

Tukusiの情報管理とセキュリティ

Tukusi AIの情報管理とセキュリティ

更新: 2026/06/18

作成: 2025/02/12

Tukusi株式会社

はじめに.....	2
本資料の目的.....	2
Tukusi AIの目的と概要.....	2
法令遵守.....	2
Tukusi AIについて.....	2
主な機能.....	2
アプリケーション.....	3
インフラストラクチャー.....	3
インフラおよびデータ保全に関する仕様.....	4
記録媒体および記録機器の管理.....	4
クラウド側の記録媒体管理(サプライチェーンと責任分界).....	4
医療機関側で管理すべき機器(推奨環境).....	5
情報の保存とバックアップ仕様.....	5
データの保存場所と領域.....	5
保存データの暗号化.....	5
バックアップの運用.....	5
情報セキュリティ対策.....	6
責任の共有.....	6
医療機関.....	6
当社.....	6
クラウドサービスプロバイダ.....	6
クラウドサービスの選定.....	6
AI倫理とデータ利用に関するポリシー.....	7
アクセス制御.....	7
アプリケーション通信のセキュリティ.....	7
組織的安全管理.....	7
事業継続計画 (BCP) とサポート.....	7
障害・災害時の対応体制.....	7
医療機関等のBCP策定支援.....	7
お問い合わせ窓口.....	8
資料.....	8

はじめに

本資料の目的

本資料は、Tukusi株式会社（以下「当社」）が提供する医療AIプラットフォーム「Tukusi AI」における情報セキュリティ対策、個人情報保護の取り組み、およびサービスレベル（SLA）に関する仕様を明示するものです。本サービスを利用される医療機関等が、厚生労働省「医療情報システムの安全管理に関するガイドライン 第6.0版」等の法令・ガイドラインに基づく管理者責任（説明責任、監督責任）を果たすための参考資料として作成しています。

Tukusi AIの目的と概要

Tukusi AIは、医療現場においてAIを最大限に活用した業務効率化を支援することを目的とした、統合的な医療情報処理プラットフォームです。医療現場のニーズに合わせて、音声認識、自然言語処理、画像認識などのAI技術を柔軟に活用できる環境を提供することで、医療従事者の負担を軽減し、より質の高い医療サービスの提供に貢献することを目指しています。

法令遵守

本サービスは、以下のガイドラインおよび法令を遵守して設計・運用されています。

- 厚生労働省：医療情報システムの安全管理に関するガイドライン 第6.0版
- 総務省・経済産業省：医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン 第2.0版
- 個人情報保護委員会：医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス

将来的にPマーク、ISMS認証の取得を目指しています。

Tukusi AIについて

主な機能

Tukusi AIの主な機能は以下の通りです。

AIによる患者記録生成

音声、書類、テキストデータから患者のサマリーを考慮した記録を自動作成します。

カスタムフォーム

自由にフォームを作成し、内外に向けて公開できます。

モバイルアプリ

スマホから録音、音声、書類をアップロードできます。

デスクトップアプリ

ファイル変化を監視し、ローカル操作やファイル取得、ブラウザ操作を自動化できます。

ワークフロー

AIによる情報処理や、外部チャットツールへの情報送信などの小さな作業を組み合わせて様々な自動化を実現できます。

データモデル

任意のデータ構造を定義・管理できます。

アプリケーション

Tukusi AIは以下の4つのアプリケーションから構成されます。

フロントエンドアプリ

ブラウザで動作するユーザーインターフェースです。ユーザーは本アプリを通じて、バックエンドアプリと通信し、記録の生成、フォームやワークフローの設定、フォームの回答などの様々な機能を利用することができます。

