



SECURITY WHITE PAPER

AILEX セキュリティ白書 v2.0

AILEX v2 (app.ailex.co.jp) における情報の保護と統制

AILEX v2 が法律事務所から預かる事件記録を、どこで保管し、どこで AI に処理させ、誰が触れうるのかを、根拠とともにまとめました。提供していないもの、国内完結の範囲に含まれないものも記載しています。

版	第 2.0 版 (2026年10月6日)
対象	AILEX v2 (https://app.ailex.co.jp)
発行	AILEX合同会社
Web 版	https://ailex.co.jp/security-whitepaper/

目次

この白書について	3
1. 要約	4
2. v1.0 からの変更	4
3. 責任の分担	5
4. データの所在と流れ	6
5. AI の処理と入力データ	9
6. アクセスの制御	10
7. 通信とアプリケーションの保護	12
8. 操作の記録	12
9. 保存・削除・返還	13
10. 再委託先と、法令に関する整理	14
11. インシデントへの対応と継続性	16
12. 事務所で行っていただくこと	16
13. 行っていないこと、提供していないもの	17
14. 法令・規程との対応	18
付録 A 確認の記録	19
付録 B 参照した資料	22
改訂履歴	23

本文の記述の後ろに付けた表示（契約・規約・観測・検証・AWS・当社申告）は、根拠の種別です。意味は「この白書について」の「根拠の示し方」に記載しています。

この白書について

AILEX v2 が、法律事務所から預かる事件記録をどこで保管し、どこで AI に処理させ、誰が触れうるのかを、根拠とともにまとめた文書です。導入を検討する法律事務所の方、弁護士会などで確認にあたる方に向けて書いています。できることだけでなく、行っていないこと、まだ提供していないものも記載します。

- **対象** AILEX v2 (<https://app.ailex.co.jp>)。ブラウザで利用する画面と、外部連携（MCP）の接続先を対象にします。
- **対象外** 従来版（users.ailex.co.jp）。従来版の仕組みは、2026年2月13日公開の v1.0 に記載しています。App Store で配布している iOS アプリは、現在は従来版に接続するため、対象に含みません。当社のコーポレートサイト（ailex.co.jp）も対象外です。
- **時点** 2026年10月6日。記載の内容は、機能の追加や契約の改定に伴って変わります。改訂したときは、末尾の改訂履歴に記録します。
- **用語** 「利用データ」は、利用者がアップロードまたは入力した事件情報・文書・相談内容などと、相談フォームや依頼者向けの画面を通じて相談者・依頼者から受け取った情報を指します。「事務所」は、利用者が所属する法律事務所などの、AILEX の上でひとまとまりに管理される単位です（利用規約 第2条）。「外部連携（MCP）」は、事務所が使う AI アシスタントなどから、AILEX の記録を参照するための接続口です。「推論プロファイル」は、Amazon Bedrock で、モデルと、その呼び出しを処理できるリージョンの組を定めたものです。「国内完結」は、保管と AI の処理が、日本国内のリージョンで行われることを指します。

根拠の示し方

記述の後ろに、根拠の種別を示しています。種別によって、読む方が自分で確かめられる範囲が異なります。

表示	根拠	確かめる方法
契約	利用契約（版 2026-09）。第一部、別紙1 秘密保持契約、別紙2 データ処理契約、付属書 A～C で構成	登録後、設定画面（設定 → 契約とデータ）で全文を確認できます。登録の前に確認したい場合は、お問い合わせください
規約	公開している利用規約とプライバシーポリシー（いずれも制定 2026 年9月18 日。最終改定は、利用規約が 2026年10月1日、プライバシーポリシーが 2026年9月29日）	利用規約・プライバシーポリシー
観測	2026年10月6日に、公開されている応答や、当社の検証用の事務所の画面で確かめた事実	付録 A に、確かめた内容と方法を記載しています
検証	当社が本番環境で行った検証の記録（実施日を付記）	付録 A-4
AWS	Amazon Web Services が公表している文書（2026年10月6日閲覧）	付録 B に URL を記載しています
当社申告	当社の設計文書と実装に基づく記載	外部からは確かめられません。当社の申告としてお読みください。ご質問には個別にお答えします

利用契約は、事務所の管理者が設定画面で同意した時から、その事務所に適用されます。同意の前に適用されるのは、公開している利用規約とプライバシーポリシーです。利用規約と利用契約が矛盾するときは、利用契約が優先します（利用規約 第1条）。本白書が引用する利用契約の条項は、2026年10月6日に設定画面に表示されていた本文（版 2026-09）によります。

利用契約と利用規約は、同じ内容を定めていても項番号が異なる箇所があります（たとえば、AI への入力を学習に使わない旨は、利用契約では第7条3項、利用規約では第7条4項）。本白書では、どちらの番号かを明記します。

1. 要約

- 1. 保管は東京、AI の処理は東京または大阪。** 事件情報・文書・データベースは AWS 東京リージョンに保管し、AI の処理は Amazon Bedrock の東京または大阪リージョンで行います。当社の判断で国外のリージョンへ送ることはありません。 契約：第7条2項・第12条2項、別紙2 第8条
- 2. 入力と出力は、モデルの学習に使われません。** 当社は利用データを AI モデルの学習・改善に使いません。AWS も、Amazon Bedrock への入力・出力をモデルの学習に使わず、モデルの提供者に共有しないと公表しています。不正利用の検知に伴う AWS 側の例外は、5.2 に記載します。 契約：第7条3項・第12条1項、別紙2 第4条3項
AWS：付録 B-2・B-3
- 3. 送信前のマスキングは行いません。** 従来版は、外部の AI 事業者へ送る前提でマスキングを行っていました。AILEX v2 は、AI の処理を保管と同じ管理下・日本国内に置く方式に変えました。 契約：第7条4項
- 4. 事務所ごとにデータを分離します。** 事件ごとに閲覧できる利用者を限定でき、限定した事件は、管理者であっても取扱者に登録されない限り開けません。 契約：第12条4項・5項
- 5. 入口を絞れます。** 2 要素認証を事務所の全員に求める設定と、接続を許す IP アドレスの指定を、事務所の設定で選べます。Microsoft Entra ID・Google Workspace との連携も、設定の項目として用意しています。
契約：付属書 B 4. 観測：付録 A-6 検証：2026年9月17日
- 6. 操作を記録します。** 事件の閲覧や AI の呼び出し（使ったモデルを含む）などの操作を記録し、事務所の画面で確認できます。記録には、入力した氏名や検索語、ファイル名が含まれ、利用データを削除したあとも保管します（8.3）。 契約：第12条6項 観測：付録 A-3
- 7. 無料期間の終了や更新の停止を理由に、利用データを削除しません。** 事務所の利用データをまとめて削除するのは、事務所から「利用終了およびデータ削除」の申請を受けたときです。利用者が画面で削除したものは、30 日間ゴミ箱に残ります。 契約：第8条の2・第10条の2 規約：利用規約 第10条の2
- 8. 利用データが届く再委託先は、AWS です。** 利用契約がサブプロセッサーとして挙げる先のうち、利用データが届くのは AWS です。このほか、不具合報告を AI が書き直した要約が、当社が開発に使う GitHub（米国の事業者のサービス）に送られます（4.4）。当社の役職員が利用データにアクセスできる場面は限定し、記録を残して、事務所の求めに応じて開示します。 契約：別紙1 第3条、別紙2 第5条・第7条、付属書 C 当社申告
- 9. 限界もあります。** 第三者機関による認証は取得していません。操作の記録を、当社に依らずに確かめる手段は、まだ提供していません。事務所が指定した宛先へのメール、利用者が接続した外部サービスや AI サービスへ渡った情報、不具合報告の要約は、国内完結の範囲に含まれません。詳しくは 4.5、8.4、13 に記載します。

2. v1.0 からの変更

v1.0（2026年2月13日）は、従来版を対象にしていました。AILEX v2 は、従来版の改良ではなく、AWS 上で組み直した別のシステムです（2026年9月に提供を開始）。守り方の前提が変わったため、白書も全面的に書き直しました。v1.0 の章立て（脅威の分類ごとの対策の一覧など）は、引き継いでいません。

