Leadsia

AI受付「SOPHIA」セキュリティホワイトペーパー

お預かりする情報の取扱いについて

第1.2版　2026年10月9日　株式会社Leadsia

はじめに

この文書は、AI受付「SOPHIA」がお電話でお預かりする情報について、どこに置き、誰が見られ、いつ消え、万が一の事故の時にどうするかを、まとめたものです。

- 対象のサービス：AI受付「SOPHIA」（https://sophia.leadsia.ai/）
- 提供：株式会社Leadsia（以下、当社）
- 契約上の取り決めは、利用規約（https://leadsia.ai/terms）とプライバシーポリシー（https://leadsia.ai/privacy）に定めております。この文書の内容と異なる場合は、利用規約とプライバシーポリシーが優先いたします。

要点

1. 録音するかどうかと保存期間は、お客様が管理画面で選べます。保存期間を過ぎたデータは、自動で削除いたします。
2. お預かりした通話のデータを、AIの学習に使うことはございません。
3. データはご契約のアカウントごとに分けて管理し、管理画面のログインは二段階認証で守っております。管理画面での操作は、記録として残しております。
4. 万が一の事故の時は、発覚から24時間以内にご連絡し、原因の調査から再発の防止まで、当社が責任を持って対応いたします。
5. ご契約の終了後、30日以内に、お預かりした通話のデータと設定をすべて削除し、削除のご報告をいたします。
6. 開発と保守は、すべて当社で行っております。ISO/IEC 27001 と ISO/IEC 27017 の認証の、2027年4月までの同時取得に向け、現在準備中です。

01 サービスの概要と、情報の流れ

SOPHIAは、お客様の電話番号にかかってきたお電話に、AIが出て受付をするサービスです。ご用件を伺い、お客様が決めた内容をご案内し、必要に応じて担当の方へおつなぎし、受付の内容を管理画面と通知で

お届けいたします。

1件のお電話で、情報は次の順に流れます。

1. お電話は、お客様の番号からの転送で、SOPHIAの受付番号に届きます。電話の発着信は、電話の事業者（Twilio）が担っております。
2. 通話中の音声は、当社の音声サーバー（Fly.io）を通して、音声AIの事業者（OpenAI）の基盤で処理いたします。AIは、お客様が決めた台本と登録情報に沿ってお話しいたします。
3. 通話が終わると、文字起こしをもとに、要約AIの事業者（Anthropic）の基盤で要約と分類を作り、当社のデータベース（Supabase）に保管いたします。
4. 受付の内容は、管理画面に表示し、お客様が設定した通知先（メール、SMS、Slack、Chatwork、kintone など）にお届けいたします。
5. 録音する設定の場合、録音は電話の事業者（Twilio）の保管領域に保管いたします。

万が一、音声AIの事業者の基盤に接続できない時も、予備の仕組みに切り替えて、受付を継続いたします。予備の仕組みでは、音声の認識に株式会社アドバンスト・メディアの AmiVoice、応対の文章づくりに Anthropic、音声の読み上げに OpenAI を使っております。

02 お預かりする情報

区分	内容
お電話の相手の情報	お名前、お電話番号、ご用件、ご住所などお電話で伺った内容と、通話の録音・文字起こし・要約
受付の設定	台本、登録情報（営業時間、ご案内する内容など）、取次先、通知先、顧客リスト
ご契約者の情報	ご担当の方のお名前、メールアドレス、ご請求の情報
操作の記録	管理画面で、いつ、誰が、何をしたかの記録（8章）

- お電話で伺う項目は、お客様が受付の設定で決められます。
- 台本の下書きは、お客様のホームページの公開情報と、設定画面にご入力いただいた内容をもとに作成いたします。
- クレジットカードでお支払いの場合、カードの番号は決済の事業者（Stripe）が直接受け取ります。当社では、カードの番号を保持しておりません。

