別紙2「非機能要件一覧」

No.		非機能項目		内容
		大項目	小項目	
1	サービス（アプリ・管理システム）	可用性	サービス稼働提供時間	保守等の予定された停止は除き、原則、24時間、業務期間まで利用可能とすること。
2			サービス稼働率	アプリのサービス稼働率は99%以上とすること。 ただし事前計画に基づいた停止時間やサービス提供に支障をきたさなかった（一部サービス停止も含む）時間は除くものとする。
3			計画停止	定期点検等で計画的にシステムを停止する時間は月10時間以内とし、事前に本市担当者に連絡すること。
4			サービス冗長化	提供するサービスは冗長構成とすることで、障害発生時も利用継続できるよう耐障害性を確保すること。
5			大規模災害	提供するサービス環境は日本国内に設置することとし、大規模災害などの不測の事態が発生した際も事業継続できるような対策を講じること。
6		性能・拡張性	サービス性能	短期間および短時間に集中的に多数のユーザーが入力を行っても業務に支障を与えない動作の実現ができること（利用ユーザー数は、参加者目標人数を想定）
7			サービス拡張	想定している利用ユーザー数を超えた場合にも容易にサービスを拡張できること。
8			0Sバージョンアップ	最新ＯＳがリリースされ次第、本サービス評価のうえ、不具合などが発生しないように必要な措置を講じたうえで、最新のＯＳに対応すること。
9			稼働後の変更対応	システム稼働後に運用の変更が生じた場合、各機能の設定値等について、改修ではなく、システムの設定（パラメータ）変更で実現できるよう考慮しておくこと。 また、既存の法制度の改正対応は、サービスのバージョンアップ等により本サービスの提供の範囲内で実施されること。
10		サービス終了時・契約満了時等の対応	稼働後の変更対応	事業開始後に利用者が入力した情報及び市が登録した情報のうち、市の情報管理権限を有する情報については、契約終了後全て抽出し提供すること。
11				契約終了後は、保有データの提供ののち、速やかに消去すること。消去においては、復元不可能な状態にすること。 また、利用者がアカウント登録抹消の手続きを行った場合も速やかにシステムから削除すること。
12		運用・保守性	定期保守	定期的に稼働状況の確認を行い、必要に応じて障害予防措置をとること
13			サービス監視	サービス環境は、２４時間、業務期間まで稼働を監視（死活、不正侵入検知など）すること。
14				リソースや実行されているアプリケーションをリアルタイムでモニタリングし、致命的なエラーやCPU/メモリ/ディスク状況などを監視すること。 また、不具合発生時には自動検出を行い、自動でアラート通知が届く仕組みとすること。
15				ネットワークの性能監視ができること。 また、不具合発生時には自動検出を行い、自動でアラート通知が届く仕組みとすること。
16			バックアップ	サービスの各種設定情報、ユーザー情報などについては、更新・削除を含め過去35日間の保管を行うこと。 また、5分間隔で復旧ポイントを設け、障害発生（異常更新）発生直前のデータに戻すことができるようにすること。
17				デバイス内には情報は保有せず、サービス提供クラウド環境（データセンター内）でデータを保有すること。
18				ヘルスデータなどのユーザー記録データ及び活動データについては、更新・削除を含め全てのバージョンを管理し、全世代保管を行うこと。
19		セキュリティ	不正なアクセス対策	不正アクセス等が行われた場合、速やかに検知できるようシステム監視を行うこと。不正アクセス等が確認された場合には、速やかに状況を調査するとともに、必要な対策を行うこと。
20				本サービスでのインターネット通信及びプライベートネットワークでの通信の両方とも、SSL（暗号化）通信とすること。
21				本サービスで利用するサーバーには、侵入検知(IDS)、ファイル改ざん(WAF)、F/W（接続制限）などのセキュリティー対策を施し厳格に管理を行うこと。
22				監査ログ、APIなどアプリケーションによる実行ログ/アクセスログ、ＷＡＦ（Web Application Firewall）によるトラフィックログなど、目的別に必要なログを出力・管理し、5年以上保管すること。
23			アクセス制御	ユーザ単位で権限のある特定サービス、機能のみ利用できるようアクセス制御を実施すること。 また、サービス運用保守においても機密レベルに応じて必要最低限の権限（ロール）のみ付与し作業するよう制御・運用すること。
24				ユーザ単位で権限のある特定サービス、機能のみ利用できるようアクセス制御を実施すること。 また、サービス運用保守においても機密レベルに応じて必要最低限の権限（ロール）のみ付与し作業するよう制御・運用すること。
25			保管データの保護	データベースに保管するデータは、暗号化を行い、保護すること。 また、気密性の高いデータについては、アプリケーションで暗号化したうえで、データベースに保管するデータも暗号化し、二重で対策し、保管すること。
26				本サービスのデータが格納されるデータベースは、グローバル環境からアクセスできないよう制御すること。
27			マルウェア対策	本サービスに対して、ウイルス対策を行い、最新のパターンファイルを適用し、セキュリティレベルを維持すること。
28			脆弱性対策	ＯＳ、アプリケーション等のバグ・セキュリティホールなどが脆弱性が発見された場合は、必要な対策を講じること。
29			インシデント対応	重大なセキュリティホール/インシデントが発生した際、統一的な対策を検討、対応方針を明確化し、総点検すること。
30				ISMSなど事業者における認証制度・評価制度への対応
31				データセンターは Tier３4相当であり、建築基準法（昭和 25 年法律第201 号）の新耐震基準に適合していること。データセンターの物理的所在地を日本国内とし、情報資産について、合意を得ない限り日本国外への持ち出しを行わないこと。
32		著作権		著作権が発生する画像等を使用する場合、事前に権利者から承諾を得たうえ、必要な手続き及び使用料の負担等は受託者が行うこと。
33		UI/UXの改善等		アプリレビューなどの情報を基に必要に応じて利用者の操作性・利便性を高めるアップデートを実施すること。