pyscn

合同会社 Ludo Technologies

Enterprise データ取り扱い・セキュリティ概要

Data Handling and Security Overview

Version 1.0

最終更新日: 2026年2月4日

目次

1. 取り扱うデータ

pyscn Enterprise は、主に次の情報を扱います。

- GitHub 連携情報（インストールID、アカウントID、アカウント名、リポジトリ名）
- PRレビュー対象のコード（変更ファイルの内容）
- 監査（Audit）対象リポジトリのコード（解析時に一時取得）
- 解析結果（品質スコア、指摘事項、改善提案）
- 契約プラン情報（free/pro/team/enterprise）
- 決済連携情報（プラン反映に必要な識別情報）

2. 保存するデータ / 保存しないデータ

2.1 保存するデータ（データベース）

データ種別	内容
インストール情報	installation_id, account_id, account_login, account_type
リポジトリ管理情報	owner, repo_name, installation_id, last_audit_at, is_enabled など
プラン情報	account_id, plan_name
レート制御情報	org_id, count, reset_at
監査レポート情報	スコア、指摘一覧、推奨事項、Issue URL など

2.2 保存しないデータ

- GitHubのユーザーパスワードや個人アクセストークン
- リポジトリ全体の生コードを恒久保存すること
- クレジットカード情報（決済情報はStripe側で保持）

> **補足**
>
> PRレビューで扱うコードは処理時に使用されますが、DBへ恒久保存しません。ただし監査レポートには、ファイルパス・行番号・関数名など、コード由来の要約情報が保存されます。

3. 保存場所・保持期間・バックアップ

3.1 保存場所

本番環境の標準構成では、PostgreSQL（Render）を使用しています。現行デプロイ設定のリージョンは米国オレゴン州（oregon）です。

3.2 保持期間

データ種別	保持期間
PRレビュー用コード	処理時のみ（一時領域）。恒久保存しません
インストール/リポジトリ/プラン/レート制御情報	サービス運用期間中に保持
監査レポート	自動削除されません

3.3 バックアップ

バックアップ運用は利用するDB基盤の設定に依存します。データ削除後も、バックアップ世代には保持期限まで残る場合があります。

4. 外部サービスへのデータ送信

4.1 GitHub API

PR情報取得、レビューコメント投稿、監査Issue投稿のために利用します。

4.2 Anthropic Claude API

レビュー/監査コメント生成のために利用します。

> **データ利用に関する重要事項**
>
> - 当社のAnthropic API利用形態（商用API契約・設定）では、送信データはモデル学習に利用されません
> - 送信データは、レビュー/監査に必要な範囲に限定します
>   - **PRレビュー時:** 差分情報や高リスク箇所のコード抜粋
>   - **監査時:** 指摘内容に関連するファイルの抜粋（必要範囲）

> **⚠️運用上の注意**
>
> 送信前の自動マスキング機能は現行未実装のため、機密情報をコードに含めない運用を推奨します。

5. 主なセキュリティ対策

5.1 通信セキュリティ

- 外部API通信はHTTPS（TLS）を利用
- GitHub webhook署名（HMAC-SHA256）の検証
- Stripe webhook署名の検証

5.2 認証・認可

- GitHub Appの短期トークン（インストールトークン）を利用
- GitHub App権限は必要最小限（Contents: Read, Issues: Read/Write, Pull requests: Read/Write）
- 管理者向けエンドポイントはBearerトークンで保護

5.3 データ保護

- 監査時に取得するtarball（GitHubのソースアーカイブ）はサイズ制限とパス検証を実施
- 解析用の一時ファイル/一時ディレクトリは処理後に削除
- DB暗号化（保管時）は基盤側設定に依存し、アプリ独自の列単位暗号化は現行未実装

6. データ削除とアクセス管理

6.1 自動削除

GitHub Appのアンインストール時、インストール情報・対象リポジトリ情報は削除されます。

6.2 手動削除

監査レポート履歴は自動削除されません（運用上の保持データ）。個別の削除依頼はサポート窓口で受け付けます。

6.3 アクセス管理

本番データへの運用アクセス制御・監査ログの運用詳細は、導入時に別紙で提示可能です。

7. 準拠・保証に関する補足

- 本書は運用仕様の概要です（法的な契約文書ではありません）
- SOC 2 / ISO 27001 などの認証有無は、必要に応じて個別にお問い合わせください

8. セキュリティ問い合わせ窓口

> **お問い合わせ先**
>
> **Email:** pyscn@ludo-tech.org
>
> セキュリティに関するご質問、インシデント報告、改善提案など、お気軽にお問い合わせください。