【社外秘・複製禁止・第三者共有禁止】

AILEX（エーアイレックス）所内稟議資料

AI法務支援クラウドSaaS 導入検討のご案内

作成日	2026年02月18日
作成者	AILEX合同会社
対象	法律事務所 所内検討用
機密区分	社外秘・複製禁止・第三者共有禁止

本資料の目的

本資料は、AI法務支援クラウドSaaS「AILEX」の導入を所内で検討いただくための稟議資料です。AILEXが提供する機能、セキュリティ対策、弁護士の守秘義務との整合性、想定リスクと対策、および導入手順について整理しています。

結論：AILEXは、PII自動マスキング技術により依頼者への同意・説明の負担を軽減しやすい設計を採用しています。所内規程・案件類型に応じた運用ルール策定のうえ、ダミー案件からの段階的導入を推奨します。

1. AILEXでできること

AILEXは、小〜中規模法律事務所（弁護士1〜5名）向けに設計されたAI法務支援クラウドSaaSです。訴訟実務に必要な機能をワンストップで提供し、事件管理からAI文書生成、電子提出まで一貫して対応します。

想定される導入効果

AILEXの導入により、以下の業務で所要時間の短縮・品質向上が見込まれます。効果は事務所の規模・案件構成により異なりますが、主に定型的な下準備・整理作業の効率化に寄与します。

業務領域	AILEXによる支援内容
証拠番号の付番・整理	mints提出パッケージの自動生成で手作業を削減
時系列・争点の整理	AI事件分析で構造化された叩き台を即時生成
書面ドラフト作成	58テンプレートにより初稿作成を大幅に短縮
相手方書面への反論準備	反論ポイント自動抽出で着手速度を改善
陳述書の初稿起案	4立場対応のAIドラフトで構成検討を支援
mints電子提出のパッケージ化	コンプライアンスバリデーション付きZIPをワンクリック生成
事件情報の属人化解消	事件管理・文書管理の一元化で引継ぎ負担を低減

主要機能一覧

機能	概要
AI法律相談チャット	Claude APIを使用。日本法に特化した専門的回答を生成。 事件コンテキストを自動注入し、案件固有の相談が可能
AI文書生成 （58テンプレート）	訴訟書面・交渉文書・契約書等を事件データに基づきAI生成。 民事訴訟、家事事件、刑事事件、債務整理、労働事件等に対応
AIファクトチェック	AI回答の正確性をPerplexity APIで独立検証。法的根拠・判例の妥当性を出典URL付きで確認
AI事件分析	関係図・請求構造・時系列・争点弱点の4タブで事件を構造化分析
相手方書面AI分析	相手方の準備書面を自動分析し、反論ポイント・ドラフトを自動生成
陳述書ドラフトAI	原告・被告・証人・関係者の4立場に対応した陳述書草案をAI生成
事件管理	事件の登録・進行管理・ステータス追跡。コンフリクトチェック機能付き
文書管理	全文テキスト検索＋セマンティックサーチ。ZIPインポート（OCR自動解析）対応
契約書チェック	PDF/画像の契約書をAIがリスク分析、指摘事項と改善提案を自動生成

機能	概要
mints提出パッケージ	裁判所電子提出システム（mints）対応のZIPをワンクリック生成。 証拠番号スタンプ・コンプライアンスバリデーション搭載
スケジュール管理	期日・締切管理。書類からの自動抽出。Googleカレンダー連携対応
タスク管理	タスク作成・担当者割り当て。AI自動優先度スコアリング機能付き
請求書管理	タイムエントリー・請求書発行・PDF生成・メール送付
依頼者ポータル	トークンベースでログイン不要。進捗確認・文書共有・メッセージ送受信
AIエージェント	自然言語でデータ横断検索。14ツールによる統合的なAI支援

競合サービスとの比較について：当社が2026年2月時点で実施した調査（注1）の範囲では、AI生成結果を別のAIで独立検証するファクトチェック機能を標準搭載したリーガルテックSaaSは確認されませんでした。また、訴訟当事者情報の構造化PIIマスキングを搭載したサービスも、主要サービス比較では該当が確認されていません。

（注1）調査条件：2026年2月実施。国内主要リーガルテックSaaS 50社超を対象。各社公式サイト・プレスリリース・製品ドキュメントに基づく机上調査。非公開機能・開発中機能は調査範囲外。調査結果は調査時点のものであり、その後の各社サービス更新を反映しない場合があります。詳細な調査レポートは別途ご提供可能です。

