■非機能要件一覧

項番	大項目	中項目	メトリクス（指標）	要求目標等	補足説明等
A.1.3.1	可用性	継続性	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。
A.1.3.2			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。
A.1.3.3			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。
A.1.4.1			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、一ヶ月以内に再開することを目標とすること。	
A.1.5.1			稼働率	年間のシステム稼働率は、99.5%を目標とすること。	
A.3.1.1		災害対策	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。	
A.3.2.1			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。	
A.3.2.2			保管方法	大規模災害時のデータ保管方法は、ベンダーによる提案事項とすること。	
B.1.1.1	性能・拡張性	業務処理量	ユーザ数	利用者数は、不特定多数のユーザが利用できること。	
B.1.1.2			同時アクセス数	同時アクセス数は、不特定多数のアクセスとする。	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。
B.1.1.3			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申請手続の数や添付データの内容・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。
B.1.1.4			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。
B.1.1.5			バッチ処理件数	業務処理件数は、ベンダーによる提案事項とすること。	
B.1.2.1			ユーザ数増大率	バッチ処理件数は、仕様の対象としない。	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。
B.1.2.2			同時アクセス数増大率	同時アクセス数は、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。
B.1.2.3			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。
B.1.2.4			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。
B.1.2.5			バッチ処理件数増大率	バッチ処理件数増大率は、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。
B.2.1.4		性能目標値	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、規定しない。	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。
B.2.1.5			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、規定しない。	
B.2.2.1			通常時バッチレスポンス※順守度合い	通常時のバッチレスポンスタイムは、順守度合いを定めないこと。	バッチレスポンス：バッチ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（ターンアラウンドタイム）が必要かについて確認する。更に、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・ピーク時・縮退運転時ごとに順守度合いを決める。
B.2.2.2			アクセス集中時のバッチレスポンス順守度合い	業務繁忙等によるアクセス集中時のバッチレスポンスタイムは、順守度合いを定めないこと。	

C.1.1.1	運用・保守性	通常運用	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。	
C.1.1.2			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。	
C.1.2.2			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。	
C.1.2.3			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。	
C.1.2.5			バックアップ取得間隔	バックアップの取得間隔は、システム構成の変更時など、任意のタイミング とすること。	

C.1.3.1			監視情報	エラー監視を行うこと。	
C.2.3.5		保守運用	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。
C.4.3.1		運用環境	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。	
C.4.5.1			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。	
C.5.2.2		サポート体制	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、問い合わせ対応をベンダーが実施すること。	
C.5.3.1			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。	
C.5.9.1			定期報告会実施頻度	運用の定期報告は、四半期に1回程度実施すること。	
C.5.9.2			報告内容のレベル	保守の定期報告は、ベンダーによる提案事項とすること。	
C.6.2.1		その他の運用管理方針	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。	
D.1.1.1	移行性	移行時期	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、3ヶ月未満とすること。	
D.1.1.2			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、利用の少ない時間帯（夜間など）とすること。	
D.1.1.3			並行稼働の有無	システム移行時の並行稼働期間は、無しとすること。	
D.3.1.1		移行対象（機器）	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。	
D.4.1.1		移行対象（データ）	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については、ベンダーによる提案事項とすること。	
D.5.1.1		移行計画	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。	
E.1.1.1	セキュリティ	前提条件・制約条件	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、有りとする。	事業者が遵守すべき規定やルール等を指定する。 例） ・情報セキュリティポリシー ・個人情報保護法 ・電子署名法 ・IT基本法 ・ISO/IEC27000系 ・政府機関の情報セキュリティ対策のための統一基準
E.2.1.1		セキュリティリスク分析	リスク分析範囲	セキュリティリスクは、分析なしとすること。	
E.3.1.2		セキュリティ診断	Web診断実施の有無	Web診断は、実施すること。	
E.4.3.4		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	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。	
E.5.1.1		アクセス・利用制限	管理権限を持つ主体の認証	認証方法は、1回とすること。	
E.5.2.1			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。	
E.6.1.1		データの秘匿	伝送データの暗号化の有無	伝送データについては、認証情報のみ暗号化すること。	
E.6.1.2			蓄積データの暗号化の有無	蓄積データについては、認証情報のみ暗号化すること。	
E.7.1.1		不正追跡・監視	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。	
E.7.1.3			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。	

E.10.1.1		Web対策	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。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。
E.10.1.2			WAF※の導入の有無	WAFの導入は、無しとすること。	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。
F.1.1.1	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	システム構築時には、条例等の制約無しとすること。	
F.1.2.1			運用時の制約条件	システム運用時には、制約無しとすること。	

※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。（https://www.j-lis.go.jp/rdd/chyousakenkyuu/cms_92978324-2.html）
※「項番」は、当該シートの内容記載しており、再附番は行っていない。