【別紙 1-1】

「生成 AI を活用した
電話応答サービス導入・運用保守業務委託」
提案仕様書

令和８年４月

福岡市総務企画局 DX 戦略部 DX 戦略課

目次

1. 本業務の背景

生成AIを活用した電話応答サービスの導入により、福岡市保健所の代表電話に寄せられる問合せに対し、問合せ内容に応じた担当窓口への取次ぎ対応を自動化し、市民サービスの向上及び職員の業務効率化を図るもの。

2. 本業務の内容

2.1. 調達範囲

本件における調達範囲は、以下のとおり。

・本市が要求する機能を満たすクラウド型サービスの調達、運用・保守及びサポート。

・本システム利用に当たって必要となるシステム資産や役務を含める。

2.2. 履行期間

履行期間は契約締結日から令和９年３月 31 日までとする。

利用開始までの現時点の想定スケジュールについては以下の通りだが、契約後、本市と協議の上決定するものとする。

図表－01　　利用開始までのスケジュール

年	令和８年	
月	６月	７月
作業内容	調達、初期設定、テスト等 ◀―――	●――― ７月利用開始　運用保守 ―――▶

3. 機能要件

本システムが備えるべき機能の要件は、別紙 1-2「機能要件一覧」にて提示する。

4. 非機能要件

4.1. 前提条件

・本業務において調達するシステムは、事業者が調達するクラウド環境（パブリッククラウド）上に構築されていることを前提とする。

・福岡市保健所における固定電話への架電に対し、本システムが稼働することを前提とする。

・動作設定やその他運用に関して、適宜、助言を行うこと。

4.2. 利用環境

4.2.1.　システム利用時間

システム利用時間は以下の通りである。

ただし、システムメンテナンス等の計画停止はこの限りではない。

図表－02 システム利用時間

	分類	通常時利用時間帯
オンライン	平日	0:00 ～ 24:00
	土日祝日	0:00 ～ 24:00

4.2.2.　システム利用者

システム利用者は、以下の通り。

・本市職員（管理画面へのログイン）

・福岡市保健所の代表電話への問合せ者

4.2.3.　システム利用規模

・福岡市保健所代表電話への問合せ件数は以下のとおり。

営業時間（平日 8:45～18:00）：300 件程度/月

営業時間外（平日 18:00～翌 8:45）及び土日祝日：150 件程度/月

合計： 450 件程度/月

4.3. クラウド要件

本システムを導入するにあたっては、以下のクラウド要件を遵守すること。

・情報資産を管理するデータセンターの物理的所在地が日本国内であること。
・本市の指示によらない限り、一切の情報資産について日本国外でのデータ保存を行わないこと。
・障害発生時に縮退運転を行う際も、情報資産が日本国外のデータセンターに移管されないこと。
・クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方裁判所を専属的合意管轄裁判所とするものであること。
・契約の解釈が日本法に基づくものであること。
・情報資産の所有権が事業者に移管されるものではないこと。
・法令や規制に従って、クラウドサービス上の記録を保護すること。
・情報資産が残留して漏えいすることがないよう、必要な措置を講じること。
・事業者が保持する自らの知的財産権について、発注者に利用を許諾する範囲及び制約を通知すること。

4.4. 可用性要件

4.4.1.　継続性

システム構成の冗長化により、特定箇所に故障が発生した場合に業務への影響を局所化することとし、年間のシステム稼働率は、99%を目標とすること。

4.4.2.　耐障害性

同一構成の仮想環境を複数用意し、アプリケーションレベルの冗長化を図ること。なお、本システムで冗長化構成を実現するに当たり負荷分散装置等が必要な場合においては、仮想アプライアンス等のソフトウェア製品で負荷分散環境を実現すること（当該ソフトウェアは本利用契約範囲に含む）。