2. どう安全に使うか

AILEXは、弁護士の守秘義務（弁護士法第23条）との両立を設計の中核に据えています。以下の多層的な安全対策により、依頼者情報を保護しながらAI技術を活用できます。

2.1 PII自動マスキング（最重要防御層）

AILEXの最も重要なセキュリティ機能です。外部AI
APIへのデータ送信前に、個人識別情報（PII）を自動的にプレースホルダに置換し、API応答受信後に復元します。

処理フロー：
ユーザー入力 → PIIMasker（マスク処理）→ マスク済テキスト → 外部API送信
ユーザー表示 ← PIIMasker（復元処理）← マスク済応答 ← API応答

外部APIサーバーに到達するデータには、事件番号・当事者名・裁判所名が含まれません。

機能	使用API	PIIマスキング
AI法律相談チャット	Anthropic Claude API	適用
ファクトチェック	Perplexity Sonar API	適用
AI文書生成	OpenAI GPT-4o API	適用
ZIPインポートOCR	Anthropic Claude API	非適用（注2）
コンフリクトチェック	外部API不使用	—

（注2）OCR処理はPDFバイナリを直接送信するため、テキストレベルのマスキングは構造上不可能です。インポート画面には注記が表示され、インポート後のAI処理にはマスキングが適用されます。運用上の推奨：実データをZIP投入する前に、所内ルールに従い、必要に応じて匿名化済みPDFの使用または赤入れ（墨消し）済み文書の使用をご検討ください。

同意・説明の負担を軽減しやすい設計：PIIマスキングにより、外部APIに個人識別情報が到達しない設計のため、依頼者への同意・説明に関する負担を軽減しやすい構造です。

ただし、同意・説明の要否は、各事務所の所内規程、案件類型、委任契約条項により結論が異なります。AILEXの技術的設計をもって一律に不要と判断するものではありません。導入にあたっては、所内の情報セキュリティ規程に照らしてAILEX利用時の取扱いを定めたうえで運用いただくことを推奨します。

2.2 アクセス制御・認証

対策項目	内容
二要素認証（2FA）	メールベース6桁OTPコード。最大5回試行。11分でセッション破棄
ロールベース権限	admin / attorney / paralegal / staff の4段階。 事件データは作成者のみアクセス可（adminを除く）

対策項目	内容
LINE Login連携	LINE OAuth2認証によるシングルサインオン対応
reCAPTCHA v2	ボット攻撃・不正ログイン防止
パスワードポリシー	強度スコア4以上必須（大小文字・数字・記号・8文字以上）
CSRF対策	全POSTリクエストにCSRFトークンを適用
SQLインジェクション対策	PDOプリペアドステートメントによるパラメータバインド

2.3 監査ログ

すべての重要操作はAuditLoggerにより自動記録されます。タイムスタンプ、IPアドレス、User Agent、重要度レベルとともに記録され、インシデント発生時の影響範囲把握・原因調査に活用できます。

記録対象	重要度
ログイン成功/失敗	high
事件作成・削除	medium / high
AI文書生成・削除	medium
請求書作成・ステータス変更	high / medium
ユーザー招待・削除	high
PIIマスキング実行	medium（統計情報のみ。原文は非記録）

2.4 外部APIプロバイダのセキュリティ体制

AILEXが利用する3社のAPIプロバイダのセキュリティ体制は、各社が公開するセキュリティ文書・利用規約に基づく情報です（注3）。具体的な契約条件・認証取得状況の証跡が必要な場合は、各社の公式セキュリティページまたは当社経由でご確認いただけます。

項目	OpenAI (GPT-4o)	Anthropic (Claude)	Perplexity (Sonar)
API学習利用	APIデータ不使用 （利用規約に明記）	商用契約下で不使用 （利用規約に明記）	不使用（利用規約に明記）
データ保持	契約条件に従う （ZDRオプションあり）	契約条件に従う （ZDRオプションあり）	デフォルトで データ保持なし
SOC 2 Type II	取得（公式に掲載）	取得（公式に掲載）	取得（公式に掲載）
通信暗号化	TLS 1.2+	TLS	TLS

項目	OpenAI (GPT-4o)	Anthropic (Claude)	Perplexity (Sonar)
DPA(データ処理契約)	利用可能	自動適用	利用可能

