力が確認できる。 [26]	**仕様未確定部分が残ること自体がリスク**。保存・承認・権限・行動制約の公開情報が薄い部分は、企業側が契約・PoC で補完しない限り、責任分界が曖昧になる。加えて、画面経由で著作物・秘密情報・個人データへ到達しやすい。 [27]	Google Cloud の監査基盤と組み合わせれば、知財ワークフローの企業実装に向く。ただし Data Access ログを有効化しないと証拠性が落ちる。 [28]	契約で **学習不使用、保存方針、サポート範囲、責任制限、インシデント通知、法的保持**を確認。導入は web GUI から始め、送信系操作に人間承認を入れる。
Anthropic Claude Computer Use：デスクトップ環境を対象とし、スクリーンショット、マウス、キーボード、ズームなどのアクションを明示。データは client-side tool とされ、スクリーンショット等は利用者環境に保存され、Anthropic は応答後に保持しないと説明。 [29]	**保存責任がより明確に利用者側へ寄る**。そのため、個人情報・営業秘密・証拠の管理責任も企業側が全面的に負う。さらに prompt injection リスクを明示。 [30]	自前統制を組みやすい半面、証拠化・保全・削除・越境移転の全ライフサイクル設計が必要。	ZDR/自社保存を活かし、厳格な隔離環境と DLP を実装。公開ウェブ巡回や社内限定 sandbox に向く。
OpenAI Computer use：UI のスクリーンショットを見て、クリック・入力・スクロール等の actions を返し、既存ハーネスや custom harness とも統合できる。危険操作の直前確認、第三者コンテンツを許可とみなさないことを明記。 [31]	**承認フローが文書化されている分、統制設計がしやすい**。ただし、逆に言えばパスワード入力、アップロード、送信は高リスク行為だと公式が認めている。	既存 Playwright/Selenium/MCP と併用しやすく、知財部門の既存自動化資産を活かしやすい。	送信・提出・同意・支払・認証回避は必ず confirm gate。高リスク画面は allow list と takeover を併用。

機能	法的リスク	実務上の影響	推奨対応
Microsoft Copilot Studio Computer use：Windows コンピュータ上で web/desktop app を操作でき、OpenAI CUA や Anthropic モデルも選択可能。maker-provided credentials 共有時の権限継承リスク、allow list、human supervision、推論・スクリーンショット共有を明示。 [32]	**資格情報共有・代理実行リスクが最も顕在化しやすい**。社内横断利用では権限濫用、なりすまし、代理同意が争点になりやすい。	Power Platform 統合により業務実装は容易。ただし IT ガバナンスと分離した“現場自動化”が暴走しやすい。	maker 資格情報禁止、end-user credentials 又は専用 service identity、共有時の権限レビュー、UI allow list を必須化。

比較すると、**Google の優位は“モデル能力とクラウド統制基盤の統合余地”にあり、Anthropic の優位は“client-side で責任境界が明瞭”な点、OpenAI の優位は“confirmation semantics と harness 柔軟性がよく文書化されている”点、Microsoft の優位は“業務統合の容易さ”**にあります。逆に言えば、Google は現時点で 3.5 Computer Use の細目公開が追いついていない分、法務・監査・情シスが **PoC で自ら仕様確認する負荷** が残ります。これは製品力の問題というより、**最新統合機能ゆえの情報非対称**です。 [25]

実務対応と優先調査項目

短期・中期・長期の実務対応は、単なる「導入計画」ではなく、**責任所在の再設計**として考えるべきです。まず短期では、知財部門が勝手に PC 自動操作を始めないよう、**禁止から入って許可ユースケースを列挙する方式**が望ましいです。日本の AI 事業者ガイドラインは、リスク分析、アジャイル・ガバナンス、トレーサビリティ、アカウンタビリティを求めています。PPC も、生成AIへの個人データ入力で二次利用があれば法違反になり得ると警告しています。したがって、最初の 90 日は、①公開情報収集、②社内非機微データの転記、③社内手順のテスト、のような低リスク業務に限定すべきです。 [33]

