PLaMo翻訳

セキュリティホワイトペーパー

Preferred Networks

PLaMo翻訳の安全性について

1. はじめに

1.1 本書の目的

本ホワイトペーパーは、株式会社Preferred Networks（以下「当社」といいます）が提供するAI翻訳サービス「PLaMo翻訳」（以下「本サービス」といいます）におけるセキュリティへの取り組みについて説明することを目的としています。

お客様が安心して本サービスをご利用いただけるよう、データの取り扱い、インフラストラクチャ、運用体制など、各領域におけるセキュリティ対策を詳述します。

1.2 サービス概要

本サービスは、当社が自社開発した大規模言語モデル「PLaMo」を活用したAI翻訳サービスです。以下の翻訳機能を提供しています。

- テキスト翻訳: Webブラウザもしくはデスクトップアプリで、テキストを入力して翻訳
- 英文添削: 入力した英文の添削と修正理由の提示
- ファイル翻訳: ドキュメントファイルをアップロードし、翻訳されたファイルをダウンロード
- ブラウザ翻訳: ブラウザ拡張機能を使用したWebページのリアルタイム翻訳
- ライブ音声翻訳: Webブラウザもしくはブラウザ拡張機能で、画面・タブの音声をリアルタイムに文字起こしして翻訳
- 会議翻訳: 翻訳ボットをZoom / Google Meet / Microsoft Teamsの会議に参加させ、会議の音声をリアルタイムに文字起こしして翻訳

2. データの取り扱い

翻訳の入出力、用語集データ、会議翻訳における会議の音声・文字起こし・翻訳結果など、翻訳処理に関連するデータ（以下「ユーザデータ」といいます）の取り扱いについて記述します。

2.1 ユーザデータの処理

本サービスでは、ユーザデータの機密性を最優先に考慮した処理を行っています。有償プランご利用時は、ユーザデータがAIモデルの学習やサービスの改善などの二次利用に使われることは一切ありません。

機能	有料プラン利用時のデータ処理方式
テキスト翻訳	翻訳結果を応答した後、ユーザデータは即時破棄されます。利用量のメトリクスだけが記録されます
英文添削	添削結果を応答した後、ユーザデータは即時破棄されます。利用量のメトリクスだけが記録されます
ブラウザ翻訳	翻訳結果を応答した後、ユーザデータは即時破棄されます。利用量のメトリクスだけが記録されます
ファイル翻訳	お客様がダウンロードできるよう一時的にサーバに保存されます
ライブ音声翻訳	音声認識はお客様のブラウザ内で行われ、音声はサーバに送信されません（クラウド音声認識を選択した場合は、ブラウザから音声認識サービスへ直接送信され、認識後に破棄されます）。文字起こし・翻訳結果はブラウザ内にのみ保持され、サーバには保存されません。利用量のメトリクスだけが記録されます
会議翻訳	会議の音声は文字起こしのためにメモリ上で処理され、いかなる保存領域にも永続化されません（映像は取得しません）。文字起こし・翻訳結果・参加者の表示名は、お客様が閲覧できるよう一時的にサーバに保存されます

なお、無料プラン利用時は、ユーザデータの収集を行っております。収集したデータは、新サービスの開発またはAIモデルの学習・改善を目的として利用する場合があります。ただし、ライブ音声翻訳および会議翻訳で取り扱うユーザデータについては、有償・無償のいず

れのプランであっても二次利用を目的とした収集・蓄積を行わず、AIモデルの学習やサービスの改善などの二次利用に使われることは一切ありません（利用規約の各特則に定めています）。

2.2 ユーザデータの保存と削除

ファイル翻訳においてサーバに一時保存されるユーザデータは、以下のいずれかの条件で完全に削除されます。

- お客様がレコードの削除操作を行った場合
- アップロードから7日間の保持期間を経過した場合

用語集は、お客様がレコードの削除操作を行ったのち、別記のバックアップ保持期間を過ぎた後に完全に削除されます。

会議翻訳においてサーバに一時保存される会議ログ（文字起こし・翻訳結果・参加者の表示名）は、以下のいずれかの条件で完全に削除されます。

- 会議の作成者が削除操作を行った場合
- 会議終了時の自動削除を設定している場合、会議が終了した時点（会議ごとに設定できるほか、チームプランではテナント内の全会議に自動削除を強制できます）
- 会議終了から7日間の保持期間を経過した場合

会議ログはバックアップの対象外であり、削除後にバックアップから復元されることはありません。

2.3 契約終了時のユーザデータの削除について

別記のバックアップ期限を過ぎた後に、完全に削除されます。

2.4 クラウドサービス事業者によるユーザデータへのアクセスについて

ファイル翻訳の一時保存データ、および用語集などを含むユーザデータはクラウドサービスのデータベースに保存されます。ただし、クラウドサービス事業者の従業員によるユーザデータへのアクセスは禁止されており、アクセスされることはありません。