4.4.3.　災害対策

地震、水害、テロ、火災などの大規模災害時や、ハードウェアの大規模障害の対策として、遠隔保管を実施すること。

4.5 性能・拡張性要件

性能・拡張性については、多数の利用者が同時アクセスした場合でも、動作が極端に遅くなる等のトラブルなく、利用者が快適に利用できる容量と性能を確保すること。

4.6.セキュリティ要件

以下に示す要件に留意し、セキュリティを担保すること。

図表－03　　セキュリティ要件

要件	内容	
アクセス・利用制限	本システムは、利用者ごとのアクセス管理が行われ、割り当てられた権限の範囲で操作可能な仕組みであること。 接続可能な IP アドレスを予め設定し、市のネットワーク以外から第三者がアクセスできないよう制限を行えること。	
データの秘匿	伝送データの暗号化の有無	伝送データについては、SSL／TSL 等の暗号化通信により第三者からの盗聴や改ざん等をされること無く安全に通信できること。
	蓄積データの暗号化の有無	蓄積データについては、認証情報を暗号化し管理すること。
ウイルス対策	本システムは、ウイルスやマルウェア等を検知/防御するための WAF や IPS 等のセキュリティ対策を実施していること。 （未知のマルウェアへの対策や振る舞い検知を含む。）	
ログ対応	サーバログの取得	取得したログについて、漏洩、改ざん、消去等を防止できる機能を設けること。また、取得したログについて、可能な限り容易に確認ができること。
	取得対象ログ	システムログ： サーバ単位で発生した事象（起動/終了、ハードウェア故障等の障害、プログラム等の動作状況）の記録。
		アプリケーションログ： サーバ上のアプリケーションやソフトウェアで発生した事象の記録。
		セキュリティログ： アプリケーションログのうち、情報セキュリティに関連するログを想定している。システムへのログイン履歴及び成否等を記録した監査ログを含む記録。
バックアップ・リストア	外部データの利用可否	障害時等に新システム内部のデータのみでシステムを復旧できるようなバックアップ・リストア方式とすること。
	データ復旧の対応範囲	障害発生時のデータ損失防止策を講じること。 ※障害によりデータの損失が生じた場合、「RPO（目標復旧地点）」で定めた時点までデータを復旧すること。
	バックアップ自動化の範囲	フルバックアップ、差分バックアップを組み合わせたバックアップのスケジューリングができること。またこのスケジュールに従い自動でバックアップ処理を実行できること。
		バックアップの実施状況をシステム管理者が確認できること。 バックアップが正常に終了しなかった場合、対応方針について本市と協議すること。
	バックアップ取得間隔	システム全体（OS、ミドルウェア、業務アプリケーション等）： 初期設定時、及びシステム更新時（改修、設定変更等実施時）に取得。
		データベース：1 日 1 回程度
		ログ：1 日 1 回
データ消去	サービス期間終了後にデータの消去完了をメール等にて通知すること。 データ消去及び証明書の具体的手段については、ISMAP 管理基準マニュアル」で示されている「論理的消去」（データを暗号化した後、暗号鍵を消去し、元のデータの復号を不可能とする方法）も含め、本市と協議の上決定する。	
ウェブアプリケーションのセキュリティ実装	SQL インジェクション 、OS コマンド・インジェクション やクロスサイト・スクリプティング等の脆弱性で発生しうる脅威や特に注意が必要なウェブサイトの特徴等に対し、脆弱性の原因そのものをなくす根本的な解決策、攻撃による影響の低減を図られていること。	
サプライチェーン・リスクへの対応	システムの構成に他の事業者のクラウドサービスを含む場合は、サプライチェーン・リスクを低減する対策が行なわれていること。	

また、上記のほか、「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）」、独立行政法人情報処理推進機構「安全なウェブサイトの作り方（第７版）」等の公的ガイドラインを参考に、適切なセキュリティ対策を講じるものとする。

5. サポート要件

5.1. 導入サポート

5.1.1. ヒアリング

受託者は、導入に向けて必要な事項をヒアリングすること。ヒアリングに当たっては、「1. 本業務の背景」を踏まえて、本システムの導入効果を最大限発揮できるよう支援すること。

5.1.2. 初期設定

受託者は、ヒアリングした事項をもとに、本市が円滑に利用開始できるよう、初期設定を行うこと。

5.2. 導入後の活用支援

5.2.1. 問合せ対応

受注者は、本システムに関し、発注者からの問合せを受けた場合は、真摯かつ速やかに対応を行うよう努めること。

5.2.2. 障害時対応等

その他、システム導入後に係る業務について、以下に示す。

図表－04　業務内容

業務	作業	内容
セキュリティ管理	システムの安定運用	ソフトウェア、設備・機器、セキュリティに関して定期的な保守を行うこと
	システム監視	各システム・サービスの運用継続に係る以下の監視を行うこと。監視は、２４時間３６５日対応すること。 ・死活監視、プロセス監視、性能監視 ・計画外のアプリケーション又はプロセスの停止
	ウイルス対策	ウイルス対策ソフトのパターンファイル（定義ファイル）等のソフトウェアについて、原則として最新版に更新すること。ただし、最新版に更新することにより安定稼働が保証されない場合は、この限りではない。
障害対応	システム障害の早期発見・予防に努め、ソフトウェアやコンテンツ等に関する攻撃及び脆弱性に関連する早期警戒警報、勧告及びパッチを受理した場合は、直ちにセキュリティ対策を行うこと。	
	障害対応状況は、障害収束から速やかに報告すること。また、運用上の課題がある場合は、速やかに報告すること。	
	計画的なシステム停止以外の要因によりシステムの不具合やサービス停止が発生した場合、受託者は直ちにサービスの復旧又は代替手段を用意し、サービスの安定運用に努めること。	

6. その他留意事項

・本市及び第三者機関などによる監査・検査等が実施される場合やその他本市からの求めがあった場合は、本市と協議の上、資料作成・実地調査・質疑応答など速やかに対応すること。
・本仕様書に定める事項に疑義が生じた場合、又は本仕様書に定めのない事項で協議の必要がある場合は、受託者は本市と協議を行うこと。
・実施の詳細については、本市と密に連絡を取り合い、業務を遂行すること。

以上