別紙６　非機能要件表

No.	仕様書 該当項目	大項目	中項目	非機能要件のカテゴリ	内容・レベル等	必須	特記事項
1	９．（１）	運用時間		信頼性（障害対応、セキュリティ等）	システムの運用時間は、原則として24時間とし、365日利用可能なシステム構成とすること。	○	
2	９．（１）	運用時間		信頼性（障害対応、セキュリティ等）	システムを安定稼働させ、止まらないシステムとするために、システム負荷やリソース状況、アラーム・メッセージなどを自動で監視し、異常があればメール等で県立図書館へ通報を行うなどの仕組みも導入すること。	○	
3	９．（２）．ア	データ移行		移行性	現行システムから抽出された既存データ（CSV形式やXML形式等汎用的なデータ）のシステムへの登録は、受注者が責任もって行うこと。	○	
4	９．（２）．イ	データ移行		移行性	現行システムで管理している文字種は、システム上でも同様に扱えることとし、文字化けや違う文字コードへの変換間違いがないこと。	○	
5	９．（２）．ウ	データ移行		移行性	システム上で新たに必要となるデータがあれば、発注者と協議の上、受注者が当該データを補完すること。万が一、システム稼働後に移行データに起因する障害が発生した場合は、速やかに復旧させ、業務に支障がないようにすること。	○	
6	９．（２）．エ	データ移行		移行性	次回のシステム更新時には、発注者の要望に応じて、CSV形式やXML形式等汎用的なデータ形式でデータ抽出を行い、次期システムベンダーに協力して必要な資料・データを提供し、円滑なデータ移行を行うこと。また、これに伴う経費は保守経費の範囲内で行うこと。	○	
7	９．（３）	レスポンスタイム		性能・拡張性	本業務で整備するシステムは発注者が快適に運用できることとし、他の作業を行っていない業務端末において、以下のレスポンスタイム標準とすること。	○	
8	９．（３）．ア	レスポンスタイム		性能・拡張性	各画面は平均３秒以内に遷移すること。	○	
9	９．（３）．イ	レスポンスタイム		性能・拡張性	簡易検索において、全ての資料を対象としたフリーワード検索について、平均５秒以内で検索結果一覧画面に遷移すること。	○	
10	９．（３）．ウ	レスポンスタイム		性能・拡張性	詳細検索（項目を指定した検索とし、AND、OR検索含む５項目程度の検索）において、平均５秒以内で検索結果一覧画面に遷移すること。	○	
11	９．（４）．ア	デザイン	公開用画面	性能・拡張性	公開用画面はアクセシビリティおよびユーザビリティに考慮し、ユニバーサルデザインに基づいた、わかりやすく見やすい画面とすること。（JIS X 8341-3:2016 レベルAA以上）	○	
12	９．（４）．イ	デザイン	公開用画面	性能・拡張性	公開用画面はスマートフォンなどに対応した機能を持ち、閲覧する場合は適切なレイアウトに自動的に表示変更されるレスポンシブデザインに対応していること。	○	
13	９．（４）．ウ	デザイン	公開用画面	性能・拡張性	公開用画面デザインは、専門的なデザイナーとの協議により作成すること。	○	
14	９．（５）．ア	セキュリティ		信頼性（障害対応、セキュリティ等）	OS、ウイルス対策ソフト、ミドルウェア、ソフトウェア等は導入時最新のものとする。ここでいう最新とは、既知のセキュリティホール（脆弱性）について、全て対策を講じている状態をいう。なお、常にこれを保つこと。	○	
15	９．（５）．イ	セキュリティ		信頼性（障害対応、セキュリティ等）	インターネット上で提供するアプリケーションプログラム（パッケージ含む）について「クロスサイトスクリプティング」「SQLインジェクション」「入力値チェックの不備」「セッション管理に関する脆弱性」「アクセス制御/キャッシュ制御に関する脆弱性」「クロスサイトリクエストフォージェリ」のセキュリティチェックを実施し、問題がないことを「セキュリティ監査報告書」として運用テスト完了時に書面で報告すること。	○	
