非機能要件一覧

別紙2

重 要 度：【○：必須】、【△：目標（値）】として扱い、長期的に測定・評価を行う項目
提案事項：○の項目については、対応方法及び考え方を提案すること

No	大分類	中分類	小分類	要件	重要度	提案事項
1	可用性	継続性	稼動率	24時間365日のサービス提供が可能で、目標稼働率は年間99.5%とする。	△	
2	可用性	継続性	RPO（目標復旧地点）	業務停止を伴う障害が発生した場合は、障害発生前日（日次バックアップからの復旧）の状態に復旧できること。また、障害発生直前（日次バックアップ＋アーカイブからの復旧）は目標とする。	△	
3	可用性	継続性	RTO（目標復旧時間）	業務停止を伴う障害が発生した場合の目標復旧時間は、６時間以内とする。	△	
4	可用性	継続性	RLO（目標復旧レベル）	業務停止を伴う障害が発生した場合の目標復旧レベルは、全システム機能の復旧とする。	△	
5	可用性	災害対策	対応方法	災害発生時には、本市と対応方法を協議の上、本市と共同でシステムを早期に復旧させること。	△	
6	可用性	災害対策	保管方法	火災や大規模災害発生を想定し、データの安全性を確保すること。その具体的な方法は提案事項とする。	○	○
7	性能・拡張性	システム稼働環境	サーバ性能	稼働後、10年間利用することを前提としたサーバ性能を具備すること。その具体的な内容は提案事項とする。	○	○
8	性能・拡張性	システム稼働環境	サーバ環境	システムが稼働するサーバは内部用環境と外部公開用環境の２種類を用意すること。	○	
9	性能・拡張性	性能目標値	オンラインレスポンスタイム（内部用環境）	通常業務時のオンラインレスポンスタイムは、３秒以内を目標とする。	△	
10	性能・拡張性	性能目標値	オンラインレスポンスタイム（外部公開用環境）	通常時閲覧のオンラインレスポンスタイムは、３秒以内を目標とする。	△	
11	運用・保守性	通常運用	バックアップ（取得対象）	復旧に必要な全て（データ及びOS、アプリケーションなど）をバックアップすること。	○	
12	運用・保守性	通常運用	バックアップ（取得頻度）	バックアップは最低限次の頻度で行うこと。 データ：日次 その他：月に１度又は設定・構成変更の都度行う。	○	
13	運用・保守性	通常運用	バックアップ（自動化）	スケジュール機能による自動バックアップを行うこと。	○	
14	運用・保守性	通常運用	基本オペレーション	システムの起動・停止、プログラム実行制御、バックアップ処理、施設設備管理を行うこと。また、セキュリティの確保に努めること。	○	
15	運用・保守性	通常運用	稼動監視対象	稼働監視対象は次のとおりとする。 ア　稼動中のソフトウェア状況 イ　稼動中のハードウェア状況 ウ　ネットワーク状況	○	
16	運用・保守性	通常運用	稼動監視（正常時）	正常に稼動していることを監視して、障害発生や処理速度の異常低下等の事態を常に把握すること。	○	
17	運用・保守性	通常運用	稼動監視（予防措置）	予防措置等を講じて、外部公開サイト閲覧や業務に支障を来すようなシステム停止等の障害発生が起きないように監視を行うこと。	○	
18	運用・保守性	通常運用	稼動監視（異常終了時）	基本オペレーションの遂行において、実行結果の異常終了や、システムの動作不良などのイレギュラーな状態に陥った場合には、システム開発元の人的・技術的支援を含めた対応を行うこと。	○	

