

セキュリティ ホワイトペーパー



この文書について

この文書は、LegalBrain エージェントの情報セキュリティへの取り組みと、情報セキュリティの観点からお客さまにご注意いただきたい点について紹介するものです。

LegalBrain エージェントは、弁護士ドットコム株式会社（以下、「当社」といいます）が運営する、法務特化型AIエージェントサービスです。法務相談の対応から、法令や判例などのリサーチ、文書の作成・レビューまで、法務の幅広い業務に対応します。

LegalBrain エージェントでは、お客さまから預かるデータ（入力データ・AIとの対話履歴等）を重要な機密情報として扱います。お客さまの意思に反して第三者に読み取られないように、情報セキュリティに配慮した慎重な取り扱いを行います。

なお、この文書は「LegalBrain エージェント」のサービス本体について記述したものです。他社サービスとの連携機能や派生サービスについては、この文書の記述が当てはまらない場合があります。

目次

1. LegalBrain エージェントの

セキュリティの取り組み-----	5
1-1. 所在地と法管轄-----	5
1-2. 暗号による保護-----	5
1-2-1. 通信の暗号化-----	6
1-2-2. データの暗号化-----	6
1-2-3. パスワードのハッシュ化-----	6
1-3. データのバックアップと返却・削除-----	6
1-3-1. サービス側でのバックアップ-----	6
1-3-2. お客さま側でのバックアップ-----	7
1-3-3. 解約時のデータの扱い-----	7
1-3-4. データの削除-----	7
1-4. 時刻の同期-----	7
1-5. アカウント・アクセス管理-----	8
1-5-1. アカウントの登録・削除-----	8
1-5-2. 認証-----	8
1-6. ログ取得と監視体制-----	8
1-6-1. ログの取得と保存-----	8
1-6-2. 監視-----	9
1-7. 開発体制-----	9
1-8. 情報セキュリティインシデントの取り扱いと通知-----	10
1-8-1. 報告するインシデントの範囲-----	10
1-8-2. インシデントの通知手順-----	10
1-8-3. デジタル証拠の提供-----	10
1-9. 記録の保護-----	11
1-10. 情報セキュリティの独立したレビュー-----	11

2. お客さまにご注意いただきたい点-----	12
2-1. お客さまの環境におけるセキュリティ上の注意点-----	12
2-2. お客さまによるインシデント報告とご連絡・ご依頼-----	13
2-2-1. 通常の連絡先-----	13
2-2-2. セキュリティに関する緊急連絡先-----	13
2-2-3. ログ調査-----	13
改訂履歴-----	14

1. LegalBrain エージェントの セキュリティの取り組み

LegalBrain エージェントが実施しているセキュリティの取り組みについてご紹介します。

1-1. 所在地と法管轄

LegalBrain エージェントは、弁護士ドットコム株式会社が提供しています。当社は日本の法人であり、本社所在地は東京都です。LegalBrain エージェントのサービスの開発、運用はすべて日本国内で行っています。

LegalBrain エージェントのシステムは、Amazon Web Services（AWS）およびGoogle Cloud（GCP）を利用して構築しており、システムが保管するデータおよびそのバックアップデータは、いずれもAWSの管理するデータセンターに保管されています。

AWS、GCPはいずれもアメリカを本拠地とする企業ですが、いずれも日本国内にデータセンターを保有しています。LegalBrain エージェントでは国内リージョンにデータを保存しています。LLMなど一部の処理に海外のリージョンを利用することはありますが、お客さまのデータの保管にはすべて国内のリージョンを利用しており、海外のサーバーにお客さまのデータを保管することはありません。

また、AWSとの契約においては準拠法を日本法とする契約を結んでいます。

1-2. 暗号による保護

LegalBrain エージェントでは、通信内容や保存データ、パスワードを暗号技術によって保護しています。

1-2-1. 通信の暗号化

LegalBrain エージェントでは、通信内容を暗号化することで、データの漏洩や改ざんを防いでいます。暗号通信方式としてTLS 1.2以上を使用しています。

1-2-2. データの暗号化

LegalBrain エージェントでは、お客さまが入力したデータ、AIとの対話履歴を保存しているサーバーに対して暗号化を行い、データの漏洩や、内部不正による持ち出しを防いでいます。