16	９．（５）．ウ	セキュリティ		信頼性（障害対応、セキュリティ等）	構築する全サーバについて、踏み台にされることを防止するため、「必要最小限のポート開放」「メール不正中継確認」「DNSリカーシブ確認」のセキュリティチェックを実施し、問題がないことを「セキュリティ監査報告書」として運用テスト完了時に書面で報告すること。	○	
17	９．（５）．エ	セキュリティ		信頼性（障害対応、セキュリティ等）	ウイルス対策ソフトについては、利用期間中は常に最新のウイルス定義ファイルを適用すること。	○	
18	９．（５）．オ	セキュリティ		信頼性（障害対応、セキュリ	ファイアウォール等による不正侵入防止、侵入検知及び改ざん検知対策を行うこと。	○	
19	９．（５）．カ	セキュリティ		信頼性（障害対応、セキュリティ等）	導入するパソコンはすべて一元管理でき、常に最新のOS状態で稼働させること。管理プラットフォームを別紙１（21）「管理コンソール」内に構築すること。	○	
20	９．（５）．キ	セキュリティ		信頼性（障害対応、セキュリティ等）	情報セキュリティに関する情報収集及び脆弱性確認を随時行い、できるだけ速やかにパッチを充てる等、必要に応じた対策を行うこと。	○	
21	９．（５）．ク	セキュリティ		信頼性（障害対応、セキュリティ等）	アクセスログ及び各種通信ログを取得し、情報漏えい、不正アクセス等を監視すること。	○	
22	９．（５）．ケ	セキュリティ		信頼性（障害対応、セキュリティ等）	受注者のシステム管理者用のパスワードについて、アルファベット、数字、記号が混在した適切な長さとなっている、類推しやすい並び方やその安易な組合せにしない等の基本的な対策がとられており、予め制限された担当者内でのみ管理されていること。	○	
23	９．（５）．コ	セキュリティ		信頼性（障害対応、セキュリティ等）	情報セキュリティインシデントが発生した際には、速やかに被害拡大防止、原因特定等を行うこと。	○	
24	９．（５）．サ	セキュリティ		信頼性（障害対応、セキュリティ等）	システム上の添付ファイルについては、自動で無害化処理を行い、安全な情報のみ抽出できること。	○	
25	９．（５）．シ	セキュリティ		信頼性（障害対応、セキュリティ等）	昨今、委託先やヘルプデスク等を含めたサプライチェーンによる情報セキュリティインシデントが増していることから、サプライチェーンセキュリティ対策について提案すること。	○	
26	９．（５）．ス	セキュリティ	ドメイン	信頼性（障害対応、セキュリティ等）	システムのドメインは受注者が取得し鳥取県のドメイン取扱通知に基づき管理すること。また、利用終了後は鳥取県に無償譲渡することとし、以下のとおり対応すること。	○	
27	９．（５）．ス.（ア）	セキュリティ	ドメイン	信頼性（障害対応、セキュリティ等）	ウェブサイトによる情報発信を終了する場合は、同サイト内で６か月前を目安にドメイン利用停止に関する案内（事前告知）を行うこと。	○	
28	９．（５）．ス.（イ）	セキュリティ	ドメイン	信頼性（障害対応、セキュリティ等）	ウェブサイトによる情報発信終了後（ドメイン利用停止後）も１年以上ドメインを廃止することなく延長保有すること。	○	
29	９．（５）．ス.（ウ）	セキュリティ	ドメイン	信頼性（障害対応、セキュリティ等）	１年以上ドメインを延長保有した後の対応については、発注者に事前に協議すること。	○	
30	９．（５）．セ	セキュリティ		信頼性（障害対応、セキュリティ等）	上記項目以外に、新システムにおけるセキュリティ対策があれば提案すること。	○	