観点	v1.0（従来版）	v2.0（AILEX v2）
AI の処理	外部の AI 事業者の API へ送信	Amazon Bedrock の東京・大阪リージョン。モデルを開発する事業者の API へは直接送らない 規約：利用規約 第7条3項
個人情報の扱い	一部の機能で、送信前に自動でマスキングし、応答を受けて復元	マスキングを行わない。AI の処理を、保管と同じ管理下・日本国内に置く 契約：第7条4項
稼働基盤	国内の共有レンタルサーバー	AWS 東京リージョン 契約：第12条2項 観測：付録 A-2
事務所の境界	事務所の識別子による共有	事務所単位の変離と、事件単位の情報遮断 契約：第12条4項・5項
認証	パスワードと 2 要素認証	2 要素認証の必須化、接続元 IP の制限、外部 ID 基盤との連携を、事務所が設定できる 契約：付属書 B 4. 観測：付録 A-6
操作の記録	追記だけを許す監査ログ（変更・削除を受け付けない設計）	閲覧を含む操作を記録し、事務所の画面で確認できる。記録には、前の記録とつながるハッシュ値を持たせている。その検証を当社に依らずに行う手段は、まだ提供していない（8.4） 契約：第12条6項 観測：付録 A-3 当社申告
契約	利用規約への同意	秘密保持契約・データ処理契約を一体にした利用契約に、事務所の管理者が同意 契約：冒頭
事実の照合	別系統の外部 AI で照合	e-Gov の法令と、裁判所の公開情報を参照。Amazon Bedrock 以外の AI サービスは使わない 当社申告

v1.0 が計画として挙げていた 3 項目の現状は、次のとおりです。

- **認証アプリによる 2 要素認証（TOTP）** AILEX v2 で提供しています。 **観測：付録 A-6** **検証：2026年9月17日**
- **外部のタイムスタンプ局との連携** 操作の記録について、事務所が検証に使える形では提供していません（8.4）。
- **SOC 2 Type II** 報告書は取得していません。取得に向けて準備しています（13）。

3. 責任の分担

クラウド上のサービスでは、基盤の事業者、サービスの提供者、利用者のそれぞれが受け持つ範囲があります。AILEX v2 では、次のように分かります。

受け持つ者	範囲
AWS	クラウドのサービスを動かす基盤（ハードウェア、ソフトウェア、ネットワーク、施設）の保護。データセンターの入退室と施錠の管理 AWS：付録 B-7 契約：付属書 B 3.
当社	事務所の指示に従った処理、安全管理措置（アプリケーション、AWS 上の権限・リージョンの限定・暗号化の設定、運用）、サブプロセッサの統制、インシデントの通知と協力 契約：別紙2 第6条1項・第13条2項
事務所	個人データ等を当社に預けるための適法な権限・通知・同意などの確保、利用目的の選択、事務所側の設定とアクセスの管理（アカウント、端末と認証情報、利用者の権限）、指示の適法性、AI の出力の確認 契約：第4条の2、別紙2 第6条3項・第13条1項

4. データの所在と流れ

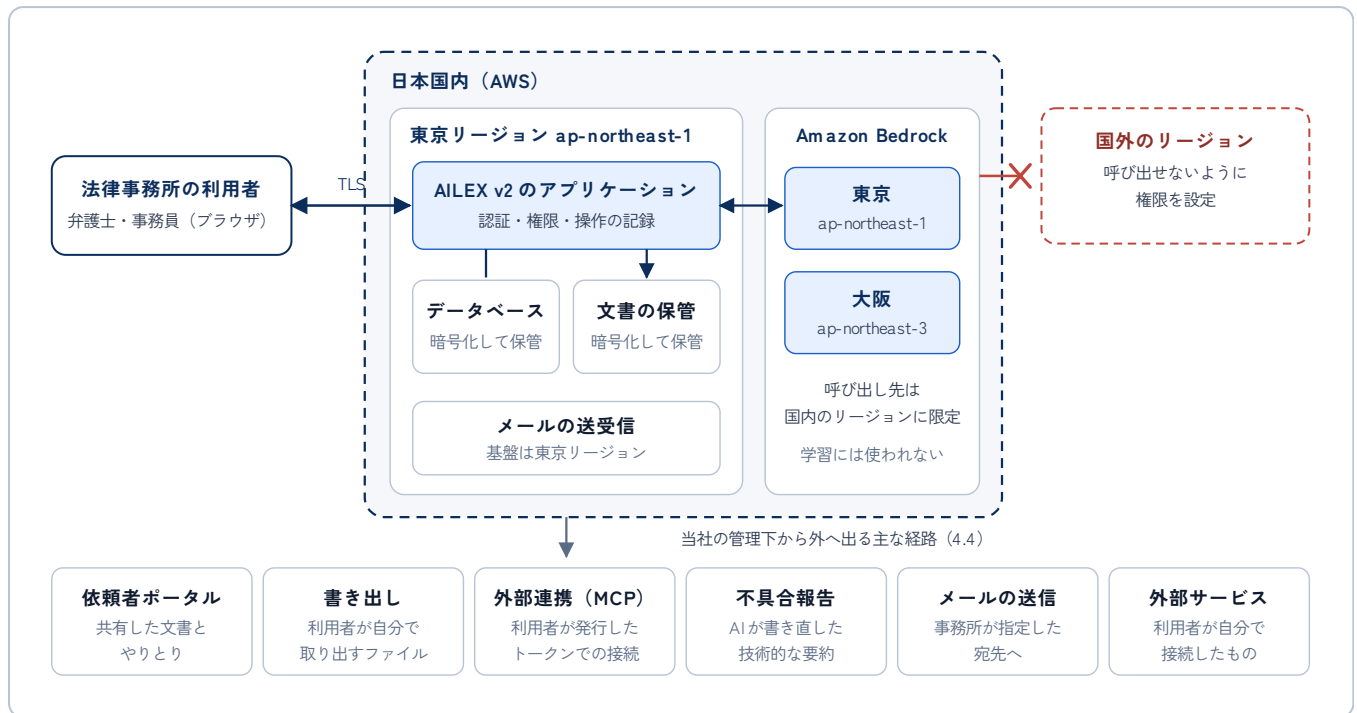


図1 AILEX v2のデータの所在と流れ。保管は東京リージョン、AIの処理は東京または大阪リージョンで行います。下段は、当社の管理下から外へ出る主な経路です（4.4）。下段の送り先での取扱いは、国内完結の範囲に含まれません（4.5）。記述の根拠は、本文の各項に示します。

4.1 保管

事件情報、文書、データベースは、AWS 東京リージョン（ap-northeast-1）に保管します。 **契約：第12条2項、別紙2 第8条**
保存するデータは、AWS の管理する鍵で暗号化します。 **契約：付属書 B 4.** データベースは 35 日間の任意の時点の状態に戻せる設定で運用し、文書は版を管理して、上書きや削除のあとも前の版を 90 日間保持する設定にしています。 **当社申告**

4.2 AIの処理

AI 機能に使うデータの処理は、Amazon Bedrock の日本国内リージョン（東京 ap-northeast-1 または大阪 ap-northeast-3）の中で完結します。 **契約：第7条2項** 国外のリージョンを呼び出さないための仕組みは、次の二つの段階に分かれています。

- 権限** 当社は、AWS の権限の設定により、日本国内に限定された推論プロファイル以外を呼び出せないように構成しています。 **契約：第7条2項** 具体的には、アプリケーションの実行に使う権限で呼び出せる推論プロファイルを、識別子が jp. で始まるものに限り、推論プロファイルを使わずに呼び出すモデルを、東京・大阪リージョンのものに限っています。アプリケーションの設定を誤っても、国外のリージョンへの呼び出しは、権限の段階で拒否されるように構成しています。 **当社申告**
- コード** 推論プロファイルを使う呼び出し（文章の生成・分析・読み取り）では、呼び出しのたびに識別子の先頭を検査し、jp. 以外は設定の誤りとして拒否します。 **当社申告**

AWS は、日本国内クロスリージョン推論について、リクエストの送り先が東京リージョンと大阪リージョンに限定され、推論の処理が日本国内で完結すると説明しています。 **AWS：付録 B-1** 一方で AWS は、データの所在地に要件がある場合、推論プロファイルの識別子の接頭辞だけに頼らず、利用する送信元のリージョンごとに送り先のリー

ジョンを確かめるよう案内しています。 **AWS：付録 B-6** 当社が使う二つの推論プロファイルについて、AWS のモデルの説明ページは、送信元が東京リージョン・大阪リージョンのいずれの場合も、送り先を東京リージョンと大阪リージョンと記載しています。 **AWS：付録 B-5** AWS が案内する API (GetInferenceProfile) による確認の結果は、本白書には掲載していません。