非機能要件一覧

別紙2

重 要 度：【○：必須】、【△：目標（値）】として扱い、長期的に測定・評価を行う項目
提案事項：○の項目については、対応方法及び考え方を提案すること

No	大分類	中分類	小分類	要件	重要度	提案事項
19	運用・保守性	通常運用	稼動監視（異常検知時の対応）	監視中に異常を検知した場合は、迅速に本市の担当者及び上位責任者等に連絡を行い、適任者に引継を行うなど適切な対応を行うこと。	○	
20	運用・保守性	通常運用	データ更新（更新期間）	更新データの作成及び更新は、本市が原議を提供してからおおむね60日以内に行うこと。	○	
21	運用・保守性	通常運用	データ更新（原議データの誤りの指摘）	更新に当たり原議に表記、形式の誤り、法制執務上の誤り等がある場合は、本市に報告の上、適宜必要な修正を行うこと。	○	
22	運用・保守性	通常運用	データ更新（外部公開用）	外部公開用環境も同様に更新を行うこと。	○	
23	運用・保守性	保守運用	計画停止	データセンターの計画停止によりシステムの利用が不可能となる日は、５日以内であること（計画停止によるシステム利用不可能日、時間の長短によらず１日とカウントする）を目標とするが、その具体的な内容は提案事項とする。	△	○
24	運用・保守性	保守運用	保守（ソフトウェア）	全てのソフトウェアの窓口は事業者が行い、システム利用に支障が出ないように保守すること。	○	
25	運用・保守性	保守運用	パッチ適用	全てのソフトウェアは、事業者又はメーカーが保守対象としているバージョンを使用することとし、セキュリティに関して重大な修正を含むパッチ等は、業務への影響を抑えつつ、できるだけ速やかに適用すること。	○	
26	運用・保守性	保守運用	バージョンアップ	パッケージのレベルアップ又はバージョンアップ版がリリースされた場合は、その提供及び適用を行うこと。なお、適用に当たっては、本市に対し、必要事項（改修内容、適用スケジュール等）を主体的に説明を行うこと。	○	
27	運用・保守性	保守運用	提供形態の変更への対応	提供形態をインターネットデータセンター（IDC）を利用したクラウド方式からLGWAN-ASP方式又は庁内サーバ設置方式に変更する必要が生じた場合においても、引き続きサービス提供が可能であること。	△	
28	運用・保守性	保守運用	証明書管理	サーバとクライアント間のSSL通信に必要な証明書を管理すること。	○	
29	運用・保守性	保守運用	運用負荷削減	保守に必要な操作を極力自動化する等、保守費用を抑えること。	○	
30	運用・保守性	障害時運用	システム異常検知時の対応	障害が発生した場合は、速やかに関連情報を収集・分析し、障害の切り分けを行い、本市に報告するとともに応急処置を行うこと。	○	
31	運用・保守性	障害時運用	復旧作業	全ての障害は、迅速に復旧作業を実施すること。	△	
32	運用・保守性	障害時運用	復旧作業（バックアップからの復旧）	バックアップデータからの復旧作業は事業者が行うこと。	○	
33	運用・保守性	運用環境	マニュアル準備レベル	システム利用に必要なマニュアルを提供すること。	○	
34	運用・保守性	サポート体制	サポート要員	事業者は、運用・保守を統括する窓口責任者と業務を遂行する担当者を設けて運用・保守を円滑に進める支援体制を整えること。また、障害発生時等の連絡を円滑に行うための連絡体制（人員構成、連絡方法、緊急時連絡先、連絡ルート等）を明確にすること。	○	
35	運用・保守性	サポート体制	サポートデスク（対応時間）	本市職員からの運用・保守及びシステム利用等に関する問合せに対応すること。なお、電話による問合せへの受付は、障害時等の緊急を要するものを除き、事業者の営業時間内を基本とし、その他メール等によるものは24時間365日とすること。	○	

