

■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アーキテクチャとして、ハードウェア構成、ネットワーク、ソフトウェア構成、手作業を明確にし、これらのいずれかにシステム要求事項を割り振り、システム方式とシステム要求事項を割り振った結果を文書化すること。				
				2	新システムは、現在、公社に導入されているシンクライアントPC及びクライアントPC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	シンクライアント端末、物理端末、スマートフォン、タブレット端末で利用可能であること。				
				2	Windows7、Windows10、MAC、iOS、Androidから利用可能であること。				
		b	webブラウザ対応要件	1	以下全てに対応できること ・Windows(Internet Explorer11以上、Google Chrome 最新版、FireFox 最新版) ・Macintosh(Safari 最新版、Google Chrome 最新版、FireFox 最新版) ・スマートフォン(Android最新版、iOS最新版、Windows10Mobile)				
				c	ネットワーク要件	1	公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。		
						2	冗長化ネットワークの機器は冗長化等により、高信頼性を確保すること。		
						3	セキュリティ対策不正アクセスやウイルス・スパイウェア対策等のセキュリティ対策を施すこと。		
		4	性能、拡張性データ量や利用者の増加に対応できる拡張性を有する						
		d	データセンター要件	1	新システムの構築に際して、データセンターを利用する場合は、以下に示す事項を考慮し、データセンターを選定すること。				
				2	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への不正侵入を防止すること。				
				3	入退室管理・24時間の入退室監視を行うこと。・生体認証や非接触型ICカード等により不正入出排除を行うこと。				
4	ディザスタリカバリ(災害対策)・災害の未然防止のため、地形、立地条件等のファシリティ条件を考慮すること。 ・災害被害の軽減のため、地震、火災、水害、停電等への対策を行うこと。 ・UPS装置や自家発電設備の冗長化等により、事業継続性を高めること。								
5	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、データセンターで対応できること。								
e	テスト環境要件	1	ソフトウェアのバージョンアップや追加改修等が生じた場合、テスト環境へリリースし、動作確認を実施した上で本番環境へリリースできること。						
3	想定規模要件	a	利用者数	1	新システムの利用者数は、システム管理者5名、公社利用職員70名(委嘱者含む)、利用者3万人である。(年間約1万人増見込む) ※公社側(システム管理者、公社利用職員)の公社向け機能の同時利用者は、各拠点20名を想定している。※利用者側の利用者向け機能の同時利用者は100名を想定している。				
		b	利用場所	1	新システムの利用場所は、公社が運用する都内3拠点(VPN環境あり)を想定している。				
		c	業務処理件数	1	創業から現在までの業務処理件数と昨年度の業務処理件数は、仕様書に記載ある表5・6を参照すること。なお、設計・開発にあたっては、業務処理件数の将来的な増減を十分に考慮すること。				

		d	データ量	1	創業から現在までの業務処理件数と昨年度の業務処理件数は、仕様書記載ある表7を参照すること。なお、設計・開発にあたっては、データ量の将来的な増減を十分に考慮すること。		
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。なお、業務処理負荷の高い時間帯等でも、最長10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会社が認められた場合は、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、会社と協議の上、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、復旧に係る時間を最短とする構成とすること。		
		a	稼働時間	1	新システムは、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。		
		b	冗長構成等	1	ハードウェア等については、SPOF(その箇所が停止すると、他の箇所が正常でもシステム全体が停止するような箇所の総称)を回避するシステム構成を取り、障害発生によるサービス停止を極力避けること。具体的には、サーバ機器の多重化、重要部位(電源、ファン、ディスク装置等)の多重化等を実施すること。なお、サーバ機器については、ホットスタンバイ構成とすること。また、新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には、停電・瞬断対策としてUPS(無停電電源装置)を設置すること。なお、UPSは、各機器の消費電力およびシャットダウンに必要とされる時間を考慮の上、シャットダウンするまでに必要な時間を十分確保できるだけの電源容量を保有したものとすること。		
		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、日次にて差分バックアップ、週次にてフル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、データの復旧はバックアップデータのリストアで対応可能なこと。なお、バックアップデータは、1ヶ月分を保管すること。		
6	中立性要件	a		1	特定の技術や製品に依存せず、継続的に安定した品質保証が受けられるオープンな標準に基づいた技術を採用すること。		
		b		1	新システムの運用保守は、他事業者でも変更および引継ぎが可能であること。		
		c		1	システム更改時において、円滑なデータ移行が可能なシステム構成であること。		
		d		1	第三者による保守性を向上させるため、成果物等は公社で標準的に利用されているドキュメント作成ソフトを用いること。		
7	継続性要件	-		1	災害等発生時には事業継続のためのシステム復旧が必要となるため、速やかなデータ復旧ができることを考慮したハードウェア・ソフトウェア構成、保守体制とすること。		
8	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。なお、対策の詳細については、公社の情報セキュリティの関連規程等を遵守することとする。		
		b	個人情報保護	1	新システムでは、個人情報等を保有するため、プライバシーマーク制度に準拠した「個人情報保護方針」を定め、適切に運用するなど、情報漏えい等を防止するための対策を講じること。なお、IP登録によるアクセス許可を実施する。(個別相談内容含む)		
		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・改ざん防止	1	新システムで使用する通信プロトコルおよび通信ポート以外での接続を禁止し、不正な接続等があった場合は、それを検知し、ログを取得する仕組みを構築すること。また、ファイルやデータ等が改ざんされていないかチェックする仕組みを構築すること。改ざんがあった場合は、速やかにシステム管理者に通知することが可能なこと。		
		e	ウイルス対策	1	マルウェア(ウイルス、ワーム、ボット等)による脅威に備えるため、新システムで導入する機器にはウイルス対策ソフトを導入すること。なお、当該ソフトは、新たに発見されるマルウェアに対応するため、パターンファイル等の自動更新が可能であること。		

		f	データの暗号化	1	新システムで保有する情報の漏えい等を防止するため、利用者が直接アクセスできないように制限し、個人情報や機密データ等は暗号化する機能を備えること。 また、通信回線に対する盗聴防止のため、通信回線を暗号化する機能を備えること。		
		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。		
9	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	本システムとの整合性に配慮しつつ、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	表示する情報は簡潔にすること。例えば、関連する情報は、一画面内で参照できるような画面構成や、画面内での位置が近くなるように配置すること。		
		d		1	操作についてはTabキー等による入力ターゲットの移動を定め、誤入力等の防止に配慮すること。		
		e		1	視線の流れが、「左→右」方向、「上→下」方向となるように情報の配置を工夫すること。		
		f		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、問題点と解決方法がわかるように配慮すること。		
		g		1	利用者に対し適切なデフォルト値を設定し、少しでも利用者の操作を軽減できる仕組みを考慮すること。		
		h		1	データ登録、更新、削除を行う操作については、必ず確認画面を表示する等の誤操作がないよう考慮すること。		
		i		1	異なる画面上についても、名称等については利用者の誤解が生じないようにシステム内で統一すること。		
		j		1	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すること。		
		k		1	エラーメッセージは、エラー発生を知らせるだけでなく、エラーの原因・解決方法を明示するようにすること。(例えば、エラー項目を強調表示し、フォーカスを遷移させる等)		
		l		1	利用者への警告やメッセージは、画面内にメッセージを表示して伝えること。		
		m		1	利用者に表示するメッセージは、問題点が何かを明示し、利用者が何をすべきかを表示すること。		
		n		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。(例えば、「処理経過の表示」ダイアログや「処理中」メッセージ等)		