当社の検証用の事務所の操作ログ（全 578 件）を 2026年10月6日に確認したところ、AI の呼び出しに記録されていたモデルの識別子は、次の 3 種類でした。 **観測：付録 A-3**

- jp.anthropic.claude-haiku-4-5-20251001-v1:0（文章の生成・分析・読み取りに使うモデル）
- jp.anthropic.claude-sonnet-4-6（同上）
- amazon.titan-embed-text-v2:0（検索のために、文章を数値の並びに変換するモデル。推論プロファイルを使わず、東京リージョンの中で呼び出します **当社申告**）

使うモデルは、日本国内のリージョンで処理できるものに限りです。新しい世代のモデルが国外向けの提供に限られる間は、採用しません。そのため、モデルの世代では一歩遅れることがあります。 **当社申告**

どのリージョンで処理されたかは AWS の記録（AWS CloudTrail）に残ると、AWS は説明しています。 **AWS：付録 B-1** この記録を呼び出しごとに照合して、結果を事務所に示す仕組みは、まだ提供していません（8.4）。

4.3 公開している接続先

app.ailex.co.jp は、AWS 東京リージョンのロードバランサー（ap-northeast-1.elb.amazonaws.com の配下）を指しています。 **観測：付録 A-2** 通信は TLS で暗号化します（7）。

4.4 当社の管理下から外へ出る経路

利用データが当社の管理下から外へ出る主な経路は、次のとおりです。いずれも、利用者の操作か、事務所の設定をきっかけにします。

経路	出るもの	制御
依頼者ポータル	事務所が共有を指定した文書と、依頼者とのやりとり	事件ごとに URL を発行する。パスワードによる解錠を必須にできる。いつでも無効にできる 当社申告
書き出し	事件の一覧・期日・報酬と実費（Excel）、書面（Word）、文書とその本文	利用者が自分の端末に取り出す。書き出しの画面に、操作が操作ログに記録される旨の表示がある 観測：付録 A-6
外部連携（MCP）	事件・期日・タスク・文書の検索結果と、文書の本文	利用者が設定画面で発行したトークンが必要 観測：付録 A-5 検証：2026年9月17日 設定画面の表示では、参照できるのは発行した利用者の権限の範囲で、既定は読み取り専用。発行時に書き込みを許可すると、タスクの作成と期日の提案ができる（期日は確認待ちに入り、承認するまで登録されない） 観測：付録 A-6 書き込みを許可した場合の動作と、取扱者を限定した事件が参照から外れることは、本白書の作成にあたって確認していない
不具合報告	利用者が送った報告を、AI が書き直した技術的な要約	送り先は、当社が開発に使う課題管理のサービス（GitHub。米国の事業者のサービス）。利用者が書いた原文は送らない 当社申告

経路	出るもの	制御
メールの送信	事務所の指示・設定に基づく、指定した宛先（依頼者、相手方、裁判所、利用者本人など）へのメール	当社が管理する送受信の基盤は、AWS 東京リージョン。配送先での取扱い は 4.5 を参照 規約：プライバシーポリシー 4.、利用規約 第12条2項 契約：付属書 C
外部サービスとの連携	利用者が自分で接続した外部サービス（カレンダーなど）へ送る、期日の件名・日時など	接続は利用者の選択による。いつでも解除できる 規約：利用規約 第3条の3 2026年10月6日時点では、Google カレンダーへの書き出しと LINE での通知は、設定画面に「認証情報が設定されていません」と表示され、利用できない状態 観測：付録 A-6

このほかに、次の通信があります。

- 法令・裁判例の参照** 法令の検索では、AILEX のサーバーが e-Gov 法令検索（デジタル庁）から条文の原文を取得します。 **観測：付録 A-6** 裁判例の検索では、裁判所が公開している裁判例の情報を参照します。 **当社申告** 検索に使う語（法令名、検索語）は、参照先に送られることがあります。依頼者名など、事件を特定できる語を検索語に入れないでください。
- 外部 ID 基盤** 事務所が Microsoft Entra ID または Google Workspace との連携を選んだ場合、ログインの際に、その ID 基盤との間で認証の通信が行われます。当社が受け取るのは、利用者の識別情報（利用者 ID、表示名、メールアドレス、所属組織の識別子）で、認証の目的にだけ使います。 **契約：第3条の2**
- 書体の配信** 画面の表示に使う書体を、利用者のブラウザが Google の配信サーバー（fonts.googleapis.com・fonts.gstatic.com）から取得します。事件情報は送られませんが、接続元の IP アドレスなど、通信に伴う情報は Google に伝わります。ログイン画面と、ログイン後の操作ログの画面で確認した範囲では、画面が読み込む外部の接続先は、この二つでした。 **観測：付録 A-1**

mints への提出は、弁護士が mints の画面で行います。AILEX v2 が裁判所のシステムに接続して提出することはありません。 **当社申告**

4.5 国内完結の範囲に含まれないもの

- メールの配送先** メール本文、添付ファイル、宛先などは、配送先のメールサービスに渡ります。配送の経路と、配送先での保管・処理の所在地を、当社が指定することはできません。国外で取り扱われる場合があります。 **契約：第12条2項、別紙2 第8条1項**
- 利用者が接続した外部サービス** 接続先でのデータの取扱いは、その提供者の規約によります。国外で取り扱われる場合があります。 **規約：利用規約 第3条の3、プライバシーポリシー 4.**
- 外部連携（MCP）で接続した AI サービス** 参照した事件の情報や文書の本文は、接続した AI サービスに渡ります。処理する地域、学習への利用、保存期間は、その AI サービスの規約によります。
- 不具合報告の要約の送り先** 4.4 のとおり、要約は、外部の課題管理のサービス（国外の事業者のサービス）に保存されます。不具合報告の文面と、添える画面の画像には、依頼者名や事件の内容を含めないでください。 **当社申告**
- 利用者・依頼者の端末** 書き出したファイルや、端末に保存された情報の管理は、事務所で行っていただく範囲です。

5. AI の処理と入力データ

5.1 学習に使われないこと

当社は、利用データを本サービスの提供目的以外に使わず、当社または第三者の AI モデルの学習・改善（教師データ化、継続学習、再学習を含む）に使いません。 **契約：第12条1項、別紙2 第4条3項** Amazon Bedrock に送ったデータは、AWS の規定に基づき、基盤モデルの訓練・改善に使われません。 **契約：第7条3項**

AWS は、Amazon Bedrock について次のように公表しています。 **AWS：付録 B-2・B-3**

- AWS とモデルの提供者は、Amazon Bedrock への入力・出力を、モデルの学習に使わない。
- 利用者の入力とモデルの出力は、モデルの提供者に共有されない。モデルの提供者は、モデルを配置するアカウントにも、Amazon Bedrock のログにも、利用者の入力・出力にもアクセスできない。

当社が、モデルを開発する事業者の API へ利用データを直接送ることはありません。 **規約：利用規約 第7条3項**

5.2 AWS による保存・確認の例外

AWS は、Amazon Bedrock について、サービスの運用者がモデルの入力・出力にアクセスできず、既定では入力・出力を保存しないと説明しています。そのうえで、不正利用の検知について、次の例外を公表しています。

AWS：付録 B-4

- **特定のモデル** AWS が挙げる一部のモデルでは、不正利用の検知のために、入力・出力を最長 30 日間保存する（検知の仕組みが抽出した分だけを保存するモデルと、すべての入力・出力を保存するモデルがある）。後者では、抽出した入力・出力を、AWS の担当者が確認することがある。保存したデータは AWS が保管・処理し、モデルの提供者には共有しない。複数のリージョンにまたがる推論を使う場合、保存先は、推論を処理したリージョンになる。
- **画像の入力** 画像の入力に児童性的虐待コンテンツの疑いを検知した場合、AWS はそのリクエストを遮断する。該当するかどうかを判断する目的に限って、その入力・出力を保存・確認することがあり、米国の全米行方不明・被搾取児童センター（NCMEC）などの関係機関に報告することがある。

一つ目の例外について、AWS が保存の対象として挙げているモデルに、当社が使っているモデル（4.2）は含まれていません（2026年10月6日時点）。なお、不正利用を自動で検知する仕組みそのものは、当社が使う二つのモデルにも適用されます。 **AWS：付録 B-5** 上の記載は、検知が行われないという意味ではなく、保存の対象に挙がっていないという意味です。対象のモデルは、AWS が変更することがあります。二つ目の例外は、モデルを限っていません。AILEX v2 が、画像や PDF の読み取りのために画像を入力する処理にも当てはまります。

