AILEX

Public Security Overview

セキュリティ概要（公開版）

弁護士向けAI法務プラットフォームのセキュリティ設計原則

文書分類: PUBLIC
バージョン: 1.0 ｜ 発行日: 2026年2月13日
AILEX合同会社 ｜ info@ailex.co.jp

（顧問弁護士事務所：弁護士法人えそら）

本書について

本書はAILEX のセキュリティ設計原則の概要を公開用に記述したものです。実装の詳細仕様・脆弱性対応状況・インフラ構成等は、導入検討事務所向けの「Security Whitepaper（CONFIDENTIAL版）」に記載しています。CONFIDENTIAL版のご請求は info@ailex.co.jp までお問い合わせください。

1. 設計原則 ── 検証可能なAIリーガルOS

AILEXは「AIの便利さ」ではなく「AIの証明可能性」を提供するプラットフォームです。設計の全領域において、以下の4原則を貫いています。

01 守秘義務ファースト

外部AI APIに送信されるデータから、個人識別情報を技術的に除去します。弁護士法第23条の守秘義務とAI活用を両立させるための、プラットフォームの中核防御層です。

02 Human-in-the-Loop

すべてのAI出力は「参考情報」です。弁護士による確認・修正・確定を経なければ、依頼者への提供やエクスポートは技術的に実行できません。

03 改ざん不能な証跡

すべての操作・AI生成・弁護士の判断は監査ログに記録され、事後的な改変は技術的に防止されます。「誰が・いつ・何を・どう判断したか」が検証可能です。

04 最小権限の原則

4段階のロールベースアクセス制御により、各ユーザーは業務上必要な最小限の情報にのみアクセスできます。

2. PII自動マスキング

AILEXのすべてのAI機能（法律相談チャット・文書生成・ファクトチェック）において、外部AI APIへの送信前に個人識別情報（PII）をプレースホルダに自動置換し、応答受信後に復元するセキュリティレイヤーを実装しています。

2.1 処理フロー

弁護士の入力テキスト中の個人識別情報は、AILEXサーバー内で自動的にプレースホルダに変換されてからAI APIに送信されます。AI APIからの応答を受信した後、プレースホルダを原文に復元して弁護士に表示します。

```
弁護士入力:   「原告 山田太郎 の令和5年(ワ)第123号について...」
      |
      v
PIIMasker:    「原告 [原告A] の [事件番号] について...」
```

```
      |
      v      (TLS 1.2+ 暗号化通信)
外部AI API:  プレースホルダのみを受信 ── 個人識別不可能
      |
      v
PIIMasker:   プレースホルダを原文に復元
      |
      v
弁護士表示:  「原告 山田太郎 の令和5年(ワ)第123号について...」
```

2.2 マスキングモード

モード	対象	用途
structured（デフォルト）	事件データベースから自動構築されたマッピング（事件番号・原告名・被告名・裁判所名）	通常の業務利用
full	上記に加え、正規表現パターンによる追加検出（電話番号・郵便番号・メール・生年月日等）	高セキュリティ設定
off	マスキング無効	管理者による明示的設定時のみ

2.3 なぜPIIマスキングが必要か

弁護士がAIツールを利用するたびに、依頼者一人ひとりに対して「AIにあなたの情報を入力します」と説明し同意を得ることは、実務上極めて高い導入障壁となります。PIIマスキングはこの問題を技術的に解決します。外部AI APIに到達するデータに個人識別情報が含まれないため、依頼者のプライバシーは構造的に保護されます。

透明性に関する注記: ZIPインポートOCR処理においてはPDFバイナリデータが直接AI APIに送信されます（テキスト抽出の技術的制約）。この設計上の例外は利用規約および技術文書において明示的に文書化しています。インポート後のテキストデータに対してはマスキングが適用されます。

3. Human-in-the-Loop ── 弁護士が最終判断者

AILEXのAI出力は、すべて「参考情報」として生成されます。弁護士による確認を経ずに、確定・エクスポート・依頼者への提供が行われることは、技術的に不可能な設計です。

3.1 統制の仕組み

統制ポイント	内容
免責表示の自動付与	すべてのAI出力に「本ドラフトはAIが自動生成したものであり、法的助言を構成しません。必ず弁護士が内容を確認・修正のうえご利用ください。」を自動挿入

弁護士による確定操作	AI出力の確定・エクスポートはattorneyロール以上に限定。確定者のID・日時を記録し、否認防止を実現
採用/棄却の記録	弁護士がAI出力を採用したか棄却したかを監査ログに記録。AI依存度の事後検証が可能
AIファクトチェック	AI生成物を別のAIで独立に検証するファクトチェック機能を標準搭載。引用カバー率をスコアとして記録
AI整合性チェック	申立書類間の数値整合（例：債権者一覧の総額と陳述書記載額の一致）をAIが自動検証し、不整合を弁護士に提示

3.2 弁護士法第72条との整合性

弁護士法第72条は、弁護士でない者が法律事務を取り扱うことを禁止しています。AILEXはAI出力を弁護士の判断材料として提供するのみであり、法律事務の主体は常に弁護士です。「申立書を作成しました」ではなく「申立書のドラフトを生成しました」と表記し、AIの役割を補助ツールに限定しています。

4. 監査ログと改ざん防止

AILEXは、すべての重要操作を監査ログに記録します。このログは追記専用（append-only）として設計され、アプリケーション層からの事後的な変更・削除は技術的に防止されます。