データベースは、AWS KMS を用いた保存時暗号化（AES-256）により、ストレージレベルで暗号化されています。

1-2-3. パスワードのハッシュ化

LegalBrain エージェントの利用者のパスワードは平文では保存せず、ハッシュ化し、元の形に復元できないようにした上で保存しています。

1-3. データのバックアップと返却・削除

お客さまからお預かりしたデータは、LegalBrain エージェントのシステム上で保管されています。

1-3-1. サービス側でのバックアップ

LegalBrain エージェントでは、日次でフルバックアップを取得しております。また、IaaS 機能により差分バックアップを随時取得しています。

1-3-2. お客様側でのバックアップ

現状、LegalBrain エージェントにはお客様側でデータを一括ダウンロードする機能はご用意しておりません。個別のチャット履歴・出力結果等については、画面上でご確認いただくことが可能です。

1-3-3. 解約時のデータの扱い

お客様がLegalBrain エージェントのサービスを解約された場合、解約後はデータを閲覧できなくなります。

契約終了後は、お客様からの要望に応じて個人データの削除を行っております。

1-3-4. データの削除

お客様からの正当な削除依頼がある場合に、当社が定めた手順にしたがい、LegalBrain エージェント上に保存されたデータを削除します。

1-4. 時刻の同期

LegalBrain エージェントのシステムでは、AWSおよびGCPが提供する時刻同期サービスに同期された時刻を使用しています。これにより、システム内の各種ログのタイムスタンプはいずれもUTC（Coordinated Universal Time、協定世界時）に同期されています。

1-5. アカウント・アクセス管理

1-5-1. アカウントの登録・削除

現状、LegalBrain エージェントではお客さま側でユーザーアカウントを登録・削除する機能はご用意しておりません。アカウントの登録・削除は、お客さまの管理者（契約者）からご依頼をいただいたうえで、当社が以下の管理プロセスにもとづき実施いたします。

- お客さまからの依頼にもとづいて受付
- アカウント作成・権限付与・削除を、統制のとれた当社担当者が実施
- アカウントのライフサイクル（作成から削除まで）の記録を保持

1-5-2. 認証

LegalBrain エージェントでは、当社が登録・管理したユーザーアカウントとパスワードによる認証を提供しています。

1-6. ログ取得と監視体制

1-6-1. ログの取得と保存

LegalBrain エージェントでは、不正アクセスやインシデントの調査のために、アクセスログ、操作ログ、エラーログ等のログを取得しています。また、改ざん防止のための保護も行っています。

1-6-2. 監視

LegalBrain エージェントでは、システムの状態・パフォーマンス・エラー発生状況等を常時監視しています。異常を検知した場合には、速やかに関連部署と連携し、対処を進める体制としています。

インシデントやお客さまに影響が及ぶ事象を検知した場合は、「1-8. 情報セキュリティインシデントの取り扱いと通知」に記載の手順に従ってお客さまに通知いたします。

1-7. 開発体制

LegalBrain エージェントのシステム開発は、当社の社内で行っています。

※他社サービスとの連携機能については、連携先の各社にて開発・運用が行われている場合があります。

LegalBrain エージェントでは、セキュリティ要件を含めた開発ガイドラインを設けており、開発時にはコードレビューを実施し、レビューを経なければ本番反映できない仕組みとすることで、実際のコードがガイドラインに従っていることを確認しています。

また、開発環境・テスト環境・本番環境を論理的に分離し、開発時の作業が本番サービスに影響を与えないように配慮しています。

さらに、必要に応じて第三者によるウェブアプリケーション脆弱性診断を実施し、重ねて安全性を確認しています。

1-8. 情報セキュリティインシデントの取り扱いと通知

LegalBrain エージェントにおいて、情報セキュリティインシデント（情報漏洩など、情報セキュリティに関連した事故、事象。以下「インシデント」といいます）が起きた場合、以下のように対処を行います。

1-8-1. 報告するインシデントの範囲

利用者に明確な被害が及ぶか、もしくは、LegalBrain エージェントのサービスの継続に影響を及ぼすと判断したものについては、お客さまに報告いたします。

1-8-2. インシデントの通知手順

インシデントを認知した場合、可及的速やかにお客さまに通知いたします。

以下の手段で通知いたします。

- インシデントが多数のお客さまに影響する場合は、サービスサイト上にて告知いたします。
- インシデントにより特定のお客さまに影響が出たと判断した場合、個別に電子メール等にてご連絡いたします。
- インシデントが継続的に発生している場合や、調査報告に時間を要する場合、サービスサイト上で続報を提供いたします。