31	９．（６）	運用テスト		信頼性（障害対応、セキュリティ等）	システムの本稼働前に正常に動作しているか検証するため、事前に検証項目などを明確にしたテスト仕様書を作成し発注者の承認を得たうえで、当該テスト仕様書に基づき、検証すること。	○	
32	９．（６）	運用テスト		信頼性（障害対応、セキュリティ等）	テスト結果を報告書にまとめ、発注者に提出すること。	○	

別紙６　非機能要件表

No.	仕様書 該当項目	大項目	中項目	非機能要件のカテゴリ	内容・レベル等	必須	特記事項
33	９．（７）.ア	操作研修	研修	信頼性（障害対応、セキュリティ等）	仕様書３（４）に係る操作研修を実施すること。	○	
34	９．（７）.イ.（ア）（エ）	操作研修	マニュアル	信頼性（障害対応、セキュリティ等）	システムの利用に当たって必要となる各種マニュアルを作成すること。 ※なお、作成するマニュアルの種類に関しては、業務及び運用を行うために必要な内容が記載されていれば、提案に委ねることも可能とするが、県立図書館の承認を得ること。	○	
35	９．（７）.イ.（イ）	操作研修	マニュアル	信頼性（障害対応、セキュリティ等）	各種マニュアルは、システムを操作する端末からいつでも最新情報を参照できるようにすること。	○	
36	９．（７）.イ.（ウ）	操作研修	マニュアル	信頼性（障害対応、セキュリティ等）	パッケージの標準的なマニュアルがある場合においても、県立図書館の業務に沿って必要な内容の修正を行うこと。また、アドオン機能等の内容についてもマニュアルに反映すること。	○	
37	９．（７）.イ.（エ）	操作研修	マニュアル	信頼性（障害対応、セキュリティ等）	マニュアルは、県立図書館が、各種業務を行うための操作マニュアル及びシステム運用を行うための運用マニュアルを作成すること。	○	
38	９．（７）.イ.（オ）	操作研修	マニュアル	信頼性（障害対応、セキュリティ等）	マニュアルは、PDFファイルの電子データを納品すること。なお、原本ファイルとして、県立図書館が加工可能なファイルを提供できる場合は、あわせて提供すること。	○	
39	９．（８）.ア	運用・保守		信頼性（障害対応、セキュリティ等）	システムの運用・保守　（サーバ機器類監視、障害対応等）を行うこと。	○	
40	９．（８）.ア	運用・保守	体制	信頼性（障害対応、セキュリティ等）	運用・保守業務を統括する責任者と業務を遂行する担当者を設けて、新システムの運用を円滑に進める運用・保守体制**を**整えること。	○	
41	９．（８）.イ	運用・保守	技術支援	信頼性（障害対応、セキュリティ等）	本業務整備機器が所定の性能及び機能を確保できるよう十分な情報交換、連携作業を維持し、円滑なシステム運用ができるように技術支援を行うこと。	○	
42	９．（８）.イ.（ア）	運用・保守	技術支援	信頼性（障害対応、セキュリティ等）	データメンテナンス及びログやアクセス件数の収集	○	
43	９．（８）.イ.（イ）	運用・保守	技術支援	信頼性（障害対応、セキュリティ等）	パラメータ、区分コードなどの追加・修正	○	
44	９．（８）.イ.（ウ）	運用・保守	技術支援	信頼性（障害対応、セキュリティ等）	運用相談、他事例紹介	○	
45	９．（８）.イ.（エ）	運用・保守	技術支援	信頼性（障害対応、セキュリティ等）	軽微なプログラム修正（表現、文言の追加・修正）	○	
46	９．（８）.ウ.（ア）	運用・保守	保守内容	信頼性（障害対応、セキュリティ等）	システムログ、アクセスログ等を取得し、最低２年分蓄積できること。	○	
47	９．（８）.ウ.（イ）	運用・保守	保守内容	信頼性（障害対応、セキュリティ等）	ハードウェア障害の監視・対応を行うこと。	○	
48	９．（８）.ウ.（ウ）	運用・保守	保守内容	信頼性（障害対応、セキュリティ等）	ソフトウェア障害の監視・対応を行うこと。	○	