4.1 記録される情報

監査ログには、操作の種別、実行者、対象、タイムスタンプ、リクエストのトレーシングID、応答遅延、およびAI利用時のメタデータが記録されます。PIIマスキングの実行統計（マスク項目数・カテゴリ分布）もログに含まれますが、原文やマッピングテーブルは記録しません。

4.2 改ざん防止の設計思想

監査ログテーブルにはデータベースレベルの制約を設定し、レコードの削除・更新を拒否する設計としています。インフラ層における特権アクセスはホスティング事業者の管理ポリシーに依存するため、将来的には外部タイムスタンプ局（RFC 3161 TSA）との連携により、第三者検証可能な改ざん耐性を追加する計画です。

4.3 AI入出力の整合性検証

AI生成物の入力データおよび出力データは、暗号学的ハッシュとして記録されます。入出力の原文はデータベースに保持しません（データ最小化原則）。ハッシュにより、特定のAI出力がどの入力から生成されたかを事後的に検証できます。

5. 認証とアクセス制御

5.1 多層認証

AILEXは、パスワード認証（業界標準のハッシュアルゴリズム）、2要素認証（メールOTP）、ボット防止（reCAPTCHA v2）、ソーシャルログイン（Google / LINE OAuth2）を組み合わせた多層認証を実装しています。ブルートフォース攻撃に対するログイン試行制限、セッションの自動失効も実装済みです。

5.2 ロールベースアクセス制御（RBAC）

ロール	AI文書生成	生成物の確定	ユーザー管理	監査ログ閲覧
admin（管理者）	可	可	可	可
attorney（弁護士）	可	可	不可	不可
paralegal	可（弁護士承認要）	不可	不可	不可
staff	不可	不可	不可	不可

すべてのデータベースクエリにユーザーIDによるフィルタリングを適用し、テナント間のデータ隔離を保証しています。

6. 法令との整合性

6.1 弁護士法

条項	要件	AILEXの対応
第72条（非弁行為禁止）	弁護士でない者が法律事務を取り扱うことの禁止	AI出力はすべて「参考情報」。弁護士の確認・修正・確定を技術的に必須化。免責表示を自動付与
第23条（守秘義務）	職務上知り得た秘密の保持義務	PIIマスキングにより、外部AI APIに送信されるデータから個人識別情報を除去。依頼者のプライバシーを構造的に保護

6.2 個人情報保護法

条項	要件	AILEXの対応
第23条（安全管理措置）	個人データの安全管理	RBAC、2要素認証、監査ログ、PIIマスキング、TLS通信の多層防御
第28条（外国第三者提供）	外国にある第三者への個人データ提供規制	PIIマスキング後のデータは外部AIにおいて個人識別性を有しない形式に変換。データ越境移転に関する法的整理を別途文書化

6.3 日弁連情報セキュリティ規程

条項	AILEXの対応	適合評価
第3条 基本的な取扱方法	RBAC + 監査ログによるリスク可視化基盤を提供	適合
第4条 安全管理措置	2FA + RBAC + PIIマスキング + TLS + CSRF/XSS防止 + 監査ログ	適合
第5条 ライフサイクル管理	PIIマスキング + ゼロデータリテンション対応 + アクセス制御	適合
第6条 点検及び改善	監査ログによる点検データ + SaaSモデルによる継続アップデート	適合
第7条 漏えい等事故対応	自動通知 + 監査ログによるフォレンジック + 即座停止機能	適合

7. 外部AIプロバイダのセキュリティ

AILEXは複数のAI APIプロバイダを利用しています。各プロバイダのセキュリティ認証およびデータ取扱い方針は以下の通りです。

項目	プロバイダA	プロバイダB	プロバイダC
SOC 2 Type II	取得済	取得済	取得済
APIデータの学習利用	不使用	不使用	不使用
データ処理契約（DPA）	利用可能	自動適用	利用可能
通信暗号化	TLS 1.2+	TLS 1.2+	TLS 1.2+
ゼロデータリテンション	契約により対応可	契約により対応可	デフォルト適用

注: プロバイダ名称の詳細はCONFIDENTIAL版に記載しています。いずれも国際的なセキュリティ認証を取得した主要AIプロバイダです。

8. セキュリティ強化ロードマップ

AILEXは、以下のセキュリティ強化を段階的に実施する計画です。

時期	施策
2026年 前半	TOTP認証対応（Google Authenticator等）の追加、外部AIプロバイダとのゼロデータリテンション契約の明示的開示
2026年 後半	外部タイムスタンプ局（RFC 3161 TSA）連携による第三者検証可能な改ざん耐性の追加、WAF導入
2027年	SOC 2 Type II認証の取得準備、第三者脆弱性診断の定期実施体制の構築

すべての生成は記録され、すべての判断は検証できる。

本書に記載の設計原則の実装詳細、インシデント対応手順、データベース設計仕様、脅威モデルの全容については、導入検討事務所向けの「AILEX Security Whitepaper v1.0（CONFIDENTIAL版）」に記載しています。

CONFIDENTIAL版のご請求

セキュリティ白書の全文（CONFIDENTIAL版）は、導入を検討される法律事務所に対し個別に提供しています。以下よりお問い合わせください。メール: info@ailex.co.jp公式LINE: https://lin.ee/P9JAWZp公式サイト: https://ailex.co.jp

---

本書は技術概要文書であり、法的助言を構成しません。具体的な法的判断については弁護士にご相談ください。

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 ｜ info@ailex.co.jp

（顧問弁護士事務所：弁護士法人えそら）

文書ID: AILEX-SEC-PUB-v1.0-20260213 ｜ 分類: PUBLIC