

Vaipm セキュリティ概要

バージョン 3.0 | 施行日 2026 年 6 月 6 日 | 区分: 公開

1. 会社概要

商号	株式会社 Vaigate
設立	2026 年 5 月 29 日
所在地	千葉県流山市
サービス	Vaipm — AI 認知モニタリングサービス
セキュリティ連絡先	compliance@vaigate.com

2. アーキテクチャ概要

Vaipm は、お客様の公式サイト（HTML および PDF）の公開情報を取得し、AI プラットフォームへの質問送信・回答収集、分析・判定、レポート生成・翻訳を行うサービスです。

2.1 インフラストラクチャ

コンポーネント	概要
データ保管	AWS ap-northeast-1（東京）。保存時暗号化（クラウド事業者の暗号化機能）
ポータル	Vercel + Next.js。転送時暗号化（TLS 1.2+）
認証	Clerk（メール/パスワード）
決済	Stripe。カード番号は当社に保存されない
ローカル推論	一部の分析処理は当社管理環境内で実行。外部送信なし
外部 AI API	OpenAI、Google Gemini、Anthropic Claude、Perplexity Sonar

3. セキュリティ管理策

当社は、事業規模、処理する個人データの性質およびリスクに応じて、以下の技術的・組織的安全管理措置を実施し、または段階的に整備しています。

3.1 暗号化

保存時: クラウド事業者の暗号化機能による暗号化

転送時: 主要な外部通信および本番公開エンドポイントに TLS 1.2 以上を適用

3.2 アクセス制御

ロールベースアクセス制御（RBAC）。顧客データは組織 ID で論理分離。

管理アカウントには MFA（多要素認証）を適用。

3.3 ログ・監視

API および管理操作のログを収集。必要に応じて確認・アラート設定を実施。ログの保持期間はログ種別およびサービス設定に従います。

3.4 脆弱性管理

依存パッケージの定期的な更新。セキュリティパッチの適時適用。

3.5 インシデント対応

文書化されたインシデント対応計画（IRP）を整備。Customer Personal Data に影響を与える確認済みのセキュリティインシデント、または通知が必要と合理的に判断される重大な疑いを認識した場合、不当な遅延なく、可能な限り 72 時間以内にお客様へ通知。詳細は DPA および IRP に定めます。

4. 外部 AI API のセキュリティ

当社は、送信データが基盤モデルの学習に使用されない条件で提供される商用 AI API の利用を前提としています。各プロバイダーの保持・ログ・学習利用は各社 API 条件に従います。

プロンプトの構造化、入力検証、出力検証により、プロンプトインジェクション等のリスク低減に取り組んでいます。

顧客データは組織 ID・Track ID で論理分離し、顧客間のデータ混在・漏えいリスクを低減しています。

5. データ保持および削除

お客様のデータは、サービス提供に必要な期間保持します。契約終了後、アクティブ本番環境上の対象データを 30 日以内に削除またはアクセス不能化します。詳細は DPA に定めます。

6. コンプライアンス

法令・基準	対応状況
APPI	プライバシーポリシー公開済み。DPA 提供可能
GDPR	DPA・SCC 提供可能。管理策整備中
SOC 2	SOC 2 基準を参考に管理策を整備中。第三者監査の実施は事業規模・顧客要請・運用成熟度に応じて検討

7. サブプロセッサー

当社が利用するサブプロセッサーの一覧は Subprocessor List で提供します。

8. お問い合わせ

セキュリティに関するお問い合わせ: compliance@vaigate.com

Web: <https://vaipm.ai>

© 2026 株式会社Vaigate