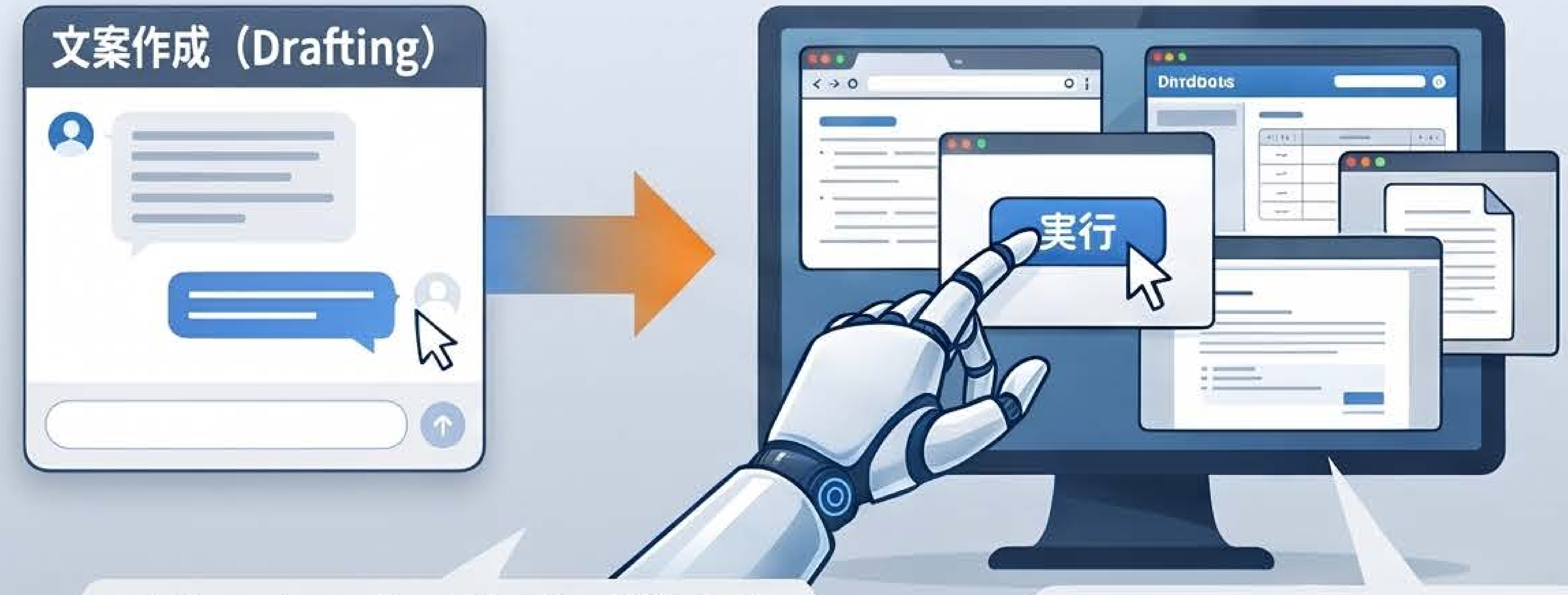
Gemini 3.5 Flash「Computer Use」：知財実務への導入とリスク管理ガイド

