福山市AI音声認識を活用した電話対応事業業務委託仕様書

1　業務名

福山市AI音声認識を活用した電話対応事業

2　目的

福山市（以下、「本市」という。）において、児童虐待・通報等の電話対応業務に従事する職員は、相談者に対し専門的知見に基づき相談に応じるとともに、一連の経過を時系列に記録している。迅速かつ適切な業務実施や職員の時間外勤務の削減を図るため、AI音声認識を活用したシステムを導入するものである。

3　事業内容

本事業は、児童虐待・通報に係る相談業務を適切かつ効率的に実施するためのシステムを導入し、相談業務にかかる基盤を構築する事業である。

4　委託期間

契約締結の日から2027年(令和9年)3月31日まで

5　基本事項

(1) 導入場所・ライセンス数等

ア　導入場所

福山市ネウボラセンター及び福山市が指定する場所

イ　ライセンス数

19台

ウ　PC要件等

OS：Windows 11 Pro　24H2、ブラウザ：Microsoft Edge

CPU：Intel Core i5 第14世代、RAM：16GB、SSD：256GB相当

エ　電話環境等

デジタル回線となっており、デジタル多機能電話（AQUOS wish5 SH-52F）を利用して受電している。

(2) 動作環境等

ア　システムはオンプレ環境で動作するものとする。サーバはラックマウント型とし、市が指定する場所のサーバラックに設置し、6U程度（コンソール含む)、電源100V 15A以内に収まるようにすること。UPSは不要とするが、電源タップ、コンソール等必要な機器は本提案に含めること。

イ　システム導入に当たっては、本市の業務用PC（富士通ESPRIMO G6014/R）との連

携等について動作確認された製品を使用すること。

ウ　デジタル多機能電話（AQUOS wish5 SH-52F）を利用する電話環境を想定したシステム構成とすること。

エ　テキスト、音声データともに、サーバ上に一定期間保存可能な構成とすること。

オ　システムが安定稼働するために必要なディスクの冗長化、データの暗号化等のセキュリティ対策を行うこと。

カ　既存ネットワーク機器の設計・設定、電源工事等の作業は本市が指定する事業者が行うため、必要な情報を提供すること。

6　システム機能要件

(1) 音声リアルタイムテキスト化機能

ア　音声認識技術を用いて、電話の通話内容を話者分離し、リアルタイムでのテキスト化が可能なこと。

イ　システムに表示された音声認識結果から、必要な内容のみコピーできること。

ウ　既存システムの画面を従来どおり利用できるよう、音声認識の結果を表示する画面を最小化できること。

エ　通話中もしくは電話終了後速やかに、発話時刻を含む音声認識結果が汎用的な形式で容易に出力が可能なこと（csv、pdf、docx 等）。

オ　通話時間に限らずテキスト化できること。

カ　電話を同時に使用するときでも、可能な限り動作に遅延や中断が生じず性能発揮できること。

(2) 通話履歴再生機能

ア　システム上で音声認識結果を見ながら、聞き直したい発話を選択し、該当部分だけ再生できること。

イ　収録した通話に無音箇所がある場合、無音箇所をスキップできること。

ウ　再生速度が変更可能なこと。

エ　音声が明瞭に録音・再生できること。

(3) 単語登録機能

単語登録を利用者側で実施できること。また、単語登録機能として、専門用語の表記と発音を利用者側にて画面上で容易に登録・削除でき数分以内に反映されること。

(4) キーワード機能

事前に登録したキーワードが発話された場合、通話内容のテキストにハイライト表示やリスト表示により明示できること。

(5) 要約機能

ア　生成 AI を活用し、会話内容の重要文を抽出して要約化ができること。

イ　要約化された結果をシステムに保存すること。また、画面上で要約結果を簡易に

編集できること。

ウ　システム利用者が生成 AI に関する専門的知識を必要とせず実行できること。

エ　要約する文字数について、利用者側で任意に設定できること。

オ　要約する形式は、利用者側で任意に設定できること。

(6) その他

ア　アップロードした音声データ及び変換後のテキストデータを、一定時間経過後に自動消去する機能を有すること。

イ　テキスト、音声データともに、サーバ上に一定期間保存可能な構成とし、本市の業務用 PC 内に保存されないこと。

ウ　デジタル多機能電話から業務用 PC へ送信されるデータは、音声データのみに限定すること。

7　情報セキュリティ要件

受託者は、導入する情報システムの情報セキュリティ要件として、以下の項目を遵守すること。 また、本市におけるセキュリティ対策基準等を遵守すること。

(1) セキュリティ対策

情報セキュリティマネジメントにかかる国際規格の認証（ISO／IEC27001 など）又はこれと同等の認証を取得しているなど、情報セキュリティ対策が確保されていること。