03 預け先（外部の事業者）

SOPHIAは、次の事業者のサービスを使っております。事業者ごとに、役割と、預ける情報をお示しいたします。

事業者	役割	預ける情報
Supabase	データベースと認証の基盤（データの保存先は東京リージョン）	受電履歴、文字起こし、要約、設定、顧客リスト、ログインの情報、操作の記録
Twilio	電話の発着信、録音の保管、SMSの送信	通話の音声、録音、発着信の電話番号、SMSの本文
OpenAI	通話中のAIの応対と、音声の認識	通話中の音声と、受付の設定
Anthropic	通話後の要約と分類、台本の下書きづくり、予備の仕組みでの応対	文字起こし、お客様のホームページの公開情報、設定画面にご入力いただいた内容
Fly.io	当社の音声サーバーの基盤（東京リージョン）	通話中の音声（中継のみ）
株式会社アドバンスト・メディア（AmiVoice）	予備の仕組みでの音声の認識	通話中の音声
Twilio SendGrid、Resend	メールの送信（受電の通知、月次のレポート）	メールの宛先と本文
Lovable	データベース（Supabase）の管理、電話とメールの事業者への中継	データベースに保管する情報、電話の事業者への指示、録音の再生時の音声、通知メールの本文
Google	Googleカレンダーとの連携、Googleアカウントでのログイン	予約の内容（連携した場合）、ログインの情報
Apple	Appleアカウントでのログイン	ログインの情報
Stripe	料金の決済	ご契約者のお名前、メールアドレス、決済の情報
Firecrawl	台本の下書きのための、お客様のホームページの読み込み	お客様のホームページの公開情報

- 各事業者は、当社の基準で精査し、定期的なモニタリングを行ったうえで選定しております。
- 個人情報の取扱いを委託している事業者の一覧は、プライバシーポリシーの第6条に載せております。
- お客様が通知や連携を設定した場合は、その宛先（Slack、Chatwork、kintone、Googleカレンダーなど）にも、受電の内容をお届けいたします。どれを使うかは、お客様が決められます。

04 録音と保存期間

- 通話を録音しない設定を選べます。その場合は録音を残さず、文字起こしと要約だけを保管いたします。
- 保存期間は、30日・90日・180日・365日・ご契約中ずっと、から選べます。何も選ばない場合は、ご契約中ずっと保管いたします。
- 保存期間を過ぎると、毎日の自動の処理で、録音（電話の事業者の保管領域にあるものを含みます）、文字起こし、要約と、お名前・お電話番号・ご住所などお電話で伺った内容を削除いたします。日時、受付の結果、通話時間など、件数の集計に使う情報だけを残しております。
- 録音の再生は、当社の仕組みを通し、ログインの確認が済んだ方にだけお返しいたします。本番のアカウントでは、二段階認証の確認まで済んだ方に限ります。電話の事業者の保管先のURLが、画面に出ることはございません。

05 AIの学習

- お預かりした通話のデータを、AIの学習に使うことはございません。利用規約の第7条に定めております。
- 通話の処理に使うAIの事業者（OpenAI、Anthropic、アドバンスト・メディア）は、いずれも、お預かりしたデータを事業者のAIの学習に使わない条件で利用しております。
- 通話中の音声を処理する音声AIの事業者（OpenAI）とは、データを保持しない取り決め（ゼロデータ保持）を結んでおります。処理が終わった通話は、事業者の側にも残りません。

06 AIが話す内容の管理

- SOPHIAがお電話で話す内容は、お客様が決めた台本と登録情報の範囲に限っております。範囲の外のご質問には答えを作らず、担当の方からの折り返しをご案内いたします。
- 台本と設定は、お客様がいつでも管理画面で変更できます。AIが自分で台本を書き換えることはございません。
- 使うAIの版は、当社が固定しております。知らないうちに切り替わることはございません。
- 会話に不正な命令を紛れ込ませる攻撃（プロンプトインジェクション）への備えは、当社の記事にまとめております（https://leadsia.ai/blog/prompt-injection-defense-architecture）。

07 誰が見られるか

- データは、データベースの行ごとのアクセス制御（Row Level Security）で、ご契約のアカウントごとに分けて管理しております。ほかのお客様から見えることはございません。
- お客様の側では、管理画面にログインできる方がご覧になれます。お客様が設定した通知先にも、受電の内容をお届けいたします。
- 当社の側で通話の内容に触れられるのは、当社が選任した管理者のみです。管理者が使う各事業者の管理画面も、二段階認証で守っております。

- 受付の内容の変更を当社が代行する時は、お客様のご了承を得て管理画面に入ります。その操作も、操作の記録に残ります。

08 ログインの保護と、操作の記録

ログイン

- ログインの方法は、メールアドレスとパスワード、Googleアカウント、Appleアカウントの三つです。
- どの方法でログインする場合も、スマートフォンの認証アプリに表示される6桁の番号で確認いたします（二段階認証）。同じブラウザでログインが続いている間は、番号を改めてお求めすることはございません。
- 1つのアカウントに、複数のスマートフォンを登録できます。
- 万が一、スマートフォンを無くされた時は、support@leadsia.ai にご連絡ください。ご契約時のご担当の方のお電話番号に当社から折り返し、ご本人であることを確かめてから、登録を解除いたします。
- パスワードは、認証の基盤（Supabase）の仕組みで、元に戻せない形（ハッシュ）にして保管しております。パスワードの変更は、管理画面から行えます（8文字以上）。
- トライアル用のアカウントも、お引き渡しの時に二段階認証を設定いたします。