49	９．（８）.ウ.（エ）	運用・保守	保守内容	信頼性（障害対応、セキュリティ等）	システムへのアクセス監視による不正アクセス、異常アクセスなどを検知した場合は発注者に速やかに報告するとともに適切な対応を行うこと。	○	
50	９．（８）.ウ.（オ）	運用・保守	保守内容	信頼性（障害対応、セキュリティ等）	障害等への問合せに対応すること。	○	
51	９．（８）.ウ.（カ）	運用・保守	保守内容	信頼性（障害対応、セキュリティ等）	操作説明書等の各種納品物について、システム利用期間中に内容の変更が生じた場合には、適宜改訂を行い、発注者に提出すること。	○	
52	９．（８）.ウ.（キ）	運用・保守	保守内容	信頼性（障害対応、セキュリティ等）	運用において、受注者の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。	○	
53	９．（８）.ウ.（ク）	運用・保守	保守内容	信頼性（障害対応、セキュリティ等）	やむを得ずリモート保守を行う場合は、発注者の承認を得た上で必ず専用線やIP－VPN等の閉域網回線を利用し、他のネットワークと接続されない専用端末で行うこと。その際、回線の設置、利用料は受注者が負担すること。	○	
54	９．（８）.ウ.（ケ）	運用・保守	保守内容	信頼性（障害対応、セキュリティ等）	上記項目以外に、システムの運用・保守について提案があれば記載すること。	○	
55	９．（８）.エ.（ア）	運用・保守	障害対応	信頼性（障害対応、セキュリティ等）	障害発生時の緊急連絡・対応体制を構築すること。	○	
56	９．（８）.エ.（イ）	運用・保守	障害対応	信頼性（障害対応、セキュリティ等）	障害発生時には、発注者に連絡を行うとともに障害の切分け、原因究明及び影響を最小限に抑えるための対策を実施し、システム復旧対策を行うこと。	○	
57	９．（８）.エ.（ウ）	運用・保守	障害対応	信頼性（障害対応、セキュリティ等）	本業務で納入したハードウェア及びソフトウェアに障害が発生した場合は、発注者と連携して速やかに復旧の措置をとること。取扱いの過誤によらない原因で設備の故障、損傷などの不良・不備と認められる箇所が生じた場合には、受注者において速やかに修理すること。	○	
58	９．（８）.エ.（エ）	運用・保守	障害対応	信頼性（障害対応、セキュリティ等）	(対応時間は、午前８時30分から午後７時30分までとすること。（土曜日、日曜日及び国民の祝日に関する法律（昭和23年法律第178号）に規定する休日を含む）	○	
59	９．（８）.エ.（オ）	運用・保守	障害対応	信頼性（障害対応、セキュリティ等）	保守形態はオンサイト（現地修理、現地交換）とすること。止むを得ない場合には代替機を先出しし、持帰り修理も可とする。ただし、個人情報保護の観点からハードディスクの持帰りは不可とする。	○	
60	９．（８）.エ.（カ）	運用・保守	障害対応	信頼性（障害対応、セキュリティ等）	障害連絡を受けてから４時間以内に対応が必要な場所に到着すること。	○	
61	９．（８）.エ.（キ）	運用・保守	障害対応	信頼性（障害対応、セキュリティ等）	障害復旧時間は機器交換を含めて６時間程度を目安にすること。	○	

別紙６　非機能要件表

No.	仕様書 該当項目	大項目	中項目	非機能要件のカテゴリ	内容・レベル等	必須	特記事項
62	９．（８）.エ.（ク）	運用・保守	障害対応	信頼性（障害対応、セキュリティ等）	故障等により、ハードディスクの初期化、ソフトウェアのアンインストール等を行った場合は、本業務で構築を行ったOS等のソフトウェアを障害発生前の状態（OS等のソフトウェアのバージョンや設定等）に復元、再設定すること。	○	
63	９．（８）.エ.（ケ）	運用・保守	障害対応	信頼性（障害対応、セキュリティ等）	修理に伴い不要になった記録媒体は破壊すること。	○	
