非機能要件一覧表

No	分類	要件内容
1	セキュリティ	稼動率、目標復旧時間（RTO）、目標復旧ポイント（RPO）、バックアップの保管方法などの可用性に関する事項をサービスレベル契約（SLA）等で明確にすること。
2		外部サービス(クラウドサービス)における物理的及び環境的セキュリティ対策について、「クラウドサービスの利用に関する情報セキュリティの国際規格（JIS Q 27017：JIS Q27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）」に定められた項目相当の内容で対策が講じられていること。
3		日本の裁判管轄、法令が適用されること。
4		データの保管場所（リージョン）およびデータセンターは、日本国内であること。
5		定期的なデータバックアップを実施し、障害発生時のデータ復旧手順や連絡体制が整備されていること。
6		外部サービス（クラウドサービス）の終了又は変更時における事前の通知等を取り決めること。
7		サービス利用終了後、サーバー上のデータを確実に消去する規定があること。
8		提供されたデータを本業務以外の目的で利用しないこと（目的外利用の禁止）。
9		提供者の情報セキュリティ対策（なりすまし、改ざん防止等）や変更管理体制について、公開資料や監査報告書で確認できること。
10		セキュリティインシデント発生時の対処方法、責任分担および連絡体制について、基本契約またはSLA等で明確に定めていること
11		情報セキュリティ対策の履行が不十分な場合の対処方法について、基本契約又はサービスレベル契約(SLA)に定めること。
12		外部サービス(クラウドサービス提供者)により、利用規約、各種設定が変更される可能性があるため、変更内容の確認方法や連絡方法を基本契約又はサービスレベル契約(SLA)に定めること。
13		クラウドサービス内における時刻同期の方法について確認し、取得するログの時刻、タイムゾーンを統一（NTP等による同期）していること。
14		セキュリティを保つための開発手順やフレームワーク等の情報を活用し、セキュアな設計・実装（ネットワーク分離、アクセス制御、暗号化等の考慮を含む）が行われていること。
15		クラウドサービス上で提供されるソフトウェア等のライセンス規定が明確であり、適切に管理されていること。
16		再委託先や調達物品に関する情報セキュリティリスク（サプライチェーンリスク）について、必要な情報の収集・共有等の対策を講じていること。
17		サービス障害やセキュリティインシデントに備えた対応計画（コンティンジェンシープラン）を策定し、定期的な訓練を実施していること。
18		WAF（Webアプリケーションファイアウォール）等の導入により、SQLインジェクションやXSS等のWeb攻撃を検知・遮断する対策を講じていること。
19		管理者アカウントに対し、多要素認証、または接続元IPアドレス制限のいずれか（もしくは両方）により、不正アクセスを防止できること。また、アカウントロック機能を有すること。
20		サーバー等のシステム構成要素において、ウイルス対策ソフトの導入など適切なマルウェア対策を講じ、定義ファイルを常に最新に保つこと。
21		アプリケーションの脆弱性診断を定期的に（年1回以上）実施していること。なお、プラットフォーム（OS/MW）等の診断については、利用するクラウド基盤（IaaS/PaaS）の第三者認証（ISMAP等）をもって代えることができる。
22		利用者および管理者端末とサーバー間の通信は、TLS 1.2以上等の強固な技術を用いて全て暗号化すること。
23		監査や障害調査のため、管理者のログイン履歴および操作履歴（予約データの閲覧・出力・削除等）を記録し、一定期間保管・参照できること。なお、システム上の保管期間が短い場合は、データをダウンロードして市側で長期保管する運用が可能であることを以て要件を満たすものとする。
24		開発環境及び運用環境は、物理的または論理的にネットワーク分離されていること。

25		情報システムに対する通信（トラフィック）やアクセスを監視し、不正な通信や操作（大量データのダウンロード等）を検知・確認できる仕組み（WAF/IPSログ、操作ログの定期確認等）を有すること。
26	サポート	利用部署が直接問い合わせ可能な窓口（電話／メール）があること。
27		必要に応じて運用方法についてオンラインによる相談が可能であること
28	実績	他自治体での導入実績があること。