クラウドサービス要件

別紙3

回答業者名：

対応方法を、「標準対応：〇、個別対応：△、対応不可：×」で記入すること

業務		項番	説明	対応
公的認証	情報開示認定制度への登録	1	サービスを行う図書システムがASPIC等の情報開示認定を受けていること。	
	クラウドサービスセキュリティ	2	図書館SaaSとしてISO27017を取得していること。	
契約	契約期間	3	契約期間には、最短・最長とも期限を設けずに柔軟に対応すること。	
	中途解約	4	1カ月程度の期間を設ければ、違約金を生じずに中途解約できること。	
可用性	職員機能の運用時間	5	全ての開館日、7:30～20:00に使用できること。	
	市民サービス提供時間	6	計画停止を除く365日24時間サービスを提供できること。	
	計画停止予定通知	7	最短でも14日前までには必ず通知をすること。	
	重大障害時の代替手段	8	重大障害時にもPC単独で貸出業務を継続できること。	
	計画停止（メンテナンス）	9	計画停止は、月1回（最大6時間まで）までとする。	
	レベルアップ方針	10	年2回の定期レベルアップを実施することとし、最短でも30日前までに内容を連絡すること。	
	パッチ適用	11	事前に図書館と協議し、適用タイミングを調整すること。	
障害対応	データベース	12	RAIDによる二重化等の冗長化を施してあること。	
	重大障害からの復旧時間	13	アプリケーションレベル(サービス再起動による障害復旧)：1時間以内、それ以外(OS/ハード障害)は48時間以内であること。	
	復旧範囲	14	前日閉館状態のバックアップまで復旧できること。	
	障害通知プロセス	15	緊急時は、図書館担当者へ電話連絡すること。	
性能	オンライン応答時間	16	応答時間は、平均1秒以内（貸出）であること。	
	大量バッチ処理時間	17	一括登録は3000件/時間以上行えること。	
	夜間自動バッチ処理時間(日次、	18	即時処理でない場合、日次、月次とも10分以内に処理されること。	
	年次バッチ処理時間	19	即時処理でない場合、年次処理はセンター内で計画実行すること。	
拡張性	パラメータ設定	20	各機能は、パラメータ設定で業務運用に対する柔軟性と拡張性を持つこと。	
	カスタマイズ性	21	MARC変換プログラム、WebOPAC定義体、館内OPACデザイン、各種の文言表現、画像など図書館固有の要件に関しては個別調整の余地を備えること。	
	オプション製品追加	22	標準的なオプションシステムの追加においては、基幹システムに対する構築作業費用を要さずに導入できること。	
	外部サービス連携	23	県立図書館の横断検索と連携を図れること。	
	読書活動推進サービス	24	書評、コメント、本棚サービス等の読書推進サービスは利用者自身の選択により相互参照することもできること。	
	同時接続利用者数（業務）	25	契約端末ライセンス数まで同時接続可能なこと	
	同時接続利用者数（Web）	26	同時接続利用者数は、500アクセス以上であること。	
	拡張要望への対応	27	年2回以上図書館からの要望を収集し、優先度に基づき順次パッケージ機能の追加開発へと反映させること。	
センター団ポート	受付時間帯	28	WebによるQA受付は24時間365日対応すること。	
	対応時間帯	29	受付後は開館日の8:30～19:00に速やか対応をすること。	
	対応体制	30	現地担当SEと連携してサポートを行うこと。	
運用管理	運用者	31	クラウドサービス及びシステム基盤の運用は契約企業（もしくは100%資本の関係会社）自身で運用・保守を実施していること。	
	稼動監視	32	アプリケーション変更、ポート監視、ハードトラブル監視を行うこと。	
	検知時対応	33	異常値やトラブル、ハードウェア故障の予兆を確認した場合は、速やかに必要な措置を取れること。	
	緊急時対応	34	重大障害への対処や緊急性の高いセキュリティ対応が必要な際に、パッケージシステム運用担当者が即時対応で駆けつけること。	
	資源監視	35	サーバの資源使用量を随時監視し、必要に応じて拡張計画を立案し、使用料の範囲で実施すること。	
データ管理	バックアップ方法	36	日次で自動取得し、センター内にディスク形式で保存すること。アクセス権は運用管理者のみに制限すること。	
	バックアップ保存期間	37	3世代以上保存すること。	
	統計データ保持期間	38	6年以上保持すること。	
	画像データ領域	39	画像データ、配架図ファイルは2GBまで保持すること。	
	データ管理の開始	40	移行データをセンターDBに格納した時点からサービス開始とすること。	
	解約後のデータ消去	41	サービス解約1ケ月の保持期間の後、完全消去すること。	
情報保護	脆弱性チェック	42	脆弱性情報を常に収集し、改善事項に対して速やかに対策を講じること。	
	セキュリティパッチ	43	OS・ミドルウェアのセキュリティパッチを適用し、安全性を保つこと。	
	セキュリティに関する評価	44	年1回以上セキュリティ全般に関する監査を実施すること。	
	ウィルスチェック	45	保護ツールによるリアルタイム対策を行うこと。	
	情報取得者の制限	46	利用者データにアクセスできる技術者は、セキュリティ管理者の許可を得た者に制限し、担当者は個人情報保護に関する教育を定期的に受講すること。	
	情報取扱い環境	47	データ取扱い環境にはICカード・生体認証等による入室制限を行い、高セキュリティが確保された端末以外からアクセスできないようにすること。	
	通信の暗号化レベル	48	TLS1.2以上もしくはVPNによって接続すること。	
	個人情報の暗号化	49	利用者の個人情報項目は、データベースに暗号化を施すこと。	
	個人情報アクセスログ取得	50	利用者情報に対する操作ログを、管理者職員が確認できること。	