2.5 外部AIサービス・外部サービスの利用

本サービスでは、翻訳データの処理の一部において、以下の外部サービスを利用しています。いずれのサービスにおいても、送信されたユーザデータは日本国内リージョンで処理され、3.2項に記載のとおり、日本国外のサーバに送信されることはありません。また、送信されたユーザデータが各事業者のAIモデルの学習に利用されることはありません。

事業者・サービス	利用する機能	送信するデータ	処理リージョン
Microsoft Azure	OCR、英文添削、会議翻訳、ライブ音声翻訳（クラウド音声認識を選択した場合）	テキストおよび音声	日本
Google Cloud（Vertex AI）	会議翻訳	音声および音声認識結果	日本
Recall.ai	会議翻訳	会議URL、翻訳ボットの設定	日本

いずれも、会議の音声・映像を保存しない設定で利用しており、映像は取得しません。

各事業者は、製品・サービスにおけるデータ保護に関して Data Processing Addendum（DPA）を公開しています。各サービスに送信されるデータは、当該 DPA の定めに従い取り扱われます。

- Microsoft Products and Services Data Protection Addendum (DPA): https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA
- Google Cloud Data Processing Addendum: https://cloud.google.com/terms/data-processing-addendum
- Recall.ai Data Processing Agreement: https://www.recall.ai/data-processing-agreement

3. データの管理とセキュリティ

3.1 日本国内リージョン

本サービスのすべての翻訳処理は、日本国内のデータセンターで実行されます。サーバインフラは日本国内リージョンに構築され、お客様の翻訳対象テキスト・音声を取り扱うすべてのコンポーネントが国内で稼働しています。2.5項に記載の外部サービスについても、ユーザデータの処理リージョンはすべて日本国内です。

3.2 データの越境移転

ユーザデータは日本国内のサーバでのみ処理・保存され、日本国外のサーバに送信されることはありません。

なお、会議翻訳においては、翻訳ボットが会議に参加する際に、録音・翻訳を行う旨の告知文と翻訳ボットを参加させた利用者のメールアドレスを会議プラットフォームのチャット欄に投稿します。この投稿は会議プラットフォーム上で行われるため、会議プラットフォームの運営事業者および会議参加者（日本国外に所在する者を含む場合があります）において取り扱われます（利用規約の会議翻訳に関する特則に定めています）。

3.3 暗号化

本サービスで管理する以下のデータは、全て保存の際に暗号化を行っています。

- ファイル翻訳の原文ファイル、翻訳ファイル、処理時の中間データ
- 会議翻訳の会議ログ（文字起こし・翻訳結果・参加者の表示名）、および会議の設定情報
- 用語集を含む全てのユーザデータ、およびそのバックアップ

4. クラウド・インフラセキュリティ対策

4.1 ICTサプライチェーン

当社は、SaaS型クラウドサービスの提供者として、クラウドサービスベンダーが提供するクラウド環境を利用して、本サービスを構築しています。そのため、このクラウドサービスの供給者関係において、当社はクラウドサービス提供者であると共に、クラウドサービス利用者でもあります。

当社は、クラウドの責任共有モデルに則り、クラウドサービス提供に際して当社が責任を持つべき構成要素について、適切なリスク管理策を実施しています。

4.2 セキュリティ監視

CNAPP（Cloud Native Application Protection Platform）を導入し、継続的なセキュリティ監視を行っています。使用している構成要素（ミドルウェア・サービスコンポーネントなど）に脆弱性が発見された場合、影響が懸念されるものについては 速やかにアップデートの対応を行っています。

その他、CNAPPを活用して以下の対策を行っています。

- クラウド環境の多層防御を考慮した脅威検知

- 不正アクセスの検知と対応
- セキュリティイベントのリアルタイム監視

4.3 最小権限の原則

社内で規定されたデータ管理ポリシーに従い、ユーザデータにアクセス可能な従業員を制限し、最小権限の原則に基づき管理しています。

4.4 可用性

本サービスを構成するクラウド上の主要なコンポーネントはすべて、クラウドサービスの機能を用いて適切に冗長化され、可用性を高めています。

5. 通信セキュリティ

5.1 TLS暗号化

お客様と本サービス間のすべての通信は、TLS（Transport Layer Security）により暗号化されています。

- すべてのAPIエンドポイントでHTTPS（TLS1.2以上）を使用しています。
- 電子政府推奨暗号リスト（ https://www.cryptrec.go.jp/list.html ）に掲載されている暗号スイートのみを許可しています。