1-8-3. デジタル証拠の提供

お客さま側でのインシデント調査のためのログの提供依頼については、「2-2-3. ログ調査」に記載の手順にしたがい対応いたします。

1-9. 記録の保護

LegalBrain エージェントでは、お客さまによるサービス利用に関連して収集・保存する記録（操作ログ、アクセスログ、AIとの対話履歴等）を、以下のように保護しています。

- **暗号化**：「1-2. 暗号による保護」に記載のとおり、暗号化しています
- **アクセス制御**：当サービスでは、お客さまのデータを保護するため、本番環境へのアクセスを厳格に管理しています。通常の運用業務において、担当者がお客さまのデータが格納された領域を参照することはありません。
例外として、障害対応など運用上必要な場合に限り、権限を付与された一部の担当者が本番環境のシステムに対してアクセスする場合があります。これらのアクセスは規定された承認プロセスに基づいて実行され、すべての操作ログが記録・監視されています。
- **改ざん防止**：AWS CloudTrailの監査ログは、組織ポリシーによる削除・無効化の禁止と、専用の監査ログアカウントへの集約により、改ざんから保護しています。さらにログファイル検証機能（ハッシュ値＋電子署名）により改ざん検知も行っています。
- **バックアップ**：「1-3. データのバックアップと返却・削除」に記載のとおりバックアップを行っています

1-10. 情報セキュリティの独立したレビュー

当社は、LegalBrain エージェントについてISO/IEC 27001およびISO/IEC 27017に準拠した内部監査を実施しており、本ホワイトペーパーで提示しているセキュリティ管理策が適切に実施されていることを担保しています。

また、必要に応じて第三者による脆弱性診断を受け、その結果にもとづいて改善を進めています。

2. お客様にご注意いただきたい点

LegalBrain エージェントのサービスを安全に利用するために、お客様にご注意いただきたい点がいくつかあります。

2-1. お客様の環境におけるセキュリティ上の注意点

LegalBrain エージェントのシステムの構成要素については、当社の責任において管理と運用を行っています。クラウドサービス側のアプリケーション、ミドルウェア、サーバー、ネットワーク機器については、当社が責任を持って管理いたします。お客様にてソフトウェアのアップデートを行う必要もありません。

一方で、お客様がインターネットに接続する環境、利用される端末、Webブラウザ、電子メールアドレス等については、お客様側でご用意いただく必要があります。これらの情報セキュリティについては、お客様にて管理いただく必要があります。

お客様側の環境について、特に以下の点についてご配慮ください。

- ネットワーク環境の安全性
- 端末の盗難防止策
- 端末OSのセキュリティアップデート
- Webブラウザのセキュリティアップデート
- その他のソフトウェアのセキュリティアップデート
- 電子メールの盗聴・傍受への対策
- 電子メールへのウイルス対策

2-2. お客さまによるインシデント報告とご連絡・ご依頼

お客さまがLegalBrain エージェントに関するインシデントを発見された場合、もしくは、インシデントに発展する可能性のある不審な事象を発見された場合には、速やかにLegalBrain エージェントのお問い合わせ窓口までご連絡ください。

2-2-1. 通常の連絡先

お客さまがLegalBrain エージェントをご利用中の場合、通常のお問い合わせと同様に、[LegalBrain エージェントの問い合わせフォーム](#)の窓口からご連絡いただくことができます。

2-2-2. セキュリティに関する緊急連絡先

なんらかの理由で通常のサポートがご利用いただけない場合や、緊急で連絡を取る必要がある場合、当社の情報セキュリティ窓口に電子メールでご連絡いただくことができます。窓口のメールアドレスは、「弁護士ドットコム株式会社 情報セキュリティポリシー」の「情報セキュリティに関するお問い合わせ」の項目に記載しています。

情報セキュリティポリシー

<https://www.bengo4.com/corporate/privacy/it-security>

2-2-3. ログ調査

ログ類は原則的には非公開とさせていただいておりますが、個々の事案に対してご相談いただき、ログの提供も含めて、弊社にて検討をさせていただきます。

「2-2-1. 通常の連絡先」または「2-2-2. セキュリティに関する緊急連絡先」よりご相談ください。

また、当社の運用ルールと法令に従い、ログを監査法人や第三者機関へ開示することがございますのでご了承ください。

改訂履歴

- 2026年7月16日 初版作成。2026年7月30日以降の体制について記載
- 2026年9月9日 「この文書について」の文章を一部修正。「1-6-2. 監視」「1-8. 情報セキュリティインシデントの取り扱いと通知」「1-10. 情報セキュリティの独立したレビュー」の内容を一部修正。