

■非機能要件一覧

(資料1 別紙4)

項番	大項目	中項目	マトリクス(指標)	要求目標等	基準値	補足説明等
-	可用性	継続性	計画停止予定通知	データセンターの改修等による計画停止及び定期保守等に伴いサービスの利用停止を行う場合、電話又はメールにて、原則14日以上前までに通知すること。 ※ただし、年次計画で提出している作業については、10日以上前	30日以上前 ※ただし、年次計画で提出している作業については、10日以上前	
A.1.3.1			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、障害発生時点(日次バックアップ+アーカイブ※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、12時間以内にシステムを復旧すること。		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、1ヶ月以内に再開することを目標とすること。		
-			障害発生通知	システム障害が発生した際には、1時間以内に電話又はメールで通知すること。		
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	バックアップデータの保管場所について、提案書に記載すること。		
A.3.2.2			保管方法	大規模災害時のデータ保管方法について、提案書に記載すること。		
B.1.1.1	性能・拡張性	業務処理量	ユーザ数	現在の利用者数から増加することを勘案し、ユーザが問題なく利用できること。対応可能な増大率を提案書に記載すること。(システムを導入する施設及び利用件数(令和6年度実績)を参照のこと)		
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有りと想定すること。(300人程度)。対応可能な増大率を提案書に記載すること。		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。
B.1.1.3			データ量(項目・件数)	現在の利用数から増加することを勘案し、ユーザが問題なく利用できること。対応可能な増大率を提案書に記載すること。		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.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を提案書に記載すること。		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。
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を提案書に記載すること。		

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を提案書に記載すること。		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を提案書に記載すること。		
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、外部データは利用できないとすること。		
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、日次で取得すること。		
C.1.3.1			監視情報	エラー監視(トレース情報を含む)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こと。	
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.5.2.2	サポート体制	保守契約(ソフトウェア)の種類	運用保守契約の中で、アップデートを実施すること。			
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		定期報告実施頻度	運用保守の定期報告は、半年に1回程度実施すること。			
C.5.9.2		報告内容のレベル	運用保守の定期報告方法や内容を提案書に記載すること。			
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。			
E.2.1.1	セキュリティ	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分析を実施する範囲は、重要度が高い資産を扱う範囲及び外接部分とすること。		
E.3.1.2		セキュリティ診断	Webアプリケーション診断実施	システム構築及び改修時等必要と思われるタイミングで、Webアプリケーション診断を実施すること。なお、具体的な実施タイミングを提案書に記載すること。		
			プラットフォーム診断の実施	プラットフォーム診断は、年1回以上実施すること。なお、具体的な実施頻度を提案書に記載すること。		
		改ざん検知等の実施	Webサイトのアプリケーションやコンテンツ、設定等の重要なファイルの改ざんがないか週に1回以上チェックすること。なお、具体的な実施頻度を提案書に記載すること。			
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等必要と思われるタイミングで実施すること。			
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。 なお、具体的なアクセス・利用制限の例を提案書に記載すること。		
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、すべてのデータを暗号化すること。		
E.6.1.2		蓄積データの暗号化の有無	蓄積データの暗号化について、提案書に記載すること。		
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。なお、ログの取得期間及び種類を提案書に記載すること。		
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及び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、有りとする。		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。

※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。