中期では、**契約・手順・訴訟戦略を連動**させる必要があります。契約面では、ベンダー契約・DPA・情報セキュリティ条項に、少なくとも「入力/スクリーンショット/出力の保存先」「学習利用有無」「越境移転」「サブプロセッサ」「監査ログ提供」「インシデント通知」「法的保持対応」「証拠保全協力」を入れるべきです。社内手順面では、操作分類を「収集」「閲覧」「入力」「送信」「同意」「決裁」に分け、送信・同意・外部提出は別承認にします。訴訟戦略面では、Computer Use ログを discovery / 文書提出 / 電子証拠保全の対象として早い段階から位置付け、**訴訟ホールドの発令対象に agent logs, screenshots, approval records を含める**必要があります。NIST も、インシデントが後日発見されることを前提にログ保持の重要性を述べています。 [34]

長期では、知財部門は Computer Use を単独導入するのではなく、**API 優先、GUI は補完**というアーキテクチャ原則へ移るべきです。OpenAI 文書が既存 Playwright / Selenium / MCP ハーネスの活用を推奨するように、GUI 操作は UI 変動、誤クリック、提示情報改ざん、プロンプトインジェクションに弱いです。よって、権利データの更新、DMS へのメタデータ登録、課金、年金といった deterministic な処理は API や従来 RPA を使い、Computer Use は **閲覧・探索・例外処理・最終 UI 到達が必要な箇所**に限定するほうが、法的にも監査上も安定します。 [35]

推奨アクション

期間	優先アクション	目的
短期	許可ユースケース表の策定、専用実行環境の分離、資格情報棚卸し、Data Access ログ有効化、送信系操作の human-in-the-loop 化	無秩序な利用開始を防ぎ、最低限の証拠性と権限統制を確保する。 [36]
中期	ベンダー契約改定、知財 SOP 改訂、監査・法務・情シスの三者レビュー、訴訟ホールド手順への agent logs 組込み	責任分界と紛争時対応を制度化する。 [37]
長期	API-first / GUI-second 原則、ユースケースごとの DPIA/PIA、モデル比較評価、社内証拠保全基盤の WORM 化	持続運用可能なガバナンスに移行する。 [38]

未確定事項

現時点で実務上とくに重要な未確定事項は、**Gemini 3.5 Flash の Computer Use について、Google が 3.5 専用の詳細モデルカード、保存ポリシー、confirmation UX、明示的 action taxonomy をどこまで公開するか**です。3.5 統合は公式発表済みですが、2.5 のような詳細ベンチマーク・限界・リスク文書が十分公開されるまで、企業は PoC で自ら確認すべきです。これは導入可否そのものではなく、**どの法的リスクをベンダー責任に置けるかの見極め**に直結します。 [39]

また、**Google の 3.5 Computer Use が “across platforms” をどの程度意味するか**も未確定です。2.5 モデルカードは主に web browser を最適化対象とし、OS-level control は未最適化としていました。3.5 でどこまで Windows/macOS/VDI/仮想デスクトップへ安定拡張されたのかは、公開文書からはまだ読み切れません。知財業務では UI の差異が大きいため、この点は PoC の最優先確認項目です。 [40]

優先調査チェックリスト

- 自社が想定する知財ユースケースは、**閲覧・収集・入力・送信・同意・提出**のどれに当たるか。高リスク操作が含まれるか。 [41]
- 画面に表示される情報は、**個人データ、営業秘密、著作物、訴訟保留対象文書**のいずれを含むか。 [42]
- Google 側で **Cloud Audit Logs / Data Access / Observability** を有効化し、案件IDで追えるか。 [43]
- ベンダー契約で、**学習不使用、保存期間、サブプロセッサ、越境移転、法的保持協力**が明確か。 [44]
- 発明創出支援に使う場合、**人間の創作的寄与を後から説明できるログ**が残るか。 [45]
- 著作権・データベース・利用規約上、**画面読取りや大量抽出が許容されるか**。許容されないなら API 又はライセンス取得へ切り替えるか。 [46]
- 証拠利用を予定するなら、**ハッシュ、タイムスタンプ、承認履歴、WORM 保管**があるか。 [21]