(注3)記載内容は各社の以下の公式セキュリティ文書に基づきます (OpenAI: trust.openai.com / Anthropic: trust.anthropic.com / Perplexity: docs.perplexity.ai)。各社の認証取得状況・DPA締結状況の証跡は、ご要望に応じて個別にご提供可能です。記載は2026年2月時点の情報であり、各社のポリシー変更により内容が更新される場合があります。

多重防御の設計思想:仮にAPIプロバイダ側でセキュリティインシデントが発生し、保持データが漏洩したとしても、PIIマスキング済みのデータからは個人を特定できません。PIIマスキングはAPIプロバイダのセキュリティ体制とは独立した防御層として機能します。

2.5 データ管理

項目	内容
データ保管場所	日本国内サーバー(XServer)
通信暗号化	全通信HTTPS/TLS暗号化
データ分離	ユーザーID(user_id)による厳格なデータ分離
削除対応	事件データ・文書・チャット履歴の個別削除が可能
AI学習利用	入力データのAI学習利用なし(フッター・トップページに明示)

3. どこまでを人が責任持つか

AILEXは「AIの出力はあくまで参考情報」という原則を技術的に担保しています。すべてのAI出力には参考情報である旨が表示され、弁護士の精査・修正を経ることなく依頼者に提供されることは技術的に防止されています。

3.1 弁護士とAIの責任分界

機能	AIが担当する範囲	弁護士が担当する範囲
AI法律相談チャット	法的論点の整理、判例・条文の参照提示	回答内容の正確性確認、最終的な法的判断
AI文書生成	テンプレートに基づく草案作成、出典タグ付与	内容の精査・修正、依頼者への提出判断
ファクトチェック	AI回答の独立検証、出典URL提示	検証結果の妥当性判断、最終的な採否決定
AI事件分析	事件の構造化分析（関係図・争点等）	分析結果の検証、訴訟戦略の最終決定
相手方書面分析	反論ポイントの自動抽出・ドラフト生成	反論内容の精査、準備書面の最終作成

3.2 最終確認ステップ（人間のゲートキーピング）

・AI生成文書は必ず弁護士が内容を精査してから利用する

・ファクトチェック機能を積極的に活用し、AI回答の正確性を検証する

・AI出力をそのまま裁判所提出書面や依頼者への回答に使用しない

・判例・条文の引用は原典で確認する（ハルシネーションリスクへの対応）

・AI事件分析の結果は訴訟戦略の「叩き台」として使い、最終判断は弁護士が行う

日弁連の姿勢との整合：日弁連は「弁護士も思考することを止めてはいけない」とする立場を示しています。AILEXはこの姿勢と一致する設計を採用しており、AI出力には常に「参考情報」である旨を表示しています。

ハルシネーション対策の設計方針：AIの法律回答には誤情報（ハルシネーション）が含まれるリスクがあることが広く知られています。AILEXは、独立したファクトチェック機能（Perplexity API）と原典確認をワークフローに組み込むことで、弁護士が効率的に検証を行える仕組みを標準搭載しています。

4. 想定リスクと対策

リスク項目	影響度	対策
AIのハルシネーション（誤った法的情報の生成）	高	・ファクトチェック機能で独立検証 ・判例・条文は原典で確認 ・AI出力には「参考情報」と明示 ・弁護士による最終精査を必須化
PIIマスキングの漏れ（個人情報の外部流出）	低	・structuredモード：事件DBから自動マッピング ・fullモード：正規表現で電話番号等も検出 ・マスキング実行は監査ログに記録 ・継続的な精度検証の仕組みを整備中
APIプロバイダの セキュリティインシデント	低	・PIIマスキングにより個人特定不可能 ・3社すべてSOC 2 Type II取得（注3参照） ・APIデータの学習利用なし ・デュアルLLM構成で単一障害点を排除
不正アクセス・アカウント乗っ取り	中	・二要素認証（2FA）による多要素認証 ・reCAPTCHA v2によるボット防止 ・ログイン試行回数制限 ・包括的監査ログによる異常検知
事務所内の権限逸脱 （スタッフの不適切なアクセス）	中	・4段階のロールベースアクセス制御 ・事件データは作成者のみアクセス可 ・admin権限によるアカウント管理 ・操作ログによる事後追跡
弁護士法・懲戒リスク	低	・PII自動マスキングで守秘義務保護 ・AI出力は「参考情報」として提供 ・弁護士法第72条非該当の設計 ・所内規程に沿った運用を前提とした設計