AIが実行主体となる変革、法的・技術的リスク、そして安全な導入ステップ

進化するAI：文案作成から「実行主体」へ



スクリーンショット、テキスト、行動履歴を解析し、次のUI操作（関数呼び出し）を生成。プラットフォームを横断した操作が可能。

知財業務における具体的な活用例

- 先行技術調査
- 特許庁ポータルからの定型ダウンロード
- 契約台帳への自動入力
- 侵害モニタリングの証拠保全キャプチャ

RPAの上位互換としてのポテンシャル

APIが未整備な特許庁や裁判所のサイト、商用データベース、レガシーな契約管理システムでも、GUIを介して人間同様に操作可能。

知財実務における4つの重大リスク

⚠ 秘密情報の「死角」からの持ち出し

従来のDLPが検知しにくいスクリーンショット経由で、M&Aデータルームや出願ドラフトなどの機密情報がモデルに処理されるリスク。

⚠ 意図しない「法的同意」の代行

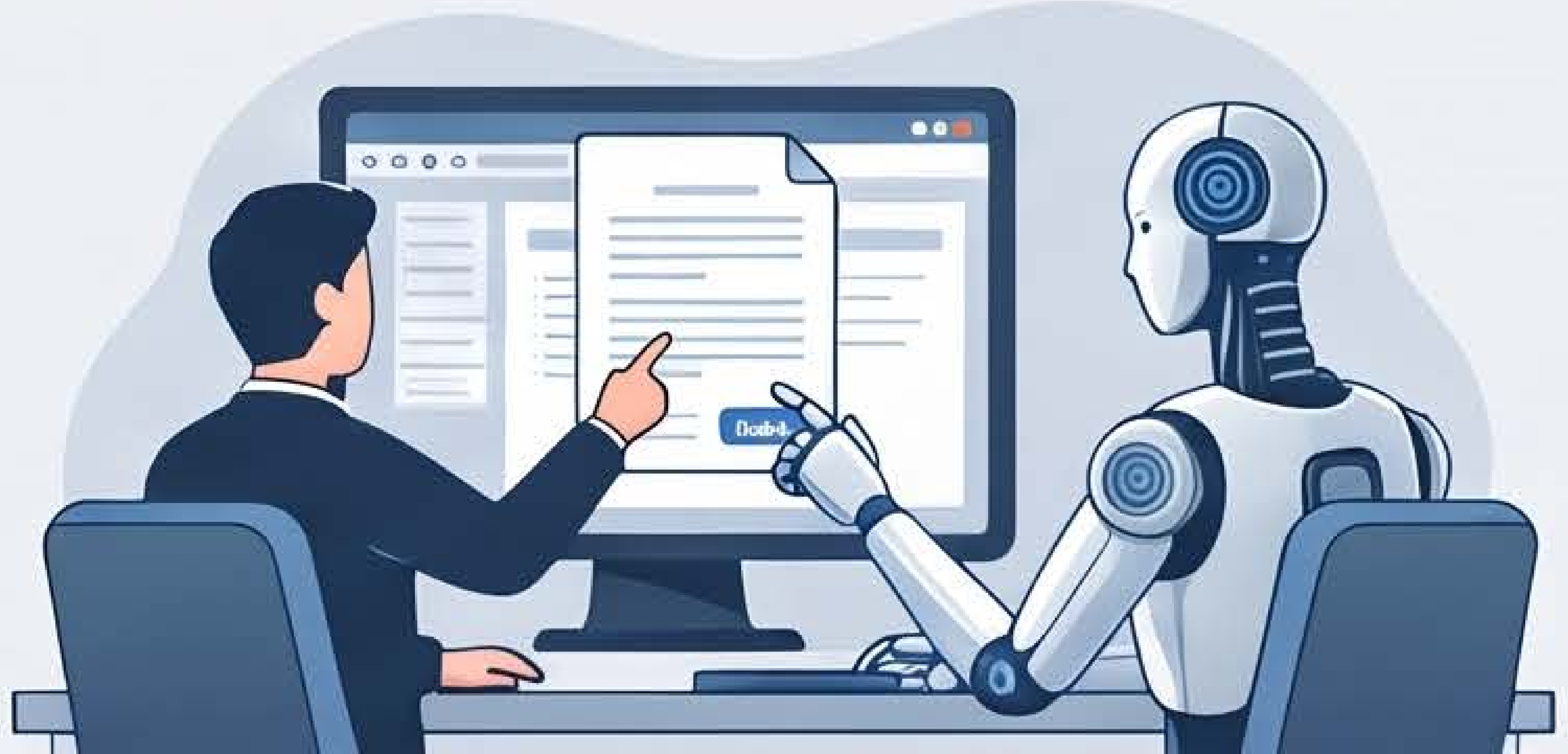
AIが利用規約の「同意」や「送信」を代行することで、意図しない契約締結や機密データの外部送信が発生する危険性。

⚠ 発明者性と立証の困難化

AIが着想・選択・組合せを高速反復することで、人間の「創作的寄与」の境界が曖昧になり、将来の職務発明紛争における立証が難しくなる恐れ。

⚠ 著作権・契約の遵守

GUI経由の大量取得（スクレイピング）は、たとえ解析目的であっても、利用規約や著作権法上の享受目的の有無により違法と判断される可能性。



推奨される「人間中心」の実装フロー

1. 利用者の指示とポリシー判定

ユーザーの指示が社内ポリシーに合致しているか、専用実行環境で安全に処理できるかをまず確認。

2. 提案アクションの生成と検閲

人間の承認（Human-in-the-Loop）

高リスクな操作（送信・同意・支払）については必ず「人間の承認」を必須とします。

3. 実行ハーネスによる操作とログ保存

直接AIに権限を与えず、仲介するプログラム（ハーネス）が操作を実行し、完全なログを記録。

4. 証拠性の確保とレビュー

入力 → 画面 → 操作 → 承認 → 結果

入力、画面、操作、承認、結果を紐づけて保存し、後から「誰が何をしたか」を説明可能な状態（トレーサビリティ）にする。

実務対応ロードマップ

期間	優先アクション	目的
短期	許可ユースケースの限定、Data Accessログ有効化、送信操作のHuman-in-the-loop化	無秩序な利用を防止、最低限の証拠性を確保
中期	ベンダー契約改定（学習不使用等）、知財SOP改訂、訴訟ホールド手順へのログ組込み	責任分界と紛争時対応の明確化
長期	API-first / GUI-second 原則の確立、ユースケース別のDPIA実施、証拠保全のWORM化	持続可能なガバナンス体制への移行