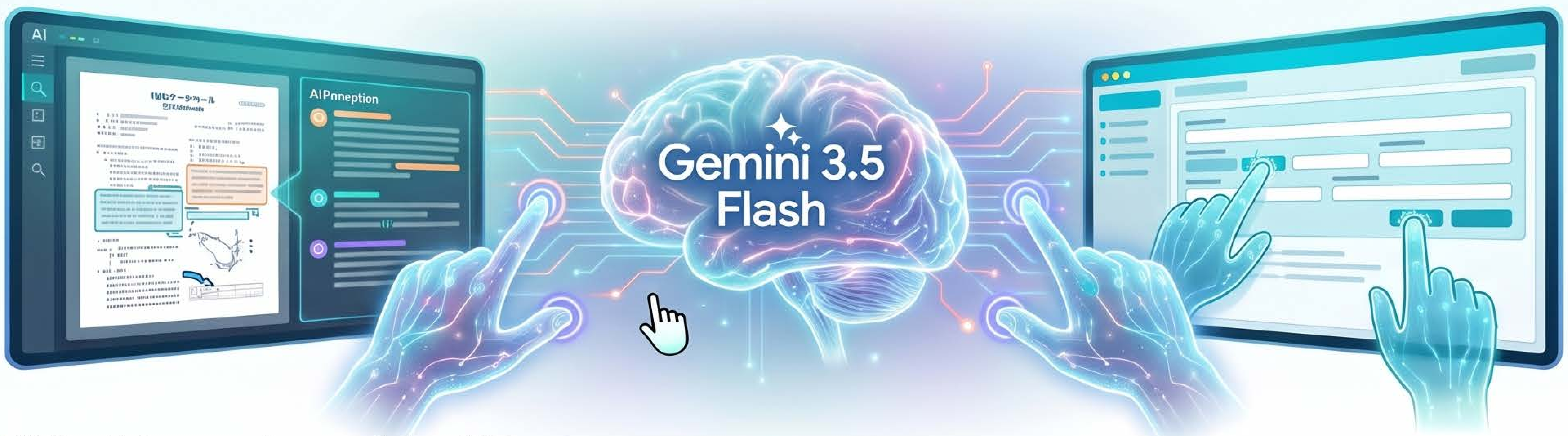
Gemini 3.5 Flash「Computer Use」が拓く知財実務の未来：自動化の進化とリスク管理

