仕様書別紙4

非機能要件一覧

大項目	中項目	項番	メトリクス（指標）	要求目標等	補足説明等
可用性	継続性	1	RPO（目標復旧地点）※（業務停止時）	平常時、業務停止を伴う障害が発生した際には、1営業日前の時点（日次バックアップからの復旧）までのデータ復旧を目標とすること。	RPO：業務停止を伴う障害が発生した際、バックアップしたデータなどから情報システムをどの時点まで復旧するかを定める目標値。
		2	RTO（目標復旧時間）※（業務停止時）	平常時、業務停止を伴う障害が発生した際には、1営業日以内でのシステム復旧を目標とすること。	RTO：業務停止を伴う障害（主にハードウェア・ソフトウェア故障）が発生した際、復旧するまでに要する目標時間。
		3	RLO（目標復旧レベル）※（業務停止時）	平常時、業務停止を伴う障害が発生した際には、一部システム機能の復旧を実施すること。	RLO：業務停止を伴う障害が発生した際、どこまで復旧するかのレベル（特定システム機能・すべてのシステム機能）の目標値。
		4	システム再開目標（大規模災害時）	大規模災害時、システムに甚大な被害が生じた場合、システムは、一週間以内に再開することを目標とすること。	―
		5	稼働率	年間のシステム稼働率は、99.5%を目標とすること。	―
	災害対策	6	復旧方針	デスクアレイなどの外部記憶装置を物理的に複数台用意するなど、冗長性が確保された同一の構成で情報システムを再構築すること。	―
		7	保管場所分散度	遠隔地へのデータ保管は、ベンダーによる提案事項とすること。	―
		8	保管方法	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、運用サイトとは別途で、媒体による保管により、データ・プログラムを保管する場所を設置すること。	―
性能・拡張性	業務処理量	9	ユーザ数	公開型GIS及び統合型GISについて、利用者数（登録アカウント数）の上限を設けないこと。	―
		10	同時アクセス数※	公開型GIS：同時アクセス数の上限を設けないこと。 統合型GIS：全職員（1,000名程度）が万遍なく利用できるよう、最適な同時アクセス数を提案すること。	同時アクセス数：ある時点でシステムにアクセスしているユーザ数のこと。パッケージソフトやミドルウェアのライセンス価格に影響することがある。
		11	データ量（項目・件数）	データ量は、ベンダーによる提案事項とすること。	利用期間中に想定される追加データの内容・種類等を勘案し、必要と想定されるデータ量を見込むこと。
		12	オンラインリクエスト件数※	オンラインリクエスト件数は、ベンダーによる提案事項とすること。	オンラインリクエスト件数：単位時間ごとの業務処理件数。性能・拡張性を決めるための前提となる項目。
		13	データ量増大率	データ量増大率は、ベンダーによる提案事項とすること。	利用期間中に想定される追加データの内容・種類等を勘案し、想定される増大率を見込むこと。
		14	オンラインリクエスト件数増大率	オンラインリクエスト件数増大率は、ベンダーによる提案事項とすること。	利用期間中に想定される申請手続の数や添付データの内容・種類等を勘案し、想定される増大率を見込むこと。
	性能目標値	15	通常時オンラインレスポンスタイム※	通常業務時のオンラインレスポンスタイムは、一操作5秒以内とすること。	オンラインレスポンスタイム：オンラインシステム利用時に要求されるレスポンス。 システム化する対象業務の特性を踏まえ、どの程度のレスポンスが必要かについて確認する。 アクセスが集中するタイミングの特性や、障害時の運用を考慮し、通常時・アクセス集中時・縮退運転時ごとにレスポンスタイムを決める。
		16	アクセス集中時のオンラインレスポンスタイム	業務繁忙等によるアクセス集中時のオンラインレスポンスタイムは、一操作10秒以内とすること。	―
運用・保守性	通常運用	17	運用時間（平日）	平日運用時間は、24時間利用を前提とすること。	―
		18	運用時間（休日等）	休日運用時間は、24時間利用を前提とすること。	―
		19	外部データの利用可否	データ復旧の際、外部データの利用は、一部のデータ復旧に利用できること。	―
		20	データ復旧の対応範囲	データ復旧の対応範囲は、障害発生時のデータ損失防止とすること。	―
		21	バックアップ取得間隔	バックアップの取得間隔は、週次で全体バックアップを取得、また日時で差分バックアップを取得すること。	―
		22	監視情報	システムの監視については、トレース情報を含むエラー監視を行うこと。	―
	保守運用	23	OS等※パッチ適用タイミング	OS等のパッチについては、緊急性の高いパッチは即時に適用し、それ以外は定期保守時に適用を行うことを目標とする。	OS等パッチ情報の展開とパッチ適用のポリシーに関する項目。OS等は、OS、ミドルウェア、その他のソフトウェアを指す。
	運用環境	24	マニュアル準備レベル	運用マニュアルについては、各製品標準のマニュアルを利用すること。	―
		25	外部システムとの接続有無	外部システムとの連携は、ベンダーによる提案事項とすること。	公開型と統合型で運用する環境が異なることに留意すること（公開型：インターネット環境、統合型：LGWAN環境）。
	サポート体制	26	保守契約（ソフトウェア）の種類	ソフトウェア保守契約種類は、問い合わせ及びアップデート対応をベンダーが実施すること。	アップデート権の範囲については、事前に協議の上決定すること。
		27	ライフサイクル※期間	ライフサイクル期間は、5年とすること。	ライフサイクル：情報システムの利用期間（次回のシステム更改までの期間）のことを示している。