5.2 仮想ネットワークのセキュリティ

クラウドの責任共有モデルに則り、クラウドサービス利用者としてセキュリティに責任を持つべきネットワーク領域について、セキュリティ強化と検査を行っております。

5.3 ネットワークの分離

お客様の通信は、本サービスの内部通信において同一の経路を通りますが、それぞれの通信は適切に分離されています。

5.4 外部サービスからの受信通信の認証（会議翻訳）

会議翻訳では、翻訳ボットが取得した会議の音声を Recall.ai から本サービスへ送信します。この通信は TLS で暗号化されるとともに、送信元が正規のサービスであることを検証する署名と、会議ごとに発行する受信用トークンの2段階で認証し、いずれかを満たさない接続は受け付けません。これにより、第三者による会議への音声データの注入や、音声データの漏洩を防止しています。

6. アプリケーションセキュリティ

6.1 アプリケーション脆弱性対策

使用しているソフトウェア部品（ライブラリなど）の脆弱性は、開発時のSCAスキャンによる解析・可視化、およびCNAPPを用いた本番環境監視により継続的に確認しています。ソースコードを対象としたAIベースの静的解析（SAST）も併せて実施しています。影響が懸念される脆弱性が発見された場合には、速やかにアップデートの対応を行っています。

また、第三者によるWebアプリケーション・デスクトップアプリケーションの脆弱性診断をメジャーアップデートや新機能の追加などのタイミングで不定期に実施し、安全性を確認しています。

6.2 情報セキュリティに配慮した開発方針

開発時には、自動テストや整形ツールによるプロセスに沿ったコードレビューを実施し、コードの潜在的なバグやパフォーマンスの問題、安全でないコーディングパターンの検出に努めています。また、特にお客様の情報資産を取り扱う新機能をリリースする場合には、社内のセキュリティチームによるレビューを実施しています。

7. アクセス制御

7.1 認証方式

本サービスでは、セキュリティを強化するため、パスワードを使用しない以下の認証方式のみを採用しています。これにより、パスワード漏洩のリスクを排除し、フィッシング攻撃への耐性を向上しています。

- GoogleアカウントによるOAuth 2.0
- メールアドレス所有検証を伴うメールリンクログイン
- SAML 2.0（チームプランのみ）
- OIDC（チームプランのみ）

7.2 お客様のIDプロバイダとの認証連携（チームプラン）

チームプランをご利用の場合、SAML 2.0 もしくは OIDC を用いて、お客様がご利用のIDプロバイダと認証連携してご利用いただくことが可能です。

7.3 テナントディスカバリ機能（チームプラン）

チームプランをご利用の場合、メールアドレス確認による所有証明が完了しているアカウントに限り、ご利用のテナントをログイン可能なテナントとしてテナント一覧に表示していま

す。チームプランでブラウザ拡張やデスクトップアプリをご利用頂くには、ご利用のテナントをテナント一覧に 表示させる必要があるため、事前にメールアドレス確認を実施いただく必要があります。

これは、Pre-Hijacking Attack を防止し、フィッシング攻撃への耐性を向上させることを目的としています。

8. 会議翻訳における閲覧の管理と参加者への透明性

会議翻訳は、お客様のアカウントを持たない会議参加者にも文字起こし・翻訳結果を提供する機能であるため、他の機能とは異なる閲覧管理と、会議参加者に対する透明性確保の仕組みを設けています。

8.1 会議ログの閲覧範囲

会議ログ（文字起こし・翻訳結果）は、会議ごとに発行する推測不可能な閲覧用リンク（256ビットの乱数トークンを含む）を通じて閲覧します。 会議参加者が本サービスのアカウントを持たない場合にも閲覧できるようにするための設計であり、閲覧範囲は以下のとおり制御されます。

- 会議中: 閲覧用リンクを受け取った人が閲覧できます。チームプランをご利用の場合、閲覧範囲を「同一テナントのログイン利用者のみ」に限定することもできます
- 会議終了後: 会議の作成者本人および作成者と同一テナントのログイン利用者のみが閲覧できます。テナント外の利用者は閲覧できません。
- 削除後: 閲覧用リンクは無効になり、会議の作成者を含む全ての利用者が閲覧できなくなります。

閲覧用リンクのトークンはサーバのアクセスログに記録されない形式で受け渡しされます。また、会議ログのエクスポート・印刷は、会議の作成者本人および作成者と同一テナントの利用者に限定されます。

8.2 会議ログの閲覧記録

会議ログへのアクセスは、成功・拒否を問わず、アクセス日時、IPアドレス、User-Agent、ログイン利用者の場合はその識別子とともに記録されます。この記録は不正アクセスの調査のために保持するもので、保持期間は3年間です。会議ログを削除しても閲覧記録は削除されません。