利用規約は、不正利用の防止を目的として、AWS が一定期間データを保存し、または確認する場合があることを定めています。 **規約：利用規約 第7条4項**

5.3 マスキングを行わない理由

AILEX v2 は、AI 機能への送信にあたって、利用データの匿名化・仮名化を行いません。処理が日本国内で完結し、当社が利用データを保管する環境と同じ管理下にあるためです。 **契約：第7条4項**

従来版のマスキングは、外部の AI 事業者へ送ることを前提にした対策でした。氏名には、電話番号のような決まった形がありません。あらかじめ登録された氏名は置き換えられても、表記の揺れや、書類に初めて現れる氏名は残

ります。漏れなく伏せることを保証できないため、AILEX v2 では、伏せてから外へ出す方式をやめ、AI の処理を、保管と同じ当社の AWS の環境の中に置く構成を選びました。

したがって、外部連携（MCP）で接続した AI サービスや、メールの宛先など、4.5 に挙げた先へ渡る情報にも、マスキングは行いません。

5.4 AI の出力の位置づけ

AI が生成した内容は、参考情報・下書きです。不正確な記載や、最新の法改正・判例を反映していない記載を含む可能性があります。[契約：第4条](#) 弁護士資格を有する方が、依頼者への送付や裁判所への提出の前に内容を精査し、必要な修正を加えなければなりません。[契約：第4条の2](#)

- AI が生成した内容には、AI による生成である旨を画面に表示します。[契約：第4条5項](#)
- 生成した書面のうち確認を要する箇所は、書面の中に【要確認】と明示します。この表示は網羅的なものではなく、表示がないことは、内容が正確であることを意味しません。[契約：第4条6項](#)
- AILEX が自動で進める処理のうち、次の三つは、事務所の設定で個別に有効・無効を選べます。相手方の書面が届いたときの主張の整理と下書きの用意、裁判所の書面からの期日の読み取りと登録、通知書などを保存したときの表現の点検です。自動で登録した期日には「要確認」の印が付きます。元の書面と照らして確認してください。[観測：付録 A-6](#)
- 利益相反の確認は、事務所に登録された情報の範囲で突き合わせるもので、利益相反がないことを保証するものではありません。[契約：第4条の2 第5項](#)

AILEX は、弁護士の業務を補助する道具です。法律事件に関する鑑定、代理、仲裁、和解その他の法律事務を行うものではありません（弁護士法第72条）。[契約：第4条の2 第1項](#)

5.5 AI が使えないとき

AWS の障害、仕様の変更、モデルの提供終了などにより、AI 機能が一時的に使えないことがあります。その場合は、その旨を画面に表示します。事件情報の閲覧・登録・書き出しなど、AI に依存しない機能は引き続き使えます。[契約：第7条5項・6項](#)

6. アクセスの制御

6.1 事務所単位での分離

事務所ごとにデータを分離し、他の事務所の利用データにアクセスできない構成にしています。

[契約：第12条4項、付属書 B 4.](#) 分離は、論理的なものです。事務所ごとに別のデータベースを用意する方式ではなく、記録に事務所の識別子を持たせ、アプリケーションが参照のたびに事務所で絞り込む方式です。[当社申告](#) 一覧、URL の直接指定、横断検索、外部連携（MCP）のいずれから他事務所の記録に到達しないことを、自動テストで検査しています。[当社申告](#)

本番環境では、検証用の事務所の間で、次の確認を行いました。[検証：付録 A-4](#)

- 2026年9月17日 外部連携（MCP）で、別の事務所が発行したトークンを使って検索と取得を試み、記録が返らないことを確認しました。

- 2026年9月21日 ブラウザの画面について、別の事務所の記録の識別子を直接指定する 23 通りの経路を試し、すべて 404（見つかりません）が返ることを確認しました。

6.2 事件単位の情報遮断

事務所は、事件ごとに、閲覧できる利用者を限定できます。限定した事件は、事務所の管理者であっても、取扱者に登録されない限り閲覧できません。 [契約：第12条5項](#) この限定は、その事件に属する文書・期日・書面などにも及びます。 [当社申告](#)

6.3 役割

利用者の役割は、管理者・弁護士・事務員の三つです。 [観測：付録 A-6](#) 誰にどの役割を与えるかは、事務所の管理者が決めます。 [規約：利用規約 第3条4項](#) 役割ごとにできる操作の一覧は、本白書には掲載していません。

6.4 認証

項目	内容
パスワード	ハッシュ化して保存する 契約：付属書 B 4.
試行の制限	同じ接続元から続けて失敗すると、一定時間ログインを受け付けない。接続元を変えながらの試行までは防げない 検証：2026年9月25日 当社申告
エラーの表示	メールアドレスが登録されていない場合と、パスワードが違う場合とで、表示する文言を変えない 当社申告
2 要素認証	認証アプリの 6 桁のコード（TOTP）。事務所の設定で全員に必須にでき、未登録の利用者は、登録するまで他の画面を開けない。2要素認証を使う利用者は、コードの確認が済むまでログインが成立しない 観測：付録 A-6 検証：2026年9月17日
接続元の制限	接続を許す IP アドレスを指定できる（CIDR 表記に対応）。許可していない接続元からは利用できない 観測：付録 A-6 検証：2026年9月17日
外部 ID 基盤との連携	利用契約は、Microsoft Entra ID または Google Workspace との連携を選べること、AILEX 独自のパスワードでのログインを止められること、その場合は、事務所が ID 基盤でアカウントを停止した時点で AILEX も使えなくなることを定めている。設定画面に項目があることは確認した。連携先との間の動作は、本白書の作成にあたって確認していない 契約：第3条の2 観測：付録 A-6
セッション	セッションの Cookie に Secure・HttpOnly・SameSite=Lax を指定している。Cookie の有効期間（Max-Age）は 8 時間 観測：付録 A-1

2 要素認証の必須化と接続元の制限は、適用するかどうかを事務所が決める機能です。 [規約：プライバシーポリシー 6.](#) 試行の制限には上のとおり限界があるため、全員への 2 要素認証の必須化をお勧めします（12）。

6.5 当社の役職員によるアクセス

当社の役職員が利用データにアクセスできるのは、障害への対応、事務所からの依頼に基づく支援、法令に基づく対応など、サービスの提供に必要な場合に限ります。当社は、アクセスできる役職員を限定し、多要素認証を課し、アクセスの記録を保存します。記録は、事務所の求めに応じて開示します（アクセスの日時、担当者、目的）。 [契約：別紙1 第3条3項、別紙2 第5条](#)

当社は、利用データに含まれる依頼者の秘密について、サービスの提供に必要な最小限の範囲を超えてアクセスせず、当社自身の利益のために利用しません。 [契約：別紙1 第3条2項](#)

6.6 外部連携のトークン

外部連携（MCP）は、利用者が設定画面で発行するトークンで認証します。トークンのない接続は拒否します。

観測：付録 A-5 削除したトークンでの接続も拒否します。 **検証：2026年9月17日** 設定画面には、参照できるのは発行した利用者の権限の範囲で、既定は読み取り専用であると表示しています。発行時に書き込みを許可した場合の範囲は、4.4 のとおりです。 **観測：付録 A-6** 書き込みを許可した場合の動作と、取扱者を限定した事件が参照から外れることは、本白書の作成にあたって確認していません。

7. 通信とアプリケーションの保護

この表で「観測」と表示した項目は、外部から確かめられます。応答の内容は、付録 A-1 に記載しています。

項目	内容
通信の暗号化	TLS。HTTP での接続は HTTPS に転送する。ブラウザに HTTPS での接続を 1 年間求める指定（HSTS、サブドメインを含む）を付けている 契約：付属書 B 4. 観測：付録 A-1 検証：2026年9月25日
読み込み元の制限	コンテンツセキュリティポリシーで、スクリプトの読み込み元を自サイトに限る。ページに直接書かれたスクリプトは、応答のたびに発行する値（nonce）が付いたものだけを実行する。スクリプトからの通信先（connect-src）は自サイトのみ。スタイルについては、ページに直接書かれた指定を許している 観測：付録 A-1
画面の埋め込みの禁止	他のサイトの枠の中に AILEX の画面を表示させない（frame-ancestors 'none'、X-Frame-Options: DENY） 観測：付録 A-1
端末の機能	カメラ・マイク・位置情報の利用を、ページの側で無効にしている 観測：付録 A-1
意図しない送信の防止（CSRF 対策）	確認用の値（CSRF トークン）のない送信は受け付けない 検証：2026年9月21日・25日
脆弱性への対応	ソフトウェアの更新と、セキュリティパッチの適用を行う 契約：付属書 B 4.