64	９．（８）.エ.（コ）	運用・保守	障害対応	信頼性（障害対応、セキュリティ等）	サーバ障害等でデータに係るトラブルが発生した場合は、バックアップデータからのリストアを行う等データ復旧作業を行うこと。	○	
65	９．（８）.エ.（サ）	運用・保守	障害対応	信頼性（障害対応、セキュリティ等）	障害原因を明らかにし、恒久的な対応策を実施し、再発の防止に努めること。併せて対応結果を発注者に報告すること。	○	
66	９．（８）.オ	運用・保守	データ消去	信頼性（障害対応、セキュリティ等）	本業務により整備したシステムの利用期間が満了したときは、発注者の要望に応じてデータを抽出した後に、マスターデータを含むシステムの全データ及びバックアップデータが記録された記録媒体内のデータを消去又は記録媒体を破壊すると共に、発注者に作業日時、作業担当者名及び処理内容が記載されたデータ消去に係る報告書の提出を行うこと。	○	
67	10.（２）	運用・保守	作業場所	信頼性（障害対応、セキュリティ等）	本業務の開発及び運用保守工程に係る作業場所については受注者にて用意すること。	○	
68	10.（３）.ア	運用・保守	進捗管理	信頼性（障害対応、セキュリティ等）	スケジュールを含むプロジェクト管理の責務は、受注者が負うものとする。	○	
69	10.（３）.イ	運用・保守	進捗管理	信頼性（障害対応、セキュリティ等）	受注者は、作業に先立ちWBS、導入スケジュールを書面で提出し、発注者の承認を得ることとし、やむを得ず作業スケジュール等を変更する場合は、事前にお互い書面をもって協議することとする。	○	
70	10.（３）.ウ	運用・保守	進捗管理	信頼性（障害対応、セキュリティ等）	会議・打合せ議事録の作成義務は受注者にあり、発注者はそれを承認するものとする。	○	
71	10.（４）.ア	定期協議		信頼性（障害対応、セキュリティ等）	発注者及び受注者は、システム導入が完了するまでの間、進捗状況の報告、問題点の検討・解決、成果物のレビュー、その他対象システム導入の推進のために必要な事項を協議するための協議を定期的に開催する。当該協議の開催頻度は、発注者及び受注者が協議の上別途決定する。（開催頻度は月１回を基準とする）	○	
72	10.（４）.イ	定期協議		信頼性（障害対応、セキュリティ等）	受注者は、仕様書10.（4）.アの協議会が開催されたときは議事録を作成し、発注者及び受注者双方が署名する。	○	
73	10.（４）.ウ	定期協議		信頼性（障害対応、セキュリティ等）	運用・保守に関する定期協議は、システム導入後１年間は月１回の開催とし、以降は発注者及び受注者が協議の上別途決定する。	○	
74	10.（７）	法令遵守		信頼性（障害対応、セキュリティ等）	本業務を受注するにあたって、法令等の定め及びデジタル庁等国から提示されている関連ドキュメントのほか、仕様書10.（７）＜遵守すべき法令及びその他の規定等一覧＞についても内容を十分に理解し遵守すること。	○	
75	11	SLA		信頼性（障害対応、セキュリティ等）	本業務に係る契約の際にSLAを締結するものとする。本仕様書に記載以外の事項を含め、本業務で提供されるサービスレベル項目、設定値及び測定方法を次の項目を踏まえ提案すること。 ア　サービス品質（可用性） イ　性能（オンライン応答時間等） ウ　信頼性（障害対応、セキュリティ等） エ　運用業務（ヘルプデスク等）	○	
76	11	SLA		信頼性（障害対応、セキュリティ等）	サービスレベルの評価、見直しも定期的に実施することとする。	○	
77	11	SLA		信頼性（障害対応、セキュリティ等）	SLAの提案は、サービスレベルのモニタリングの実施方法及びレベルの基準値を満たすことができなくなった場合の対応期限、サービス対価の減額等も含めることとする。	○	