非機能要件一覧

別紙2

重 要 度：【○：必須】、【△：目標（値）】として扱い、長期的に測定・評価を行う項目
提案事項：○の項目については、対応方法及び考え方を提案すること

No	大分類	中分類	小分類	要件	重要度	提案事項
36	運用・保守性	サポート体制	利用者教育	システム導入時及び人事異動時等、法務担当職員を対象にした操作説明会を実施し、法制執務の要素も盛り込んだ内容であること。実施時期等については、都度、協議して決定すること。	○	
37	運用・保守性	サポート体制	サポートデスク（費用が伴う問合せ）	問合せのうち、費用が伴う又はまとまった工数がかかるものついては、対策を検討のうえ、本市と協議すること。	○	
38	運用・保守性	サポート体制	障害時サポート体制	システムへの障害対処については、組織的かつ計画的・予防的に行えるよう準備し、実施することとし、あらかじめ緊急連絡先を本市へ届け出ること。	○	
39	運用・保守性	サポート体制	保守範囲	運用・保守の対象は、本業務で事業者が提供する全てのソフトウェア、ネットワーク等とする。	○	
40	運用・保守性	サポート体制	メンテナンス作業	システムの稼働に必要なパラメータ等の各種設定値の変更や環境変化への対応を行うこと。	○	
41	運用・保守性	サポート体制	データ提供	システムが保有する情報を本市の要望により提供すること。また、これらに対するQA対応を行うこと。	○	
42	運用・保守性	その他の運用管理方針	構成管理（納品物）	操作方法等に変更があった場合は、操作マニュアル等を常に最新の状態を維持し納品すること。その際、変更履歴を記載すること。	○	
43	運用・保守性	その他の運用管理方針	障害管理	障害対応等を含む障害の記録や障害の原因等の分析した結果を管理すること。また、発生した全ての障害は、必ず一定期間内に報告を行い、本市と協議の上、再発防止策を講じること。	○	
44	セキュリティ	前提条件・制約条件	情報セキュリティに関するコンプライアンス	本業務の実施において、関係法令のほか、本市の個人情報保護条例等を遵守すること。また、個人情報の持ち出しは本市の許可を得て行うこと。	○	
45	セキュリティ	セキュリティリスク管理	アクセス制御	内部用環境はグローバルIPアドレスでアクセス制御を行うこと。	○	
46	セキュリティ	セキュリティリスク管理	脆弱性対策	サーバのOS等は、常に最新バージョンを維持しSQLインジェクション、クロスサイトスクリプティング等の脆弱性を排除すること。	○	
47	セキュリティ	セキュリティリスク管理	ウイルス対策	ウィルス対策ソフトの導入等の適切な措置を講じること。なお、クライアントは本業務対象外とする。	○	
48	セキュリティ	セキュリティリスク管理	ウイルス定義ファイル適用タイミング	ウイルス定義ファイルリリース時に随時適用し、最新の状態に保つこと。	○	
49	セキュリティ	アクセス・利用制限	利用制限	各ユーザーの役割に応じて、必要最小限の操作しかできないように配慮し、操作ミスや情報漏えい等の危険性を低減すること。	△	
50	セキュリティ	通信の秘匿	通信の暗号化	サーバとクライアント間はSSL等による暗号化通信を行うこと。	○	
51	セキュリティ	不正追跡・監視	ログの取得	本業務で利用するシステムの操作履歴等の各種ログを確実に記録すること。万一事故が発生した場合に、原因追及のための基礎情報として利用できること。	○	
52	セキュリティ	不正追跡・監視	不正監視対象	不正アクセス等の監視のため、システム全体のログを取得すること。	○	
53	セキュリティ	不正追跡・監視	ログの提供	ログデータは一定期間保存し、セキュリティインシデント等が発生した場合、当市の求めに応じてログを提供すること。	○	
54	セキュリティ	不正追跡・監視	ログへのアクセス	権限のある者のみがログ情報へアクセスできること。	○	

非機能要件一覧

別紙2

重 要 度：【○：必須】、【△：目標（値）】として扱い、長期的に測定・評価を行う項目
提案事項：○の項目については、対応方法及び考え方を提案すること

No	大分類	中分類	小分類	要件	重要度	提案事項
55	移行性	移行時期	移行スケジュール	システム移行時期については、データセットアップ、費用、職員負担等を考慮し、適切な時期を提案すること。また、業務への影響を最小限にするため、事前に十分な検証を行った上で実施すること。その具体的な内容は提案事項とする。	○	○
56	移行性	導入作業	初期セットアップ	システムの初期セットアップを行うこと。各種パラメータ等の設定値は本市と協議し決定すること。	○	
57	移行性	将来のシステム移行	データ提供	システムに登録されている全てのデータを汎用的データ形式出力し提供すること。	○	
58	移行性	将来のシステム移行	データ削除	次期システムへの移行完了後、本市より要請があった場合は、本業務に関する全ての情報資産（データベースや文書など）を削除もしくは廃棄し、それを証明する書類を本市へ提出すること。	○	
59	システム環境・エコロジー	システム稼働環境	データセンター	システムが稼働するクラウド環境は、政府情報システムのためのセキュリティ評価制度（ISMAP）又はISMSクラウドセキュリティ認証を取得していること。その具体的な内容は提案事項とする。	○	○
60	システム環境・エコロジー	ライフサイクル期間	パッケージシステム	パッケージシステムとして、委託期間内は利用可能なシステムであること。 ただし、止むを得ず別のパッケージシステムを利用しなければならないときは、本業務の範囲内で実施し、新たな費用は発生しないこと。なお、別のパッケージへの切替を行う場合は、本市に対し、必要事項（改修内容、適用スケジュール等）を主体的に提案又は説明を行い、本市の承諾を得てから実施すること。	○	
61	システム環境・エコロジー	システム特性	専用ソフトウェア	原則、一般的なPCと一般的なブラウザのみで作動し、特殊な専用ソフトウェアを必要としないこと。	○	
62	システム環境・エコロジー	システム特性	オープンシステム	稼働環境は、オープンシステム（※）を基盤に構築されていること。 ※ ここでいう「オープンシステム」とは、汎用的に利用されているWindowsやLinux等のOSで構築されているシステムのことを指す。	○	
63	システム環境・エコロジー	システム特性	メーカーサポート	使用するOS、データベース及びミドルウェアは、一般に広く普及している製品を使用し、提案時にサポートが終了している又は終了時期が近い製品は除くこと。	○	