バックエンドアプリ

フロントエンドアプリ、モバイルアプリ、デスクトップアプリからのリクエストを処理し、データの保存、AI処理、ワークフローの実行などを行います。

モバイルアプリ

スマートフォンで動作し、音声録音、データのアップロード、ワークフローの実行などを手軽に行うことができます。

デスクトップアプリ

デスクトップで動作し、ファイルの監視、ローカル操作、ブラウザ操作などを自動化することができます。

インフラストラクチャー

本アプリのインフラストラクチャーは、以下のシステム構成図に示すとおりです。モバイルアプリ、デスクトップアプリ、フロントエンドアプリはインターネットを通じてバックエンドアプリと通信します。バックエンドアプリはGoogle CloudとMicrosoft Azureにより構成されています。

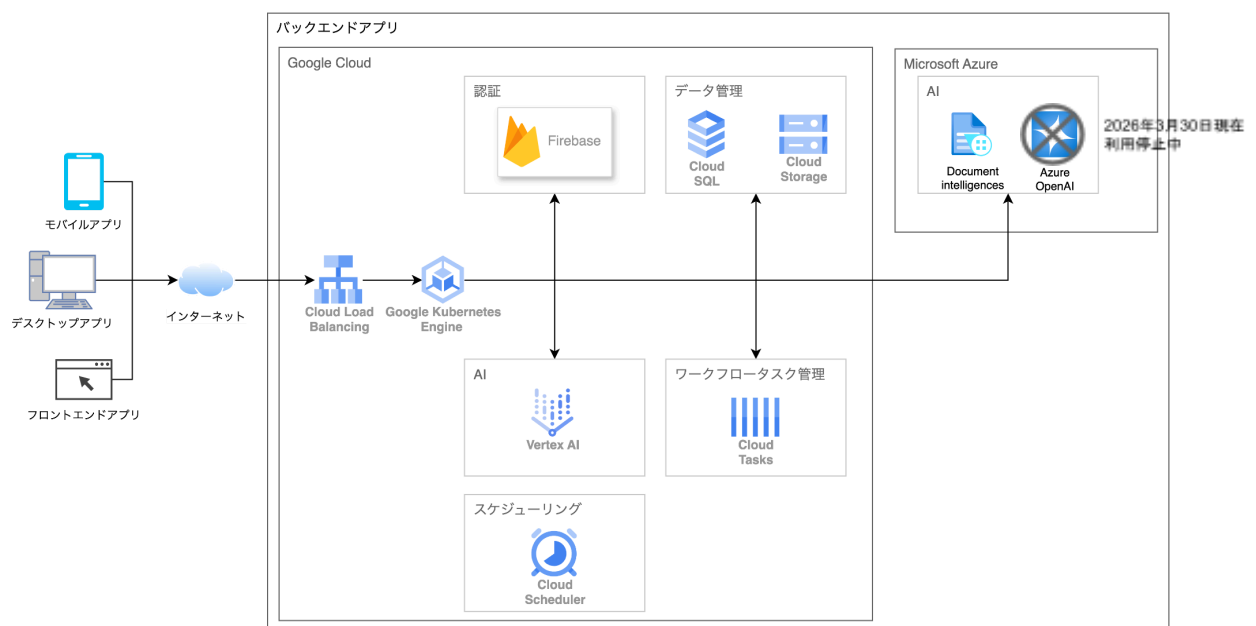
Google Cloudは、バックエンドのサーバ機能、認証機能、データ管理機能、タスク管理機能、AI機能を担っており、AI機能を除くすべてのサービスについて日本リージョンを使用しています。Vertex AIについては、生成AI利用にあたって、保持ゼロ構成を有効化しているため、入力データは推論処理のための一時メモリ利用のみで、永続ストレージへの保存・学習利用・モデル改善利用は行われません。[保持ゼロ構成の詳細](#)

AIモデルの名称の末尾に使用リージョンを明記しております。現在利用できるモデル及びリージョンは下記のとおりです。

名称	リージョン
Gemini 2.5 Flash (日本)	asia-northeast1 (日本)
Gemini 2.5 Flash 思考モード (日本)	asia-northeast1 (日本)
Gemini 3.5 Flash (日本)	asia-northeast1 (日本)
Gemini 3.5 Flash 思考モード (日本)	asia-northeast1 (日本)
Gemini 3.5 Flash (EU)	eu (EU マルチリージョン)
Gemini 3.5 Flash 思考モード (EU)	eu (EU マルチリージョン)
Gemini 3.1 Flash-Lite (EU)	eu (EU マルチリージョン)
Gemini 3.1 Flash-Lite 思考モード (EU)	eu (EU マルチリージョン)