8. 操作の記録

当社は、本サービスに対する操作の記録（誰が、いつ、何に対して、どのような操作を行ったか）を保存します。記録は、事務所で確認できます。 **契約：第12条6項** 画面では「操作ログ」、利用規約では「監査ログ（操作の記録）」と呼んでいます。同じ記録を指します。

8.1 記録する内容

- 項目は、日時、利用者、操作、対象、IP アドレスです。 **観測：付録 A-3**
- 作成・変更だけでなく、事件の閲覧も記録します。 **観測：付録 A-3**
- AI の呼び出しは、開始と完了を記録し、使ったモデルの識別子を残します。 **観測：付録 A-3**
- AILEX が自動で進めた処理は、利用者の操作とは別に、利用者の欄を「AILEX自動」として記録します。 **観測：付録 A-3**
- 利用規約などへの同意は、同意した版とともに記録します。 **観測：付録 A-3**

- 書面の書き出しを記録します。 観測：付録 A-3 データの書き出しと、外部連携（MCP）からのアクセスも記録の対象であることを、それぞれの画面に表示しています。 観測：付録 A-6
- **対象の欄には、操作の内容が残ります。**利益相反の確認で入力した氏名、裁判例の検索語、取り込んだファイルの名前などが、そのまま記録されます。 観測：付録 A-3

当社の検証用の事務所の画面では、絞り込みに使える操作の種類は 66 種類でした。 観測：付録 A-3 当社の設計では、記録の対象は 80 種類以上です。 当社申告

8.2 事務所での確認

記録は、事務所の画面（設定 → 契約とデータ → 操作ログ）で確認できます。利用者、操作、期間で絞り込みます。 観測：付録 A-3 取扱者を限定した事件（6.2）についての記録が、取扱者でない管理者の画面にどう表示されるかは、本白書の作成にあたって確認していません。

8.3 記録の位置づけと保管

操作の記録は、利用契約の付属書 A で、利用データとは別の「サービス運用データ」に挙げられています。当社が、サービスの安定運用、セキュリティの確保、課金、法令の遵守の目的で、独立に取り扱います。
契約：別紙2 第1条2項・第3条2項、付属書 A サービスの改善にも、操作の記録と、統計的に集計した情報を使います。事件情報、文書の本文、相談内容を、改善の目的で使うことはありません。 規約：プライバシーポリシー 2.

事務所の利用終了やアカウントの削除によって利用データを削除したあとも、操作の記録、利用規約等への同意の記録、資格の申告の記録は保管します。削除のあとの利用は、セキュリティの確保、不正利用の調査、法令の遵守、紛争への対応の目的に限ります。 規約：利用規約 第10条の2 第7項、プライバシーポリシー 5.

8.1 のとおり、操作の記録には、入力した氏名や検索語、ファイル名が含まれます。事務所が入力した情報に由来するこれらの内容は、利用データを削除したあとも、操作の記録の一部として残ります。保管する年数は、利用規約にも利用契約にも定めていません。

8.4 現時点で提供していないもの

操作の記録には、前の記録とつながるハッシュ値を持たせています（2026年9月28日に実装を確認）。 当社申告 ただし、次のものは、本白書の時点では提供していません。

- 操作の記録があとから書き換えられていないことを、事務所や第三者が当社に依らずに確かめる手段
- AI の呼び出しごとに、実際に処理されたリージョンを照合した結果

検証可能性についての当社の考え方は、技術仕様の提案として、IETF に Internet-Draft を提出しています（13）。提案の内容のすべてが、AILEX v2 に実装されているわけではありません。

9. 保存・削除・返還

場面	取扱い
利用中	保管を続ける 規約：プライバシーポリシー 5.

場面	取扱い
無料期間の終了、有料契約の更新停止	削除しない。新しい登録と変更はできなくなるが、閲覧と書き出しは続けられる 契約：第8条の2、第10条の2 第2項 規約：利用規約 第8条・第8条の2・第10条の2
利用者による削除	削除した事件情報などは、30 日間ゴミ箱に残り、復元できる。30 日を過ぎると当社が消去する 契約：第10条の2 第5項 規約：利用規約 第10条の2 第5項 観測：付録 A-6
削除できないもの	証拠番号を付けた文書と、確定した書面は、削除の操作そのものを受け付けない 当社申告
個人のアカウントの削除	その利用者がログインできなくなる。事務所の利用データは残る 契約：第10条3項
事務所の利用終了とデータ削除の申請	申請の日から 30 日間保管したのち、削除する。事務所は、30 日を待たずに削除を求めることができ、その場合は速やかに削除する。削除したデータは復旧できない 規約：利用規約 第10条の2
バックアップ	消去のあとも、障害からの復旧のためのバックアップに、データが残ることがある。バックアップは復元の用途にだけ使い、保存期間が過ぎると消去される。データベースのバックアップは 35 日間、文書の旧版は 90 日間保持する設定で運用している 規約：利用規約 第10条の2 第6項 契約：別紙2 第12条3項 当社申告
削除の通知	事務所の求めがあれば、削除を実行した日と対象の範囲を、書面（電子メールを含む）で通知する 契約：別紙2 第12条3項
削除のあとも残る記録	操作の記録、利用規約等への同意の記録、資格の申告の記録（8.3） 規約：利用規約 第10条の2 第7項
書き出し	利用期間中と、利用終了の申請後の保管期間中は、利用データを機械で読める形式で書き出せる 契約：第10条の2 第1項 規約：利用規約 第10条の2 第2項

データの書き出しの画面では、事件の一覧、期日・予定、報酬・実費を Excel 形式で取り出せます。事件ごとに、時系列、債権者一覧（破産・個人再生）、書面（Word 形式）、取り込んだ文書とその本文（1 件ずつ）を取り出せます。文書の件数が多く、一括での取り出しを希望する場合は、お問い合わせにより当社がまとめてお渡します。書き出しは、契約の状態にかかわらず利用できます。 [観測：付録 A-6](#)

10. 再委託先と、法令に関する整理

10.1 再委託先(サブプロセッサー)

利用契約は、サブプロセッサー（当社が利用データの処理を再委託する先）として、Amazon Web Services, Inc.（米国法人）を挙げています。クラウドの基盤、データの保管、AI の処理（Amazon Bedrock）、メールの送受信を担います。保管は東京リージョン、AI の処理は東京または大阪リージョンで行います。利用契約は、当社がサブプロセッサーに、データ処理契約と同等以上のデータ保護の義務を契約で課し、その行為について責任を負うと定めています。 [契約：第12条3項、別紙2 第7条2項、付属書 C](#)

規約と契約には、このほかに次の記載があります。いずれも、現状と異なる箇所です。

- **弥生株式会社**（請求書の発行・送付。取り扱うのは請求先の名称・住所・メールアドレスだけで、利用データは送らない） [利用契約 第12条3項・付属書 C](#)、[利用規約 第12条3項](#)、[プライバシーポリシー 4.](#)に記載があります

す。同社のサービスの利用は 2026年9月27日に終了し、現在、請求書は当社が発行しています。 **当社申告**

- **エックスサーバー株式会社**（移行期間中のメールの送信） 利用規約 第12条2項・3項、プライバシーポリシー 4. に記載があります。メールの送信は、AWS への移行を終えています。 **当社申告**

不具合報告の要約の送り先（4.4）は、当社の保管・処理の範囲の外にあるものとして扱っており（4.5）、サブプロセッサの一覧（付属書 C）には含めていません。

サブプロセッサを追加するとき、または重要な変更があるときは、原則として 30 日前までに事務所へ通知します。事務所は、変更が個人データ等の保護の水準を実質的に下げると合理的に認められる場合、通知を受けてから 15 日以内に書面で異議を述べることができます。当社が 30 日以内に合理的な代替の措置を示せないときは、事務所は契約を解約できます。 **契約：別紙2 第7条3項・4項**

10.2 個人情報保護法との関係(当社の整理)

