システム要件

1　前提

（1）自治体窓口ＤＸＳａａＳ（以下、「本システム」という。）については、「ガバメントクラウドにおける地方公共団体への窓口ＤＸＳａａＳ提供－令和７年度募集－」における条件及び条件（公募仕様書・要件定義書（必須要件））を満たしていることが前提となるが、特に下記の機能要件及び性能要件を満たすシステムとすること。

（2）本委託で構築するサーバ及び通信経路は、マイナンバー利用事務系及びガバメントクラウド以外のネットワークと接続しないこと。

（3）受託者は、安全かつ最適な構築スケジュールを計画・立案し、データ等のセットアップ、本市の業務システムとの連携等について、できる限り、本市が行う作業負担の軽減が図れる方法により実現すること。

（4）受託者は、データ量及び利用者の増加に対して、システムのパフォーマンスが低下しないよう十分なキャパシティを備えるように構築すること。

（5）受託者は、本システム構築後に関連法令等の制定及び改廃が行われた場合、本システムを継続するために必要な改修経費がなるべく少なくなるよう工夫して構築すること。

2　基本事項

（1）前提としては、「１　前提」に記載のとおりだが、詳細な要件等は、契約締結後、本市と協議の上決定すること。

（2）本システムのサービスとして、業務システムから提供を受けた資格情報（機能別連携仕様等）を保持するデータベース機能を有しない場合は、本委託の範囲内でデータベース機能を構築すること。その際、オンプレミスでの構築は許容しない。

（3）システムの運用を行う曜日・時間帯は契約締結後、本市と協議し決定するが、最低限、業務委託仕様書「３　本市の状況　(2)区役所の開庁時間（窓口受付時間）　ア開庁時間」に記載している各区役所の開庁時間及び開庁時間の前後30分以上の余裕を持たせた時間帯の運用が可能であること。

（4）生成AI機能付加の可能性がある場合は、「大阪市生成AI利用ガイドライン（第2.3版）」を遵守すること。

SLA について

自然災害や電源障害等に対し、以下に示す条件および達成水準を満たし、可用性を十分に確保するための対策を講じること。なお、これらの水準は必ず満たすべき目標値として扱う。

要件	サービスレベル指標
サービス切替時間	障害対策により、業務再開までに要する時間を 24 時間未満にできること
運用時間内の稼働率	運用時間内のサービス稼働時間の割合（計画停止を除く）は 95.0%とする
RPO（目標復旧地点）	１営業日前（日次バックアップからの復旧を想定）
RTO（目標復旧時間）	１営業日以内
RLO（目標復旧レベル）	本市があらかじめ指定する特定の業務が復旧できていること

※単一障害時は業務停止を許容せず、処理を継続させられること。

※大規模障害時は可及的速やかに復旧をめざすことを前提とし、目標復旧時間は災害の規模により本市と協議を行い決定する。

3　拡張性

対象システムが本市の指定した条件下で、使用する資源の量に対比して適切な性能を提供するものであるための要件であり、以下の取組などを通じてこの要件を満たすこと。

（1） データベースの変更を伴わない軽微な機能変更等については、追加の費用なしに実現できること。
（2） 本システムを利用するクライアント端末を増やす場合には、追加のライセンス費用なしで増設できること。また、将来的に対象窓口及び対象業務を増やす場合には、できるだけ安価に拡張できるようにシステムを構築すること。
（3） 導入後も定期的にシステム機能強化を行うこと。
（4） 職員側でデータ項目の紐づけ、帳票レイアウトの設定、CSV データの出力などのカスタムができる余地があること。また、その操作についても、職員が容易に行えるようなインターフェース、画面構成、画面遷移、操作方法であること。

4　保守性

（1）本システム機能の是正、向上又は要求の変更に対する適応のしやすさに関する要件であり、次の取組などを通じてこの要件を満たすこと。
（2）本市の組織改正、制度変更、将来導入されるシステムとの連携に柔軟かつ低コストで対応できるように考慮すること。
（3）システムを構成するソフトウェア、ハードウェアにある欠陥の診断又は故障原因の追求、修正個所の識別を行いやすくするような対策を講じること。
（4）システムの修正による、予期しない影響を避けられるような対策を講じること。また、修正したシステムの妥当性確認ができるような対策を講じること。
（5）技術の進展に柔軟かつ低コストで対応できるよう、広く利用されている国際的な標準に基づく技術を採用すること。

5　セキュリティ要件

対象システムにおける性能低下、サービス停止を含む機能の停止、破壊、さらに対象システムで管理するデータの不正更新、破壊などを防ぐために、システムで具備しておくべき要件であり、次の取組などを通じてこの要件を満たすこと。

（1）情報セキュリティの重要性について強く認識し、本業務の遂行に当たっては、本市が定める情報セキュリティポリシーに準拠し、不正アクセス・コンピュータウイルス等への適切なセキュリティ対策を講じること。
（2）内外からの不正な接続及び侵入、行政情報資産の漏洩、改ざん、消去、破壊、不正利用等を防止するための対策を講じること。
（3）許可された利用者以外がシステムやデータを取り扱えないようにするなど、ユーザーによるアクセス制御などソフトウェア面でのセキュリティ対策を講じること。
（4）利用者の利用記録を取得し、本市が定める期間保存・管理できること。