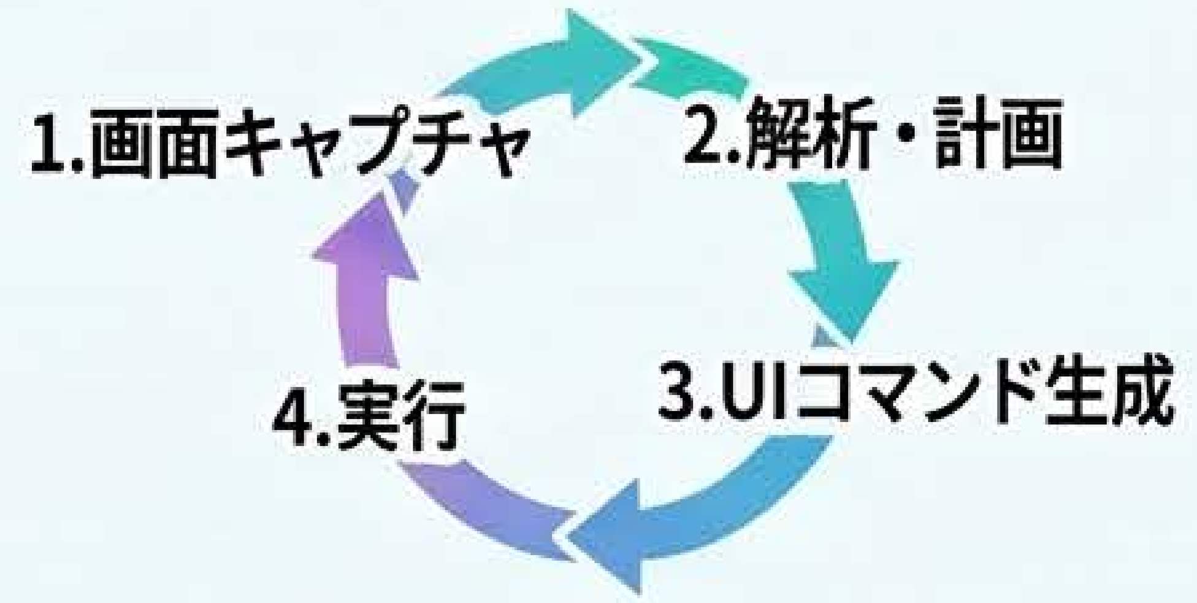


技術の核心：AIに「目」と「手」が備わった

Computer Use：汎用モデルへのネイティブ統合

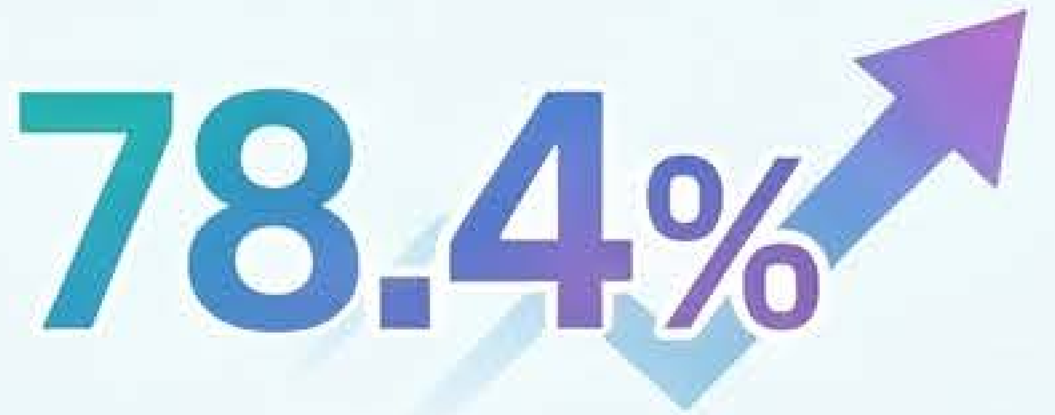
従来の特化型モデルではなく、主力のGemini 3.5 Flashそのものが画面認識・推論・クリック・入力の能力を獲得しました。

エージェントループの仕組み



タスク完了まで自律的に動作します。

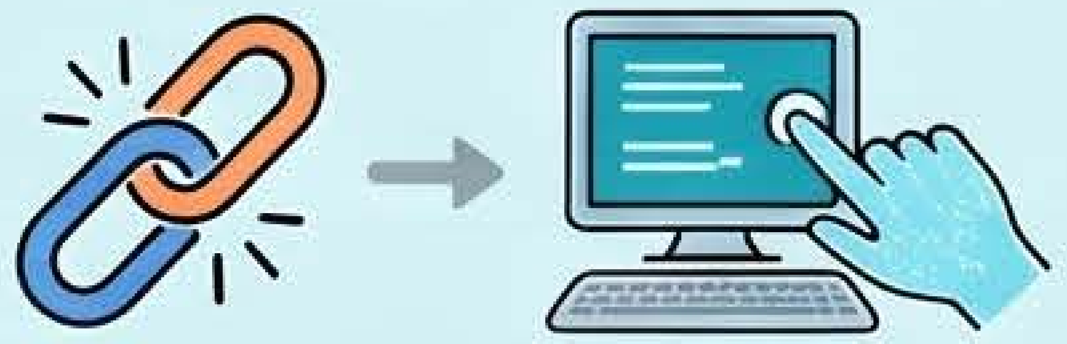
業界トップクラスの操作精度「78.4%」



ベンチマーク「OSWorld-Verified」において、先行するClaude Sonnet 4.Eと同等の高いスコアを、より低コストなFlashティアで達成しました。

