

お客様のデータを、どう守っているか。

Geo Index の信頼センターです。認証・データ取扱い・アクセス制御・監視のそれぞれで、事実として説明できる対策だけを記載しています。

データ取扱い

何を収集し、何をLLMに送らないか

計測対象は、お客様が指定した公開Webページのコンテンツと、アカウント登録情報です。

引用分析などで OpenAI・Anthropic・Google の LLM API に送信するのは、お客様が設定した分析用プロンプトと、対象サイトの公開コンテンツのみです。顧客の個人情報を送信しない設計を方針としています。

アカウント情報や計測データはSupabase (PostgreSQL) で管理し、バックエンドはGCP Cloud Run、フロントエンドはVercel、AI最適化ページの配信はCloudflare Workers上で運用しています。いずれもマネージドサービス上での運用です。

認証・アクセス制御

Auth0 Universal Login とワークスペース権限

Geo Index へのログインは、Auth0 Universal Login を通じて行います。Googleアカウントでのログインは、Auth0 の social connection として提供しており、Geo Index自身がパスワードを保持・管理することはありません。

複数人で利用する場合は、組織のオーナー・管理者・メンバーという役割に加えて、ワークスペース単位で閲覧・編集・実行の権限を分けて付与できます。招待されたメンバーは、付与された権限の範囲でのみ操作できます。

監視・運用

エラー監視・可観測性・実行制御

個人情報の送信を避けつつ、異常なアクセスや想定外の大量実行を抑止する運用です。

項目	内容
エラー監視	Sentry。send_default_pii を無効化した上で、送信前フックでメールアドレス・認証情報・Cookie・IPアドレス等を除去・マスク。セッションリプレイは不使用。
LLM可観測性	Langfuse。どのプロンプトを、どのモデルで、いつ実行したかをすべてのLLM呼び出しについて記録。
アクセス制限	APIにIPアドレス単位で1分あたり200リクエストのレート制限を適用。
実行制御	LLM呼び出しはプランのクレジット枠を予約したうえで実行・確定する仕組みのため、想定外の大量実行を抑止。

アクセス制御

テナント分離と行レベルセキュリティ

アプリケーションからのデータ取得は、バックエンドがトークンを検証したうえで、組織とワークスペースの所有関係を照合して絞り込みます。これが実際のテナント分離を担っている層です。

加えて、データベース（PostgreSQL）の行レベルセキュリティ（Row Level Security）を、公開スキーマの全テーブルで有効にしています。これはアプリケーションを経由しない直接アクセスに備えた二層目で、これ単体をテナント分離の根拠とはしていません。

行レベルセキュリティの有効化と、ポリシーを持たないテーブルに対する権限の剥奪は、継続的インテグレーションの静的監査で毎回検査しています。新しいテーブルで設定が漏れると、検査が失敗します。

データ保持

保持期間を超えたログの取り扱い

アクセスログ・セキュリティログ・代理ログインの監査ログには保持期間を定めており、期間を超えた行を日次のバッチが検出します。実行のたびに、検出した件数を専用のテーブルへ記録します。

現在は検出と記録のみを行う段階で、実際の削除を有効にするテーブルを段階的に広げています。

事前宣言つき成果台帳は、記録の完全性を保つため自動削除の対象外です。保有個人データの開示・訂正・削除のご請求は、メール窓口で承ります。

委託先

サブプロセッサ一覧

サービス提供のために利用している外部事業者です。

事業者	利用目的
OpenAI	引用分析のLLM API
Anthropic	引用分析のLLM API
Google（Gemini API）	引用分析のLLM API

事業者	利用目的
Auth0	認証基盤（Universal Login）
Google Cloud Platform	バックエンドの実行基盤
Supabase	データベース（PostgreSQL）
Vercel	フロントエンドの配信
Cloudflare	AI最適化ページの配信・ページ取得基盤
Stripe	決済・請求
Sentry	エラー監視
Langfuse	LLM実行の記録（可観測性）

上記のほか、成果台帳のタイムスタンプ取得のために外部のタイムスタンプ局（DigiCert・Sectigo）へ、記録のハッシュ値のみを送信します。記録の本文や個人情報は送信しません。

URL取得

安全なURL取得

コンテンツ解析のためのURL取得には、SSRF対策を実装しています。

お客様が指定したURLをサーバー側で取得する際は、スキーム・ホスト名・DNS解決先を検証し、ループバックやプライベートIP、リンクローカル、クラウドのメタデータアドレスなど、内部アドレスへのアクセスを遮断します。リダイレクトが発生した場合も、遷移先ごとに同じ検証を行います。

法令対応

個人情報保護法（APPI）への対応

対応状況の詳細はプライバシーポリシーに記載しています。

取得した個人情報は、本サービスの提供・本人確認・決済・お問い合わせ対応・品質向上・不正利用防止など、あらかじめ特定した利用目的の範囲で利用します。法令に基づく場合等の限られた例外を除き、本人の同意なく個人データを第三者に提供することはありません。

LLMプラットフォームやクラウド事業者の一部は日本国外に所在するため、個人情報保護法の定めに従い、あらかじめ本人の同意を得たうえで越境移転を行います。

保有個人データの開示・訂正・削除等の本人請求は、メール（support@geoindex.app）で承ります。本人または正当な代理人であることを確認のうえ、法令に従い対応します。

法務文書

利用規約・プライバシーポリシー

個人情報保護法（APPI）への対応方針は、プライバシーポリシーに記載しています。

利用規約

サービス利用にあたっての規約です。

プライバシーポリシー

個人情報保護法（APPI）を踏まえたデータの取り扱い方針です。

特定商取引法に基づく表記

特定商取引法に基づく事業者情報の表記です。

セキュリティFAQ

よくある質問

情シス・法務のご担当者からよくいただくご質問にお答えします。

計測データやアカウント情報はどこで管理されていますか？

アカウント情報や計測データはSupabase（PostgreSQL）で管理し、バックエンドはGCP Cloud Run、フロントエンドはVercel、AI最適化ページの配信はCloudflare Workers上で運用しています。いずれもマネージドサービス上での運用です。

AIプラットフォーム（OpenAI・Anthropic・Google）に自社の顧客情報は送られますか？

送信しない設計です。引用分析などでLLMのAPIに送信するのは、お客様が設定した分析用プロンプトと、対象サイトの公開コンテンツのみです。

複数人のメンバーでワークスペースを使う場合、権限はどう分けられますか？

組織のオーナー・管理者・メンバーという役割に加えて、ワークスペース単位で閲覧・編集・実行の権限を分けて付与できます。招待されたメンバーは、付与された権限の範囲でのみ操作できます。

不正利用やアクセス集中を防ぐ仕組みはありますか？

APIにはIPアドレス単位で1分あたりのリクエスト数を制限しています。あわせて、LLM呼び出しはプランのクレジット枠を予約したうえで実行・確定する仕組みのため、想定外の大量実行を抑止します。

退会・アカウント削除の際、データはどうなりますか？

データの開示や削除といった本人請求は、メール（support@geoindex.app）で承ります。アカウントの削除にともない、当社が管理する関連データは削除または匿名化します。詳細はプライバシーポリシーをご覧ください。