

■別表3 非機能要件の実現方法

大分類		中分類		内容		対応可否 ○△×	実現方法及び 特記事項		
NO		NO		NO					
1	システム化方式 要件	-		1	システム化要件を実現するハードウェア構成、ネットワーク構成、ソフトウェア構成、手作業を明確にし、これらにシステム要求事項を割り振り文書化すること。				
				2	新システムは、要求仕様書に記されている現行ネットワーク構成、ハード類及びウェブサイト要件での運用を前提とする仕組みとすること。				
2	環境要件	a	利用端末要件	1	新システムは、要求仕様書に記された稼働環境の要件を満たすこと。				
		b	ウェブブラウザ対応要件	1	要求仕様書に記されているウェブサイト要件に記したOS・ブラウザから利用可能であること。				
		c	ネットワーク要件	1	会社のネットワーク構築においては、パフォーマンスや信頼性、組織の拡大やビジネスの変化に柔軟に対応できる拡張性、情報漏えいや不正アクセス等に対抗するセキュリティ、人材的な負荷を減らすための管理や運用面のしやすさを満たした、最適なネットワーク構成や機器を導入すること。				
		d	データセンター要件 (データセンターを利用する場合は、本項に示す事項を考慮し選定すること。)	1	不正侵入防止センサーやカメラ等によりデータセンターやハードウェア設置エリアへの入退室管理・監視、不正侵入防止対策をすること。				
				2	ディザスタリカバリ(災害対策)・災害の未然防止のための、ファシリティ対策を実施していること。 ・災害被害の軽減のため、地震、火災、水害、停電等への対策 ・UPS装置や自家発電設備の冗長化等				
				3	セキュリティ監査対応・第三者によるセキュリティ監査があった場合は、監査を受ける東京都立産業貿易センターの支援を行うこと。				
3	想定規模要件	a	利用者数	1	要求仕様書に記されている性能要件を満たすこと。				
		b	利用場所	1	基幹システムは東京都立産業貿易センター内でのみ利用できること。				
		c	業務処理件数	1	要求仕様書の運用要件に記載の利用者要件、性能要件を満たすこと。				
		d	データ量	1	要求仕様書に記されている性能要件を満たすこと。				
4	性能要件	a	オンライン処理性能	1	利用者がストレスを感じない3秒以内の応答時間とすること。ただし、一部の機能において、この制限を超えることを公社が認めた場合は、この限りではない。 また、同時アクセスが発生した場合においても、新システムの処理時間に影響を与えないこと。				
		b	バッチ処理性能	1	バッチ処理は、オンライン処理・バックアップ処理に対して影響を与えない事。なお、時間を要する処理が想定される場合については、公社と協議の上、決定する。				
5	信頼性要件	-		1	新システムにおいて障害等が発生しても、業務データの整合性を担保可能とし、影響を最小範囲に留め、復旧時間を最短とする構成とすること。				
		a	稼働時間	1	ウェブサイトは計画停止および定期保守時間を除き、原則24時間365日稼働とする。要求仕様書に記されている運用要件を満たすこと。				
		b	可用性	1	ハードウェア等は障害発生によるサービス停止を極力避ける構成とすること。 また、システムに障害が発生した場合、その原因を特定するために必要な証跡(アクセスログ、イベントログ等)が出力可能であること。				
		c	停電・瞬断対策	1	導入するサーバ機器は、停電・瞬断に十分耐えられる構成とすること。				
				d	バックアップ	1	新システムで保有するデータ(業務データのほか、サーバの設定情報、動作ログ等含む)について、定期的なバックアップを自動で実施すること。また、障害が発生した場合、バックアップデータでデータ復旧可能なこと。		
6	情報セキュリティ 要件	a	セキュリティ対策	1	新システム内で取り扱う情報の機密性および外部からの脅威等を踏まえリスク分析を実施し、網羅的なセキュリティ対策を行うこと。				
		b	個人情報保護	1	要求仕様書別紙に示した「東京都サイバーセキュリティ対策基準」を満たす対策を実施すること				
		c	アクセス管理	1	ユーザ認証(ユーザID、パスワード)機能を有すること。また、ユーザ認証によって許可された利用者の権限に応じて、新システムで利用できる機能を制限する仕組みとすること。				
		d	不正侵入防止・改竄ざん防止	1	要求仕様書別紙に示した「東京都サイバーセキュリティ対策基準」を満たす対策を実施すること				
		e	ウイルス対策	1	要求仕様書別紙に示した「東京都サイバーセキュリティ対策基準」を満たす対策を実施すること				
		f	データの暗号化	1	要求仕様書別紙に示した「東京都サイバーセキュリティ対策基準」を満たす対策を実施すること				
		g	監査証跡	1	システム利用者証跡(データ更新・参照時)、印刷監視(帳票印刷時)、および出力監査(ファイルのダウンロードや転送時)の監査機能を備えること。				
7	ユーザビリティおよびアクセシビリティに関する要件	a		1	システムにおける必要性を検討の上、PC操作の成熟度によらない操作性を考慮すること。				
		b		1	フォントや色の見やすさ、入力ガイダンス、マウスやキー操作のわかりやすさを考慮すること。				
		c		1	操作性については誤入力等の防止に配慮すること。				
		d		1	利用者が誤入力等をした場合のエラーおよび警告のメッセージは利用者に誤解のないようシステム全体で統一し、問題点と解決方法がわかるような配慮をすること。				
		e		1	データ登録、更新、削除を行う操作については、確認画面を表示する等の誤操作防止対策を考慮すること。				
		f		1	処理に時間のかかる操作は、利用者が端末の処理状況を把握できる表示とすること。(「処理経過の表示」ダイアログや「処理中」メッセージ等)				