操作の記録

管理画面での、次の操作を記録しております。

1. 変更：設定、台本、取次、通知の振り分け、顧客リスト、予約、受電履歴のアーカイブや社内メモなど。追加・変更・削除のすべて
2. 閲覧：受電履歴の詳細を開いた、録音を再生した
3. 持ち出し：受電履歴と顧客リストのCSVの出力（件数を含みます）
4. ログイン：ログイン、ログアウト、番号の確認の成功と失敗、認証アプリの登録と取り外し、パスワードの変更

- 1件ごとに、日時、アカウント、操作の種類、対象のデータ、変えた項目の名前、IPアドレスとブラウザの種類を残しております。お名前、電話番号、メモの中身など、入力された値は記録いたしません。
- 記録は1年間保管し、過ぎたものは自動で削除いたします。記録は、管理画面から書き換えたり消したりできない形で保管しております。
- ご依頼をいただければ、期間を指定して記録を抜き出し、お渡しいたします。

データの取り出し

- 受電履歴は、管理画面からCSVで取り出せます。一覧の絞り込みと同じ範囲を、新しい順に最大10,000件まで出力いたします。

09 通信と保管の暗号化

- 管理画面との通信と、当社と各事業者との間の通信は、TLSで暗号化しております。

- データベースに保管するデータは、事業者（Supabase）の仕組みで、AES-256で暗号化して保管しております。
- 録音は、電話の事業者（Twilio）の保管領域で、暗号化して保管しております。
- 通知や連携に使う認証情報（Slack、Chatwork、kintone など）は、さらに個別に暗号化して保管しております。
- 音声サーバーは、通話の音声を中継するだけで、ディスクに保存いたしません。運用の記録（ログ）にも、通話の内容は残しておりません。

10 削除

- ご契約の終了後、30日以内に、お預かりした通話のデータと設定をすべて削除し、削除のご報告をいたします。契約と請求の記録は、法令に従って保管いたします。
- 無料トライアルのみで終了された場合も、同じように削除し、ご報告いたします。
- 個別に消したいデータがある時は、support@leadsia.ai にご連絡ください。当社で削除いたします。
- 保存期間による自動の削除は、4章のとおりです。

11 バックアップ

- データベースは、毎日バックアップを取り、約14日分を保管しております。万が一の障害の時も、日ごとの時点に戻せます。
- 削除したデータは、バックアップからも、約14日で順に消えます。
- バックアップから戻した場合も、削除したデータは改めて削除いたします。

12 脆弱性への対応

- データベースと、サーバーの基盤の保守は、各事業者が行っております。
- ソースコードは当社で管理し、使っている部品（ライブラリ）の既知の脆弱性を、GitHubの自動の検査で確かめております。
- 外部の専門機関による脆弱性診断も、認証の取得に合わせて受ける準備を進めております。

13 万が一の事故の時

あってはならないことだからこそ、万全の構えを取っております。

「事故」とは

「事故」は、お預かりしたデータが、権限のない第三者に渡ること（漏えい）、失われること（滅失）、書き換わること（毀損）を指しております（利用規約第17条）。原因と件数は問いません。

基盤の考え方

当社は、自社でサーバーや社内ネットワークの機器を持たず、SOPHIAの基盤を、Supabase、Twilio、OpenAI、Fly.io の上に置いております。いずれも、世界中の企業が基盤として使い、第三者機関の監査（SOC 2 Type 2）を受けている事業者です。基盤の守りは各事業者が担い、当社は、当社が守るべき入口であるアカウントと権限の管理に集中しております。

想定している事象と、当社の備え

想定している事象	当社の備え
当社のシステムへの、外部からの不正アクセス	外から社内へ入るための機器や、自社で管理するサーバーがございません。入口は各事業者の管理画面に限られ、入れるのは当社が選任した管理者のみです。すべて二段階認証で守っております。プログラムは、使っている部品の既知の脆弱性を、自動の検査で確かめております。
管理画面への不正なログイン（外部で漏れたパスワードの使い回しなどによる、なりすまし）	二段階認証により、パスワードが漏れても、ご本人のスマートフォンに表示される番号がなければ入れません。録音の再生やCSVの取り出しなど、個人情報に触れる操作は、画面だけでなく、データベースの層でも同じ確認を通しております。データはご契約のアカウントごとに分けて管理し、管理画面での操作は記録しております。
預け先の事業者で起きた不正アクセスや障害のうち、お客様のデータに影響するもの	預ける量そのものを絞っております。通話中の音声は、音声AIの事業者（OpenAI）に残らない取り決めで処理し、当社の音声サーバーにも保存いたしません。録音は残さない設定を選べ、保存期間（30日から365日）を過ぎたデータは自動で削除いたします。事業者は、当社の基準で精査し、定期的なモニタリングを行ったうえで選定しております。