Microsoft Azureは、AI機能の一部を担っており、使用する機能はすべて日本リージョンに設定されています。

また、フロントエンドアプリの配信にはGoogle Cloudを利用しており、当該サービスも日本リージョンに設定されています。



インフラおよびデータ保全に関する仕様

記録媒体および記録機器の管理

クラウド側の記録媒体管理(サプライチェーンと責任分界)

本サービスのサーバーおよびストレージ(記録媒体)は、以下のクラウドサービスプロバイダ(CSP)の設備を利用しています。当社は物理的な記録媒体を直接保有・管理せず、CSPが定める物理的セキュリティ管理および媒体廃棄プロセスに準拠します。

利用サービス: Google Cloud

管理責任: 物理的な記録媒体の保管、維持、廃棄はCSPの責任において実施されます。

安全性確認: ISO/IEC 27001、SOC 2 Type II 等の国際的セキュリティ基準を満たしており、物理媒体の廃棄時にはNIST SP 800-88準拠の手法等によりデータが復元不可能な状態で消去・物理破壊されます。

医療機関側で管理すべき機器(推奨環境)

本サービスはSaaS(Software as a Service)であり、医療機関側に専用サーバー等の設置は不要です。ただし、サービスにアクセスするためのクライアント端末(PC、タブレット、スマートフォン)については、医療機関側の責任において適切な管理(OSアップデート、ウイルス対策等)が必要です。

推奨ブラウザ: Google Chrome, Microsoft Edge, Safari (各最新版)

推奨OS: Windows 10/11, macOS, iOS/iPadOS, Android (各ベンダーサポート期間内のもの)

情報の保存とバックアップ仕様

データの保存場所と領域

- 保存場所(リージョン): 東京リージョン(日本国内)のデータセンターに保存されます。
- 冗長化: データは同一リージョン内の複数のゾーン(物理的に離れたデータセンター)に複製・分散保存され、単一のデータセンター障害ではデータが消失しない構成をとっています。

保存データの暗号化

データベース(Cloud SQL)およびファイルストレージ(Cloud Storage)に保存される全てのデータは、AES-256 アルゴリズムを用いて自動的に暗号化されます。暗号化鍵はクラウドベンダーの鍵管理システム(KMS)により厳格に管理されます。

バックアップの運用

データの「保存性」を確保するため、以下の仕様でバックアップを実施しています。

項目	仕様	備考
バックアップ方式	日次自動バックアップ + トランザクションログ保存	Point-in-Time Recovery (PITR) 対応
バックアップ頻度	常時(リアルタイム)および 1日1回のスナップショット	
保存期間	直近 7日間	7日以前のデータもデータベース本体には保持されます
目標復旧時点 (RPO)	障害発生の数分前	トランザクションログによる復元
目標復旧時間 (RTO)	4時間以内	重度障害時は別途通知

情報セキュリティ対策

責任の共有

Tukusi AIの利用における情報セキュリティ責任は、利用者である医療機関、当社、およびクラウドサービスプロバイダの間で以下のように分担されます。

医療機関

- アカウント管理: ユーザーIDの追加・削除、パスワードの管理、多要素認証 (MFA) の設定・利用励行。
- 端末管理: 利用するPC・タブレット・スマートフォンのOSアップデート、ウイルス対策ソフトの導入、盗難・紛失防止策。
- ネットワーク管理: 院内LANのセキュリティ確保、不正なWi-Fi利用の制限。
- 運用ルール策定: 自院におけるTukusi AIの利用規定、およびBCP(事業継続計画)の策定。