知財実務への具体的インパクト

API不要でレガシーシステムを操作

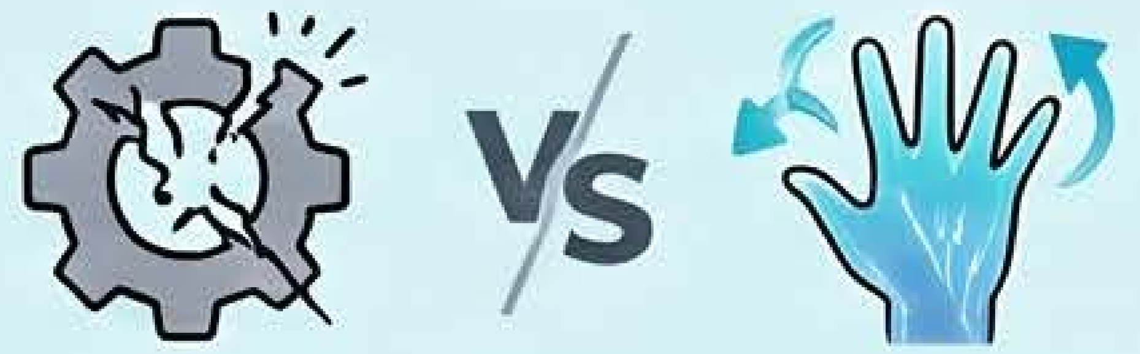


APIを持たないJ-PlatPatや社内システムも、AIがブラウザやデスクトップを直接操作することで自動化の対象になります。

複数アプリをまたぐワークフロー

といった、ツール間を横断する一連の工程を単一のエージェントが遂行します。

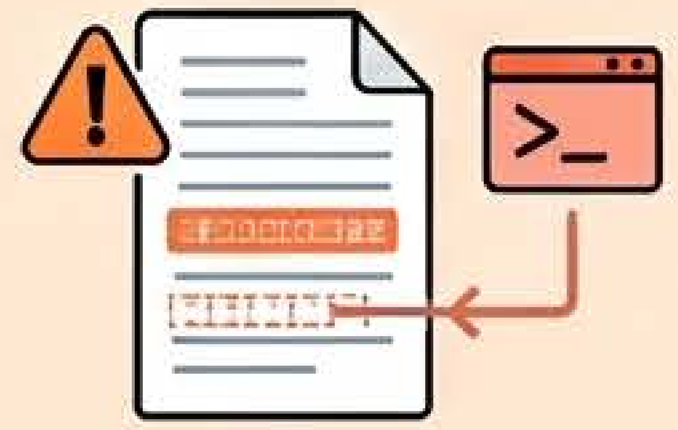
従来のRPAを超える適応力



ボタン配置の変更で壊れるRPAとは異なり、AIは画面を「理解」して操作するため、UIの変更にも柔軟に対応可能です。

⚠ 直面する構造的リスク

間接プロンプトインジェクション



外部サイトの不可視テキストからAIに不正命令が送り込まれ、意図しない操作を実行させられるリスクがあります。

営業秘密・秘匿特権の喪失

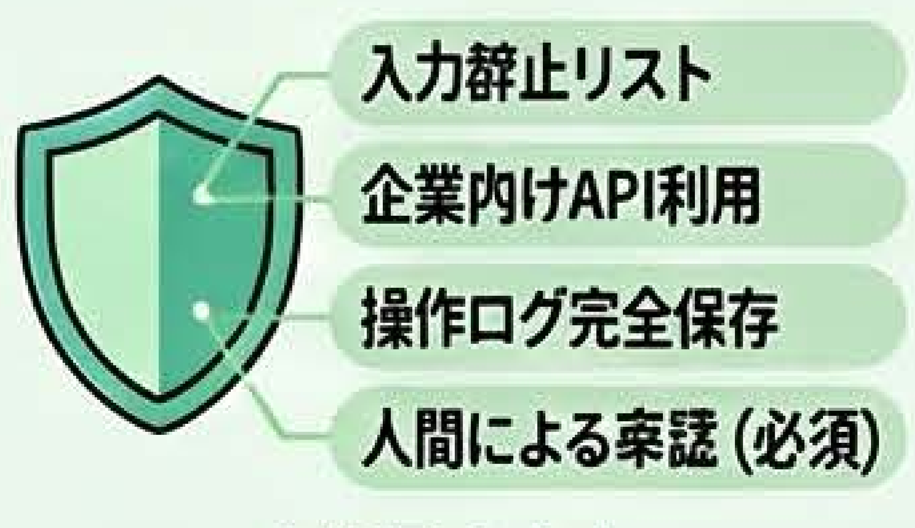
公開型AIへの入力は、営業秘密としての「合理的秘密措置」を欠くとみなされ、法的保護を受けられなくなる可能性があります。

ハルシネーションと法的責任

AIの誤操作や誤った先行技術判定が「権利の濫用」や「損害賠償」に直結するリスクがあり、最終確認は常に専門家の責任となります。

知財業務への導入ガイドライン

多層防御（Defense-in-Depth）の設計



を必須とします。

リスクレベル別導入優先順位

低リスク	業務内容：公開情報のウォッチング、一次顧客情報の整理 指針：先行情報を確認。効率化の意義が大きい。
中リスク	業務内容：社内システムへの入力、ドラフト初稿作成 指針：人間による確認（Homan-in-the-loop）を必須とする。
高リスク	業務内容：契約交渉、権利の修業・継続、FTO判断の確定 指針：AIの自動実行を禁止。人間の承認が不可欠。

専門家の役割の変化

「触れるAI」から「動かすAI」の監督へ：定型的な閲覧や操作はAIが担い、弁理士や専門家は「戦略立案」と「AIの成果物の品質検証」に注力する時代へ移行します。