SpeechSlide AI

セキュリティ
ホワイトペーパー
要約版v1.0

2025年10月30日版

株式会社 ARNE Technologies

1. 目的と概要

SpeechSlide AI は、プレゼン資料（PDF／PPT 等）からスピーカーノートを生成し、TTS 音声とスライドを合成してプレゼン動画（MP4）を作成できるクラウドサービスです。
当社は「最小権限」「ゼロトラスト」「セキュア・デフォルト」を原則に、暗号化・認証・監査・監視を多層で組み合わせてお客さまのデータを保護します。お客さまのコンテンツは**モデル学習に利用しません。**

2. 取り扱うデータと基本方針

対象データは、アップロード資料、抽出テキスト、生成ノート、生成音声、生成動画、ならびに動作に必要な最小限のメタデータです。
個人情報は、氏名、メールアドレス、アカウント識別子、利用状況に関する最小限の情報に限ります。課金のセンシティブ情報（カード番号等）はサードパーティの決済事業者が保持し、当社はトークン等のみを扱います。

基本方針

- 収集と保管の範囲を、利用目的に必要な最小限に抑えます。
- アクセスは役割に基づく最小権限で付与します。
- 保存中のデータは暗号化し、通信は TLS で保護します。
- ログには本文データを含めない設計を採用します（必要な場合でも最小化します）。

3. セキュリティ設計の要点

多層防御

- **境界防御**：WAF による攻撃遮断、DDoS 緩和、ボット対策、レート制限を実施します。
- **認証・認可**：ID プロバイダ連携（メール／外部 IdP）に対応し、API はトークンで保護します。ワークスペースやプロジェクトの所有権に基づいてアクセスを制御します。
- **データ保護**：コンテンツは非公開ストレージに保管し、配布時は有効期限つきの署名付き URL などで制御します。鍵はクラウド KMS で管理します。
- **監視とアラート**：アプリケーションやインフラの異常を常時監視し、しきい値に基づいて通知します。
- **ゼロデータ保持（ZDR）**：処理中間データの非永続化、第三者 AI への学習不使用経路、ログの最小化などを組み合わせた ZDR 運用を提供します。

4. データの保持・削除・所在地

保持

- 成果物（生成ノート／音声／動画）は、お客さまの管理下で保持されます。
- 監査や操作のログは、セキュリティ運用のため短期間のみ保持します（本文データは含みません）。

削除

- お客さまが「プロジェクト削除」を行うと、関連するスライド・音声・動画・メタデータを本番環境から直ちに削除します。
- バックアップは所定期間内（上限 30 日を目安）に完全消去します（法令上の保存義務を除きます）。

所在地

- 原則としてクラウドの日本（東京）リージョンを利用します。越境が必要な場合は、標準契約条項（SCC）等の適切な保護措置を適用します。

5. 外部事業者の利用（サブプロセッサ）

機能提供のため、信頼できる事業者を厳選し、契約上のセキュリティ条項や暗号化、地域設定などの保護措置を講じます。

- **インフラ・データベース・ストレージ**（例：主要クラウド）
- **WAF／CDN／DDoS 緩和**（例：グローバル CDN 事業者）
- **認証・データベース運用**（例：マネージド認証／DB）
- **AI 生成（LLM／TTS）**（例：大手 AI 事業者／クラウド TTS）
- **決済**（例：国際的な決済事業者／PCI DSS 準拠）

具体的な事業者名、地域、データの取り扱い区分、学習不使用設定の証跡などは、ご要望に応じて NDA の範囲で提示します。

6. インシデント対応と事業継続

インシデント対応

- 重大なセキュリティ事象を検知した場合は速やかにトリアージを行い、影響のあるお客さまに状況と推奨対応をお知らせします。原因の特定後は、恒久対策と再発防止策を共有します。

事業継続（BCP）

- データは冗長化したストレージに保管し、データベースは定期的にバックアップを取得します。
- 復旧時間目標（RTO）と復旧時点目標（RPO）は、契約に応じて合意します（目安：RTO 4 時間／RPO 24 時間）。

7. コンプライアンスとガバナンス

当社は、ISO/IEC 27001 や SOC 2 の管理策と整合する運用を目指し、アクセス管理、変更管理、ログ保全、委託先管理を継続的に改善しています。現時点で第三者認証は取得していませんが、取得に向けた準備を進めています。セキュリティ質問票の回答、診断レポートの要旨、設定・運用の証跡は、NDA の範囲で提供します。

8. お客さまへのお願い（共同責任）

クラウドサービスの特性上、セキュリティは当社とお客さまの共同責任で成り立ちます。

- 組織内のアカウントや端末を適切に保護してください。
- 共有リンクの有効期限や公開範囲を社内規程に合わせて運用してください。
- 可能な場合は SSO や MFA を有効にしてください。

9. 連絡先と改訂

セキュリティやプライバシーに関するお問い合わせ、ならびに不審な挙動のご連絡は、info@speechslide.com までお寄せください。
本書は、技術や運用の改善に合わせて更新します。最新版は当社サイトでご確認ください。