事務所は、利用契約に基づいて、日本法人である当社に利用データの処理を委託します。事務所は委託元として、当社は委託先として処理します。 **契約：別紙2 第3条1項** 当社は、この委託に伴う個人データの提供を、第三者提供に当たらないもの（個人情報保護法 第27条5項1号）と整理しています。提供を受ける当社は日本法人であり、外国にある第三者（同 第28条）には当たりません。

AWS については、二つの面があります。利用契約の上では、AWS をサブプロセッサとして扱い、当社がその行為について責任を負います（10.1）。個人情報保護法の上では、クラウドサービスを提供する事業者が、契約条項とアクセスの制御によって、保存された個人データを取り扱わないこととなっている場合には、個人データの提供に当たらないとする個人情報保護委員会の考え方があります（付録 B-11 の Q&A 7-53。サーバーが国内にあり、運営する事業者が外国にある場合は、Q&A 12-4）。この Q&A は、サーバーに保存された個人データについてのもので、AI による処理を名指ししたものではありません。当社は、AWS が、運用者による入力・出力へのアクセスを行わず、既定では入力・出力を保存しないと公表していること（付録 B-4）を前提に、AI の処理を含めて、AWS の基盤の利用がこれに当たると整理しています。

5.2 に挙げた、AWS が入力・出力を保存・確認する例外的場面は、この整理の外にあります。Q&A 12-4 は、サーバーを運営する外国の事業者が個人データを取り扱っている場合、サーバーが国内にあっても、外国にある第三者への提供に当たるとしています。不具合報告の要約の送り先（4.4）と、操作の記録など当社が独立に取り扱うサービス運用データ（8.3）も、この整理の対象に含めていません。

これは当社の整理であり、法的な助言ではありません。整理の根拠は、お問い合わせに応じてご説明します。クラウドサービスの利用が提供に当たらない場合も、利用する事業者は、自らの安全管理措置の一環として、適切な措置を講じる必要があるとされています（Q&A 7-54）。利用目的の範囲内での取扱い（同 第18条）、安全管理措置（同 第23条）、委託先の監督（同 第25条）などの義務は、引き続き事務所にあると、当社は理解しています。委託先の監督に使えるよう、処理の内容、安全管理措置、サブプロセッサの一覧を、利用契約の付属書 A～C として提供しています。依頼者への説明の要否は、委任契約と守秘義務に照らして、各事務所でご判断ください。

条番号は、2026年10月6日時点で e-Gov 法令検索に現行のものとして掲載されている条文によります。2026年7月17日に公布された個人情報保護法の改正（付録 B-12）の内容は、本白書には反映していません。

10.3 米国の CLOUD Act

CLOUD Act は、米国の法執行機関が法律上の手続によって事業者にデータの提出を求める場合に、その対象に米国外に保存されたデータも含まれうることを明確にした米国の法律です。保存先が日本であることだけで、この法律が及ぶ可能性がなくなるわけではありません。

AWS は、企業顧客のコンテンツについて法的に有効で拘束力のある要求を受けた場合、顧客に直接求めるよう法執行機関に働きかけ、法的に許される場合は顧客に通知し、法令に抵触する要求や過度に広い要求には異議を申し立てると公表しています。手を尽くしてもなお開示を強制され、技術的に可能な場合は、要求を満たす最小限を開示するとしています。また、統計の公表を始めた 2020 年以降、米国外に保存された企業・政府機関の顧客のコンテンツを米国政府に開示したことはないと公表しています（同ページの記載は、2025年6月時点）。 **AWS：付録 B-8** ここでいう顧客は、AWS と契約している当社です。当社が法令または裁判所の命令に基づいて開示を義務づけられた場合は、法令上許される限り、事前に事務所へ通知します。 **契約：別紙1 第4条**

11. インシデントへの対応と継続性

- **通知** 秘密情報の漏えい・紛失を知ったとき、またはそのおそれを認識したときは、直ちに事務所に通知し、被害の拡大を防ぐために必要な措置をとります。 **契約：別紙1 第7条**
- **初報** 利用データの漏えい、滅失、毀損などを認知したときは、遅滞なく事務所に初報を行います。遅くとも、認知から 72 時間以内を目標とします。初報には、概要、応急の措置、連絡窓口を含めます。調査中の事項は、調査中であると記載します。 **契約：別紙2 第10条1項・2項**
- **追加の報告** 影響を受けたデータの種類と範囲、原因、再発防止策が分かり次第、報告します。 **契約：別紙2 第10条3項**
- **事務所の判断への協力** 監督当局への報告と本人への通知の可否は、事務所が判断します。当社は、判断に必要な情報の提供と協力を行います。 **契約：別紙2 第10条4項**
- **復旧** データベースは 35 日間の任意の時点に戻せる設定で運用し、文書は旧版を 90 日間保持する設定にしています。 **当社申告**
- **確認の手段** 当社は、データ処理契約の遵守の状況を示すものとして、公表しているデータの取扱いに関する資料を提供します。事務所は、その資料で確認できない事項について、年 1 回を上限に、書面で当社に質問できます。当社は、30 日以内に合理的な範囲で回答します。 **契約：別紙2 第11条1項・2項**
- **訪問による監査** 上の手段では払拭できない具体的かつ合理的な懸念があり、かつ、法令または監督当局の命令によって避けられない場合に限り、事務所は、60 日前の書面による通知で、訪問による監査を要請できます。範囲は懸念の事項に限り、費用は事務所の負担です。 **契約：別紙2 第11条3項**

当社の損害賠償の責任には上限があります（当社に故意または重過失がある場合を除き、直近 12 か月に支払われた利用料金の総額）。無料期間中は、支払われた利用料金がありません。当社の故意または重大な過失による個人データ等の漏えいに起因する損害には、この上限を適用しません。 **契約：第11条、別紙2 第14条**

利用契約には、AI が生成した内容に基づく判断、AI の基盤の障害、外部の認証サービスの障害について、当社が責任を負わない旨の定めがあります。 **契約：第4条4項、第7条5項、第3条の2 第5項**

12. 事務所で行っていただくこと

次の項目は、当社が代わりに行うことができません。導入のときにご確認ください。

1. **利用契約への同意** 秘密保持契約とデータ処理契約は、事務所の管理者が利用契約に同意した時から適用されます。同意の前に適用されるのは、公開している利用規約です。事件情報を登録する前の同意をお勧めします。
2. **2 要素認証の必須化** 事務所の設定で、全員に 2 要素認証を求めてください。ログインの試行の制限には限界があります（6.4）。

3. **入口の制限** 事務所の回線だけを許す IP アドレスの指定を検討してください。設定を誤ると全員が入れなくなるため、保存の前に、書式（1 行に 1 つ。CIDR 表記も可）と、ご自身の接続元が含まれていることを確かめてください。外部 ID 基盤と連携する場合は、動作を確かめたうえで、AILEX 独自のパスワードでのログインを止めてください。独自のパスワードが残っていると、ID 基盤でアカウントを止めてもログインできてしまいます。
4. **権限と取扱者** 役割を必要な範囲で割り当て、担当外の職員に見せない事件は、取扱者を限定してください。退職・異動のときは、その方のアカウントを削除するか、権限を見直してください。
5. **端末と認証情報** 端末、パスワード、認証アプリ、発行したトークンの管理は、事務所で行ってください。使わなくなったトークンは削除してください。 **契約：別紙2 第6条3項**
6. **外へ出す操作の確認** メールの宛先、依頼者ポータルで共有する文書、外部サービスや AI サービスとの接続先は、事務所を確認してください。依頼者ポータルを使う場合は、パスワードによる解錠を必須にすることをお勧めします（4.4・4.5）。
7. **検索語と不具合報告** 法令・裁判例の検索語と、不具合報告の文面・添える画面の画像には、依頼者名など、事件を特定できる情報を含めないでください（4.4・4.5）。
8. **AI の出力の確認** 依頼者への送付や裁判所への提出の前に、弁護士が内容を確認してください（5.4）。
9. **依頼者との関係** 依頼者から預かった情報を AILEX で取り扱うことについて、委任契約と守秘義務に照らした説明の要否は、事務所でご判断ください（10.2）。
10. **修習生プランの注意** 司法修習生の方は、修習で取り扱う事件の記録など、守秘義務の対象となる情報を入力しないでください。 **規約：利用規約 第8条の3 第3項**