検知の方法

1. 管理画面の操作の記録：ログイン、番号の確認の成功と失敗、受電履歴の閲覧、録音の再生、CSVの取り出し（件数を含みます）を、IPアドレスとともに記録しております（8章）。記録は、情報セキュリティ担当が点検しております。
2. 預け先の事業者からの通知：各事業者の障害・事故の通知を、当社で受けております。お客様のデータに影響するものは、同じ24時間の手順でご連絡いたします。
3. お客様からのお知らせ：万が一、不審な動きにお気づきの時の窓口は、support@leadsia.ai です。

万が一の時のご連絡とご報告

- 万が一、お客様のデータに影響する事故が起きた時は、発覚から24時間以内に、影響を受けるお客様へご連絡いたします。起きたことと影響の範囲をお伝えし、原因の調査から再発の防止まで、当社が責任を持って対応いたします。
- 原因、影響を受けたデータの範囲、当社の対処は、書面（電磁的記録を含みます）でご報告いたします。
- お客様が行う、ご本人への通知と、個人情報保護委員会などの関係機関への報告に必要な情報をご提供し、支援いたします。
- 以上は、利用規約の第17条に定めております。

14 責任の分かれ目

担う者	範囲
基盤の事業者	データセンターと機器の物理的な管理、基盤そのものの安全
当社	SOPHIAのプログラムと運用、お預かりしたデータの保護、外部の事業者の選定と管理、万が一の事故の時のご連絡と対応
お客様	ログインの情報（パスワードと認証アプリ）の管理、台本と登録情報の内容、録音・保存期間・通知先の設定、録音することの、お電話の相手へのお知らせ

- 録音のお知らせは、受付の最初のご挨拶に入れることができます。

15 適用される法律

- 当社とお客様の契約は、日本法に準拠いたします。紛争は、東京地方裁判所を第一審の専属的合意管轄裁判所といたします（利用規約第19条）。
- 裁判所の命令など、法令に基づく要請を受けた場合は、必要最小限の範囲で応じる場合がございます。

16 体制と第三者認証

開発と保守は、すべて当社で行っております。

情報セキュリティの体制

情報セキュリティ責任者 代表取締役	情報セキュリティの方針を定め、管理者の選任と権限を承認し、万が一の事故の時の対応を指揮いたします。
管理者	責任者が選任いたします。通話の内容に触れられるのは、管理者のみです。お客様のご了承を得た設定の代行と、万が一の障害・事故の時の対応を行っております。
情報セキュリティ担当	管理者の権限と、管理者の操作の記録を点検し、事業者のモニタリング、社内の決まりと教育、認証の取得に向けた運用を担っております。通話の内容に触れる権限は持っておりません。

- 通話の内容に触れられる管理者と、その権限を点検する情報セキュリティ担当を分けております。
- 権限は業務に必要な分だけを渡し、三か月ごとに一覧を点検し、業務を離れる時は、その日のうちに取り消しております。
- 業務に携わる全員と秘密保持契約を結び、全員のアカウントを二段階認証で守っております。

第三者認証

情報セキュリティの国際規格 ISO/IEC 27001 と、クラウドサービスのセキュリティの国際規格 ISO/IEC 27017 の認証の、2027年4月までの同時取得に向け、現在準備中です。

17 お問い合わせと改訂履歴

この文書についてのお問い合わせは、support@leadsia.ai までお願いいたします。

版	日付	内容
1.2	2026年10月9日	「事故」の定義、基盤の考え方、想定している事象と当社の備え、検知の方法（13章）を加えました。
1.1	2026年10月9日	情報セキュリティの体制（16章）と、事業者の選定（3章）、バックアップから戻した時の扱い（11章）を加えました。
1.0	2026年10月7日	初版

関連する文書

- 利用規約：https://leadsia.ai/terms
- プライバシーポリシー：https://leadsia.ai/privacy
- セキュリティのページ：https://leadsia.ai/about/security