当社

- アプリケーションのセキュリティ: Tukusi AI自体の脆弱性対策、バグ修正、セキュアコーディング。
- インフラの構成管理: Google Cloud/Azure上のネットワーク設定、アクセス制御、暗号化設定。
- データ保全: バックアップの実施、障害時のシステム復旧。
- 運用管理: 当社従業員への教育、アクセス権限の最小化、内部監査の実施。

クラウドサービスプロバイダ

- 物理セキュリティ: データセンターへの入退室管理、電源・空調の冗長化、ハードウェアの廃棄処理。

- 基盤セキュリティ: ホストOS、仮想化レイヤーの脆弱性対策。

クラウドサービスの選定

本サービスのインフラストラクチャには、世界最高水準のセキュリティを有するパブリッククラウドを採用しています。

採用サービス:

- Google Cloud: アプリケーション基盤、データベース、認証
- Microsoft Azure: 一部のAI機能 (Document Intelligence等)

第三者認証: 両プロバイダともに、ISO/IEC 27001、27017、27018、SOC 2 Type II、および日本政府のセキュリティ評価制度であるISMAP (Information system Security Management and Assessment Program) の登録事業者です。これにより、物理的セキュリティ、ネットワークセキュリティ、運用プロセスにおける客観的な安全性が担保されています。

また、両プロバイダは3省2ガイドラインおよび個人情報保護法への対応状況に関する資料を公開しています。(「資料」にURLを掲載しています。)

AI倫理とデータ利用に関するポリシー

Tukusi AI内で使用するAIサービス (Google CloudのVertex AIおよびMicrosoft AzureのDocument intelligences) の全てで、データがAIの学習等、本来の業務上の目的以外に使用されることはありません。

アクセス制御

Tukusi AI内のデータへのアクセスには必ず認証を求めるようにアプリケーションを設計しています。GoogleアカウントやMicrosoftアカウントによる認証や、パスキー認証を利用することで二段階(二要素)認証の設定を行うことができます。

アプリケーション通信のセキュリティ

アプリケーションの通信にはTLS1.3のHTTPS通信を使用しており、通信内容の盗聴、改ざん、またサーバのなりすましを防ぐ認証と暗号化を行なっています。

組織的安全管理

クラウドサービスの管理画面へのアクセスは当社内の担当者だけに制限されております。また、そのアクセスには多要素認証を設定し、悪意のある第三者によるアクセスを防ぐ対策を行なっております。

事業継続計画 (BCP) とサポート

障害・災害時の対応体制

当社は、システム障害やサイバー攻撃等の非常時に備え、社内BCP(事業継続計画)およびIT-BCP(システム障害対応計画)を策定しています。

医療機関等のBCP策定支援

医療機関等が自院のBCPを策定する際の支援として、以下の資料を提供しています。

[Tukusi AI サービス利用におけるBCP手順書サンプル](#): クラウド障害時やネットワーク断絶時の代替運用(紙カルテ運用、モバイル回線利用等)を定めたテンプレートです。

お問い合わせ窓口

Tukusi AIの情報管理やセキュリティ、運用に関するお問い合わせは下記までお願いいたします。

窓口: Tukusi AI セキュリティサポートデスク

Email: support@tukusi.net

対応時間: 平日 9:00 ~ 18:00

資料

Google. “2G3M Japan - Compliance.” Google Cloud, Google,
<https://cloud.google.com/security/compliance/2g3m-japan>. Accessed 30 March 2026.

Google. “個人情報保護法(日本).” 個人情報保護法(日本), 2022,
<https://cloud.google.com/security/compliance/appi-japan>. Accessed 30 March 2026.

Microsoft. “マイクロソフトクラウドの「医療機関向けクラウドサービス対応セキュリティリファレンス(2021 年度)」公開のお知らせ.”
<https://www.microsoft.com/ja-jp/industry/blog/health/2021/07/22/security-reference-of-cloud-services-for-medical-institutions-2021/>. Accessed 12 February 2025.