別紙　非機能要件詳細

大項目	中項目	小項目	内容	説明
可用性	継続性	RPO（目標復旧地点）（業務停止時）	障害発生時点（日次バックアップ+アーカイブからの復旧）	データの損失は許容できないため、障害発生日前日までの復旧が原則。
		RTO（目標復旧時間）（業務停止時）	発生時点から1営業日以内	なるべく早く復旧する。故障時すみやかに利用可能な資源を用いた復旧を想定。
		RLO（目標復旧レベル）（業務停止時）	全システム機能の復旧	すべての機能が稼働していないと影響がある場合を想定。
		システム再開目標（大規模災害時）	1ヶ月以内に再開	電源及びネットワークが利用できることを前提に、遠隔地に設置された予備機とバックアップデータを利用して復旧することを想定。機能は、業務が再開できる最低限の機能に限定する。
		稼働率	99.50%	
	災害対策	復旧方針	同一の構成で情報システムを再構築	災害発生後に調達したハードウェア等を使用し、同一の構成で情報システムを再構築することを想定。
		保管場所分散度	遠隔地1ヵ所	地震、水害、テロ、火災などの大規模災害時に備え、運用サイトとは別にデータ・プログラム等を保管する場所を設置すること。
性能・拡張性	業務処理量	ユーザ数	8ユーザ	
		同時アクセス数	2ユーザ	
		データ量（項目・件数）	科目データ（約700件），債権者データ（約300件），固定資産台帳（償却中の資産の件数は、約1,000件），企業債台帳（既往債の件数は、20件）	
		オンラインリクエスト件数	年間執行データ入力件数（約15,000件（複式簿記のため執行データ1件の入力につき2件の仕訳））	
		バッチ処理件数	年間日次集計処理件数（約300件），年間月次集計処理件数（約30件），年間支払集計処理件数（約20件）	
	性能目標値	通常時オンラインレスポンスタイム	20秒以内	管理対象とする処理の中で、通常時の大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。
		アクセス集中時のオンラインレスポンスタイム	30秒以内	管理対象とする処理の中で、ピーク時の大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。
		通常時バッチレスポンス順守度合い	再実行の余裕が確保できる	管理対象とする処理の中で、通常時のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良いと想定。
		アクセス集中時のバッチレスポンス順守度合い	再実行の余裕が確保できる	管理対象とする処理の中で、ピーク時のバッチ処理を実行し、結果が不正の場合、再実行できる余裕があれば良いと想定。
運用・保守性	通常運用	運用時間	定時内での利用（1日8時間程度利用）	
		外部データの利用可否	外部データは利用できない	全データを復旧するためのバックアップ方式を検討しなければならないことを想定。
		データ復旧の対応範囲	障害発生時のデータ損失防止	障害発生時に決められた復旧時点（RPO）へデータを回復できれば良い。
		バックアップ取得間隔	日次で取得	全体バックアップは週次で取得する。しかし、RPO要件である、1日前の状態に戻すためには、毎日差分バックアップを取得しなければならないことを想定。
	保守運用	OS等パッチ適用タイミング	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。	緊急性の高いパッチを除くと、定期保守時にパッチを適用するのが一般的と想定。
	運用環境	マニュアル準備レベル	情報システムの通常運用と保守運用のマニュアルを提供する	
	サポート体制	保守契約（ソフトウェア）の種類	アップデート	ソフトウェアが法改正等によりバージョンアップした場合に、アップデートする権利を含めることを想定。
		ライフサイクル期間	5年	導入するソフトウェアのサポート期間に合わせて情報システムのライフサイクルを5年と想定。
	その他の運用管理方針	問い合わせ対応窓口の設置有無	ベンダーの既設コールセンターを利用する	サポート契約を締結するベンダーの既設コールセンターが問い合わせ対応窓口となることを想定。
移行性	移行時期	システム移行期間	半年未満	
		システム停止可能日時	利用の少ない時間帯（夜間など）	業務が比較的少ない時間帯にシステム停止が可能。
		並行稼働の有無	有り	移行のためのシステム停止期間が少ないため、移行時のリスクを考慮して並行稼働は必要。
	移行対象（機器）	設備・機器の移行内容	移行対象無し	
	移行対象（データ）	移行データ量	1TB未満	1TB（テラバイト）未満のデータを移行する必要がある。
	移行計画	移行のユーザ/ベンダ作業分担	ユーザとベンダーと共同で実施	移行結果の確認等、一部をユーザが実施する形態を想定。
セキュリティ	前提条件・制約条件	順守すべき規程、ルール、法令、ガイドライン等の有無	個人情報保護法	
		情報セキュリティ認証	提案事項とする	ISO/IEC27001等の情報セキュリティマネジメントシステム又はそれに基づく認証については提案事項とする。
	セキュリティリスク管理	ウィルス定義ファイル適用タイミング	定義ファイルリリース時に実施	ウィルス定義ファイルは、自動的に適用する。
	アクセス・利用制限	管理権限を持つ主体の認証	1回	攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。
		システム上の対策における操作制限度	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	不正なソフトウェアがインストールされる、不要なアクセス経路（ポート等）を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス方法を制限する必要がある。（操作を制限することにより利便性や、可用性に影響する可能性がある）。
	不正追跡・監視	ログの取得	必要なログを取得する	不正なアクセスが発生した際に、「いつ」「誰が」「どこから」「何を実行したか」等を確認し、その後の対策を迅速に実施するために、ログを取得する必要がある。（ログ取得の処理を実行することにより、性能に影響する可能性がある）。
		不正監視対象（装置）	重要度が高い資産を扱う範囲	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ等の範囲を定めておく必要がある。
システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	山陽小野田市病院局会計規程，山陽小野田市病院局事務決裁規程	
		運用時の制約条件	地方公営企業法，地方公営企業法施行令，地方公営企業法施行規則	
	システム特性	クライアント数	8台	