4.1 法令適合性の確認状況

法令	AILEXの対応	評価
弁護士法第23条（守秘義務）	PII自動マスキングにより、外部APIに個人識別情報が到達しない設計。 同意・説明の要否は所内規程・案件類型に応じて判断	○
弁護士法第72条（非弁行為）	AILEXは弁護士の業務支援ツールであり、法律事務の提供主体ではない。 AI出力は「参考情報」として弁護士の判断を補助する位置づけ	◎
日弁連情報セキュリティ規程（会規第117号）	技術的安全管理措置の大部分に適合。 2FA、RBAC、監査ログ、PIIマスキング、通信暗号化等を実装	○
個人情報保護法	PIIマスキング後のデータは「個人データ」に非該当と整理しうる。 「クラウド例外」（Q&A; 7-53）との整合性を確保した設計	○
刑法第134条（秘密漏示罪）	PIIマスキングにより秘密の「漏示」に該当しにくい設計	○

※ 上記の法令適合性評価は、AILEXの技術的設計に対する当社の評価です。具体的な法的判断については、導入事務所の弁護士にてご確認ください。評価は「◎ = 十分に対応」「○ = 概ね対応（一部運用上の考慮が必要）」を意味します。

5. 導入手順（段階的アプローチ）

AILEXの導入は、リスクを最小化するため段階的に進めることを推奨します。まずダミー案件で操作に慣れ、安全性を確認した上で実案件への適用を開始してください。

Phase 1：準備・トライアル（1〜2週間）

・AILEXアカウントを作成（無料プランで開始可能）

・管理者（admin）を決定し、二要素認証（2FA）を有効化

・ダミー案件を登録し、以下の機能を試用：

- AI法律相談チャット（架空の法的質問で回答品質を確認）
- AI文書生成（ダミーデータでテンプレートを試用）
- ファクトチェック（AI回答の検証精度を確認）
- ZIPインポート（テスト用PDFでOCR精度を確認）

・PIIマスキングの動作を確認（マスク前後の表示を確認）

Phase 2：限定運用（2〜4週間）

・低リスクの実案件（既に終結した事件の振り返り等）で試用開始

・利用する弁護士を1〜2名に限定し、運用ルールを策定

・AI生成文書の品質・正確性を実案件ベースで検証

・ファクトチェック機能の活用を習慣化

・監査ログを確認し、運用状況をモニタリング

・PROプランへのアップグレードを検討（無制限メッセージ利用が必要な場合）

Phase 3：本格運用（1ヶ月目以降）

・事務所全体への展開（paralegal / staff ロールの追加）

・全進行中案件の事件管理への登録

・文書管理（ZIPインポート）による過去案件のデジタル化

・スケジュール管理・タスク管理の本格活用

・請求書管理・依頼者ポータルの活用開始

・mints提出パッケージ生成の活用（2026年5月以降の電子提出に対応）

・定期的な運用レビュー（月次）の実施

5.1 導入時チェックリスト

チェック項目	内容
管理者（admin）の決定	情報セキュリティ責任者として指定
二要素認証の有効化	全ユーザーに2FAの有効化を推奨

チェック項目	内容
ロール設定の確認	弁護士＝attorney、事務員＝staff等の適切な権限付与
ダミー案件でのテスト	実データ投入前にAI機能の動作・品質を確認
所内運用ルールの策定	AI出力の取扱い・ファクトチェック実施基準・ 同意説明の要否判断基準の明文化
所内研修の実施	AILEX操作方法・PIIマスキングの仕組み・注意事項の共有
OCR投入時の取扱い確認	実データZIP投入前の匿名化・墨消し要否を所内ルールで規定

お問い合わせ・サポート

AILEX合同会社
〒150-0043 東京都渋谷区道玄坂1-10-8 渋谷道玄坂東急ビル
メール：info@ailex.co.jp
公式LINE：https://lin.ee/P9JAWZp
公式サイト：https://ailex.co.jp

導入に関するご質問・デモのご依頼は、上記窓口までお気軽にお問い合わせください。
外部APIプロバイダの認証取得証跡・DPA締結状況等の追加資料も、ご要望に応じて提供可能です。