13. 行っていないこと、提供していないもの

- **第三者機関による認証・報告書** ISO/IEC 27001・27017 の認証と、SOC 2 Type II の報告書は、取得していません。いずれも、取得に向けて準備しています。基盤である AWS は、Amazon Bedrock が各種の第三者評価の対象であると公表していますが、これは AWS の受け持つ範囲についてのもので、当社のアプリケーションと運用についてのものではありません。 **AWS：付録 B-2**
- **第三者機関による診断** 付録 A の確認は、当社が自ら行ったものです。第三者機関による脆弱性診断の報告書は、本白書の時点で公表していません。
- **記録の第三者による検証** 8.4 のとおり、操作の記録を事務所や第三者が当社に依らずに確かめる手段と、処理されたリージョンの照合結果は、提供していません。
- **標準化の状況** AI が関与した生成や判断の過程を、検証できる形で記録する考え方を、技術仕様「Verifiable AI Provenance (VAP) Framework and Legal AI Profile (LAP)」として、IETF に Internet-Draft として提出しています（最新は第 04 版、2026年9月30日）。作業部会が採択した文書ではなく、個人提出（individual submission）の文書です。Internet-Draft は提案の段階にある文書で、IETF による承認や標準化を意味しません（付録 B-15）。
- **稼働率の保証** 利用契約にも利用規約にも、稼働率の保証（SLA）の定めはありません。システムの保守や基盤の障害などにより、サービスを一時的に停止することがあります。 **契約：第9条** **規約：利用規約 第9条**
- **事務所が管理する鍵** 保存するデータの暗号化は、AWS の管理する鍵によります。事務所が自ら管理する鍵での暗号化は、提供していません。 **契約：付属書 B 4.**
- **事務所ごとの専用環境** 事務所ごとにデータベースを分ける構成は、提供していません（6.1）。 **当社申告**
- **資格の照合** 利用者の弁護士資格は、利用者の申告によります。当社が、日本弁護士連合会の公開情報などと照合する仕組みは、2026年9月28日に実装を確認した時点で、ありません。 **当社申告**

- **マスキング** 5.3 のとおり、行いません。
- **mints への自動提出** 行いません。提出は、弁護士が mints の画面で行います。
- **iOS アプリ** App Store で配布しているアプリは、現在は従来版に接続します。AILEX v2 は、ブラウザで利用します。

14. 法令・規程との対応

弁護士法、弁護士職務基本規程、弁護士情報セキュリティ規程（日本弁護士連合会 会規第117号）の各条文が求めることに、AILEX v2 がどう対応しているかは、弁護士法・日弁連規程との対応に 23 項目でまとめています。評価は、当社の自己評価です。同ページは 2026年9月時点の記載です。当社のほかのページと本白書とで記載が異なる場合は、本白書の記載が新しい内容です。

弁護士情報セキュリティ規程は、取り扱う情報の基本的な取扱方法を定めることを、弁護士等に求めています。取扱方法を定め、運用するのは各事務所です。本白書と利用契約の付属書は、事務所がその中で委託先の措置を記載するときの資料として使えます。

付録 A 確認の記録

A-1 応答ヘッダ

2026年10月6日 13時44分（日本時間）、<https://app.ailex.co.jp/login> を認証なしで取得したときの応答です。nonce の値は、応答のたびに変わるため省略しています。Cookie の値も省略しています。

strict-transport-security	max-age=31536000; includeSubDomains
content-security-policy	default-src 'self'; script-src 'self' 'nonce-（省略）'; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; font-src 'self' https://fonts.gstatic.com data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; frame-ancestors 'none'; object-src 'none'; base-uri 'self'; form-action 'self' https://checkout.stripe.com https://billing.stripe.com
x-frame-options	DENY
x-content-type-options	nosniff
referrer-policy	same-origin
permissions-policy	camera=(), microphone=(), geolocation=(), payment=()
cache-control	no-cache, private
set-cookie	XSRF-TOKEN=（値は省略）; Max-Age=28800; path=/; secure; samesite=lax
set-cookie	ailex_session=（値は省略）; Max-Age=28800; path=/; secure; httponly; samesite=lax

コンテンツセキュリティポリシーが外部の読み込み元として許しているのは、書体の配信（fonts.googleapis.com・fonts.gstatic.com）と、https の画像です。スタイルについては、ページに直接書かれた指定を許しています（style-src の 'unsafe-inline'）。フォームの送信先（form-action）には決済サービスのドメインが含まれていますが、現在の支払方法は銀行振込（請求書払い）で、当社はクレジットカード番号や銀行口座番号を取得しません。

規約：利用規約 第8条、プライバシーポリシー 1.

同じ日に、ログイン後の操作ログの画面でブラウザが読み込んだ外部の接続先は、書体の配信の二つだけで、外部のスキプットの読み込みはありませんでした。

A-2 名前解決

2026年10月6日、app.ailex.co.jp の DNS を、公開の DNS で照会した結果です。

CNAME	ailex-production-....ap-northeast-1.elb.amazonaws.com
A	上記のロードバランサーの IPv4 アドレス 2 件（アドレスは変わるため記載しません）
AAAA	なし

ap-northeast-1 は、AWS の東京リージョンです。

A-3 操作ログ

2026年10月6日、当社の検証用の事務所（架空のデータで検証に使っている事務所）の操作ログを、管理者の画面で確認した結果です。

件数	確認した時点で 578 件（利用者の欄が「AILEX自動」の行が143 件、それ以外が 435 件）
項目	日時、利用者、操作、対象、IP アドレス
絞り込み	利用者、操作、期間
操作の種類	絞り込みの選択肢は 66 種類（認証、事件・依頼者・文書・書面の作成と変更、事件などの閲覧、AI の呼び出し、書面の書き出し、mints の提出準備、依頼者ポータルの閲覧と解錠、規約への同意 など）
AI の呼び出し	開始と完了を記録。モデルの識別子は jp.anthropic.claude-haiku-4-5-20251001-v1:0（72 件）、jp.anthropic.claude-sonnet-4-6（69 件）、amazon.titan-embed-text-v2:0（38 件）の 3 種類
対象の欄に残る内容の例	利益相反の確認では、入力した氏名。裁判例の検索では、検索語。文書の取り込みでは、ファイルの名前。書面の書き出しでは、形式と版。メールの送信では、本文のハッシュ値。規約への同意では、同意した版

A-4 当社による検証の記録

実施日	内容	結果
2026年9月17日	本番環境で、検証用の事務所を使い、全員への 2 要素認証の必須化、接続元 IP の制限、外部連携（MCP）のトークンを確認	2 要素認証が未登録の利用者は登録画面に移され、ほかの画面を開けない。コードが違っているとログインできない。許可していない接続元からは「この接続元からは利用できません」と表示される（403）。外部連携（MCP）は、トークンなし・無効なトークン・削除したトークンでは 401。別の事務所が発行したトークンでは、記録が返らない
2026年9月21日	本番環境で、検証用の二つの事務所を使い、ブラウザの画面について、別の事務所の記録の識別子を直接指定する 23 通りの経路（事件、依頼者、相談、請求書、文書とそのダウンロード、書面とその出力、提出物など）にアクセス	すべて 404
2026年9月21日	確認用の値（CSRF トークン）を付けずに、4 種類の送信を実行	すべて拒否（419）
2026年9月25日	ログイン画面について、Cookie の属性、CSRF トークンのない送信、続けて失敗したときの制限、HTTP から HTTPS への転送を確認	セッションの Cookie は Secure・HttpOnly・SameSite=Lax。CSRF トークンのない送信は拒否（419）。同じ接続から続けて失敗すると、一定時間の制限が表示される。HTTP は HTTPS へ転送される（301）
2026年10月6日	応答ヘッダ、名前解決、認証のないアクセス、設定画面、操作ログ、書き出しの画面、ゴミ箱の画面、法令検索の画面、利用契約の本文を確認	付録 A-1～A-3、A-5、A-6 のとおり

これらは当社が自ら行った確認で、第三者機関による診断ではありません。確認した範囲は上の表のとおりで、すべての経路・すべての機能を網羅したものではありません。依頼者ポータルと相談フォームは、上の検証の対象に含まれていません。

A-5 認証のないアクセス

2026年10月6日、認証の情報を付けずに、外部連携（MCP）の接続先（<https://app.ailex.co.jp/mcp>）へ送信した結果は、401（認証が必要）でした。