8.3 会議参加者への告知

会議の音声を取得して処理するにあたり、会議参加者が録音・翻訳の存在を認識できるよう、以下の告知を行います。

- 翻訳ボットの表示: 翻訳ボットは会議の参加者一覧に表示され、翻訳ボットが会議に参加していることが全参加者に見えます
- 会議チャットへの告知: 翻訳ボットの参加時に、会議の音声がリアルタイム翻訳のために処理される旨を日本語・英語で会議チャットに投稿します。同じ投稿に、翻訳ボットの管理者として翻訳ボットを参加させた利用者のメールアドレスを表示し、会議参加者が問い合わせ先を確認できるようにしています

会議参加者への利用目的の通知や同意の取得は、会議翻訳を利用するお客様の責任において行っていただきます。当社は、会議の音声・文字起こし・翻訳結果に含まれる個人情報について、お客様の委託を受けた処理者として、会議翻訳機能の提供に必要な範囲でのみ取り扱います（利用規約の会議翻訳に関する特則に定めています）。

8.4 会議翻訳の操作の監査ログ（チームプラン）

翻訳ボットの参加、会議ログの閲覧範囲の変更、会議ログの削除などの操作は、9.4項の監査ログ機能に記録されます。監査ログには会議の内容（会議のタイトル・会議URL・参加者・文字起こし）は含まれません。

9. 運用

9.1 変更管理

お客様に何らかの影響が発生する可能性がある変更については、当社所定の方法にて事前に通知します。

9.2 ユーザ影響を及ぼす作業の事前通知

サービス停止など、お客様のサービスのご利用に影響を及ぼすメンテナンスを予定している場合、当社所定の方法にて、作業実施日時の2週間より前に事前通知します。

9.3 バックアップ

データベースに保存されるユーザデータ（用語集など）は、1日1回バックアップを取得し、30世代分を保持しています。会議翻訳の会議ログは、2.2項に記載のとおりバックアップの対象外です。

9.4 監査ログのご提供（チームプラン）

チームプランをご利用の場合、利用者のログイン・ログアウト日時、設定変更、会議翻訳の操作などの各種ログを取得できる監査ログ機能をご利用いただけます。

9.5 ログの保存期間

監査ログの保存期間は3年間です。

また、サービスのログ（アクセスログ、操作ログ、各種アプリケーションログなど）の保存期間についても、同様に3年間です。

9.6 ログの廃棄ポリシー

保存期間を経過したログは、自動的に完全削除されます。削除されたログは復元できません。

9.7 情報セキュリティの意識向上、教育及び訓練

当社の従業員が、お客様の情報資産を適切に取り扱い、情報セキュリティに関するルールや手順、適用法令及び規制上の考慮事項を順守するために、定期的もしくは必要に応じて随時、情報セキュリティ教育を実施しています。

10. ISOに準拠した厳格なセキュリティ基準と情報管理体制

当社は、お客様に安心してサービスをご利用いただけるよう、情報セキュリティの確保と向上に努めています。国際的に認められているISOの厳格な基準に準拠した情報セキュリティマネジメントシステム（ISMS）を構築・運用し、お客様の大切な情報資産を脅威から保護しています。

当社は、情報セキュリティマネジメントシステム（ISMS）に関する国際規格である ISO/IEC 27001 の認証を取得しています。本サービスの開発・運用を担う「AIプロダクツ&ソリューションズ事業本部」の業務を認証範囲としています。

本規格に基づき、情報資産の機密性・完全性・可用性を維持・改善するための管理策を継続的に運用しています。

11. 情報セキュリティインシデント管理

11.1 セキュリティインシデント対応

当社の責任範囲において重大な情報セキュリティ事象（お客様情報の漏えい等）を検知した場合には、当社が定める「緊急対応手順」に基づき、速やか、かつ適切に対応いたします。

11.2 情報セキュリティ事象の報告

当社の責任範囲において情報セキュリティ事象が発生した場合には、当社指定の方法により、お客様に報告いたします。

また、お客様が本サービスに関する情報セキュリティ事象を発見された場合には、ヘルプセンターからご連絡いただけます。

ヘルプセンターお問い合わせ窓口:
https://support.translate.preferredai.jp/hc/ja/requests/new

---

12. お問い合わせ

セキュリティに関するご質問、セキュリティチェックシートへの記入依頼などは、法人向けお問い合わせ窓口までご連絡ください。

法人向けお問い合わせ窓口: https://translate.preferredai.jp/contact/

更新履歴

日付	内容
2026年9月28日	会議翻訳・ライブ音声翻訳・英文添削に関する記載を追加。会議翻訳における閲覧の管理と参加者への透明性（8章）を新設
2026年6月3日	情報セキュリティマネジメントシステム（ISMS）認証取得に関する記載を追加
2026年4月6日	外部AIサービスの利用に関する記載を追加
2026年3月17日	初版作成