

授業料等収納管理システム「非機能要件一覧表」

別紙 3

項番	大分類	中分類	小分類	機能要求項目	区分
1	可用性	継続性	運用スケジュール	運用時間は、24時間運用を前提とし、日次メンテナンスを必要とする場合はその条件を示すこと。	必須
2				計画停止は、事前（遅くとも1週間前）通知のうえ行うこと。	必須
3			RP0（目標復旧地点）	平常時に業務停止を伴う障害が発生した際には、1営業日前の時点（日次バックアップからの復旧）までのデータ復旧を目標とすること。	必須
4		目標復旧水準（業務停止時）	RT0（目標復旧時間）	平常時に業務停止を伴う障害が発生した際には、12時間以内でのシステム復旧を目標とすること。	必須
5			RL0（目標復旧レベル）	平常時に業務停止を伴う障害が発生した際には、全システム機能の復旧を実施すること。	必須
6			システム再開目標	大規模災害時、システムに甚大な被害が生じた場合、システムは一ヶ月以内に再開することを目標とすること。	必須
7		稼働率	稼働率	年間のシステム稼働率は、99.5%以上を目標とすること。	必須
8		災害対策	システム再開目標	大規模災害時、同一の構成でシステムを再構築すること。	必須
9		外部保管データ	保管場所分散度	大規模災害時の業務継続性を担保するため、遠隔地にシステムのプログラム・データを外部保管すること。	必須
10	性能・拡張性	業務処理量	通常時の業務量	最大250ユーザーの同時接続に耐えうるものとし、システム利用職員がストレスなく円滑に業務を実施できる性能を有していること。	必須
11			業務量増大度	システムのユーザー数は、1.2倍の増大率に対応すること。	必須
12				システムの同時アクセス数は、1.2倍の増大率に対応すること。	必須
13				システムのデータ量は、2倍の増大率に対応すること。	必須
14				システムのオンラインリクエスト件数は、1.2倍の増大率に対応すること。	必須
15				システムのバッチ処理件数は、1.2倍の増大率に対応すること。	必須
16			保管期間	バックアップデータは日次で3カ月間保管すること。	必須
17		性能目標値	オンラインレスポンス	通常時のオンラインレスポンスタイムは、3秒以内を目標とすること。	必須
18				アクセス集中時のオンラインレスポンスタイムは、5秒以内を目標とすること。	必須
19			バッチレスポンス （ターンアラウンドタイム）	通常時のバッチレスポンスタイムは、再実行の余裕が確保できることを目標とすること。	必須
20				アクセス集中時のバッチレスポンスタイムは、再実行の余裕が確保できることを目標とすること。	必須
21		リソース拡張性	CPU拡張性	システムのCPU利用率は、概ね20%以上50%未満で運用されること。	必須
22			メモリ拡張性	システムのメモリ利用率は、概ね20%以上50%未満で運用されること。	必須
23			ディスク拡張性	システムのディスク利用率は、概ね20%以上50%未満で運用されること。	必須
24	運用・保守性	通常運用	運用時間	運用時間は、24時間運用を前提とし、日次メンテナンスを必要とする場合はその条件を示すこと。	必須
25			バックアップ	データ復旧の際、外部データはデータ復旧に利用できないものとする。	必須
26				データ復旧の際、少なくとも3カ月前までの間で指定した日にちのデータに復元できること。	必須
27				バックアップの取得間隔は、日次取得とすること。	必須
28			運用監視	システムにおけるソフトウェア・ハードウェアに対し、死活監視に加えてエラー監視（トレース情報を含む）を行うこと。	必須
29				OS・ソフトウェア等のパッチについては、緊急性の高いパッチのみ即時に適用し、それ以外は障害対応時等適切なタイミングで適用を行うこと。	必須
30		運用環境	試験用環境の設置	システムの試験用環境については、専用の試験用環境を設置すること。	必須
31			マニュアル準備レベル	運用マニュアルについては、システムの通常運用のマニュアルを提供すること。	必須
32		サポート体制	保守契約 （ソフトウェア）	ソフトウェア保守については、アップデートをベンダーが実施すること。	必須
33		その他の運用管理方針	品質保証	情報システムの構築において、発注者が意図しない変更や機密情報の窃取等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。当該品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。	必須
34			クラウドサービス品質	提供するサービスの品質維持や情報セキュリティに関する役割及び責任の分担について、SLA合意書の締結及びSLMによる継続的・定期的に検証を行い、品質の維持及び改善を行うこと。	必須

項番	大分類	中分類	小分類	機能要求項目	区分
35	セキュリティ	前提条件・制約条件	情報セキュリティに関するコンプライアンス	新潟県情報セキュリティポリシーを順守すること。	必須
36		セキュリティリスク分析	セキュリティリスク分析	システム開発において、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、あるいは外接部分とする。	必須
37		セキュリティ診断	セキュリティ診断	WebサーバやWebアプリケーションに対するセキュリティ診断を実施すること。	必須
38		セキュリティリスク管理	ウイルス定義ファイル適用	ウイルス定義ファイルは、定義ファイルリリース時に適用すること。 なお、定義ファイルに依存しない「振る舞い検知型」の製品の場合は、製品アップデートを定期的実施すること。	必須
39		アクセス・利用制限	認証機能	本システムの利用について、IDとパスワード等による認証機能を有すること。	必須
40				主体認証の不正試行を防止するための対策を実施すること。	必須
41			利用制限	認証された主体のシステムへの操作については、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とすること。	必須
42		データの秘匿	データ暗号化	伝送データはすべて、TLS1.2以上の方式により暗号化すること。	必須
43				蓄積データはすべて、CRYPTREC記載の暗号化方式により暗号化すること。	必須
44			データ消去	システムの利用を停止又は終了する際は、必要データについてのデータ移行を実施した後、データを復元できないよう確実に削除すること。なお、データの削除については、日時、担当者および処理内容を記録し、データ消去にかかる証明書を提出すること。	必須
45		不正追跡・監視	不正監視	不正検知に必要なログ（ログイン/ログアウト履歴（成功/失敗）、操作ログ、セキュリティ機器の検知ログ、データベースログ、アプリケーションログ等）を取得すること。	必須
46				不正監視対象は、重要度が高い資産を扱う範囲、あるいは、外接部分とすること。	必須
47		web対策	web実装対策	セキュアコーディング、Webサーバの設定等については、対策の強化を実施すること。	必須
48				ドメイン名については、外部DNSによるドメイン名を取得すること。	必須
49				WAFなどのWebアプリケーションにおける攻撃対策を導入すること。	必須
50		クラウドサービス	クラウドサービスの認証規格	本システムで利用するクラウドサービスは、ISO/IEC27017認証の取得、ISMAPクラウドサービスリストへの登録またはSOC2報告書の取得のいずれかを満たしていること。	必須
51		データセンター	設置場所	当該クラウドサービスで利用するデータセンターの設置場所が、国内であり、日本の裁判管轄、法令が適用されること。	必須
52	システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	システム構築において、庁内基準や法令、条例等の制約がある(重要な制約のみ適用)ことに留意すること。	必須
53			運用時の制約条件	システム運用において、庁内基準や法令、条例等の制約がある(重要な制約のみ適用)ことに留意すること。	必須
54			安全管理措置の認証規格	受注者は、ISO/IEC27001、JIS Q 27001又はプライバシーマーク認定のいずれかを取得していること。	必須
55		システム特性	クライアント数	システムは、300台までのクライアントを管理できるようにすること。	必須