A-6 画面の表示

2026年10月6日に、当社の検証用の事務所の画面に表示されていた文言です（抜粋）。

画面	表示されていた文言
設定 → セキュリティ	「全員に2要素認証を求める 有効にすると、未登録の方は次回ログイン時に登録画面へ進みます。登録するまで他の画面は開けません。」 「接続を許すIPアドレス 空欄なら制限しません。」「1行に1つ、CIDR表記も使えます。設定を誤ると全員が入れなくなるため、ご自身の接続元を必ず含めてください。」 「事務所のアカウントでのログイン Entra ID や Google Workspace と連携すると、そちらでアカウントを止めた時点で AILEX にも入れなくなります。」 「パスワードでのログインを止める AILEX 独自のパスワードが残っていると、事務所側でアカウントを止めても入れてしまいます。連携の動作を確認してから有効にしてください。」
設定 → メンバー	役割の選択肢は「管理者」「弁護士」「事務員」
設定 → 2 要素認証	「認証アプリ（Google Authenticator、1Password など）を開く」「QR コードを読み取る」「表示された6桁のコードを入力する」
設定 → 外部連携	「外部連携（MCP） 社内の Copilot などから、あなたの権限の範囲で事件・文書を参照できるようにします。既定は読み取り専用で、すべてのアクセスが監査ログに残ります。書き込みを許可すると、タスクの作成と期日の提案ができます（期日は確認待ちで承認するまで登録されません）。」 「Google カレンダー 期日をご自身のカレンダーに書き出します。」「この環境には Google の認証情報が設定されていません」 「LINE 通知 当日の期日と提出期限の注意喚起を LINE に送ります。送るのは日時と件名だけで、事件の中身は載せません。」「この環境には LINE の認証情報が設定されていません」
設定 → AI と書面	「AILEX が自動で進めること 事務所の全員に効きます。」として、次の3項目のチェック欄。 「相手方の書面が届いたら、主張の整理・反論タスク・準備書面の下書きまで用意する」 「裁判所の書面（呼出状・調書・決定）が届いたら、期日を読み取って登録する（登録した期日には「要確認」の印が付き、「今日」画面で確かめられます）」 「通知書・内容証明・受任通知などを保存したら、表現を点検する」
データの書き出し	「事務所に登録されている内容を、表計算ソフトで開ける形で取り出せます。ご契約の状態にかかわらず、いつでもご利用いただけます。」 一覧の書き出しとして「事件の一覧」「期日・予定」「報酬・実費」（いずれも Excel）。 「事件を開くと、その事件の時系列と、破産・個人再生の債権者一覧を書き出せます。書面は「書面」タブから Word 形式で取り出せます。」 「事件の「文書」タブから1件ずつ取り出せます。読み取った本文だけをテキストで取り出すこともできます。件数が多く一括での取り出しをご希望の場合は、お問い合わせください。まとめてお渡します。」 「書き出しの操作は操作ログに記録されます。」
ゴミ箱	「削除したものは30日間ここに残り、復元できます。」

画面	表示されていた文言
法令検索	「e-Gov 法令検索から条文の原文を取得します。」 「条文は e-Gov 法令検索の原文です。AI に条文を生成せず、必ずここから確認してください。」

付録 B 参照した資料

URL は、2026年10月6日に到達を確認しました。AWS の文書は、AWS が内容を変更することがあります。

B-1 AWS ブログ「Amazon Bedrock で日本国内に閉じた Anthropic Claude 4.5 の推論が可能に！日本国内クロスリージョン推論のご紹介」（2025年10月16日）

<https://aws.amazon.com/jp/blogs/news/amazon-bedrock-now-supports-japan-cross-region-inference/>

B-2 Amazon Bedrock FAQs（学習への利用、モデルの提供者への共有、第三者評価の対象）

<https://aws.amazon.com/bedrock/faqs/>

B-3 Amazon Bedrock User Guide 「Data protection」（モデルの提供者のアクセス）

<https://docs.aws.amazon.com/bedrock/latest/userguide/data-protection.html>

B-4 Amazon Bedrock User Guide 「Amazon Bedrock abuse detection」（保存・確認の例外）

<https://docs.aws.amazon.com/bedrock/latest/userguide/abuse-detection.html>

B-5 Amazon Bedrock User Guide のモデルの説明ページ（推論プロファイルの送信元と送り先のリージョン、対応する機能）

Claude Sonnet 4.6 <https://docs.aws.amazon.com/bedrock/latest/userguide/model-card-anthropic-claude-sonnet-4-6.html>

Claude Haiku 4.5 <https://docs.aws.amazon.com/bedrock/latest/userguide/model-card-anthropic-claude-haiku-4-5.html>

B-6 Amazon Bedrock User Guide 「Supported Regions and models for inference profiles」（接頭辞だけに頼らない旨の案内）

<https://docs.aws.amazon.com/bedrock/latest/userguide/inference-profiles-support.html>

B-7 AWS 「Shared Responsibility Model」（責任共有モデル）

<https://aws.amazon.com/compliance/shared-responsibility-model/>

B-8 AWS 「Clarifying Lawful Overseas Use of Data (CLOUD) Act」

<https://aws.amazon.com/compliance/cloud-act/>

B-9 弁護士法（昭和24年法律第205号）

<https://laws.e-gov.go.jp/law/324AC10000000205>

B-10 個人情報の保護に関する法律（平成15年法律第57号）

<https://laws.e-gov.go.jp/law/415AC00000000057>

B-11 個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン」に関する Q&A 7-53・7-54・12-3・12-4

https://www.ppc.go.jp/all_faq_index/faq1-q7-53/

https://www.ppc.go.jp/all_faq_index/faq1-q7-54/

https://www.ppc.go.jp/all_faq_index/faq1-q12-3/

https://www.ppc.go.jp/all_faq_index/faq1-q12-4/

B-12 個人情報保護委員会「令和8年改正個人情報保護法について」

<https://www.ppc.go.jp/personalinfo/legal/r8kaiseihogohou/>

B-13 日本弁護士連合会「弁護士職務基本規程」（会規第70号）

https://www.nichibenren.or.jp/library/pdf/jfba_info/rules/kaiki/kaiki_no_070.pdf

B-14 日本弁護士連合会「弁護士情報セキュリティ規程」（会規第117号。2024年6月1日施行）

https://www.nichibenren.or.jp/library/pdf/jfba_info/rules/kaiki/kaiki_no_117.pdf

改訂履歴

版	日付	内容
v1.0	2026年2月13日	初版。従来版（users.ailex.co.jp）を対象（公開時のお知らせ）
v2.0	2026年10月6日	AILEX v2（app.ailex.co.jp）を対象に、全面的に書き直し

発行	AILEX合同会社
代表	上村 十勝
所在地	〒150-0043 東京都渋谷区道玄坂1-10-8 渋谷道玄坂東急ビル
電話	03-6821-7462
お問い合わせ	info@ailex.co.jp（内容についてのご質問、利用契約に基づくご確認）
顧問弁護士事務所	弁護士法人えそら（本白書の監修を意味するものではありません）

ご注意 本白書は、一般的な情報の提供を目的とするもので、法的な助言ではありません。「当社申告」と表示した記載は、当社の設計文書と実装に基づく申告で、外部から確かめられるものではありません。記載は 2026年10月6日時点のもので、機能の追加や契約の改定により変わります。権利と義務については、利用契約・利用規約と本白書の記載が異なる場合、利用契約・利用規約が優先します。弁護士法、個人情報保護法、日本弁護士連合会の規程などへの適合は、各事務所の利用の目的と運用に照らして、各事務所の責任でご判断ください。AILEX の利用によって、弁護士の職務上の義務や責任が軽減され、または免除されるものではありません。AILEX は、法律事件に関する鑑定、代理、仲裁、和解その他の法律事務を行うものではありません（弁護士法第72条）。当社の顧問弁護士事務所は弁護士法人えそらです（本白書の監修を意味するものではありません）。

Amazon Web Services、AWS、Amazon Bedrock は、Amazon.com, Inc. またはその関連会社の商標です。Microsoft、Microsoft Entra、Excel、Word は、米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。Google、Google Workspace、Google カレンダーは、Google LLC の商標です。Claude は、Anthropic, PBC の商標です。GitHub は、GitHub, Inc. の商標です。LINE は、LINEヤフー株式会社の商標または登録商標です。App Store は、Apple Inc. のサービスマークです。mints（民事裁判書類電子提出システム）は、裁判所のシステムの名称です。当社と裁判所との提携や、裁判所による認定を意味するものではありません。その他の会社名・製品名は、各社の商標または登録商標です。