総括すると、Gemini 3.5 Flash の Computer Use 統合は、知財部門の手作業を大幅に圧縮しうる一方、**「情報を読む AI」ではなく「情報に触り、送り、変える AI」**を社内へ入れることを意味します。特許では発明者性の立証、著作権では複製・依拠・事業者責任、営業秘密では GUI 経由の持出し、契約では代理同意、コンプライアンスでは個人データ・高リスク AI・監査、訴訟では真正性の高いログという、従来は別々に扱われがちだった論点が一つの実装に集約されます。したがって、知財業務での導入可否は「精度が高いか」ではなく、**統制・証拠・責任分界を前提にしてもなお ROI が出るか**で判断すべきです。現時点では、限定ユースケースから始め、Google の今後の 3.5 向け詳細仕様公開を追いながら、監査可能性を中心に段階導入するのが、最も法務的に堅牢な選択です。 [47]

---

1 https://ai.google.dev/gemini-api/docs/changelog
https://ai.google.dev/gemini-api/docs/changelog

2 20 27 42 https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf
https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf

3 12 18 22 28 43 https://docs.cloud.google.com/gemini-enterprise-agent-platform/machine-learning/general/audit-logging
https://docs.cloud.google.com/gemini-enterprise-agent-platform/machine-learning/general/audit-logging

4 25 26 39 40 47 https://blog.google/innovation-and-ai/models-and-research/gemini-models/introducing-computer-use-gemini-3-5-flash/
https://blog.google/innovation-and-ai/models-and-research/gemini-models/introducing-computer-use-gemini-3-5-flash/

5 6 9 10 11 https://storage.googleapis.com/deepmind-media/Model-Cards/Gemini-2-5-Computer-Use-Model-Card.pdf
https://storage.googleapis.com/deepmind-media/Model-Cards/Gemini-2-5-Computer-Use-Model-Card.pdf

7 https://research.google/blog/screenai-a-visual-language-model-for-ui-and-visually-situated-language-understanding/
https://research.google/blog/screenai-a-visual-language-model-for-ui-and-visually-situated-language-understanding/

8 https://ai.google.dev/gemini-api/docs/models/gemini-3.5-flash
https://ai.google.dev/gemini-api/docs/models/gemini-3.5-flash

13 45 https://www.cafc.uscourts.gov/opinions-orders/21-2347.OPINION.8-5-2022_1988142.pdf
https://www.cafc.uscourts.gov/opinions-orders/21-2347.OPINION.8-5-2022_1988142.pdf

14 https://www.uspto.gov/sites/default/files/documents/ai-inventorship-memo.pdf
https://www.uspto.gov/sites/default/files/documents/ai-inventorship-memo.pdf

15 16 46 https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94037901_01.pdf
https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/94037901_01.pdf

17 https://laws.e-gov.go.jp/law/405AC0000000047
https://laws.e-gov.go.jp/law/405AC0000000047

19 31 34 35 41 https://developers.openai.com/api/docs/guides/tools-computer-use
https://developers.openai.com/api/docs/guides/tools-computer-use

21 https://csrc.nist.gov/pubs/sp/800/92/final
https://csrc.nist.gov/pubs/sp/800/92/final

23 33 37 https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_1.pdf
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_1.pdf

24 https://docs.cloud.google.com/docs/security/security-best-practices-genai/recommended-iam-groups?hl=ja
https://docs.cloud.google.com/docs/security/security-best-practices-genai/recommended-iam-groups?hl=ja

29 30 https://docs.anthropic.com/en/docs/build-with-claude/computer-use
https://docs.anthropic.com/en/docs/build-with-claude/computer-use

32 https://learn.microsoft.com/en-us/microsoft-copilot-studio/computer-use
https://learn.microsoft.com/en-us/microsoft-copilot-studio/computer-use

36 https://docs.cloud.google.com/gemini-enterprise-agent-platform/models/enable-audit-logs
https://docs.cloud.google.com/gemini-enterprise-agent-platform/models/enable-audit-logs

38 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016R0679
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016R0679

44 https://www.ppc.go.jp/files/pdf/generativeAI_notice_leaflet2023.pdf
https://www.ppc.go.jp/files/pdf/generativeAI_notice_leaflet2023.pdf