大項目	中項目	項番	メトリクス（指標）	要求目標等	補足説明等
		28	定期報告会実施頻度	運用の定期報告は、月に1回程度実施すること。	－
		29	報告内容のレベル	保守の定期報告は、運用状況報告を定期で行い、障害対応発生時には障害報告を行うこと。	－
	その他の運用管理方針	30	問い合わせ対応窓口の設置有無	運用保守時の問い合わせ窓口については、ベンダーの既設コールセンターを利用すること。	－
移行性	移行時期	31	システム移行期間	既存システムから新システムへの移行期間は、ベンダーによる提案事項とすること。	他の業務との兼ね合いを考慮し、十分な仮稼働期間を設けた上でシステム本格稼働を開始できる移行期間を提案すること。
		32	システム停止可能日時	システム移行時のシステム停止可能日時は、1日（計画停止日等を利用）とすること。	－
		33	並行稼働の有無	システム移行時の並行稼働期間は、ベンダーによる提案事項とすること。	既存システムは年度中は稼働を想定している。本システムの本格稼働開始が令和9年3月であるため、並行稼働期間は最低1ヶ月確保される。
	移行対象（機器）	34	設備・機器の移行内容	現行システムで利用している設備・機器は、移行対象無しとする。	－
	移行対象（データ）	35	移行データ量	現行システムから新システムへ移行するデータ量については、ベンダーによる提案事項とすること。	移行対象のデータの内容・種類等を勘案し、必要と想定されるデータ量を見込むこと。
	移行計画	36	移行のユーザ/ベンダ作業分担	現行システムから新システムへのデータ移行作業は、ユーザとベンダーと共同で実施すること。	－
セキュリティ	前提条件・制約条件	37	遵守すべき規程、ルール、法令、ガイドライン等の有無	遵守すべき規程、ルール、法令、ガイドライン等は、仕様書に記載の通りとする。	－
	セキュリティリスク分析	38	リスク分析範囲	セキュリティリスクの分析は、重要度が高い資産を扱う範囲、あるいは、外接部分について行うこと。	－
	セキュリティ診断	39	Web診断実施の有無	システムのWeb診断は、実施すること。	－
	セキュリティリスク管理	40	ウィルス定義ファイル適用タイミング	システム脆弱性等に対応するためのウィルス定義ファイルについては、定義ファイルリリース時に実施すること。	－
	アクセス・利用制限	41	管理権限を持つ主体の認証	システムの認証方法は、1回とすること。	－
		42	システム上の対策における操作制限度	操作制限は、必要最小限のプログラムの実行、コマンド※の操作、ファイルへのアクセス※のみを許可すること。	－
	データの秘匿	43	伝送データの暗号化の有無	伝送データについては、重要情報を暗号化すること。	－
		44	蓄積データの暗号化の有無	蓄積データについては、重要情報を暗号化すること。	－
	不正追跡・監視	45	ログの取得	ログの取得については必要なログを取得すること。	取得対象のログは、不正な操作等を検出するための以下のようなものを意味している。詳細は別途協議の上決定すること。 ・ログイン/ログアウト履歴（成功/失敗） ・操作ログ 等
		46	不正監視対象（装置）	不正監視対象は、重要度が高い資産を扱う範囲、あるいは、外接部分とすること。	－
	Web対策	47	セキュアコーディング、Webサーバの設定等による対策の強化	セキュアコーディング、Webサーバの設定等は、対策の強化を行うこと。	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。Webシステムが攻撃される事例が増加しており、Webシステムを構築する際には、セキュアコーディング、Webサーバの設定等による対策の実施を検討する必要がある。
		48	WAF※の導入の有無	WAFの導入は、ベンダーによる提案事項とすること。	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。WAF※とは、Web Application Firewallのことである。
システム環境・エコロジー	システム制約/前提条件	49	構築時の制約条件	システム構築時の制約条件は、仕様書に記載の通りとすること。	－
		50	運用時の制約条件	システム運用時の制約条件は、仕様書に記載の通りとすること。	－

※本資料は、地方共同法人地方公共団体情報システム機構がホームページで公開している「非機能要求グレード活用シート（地方公共団体版）業務・情報システム分類グループ②」を用いて、必要箇所を抽出の上、一部編集して作成している。