(2) 通信回線対策

本システム接続にあたり、既存の福山市公共ネットワーク側の設定変更や調整が必要な場合は、本市指定の事業者と協議の上、必要な情報提供を行うものとする。

(3) 不正プログラム対策

不正プログラム（ウイルス、ワーム、ボット等）による脅威に備えるため、想定される不正プログラムの感染経路において感染を防止する機能を備えること。

(4) 脆弱性対策

ア　本システムを構成するソフトウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。

イ　運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、本システムを構成するソフトウェアの更新を効率的に実施する機能を備えるとともに、本システム全体の更新漏れを防止する機能を備えること。

(5) ログ管理

本システムに対する不正行為の検知、発生原因の特定に用いるために、ログの記録・保存機能を有すること。

(6) 不正監視

ア　不正行為に迅速に対処するため、情報システムで送受信される通信内容の監視及びサーバ装置のセキュリティ状態の監視等によって、不正アクセスや不正侵入を検知及び通知する機能を備えること。

イ　サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバ装置、通信回線装置又は通信回線の過負荷状態を検知する機能を備えること。

(7) 情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする利用者の認証を行う機能として、ＩＤ／パスワードの方式を採用し、認証情報の推測や盗難等のリスクの軽減を行う機能として、パスワードの複雑性及び指定回数以上の認証失敗時のアクセス拒否などの条件を満たすこと。

(8) アカウント管理

ア　利用者のアクセス権を適切に管理するため、利用者が用いるアカウント（識別コード、認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること。

イ　本システムの利用範囲を利用者の職務に応じて制限するため、本システムのアクセス権を職務に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。

ウ　管理者権限の保護特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。

(9) 通信経路上の盗聴防止

通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信内容を暗号化する機能を備えること。暗号化は適切なアルゴリズムを用いた処理を行うこと。

(10) 保存情報の機密性確保

本システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。また、保護すべき情報を利用者が直接アクセス可能な機器に保存できないようにすることに加えて、保存された情報を暗号化する機能を備えること。

(11) 保存情報の完全性確保

情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。

(12) 情報の物理的保護

情報の漏えいを防止するため、記憶装置のパスワードロック、暗号化等によって、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。

(13) 侵入の物理的対策

物理的な手段によるセキュリティ侵害に対抗するため、情報システムの構成装置（重要情報を扱う装置）については、外部からの侵入対策が講じられた場所に設置する

こと。

(14) ウイルス対策

使用するサーバにはアンチウイルスソフトを導入し、ウイルスチェックを実施すること。

(15) システム利用終了後のデータ削除

本システム利用終了時には相談記録やガイダンスデータ、アカウント情報等をはじめとした本契約に関わる全ての情報を復元不可能な状態に削除し、データ削除報告書を提出すること。

(16) 構成装置の処分

本委託業務で使用した情報システムの構成装置が処分される際に、セキュリティを保った対応が行われること。

8　障害対策（事業継続対応）

(1) システムの構成管理

情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに文書どおりの構成とし、加えて情報システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。

(2) システムの可用性確保

サービスの継続性を確保するため、情報システムの各業務の異常停止時間が復旧目標時間として１日を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。また、システム稼働時間に対する稼働率の目標を９９％以上とすること。

9　サプライチェーン・リスク対策

(1) 受託者（再委託先含む）において不正プログラム等が組み込まれることへの対策

情報システムの構築において、発注者が意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。当該品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。

(2) 機器等に不正プログラム等が組み込まれることへの対策

機器等の製造工程において、発注者が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。

１０　利用者保護

(1) 情報セキュリティ水準低下の防止

システム利用者の情報セキュリティ水準を低下させないように配慮した上でアプリケーションプログラムやウェブコンテンツ等を提供すること。

(2) プライバシー保護

本システムにアクセスする利用者のアクセス履歴、入力情報等を当該利用者が意図しない形で第三者に送信されないようにすること。

１１　業務の適正な実施における留意事項

(1) 受託者は、本業務の遂行に当たり、関連法令及び本仕様書を遵守するとともに、業務の目的を十分に理解したうえで、必要な人員の配置や環境の整備等を行い、適切に実施すること。

(2) 受託者が本業務を遂行するに当たり必要となる経費は委託契約金額に含まれるものとし、市は契約金額以外の費用を負担しない。

(3) 本仕様の一部又は全部に変更等があった場合には、仕様変更部分や影響範囲について市と受託者間で協議し、必要に応じて再度の見積もりを行うこととする。

(4) その他本仕様書に定めのない事項や、その他調整を要する事項については、受託者と市が協議のうえ、決定することとする。