■非機能要件一覧

No.	大項目	中項目	メトリクス（指標）	要求目標等
1	可用性	継続性	RPO（目標復旧地点）※（業務停止時）	平常時、業務停止を伴う障害が発生した際には、障害発生時点（日次バックアップ+アーカイブからの復旧）までのデータ復旧を目標とすること。
2			RTO（目標復旧時間）※（業務停止時）	平常時、業務停止を伴う障害が発生した際には、1営業日以内でのシステム復旧を目標とすること。
3			RLO（目標復旧レベル）※（業務停止時）	平常時、業務停止を伴う障害が発生した際には、一部システム機能の復旧を実施すること。
4			システム再開目標（大規模災害時）	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。
5			稼働率	年間のシステム稼働率は、99.5%を目標とすること。
6		災害対策	復旧方針	外部記憶装置を物理的に複数台用意するなど、冗長性が確保された同一の構成で情報システムを再構築すること。
7	性能・拡張性	業務処理量	ユーザ数	利用者数は、不特定多数のユーザが利用できること。
8			同時アクセス数	同時アクセス数は、ベンダーによる提案事項とすること。 ※現行システムの同時アクセス数は管理者30端末、利用者10処理。
9			オンラインリクエスト件数	オンラインリクエスト件数(単位時間ごとの業務処理件数)は、仕様の対象としない。
10			バッチ処理件数	業務処理件数は、仕様の対象としない。
11		性能目標値	通常時オンラインレスポンスタイム	通常業務時のオンラインレスポンスタイムは、ベンダーによる提案事項とすること。
12			アクセス集中時のオンラインレスポンスタイム	業務繁忙等によるアクセス集中時のオンラインレスポンスタイムは、ベンダーによる提案事項とすること。
13			通常時バッチレスポンス	通常時のバッチレスポンスタイムは、ベンダーによる提案事項とすること。
14			アクセス集中時のバッチレスポンス	業務繁忙等によるアクセス集中時のバッチレスポンスタイムは、ベンダーによる提案事項とすること。
15	運用・保守性	通常運用	運用時間（平日）	平日運用時間は、24時間利用を前提とすること。
16			運用時間（休日等）	休日運用時間は、24時間利用を前提とすること。
17			外部データの利用可否	データ復旧の際、外部データは利用しないこと。
18			バックアップ取得間隔	差分バックアップの取得間隔は、日次で取得すること。
19			監視情報	エラー監視（トレース情報を含む）を行うこと。
20		保守運用	OS等パッチ	OS等のパッチについては、緊急性の高いパッチは即時に適用し、それ以外は定期保守時に適用を行うことを目標とする。
21		運用環境	マニュアル準備レベル	運用マニュアルについては、各製品標準のマニュアルを利用すること。
22			外部システムとの接続有無	外部システムとの連携は、仕様の対象としない。
23		サポート体制	保守契約（ソフトウェア）の種類	ソフトウェア保守契約種類は、アップデートをベンダーが実施すること。
24			ライフサイクル期間	ライフサイクル期間は、5年とすること。
25			定期報告会実施頻度	運用の定期報告は、四半期に1回程度実施すること。
26			報告内容のレベル	保守の定期報告は、ベンダーによる提案事項とすること。
27		その他の運用管理方針	問い合わせ対応窓口の設置有無	運用保守時の問い合わせ窓口については、ベンダーの既設コールセンターを利用すること。
28	移行性	移行時期	システム移行期限	既存システムから新システムへの移行については、令和7年12月末までとすること。
29			システム停止可能日時	システム移行時のシステム停止可能日時は、制約無し（必要な期間の停止が可能）とすること。
30			並行稼働の有無	システム移行時の並行稼働期間は無しとする。
31		移行対象（データ）	移行データ	現行システムから新システムへ500GB未満のデータを移行すること。
32		移行計画	移行のユーザ/ベンダ作業分担	現行システムから新システムへのデータ移行作業は、ユーザとベンダーが共同で実施すること。

33	セキュリティ	前提条件・制約条件	遵守すべき規程、ルール、法令、ガイドライン等の有無	遵守すべき法令等は、有りとする。(個人情報保護法、深谷市情報セキュリティポリシー)
34		セキュリティリスク分析	リスク分析範囲	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、外接部分とすること。
35		セキュリティ診断	Web診断実施の有無	Web診断は、実施すること。
36		セキュリティリスク管理	ウィルス定義ファイル適用タイミング	システム脆弱性等に対応するためのウィルス定義ファイルについては、定義ファイルリリース時に実施すること。
37		アクセス・利用制限	管理権限を持つ主体の認証	認証方法は、1回とすること。
38			システム上の対策における操作制限度	操作制限は、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すること。
39		データの秘匿	伝送データの暗号化の有無	伝送データについては、すべてのデータを暗号化すること。
40			蓄積データの暗号化の有無	蓄積データの暗号化については、ベンダーによる提案事項とすること。
41		不正追跡・監視	ログの取得	ログの取得については、必要なログを取得すること。
42			不正監視対象(装置)	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。
43		Web対策	セキュアコーディング、Webサーバの設定等による対策の強化	セキュアコーディング、Webサーバの設定等は、対策の強化をすること。
44			WAFの導入の有無	WAFの導入は、有りとすること。
45	システム環境	システム制約/前提条件	制約条件(適用法)	一切の紛争は、日本の裁判所が管轄するとともに、契約の解釈が日本法に基づくものであること。