6.　システムの要件

6.1.　機能に関する要件

本システムに求める機能に関する要件を、別添資料２「機能一覧」に示す。

6.2.　帳票に関する要件

本システムから出力する帳票に関する要件を、別添資料３「帳票一覧」及び別添資料４「帳票項目一覧」に示す。

6.3.　情報・データに関する要件

本システムで取り扱う情報・データに関する要件を、別添資料２「機能一覧」、別添資料４「帳票帳票項目一覧」に示す。

6.4.　外部インタフェースに関する要件[13]

本システムは、以下のシステムとの連携を行う予定である。連携方式については、「教育情報アプリケーションユニット標準仕様　校務基本情報データ連携」を参照すること。

連携先	情報等	方向	方法	頻度
学齢簿管理システム	生徒名簿	受信	ＸＭＬ連携	年１回（４月）

6.5.　非機能要件

本システムに求める非機能要件については、地方公共団体本システム機構（Ｊ－ＬＩＳ）が公開している「非機能要求グレード（地方公共団体版）」に基づき要求事項を整理している。機器選定やシステム構成の設計等を実施するにあたり、遵守すること。

6.5.1.　可用性

	要素	要件
継続性	稼働率	年間のシステム稼働率は、99.5%[14]を目標とすること。
	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。
	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、６時間以内でのシステム復旧を目標とすること。
	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、全システム機能の復旧を実施すること。
	システム再開目標（大規模災害時）	大規模災害時、本システムに甚大な被害が生じた場合、本システムは、１ヶ月以内に再開することを目標とすること。
耐障害性	冗長化（サーバ機器）	本システムを構成する、サーバ機器の冗長化については、事業者による提案事項とすること。

[13] 連携するシステムについて、各システム名等を記載してください。該当するシステムがない場合は題目を削除してください。

[14] 年間計画停止時間 14.5 時間に相当します。

	要素	要件
	冗長化（ストレージ機器）	ネットワークを構成する伝送路（ＬＡＮケーブル等）の冗長化については、事業者による提案事項とすること。
	冗長化（ストレージのディスク）	本システムのストレージにおけるディスクの冗長化は、事業者による提案事項とすること。
災害対策	復旧方針	デスクアレイなどの外部記憶装置を物理的に複数台用意し、同一の構成で本システムを再構築すること。
	保管場所分散度（外部保管データ）	地震、水害、テロ、火災などの大規模災害時の業務継続性を担保するためのデータ保管先は、１ヶ所(遠隔地)とすること。
	保管方法（外部保管データ）	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、運用サイトとは別途で、媒体による保管により、データ・プログラムを保管する場所を設置すること。

6.5.2. 性能・拡張性

要素		要件
業務処理量	ユーザ数	本システムの利用者数については、「5.2. ユーザの規模及び場所」を参照すること。
	同時アクセス数	本システムの同時アクセス数は、「5.2. ユーザの規模及び場所」の情報に基づき事業者が算定、提案すること。
	データ量（項目・件数）及び増大率	本システムのデータ量及びデータ量の増大率は、本仕様書記載の情報に基づき事業者が算定、提案すること。
	オンラインリクエスト件数及び増大率	本システムのオンラインリクエスト件数及びオンラインリクエスト件数の増大率は、本仕様書記載の情報に基づき事業者が算定、提案すること。
	バッチ処理件数	本システムの業務処理件数及びバッチ処理件数増大率は、本仕様書記載の情報に基づき事業者が算定、提案すること。
	保管期間（データ）	バックアップデータの保管期限は、業務上の必要性を考慮した保管期間で保存できるように構築すること。
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、３秒以内を目標とすること。
	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、５秒以内を目標とすること。
	通常時バッチレスポンス順守度合い	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。
	アクセス集中時のバッチレスポンス順守度合い	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、再実行の余裕が確保できることを目標とすること。

6.5.3. 運用・保守性

運用・保守性に関する要件を以下に示す。

要素		要件
通常運用	運用時間	本システムの運用時間は、平日９時から 17 時とするが、定時外も頻繁に利用すること（１日 12 時間程度利用）を前提とすること。
	バックアップ取得間隔	バックアップの取得間隔は、日次で取得すること。
	外部データの利用可否	データ復旧の際、外部データは利用できない。
	データ復旧の対応範囲	バックアップの取得は、障害発生時のデータ損失防止を目的とすること。
	バックアップ自動化の範囲[15]	バックアップ自動化の範囲は、事業者による提案事項とすること。
	監視情報	エラー監視（トレース情報を含む）を行うこと。
保守運用	OS 等パッチ適用タイミング	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。
障害時運用	対応可能時間	システム異常検知時は、事業者の営業時間内で対応を行うこと。
	駆けつけ到着時間	システム異常時の駆けつけ到着時間は、保守員到着が異常を検知してから数時間内を目標とすること。
	障害検知通知	システムの障害を検知した場合には、受託者側の管理者に対してメール等で通知が届くなど、迅速に対応できる仕組みを構築すること。
運用環境	開発用環境の設置有無	本システムの開発用環境の設置は行わない。
	試験用環境の設置有無	本システムの試験用環境の設置については、事業者による提案事項とすること。
	マニュアル準備レベル	運用マニュアルについては、本システムの通常運用と保守運用のマニュアルを提供すること。
	外部システムとの接続有無	外部システムとの接続は行わない。
リモートオペレーション	リモート監視地点	事業者拠点等外部からリモート監視を行うこと。リモート監視に際しては、専用線やＩＰ－ＶＰＮ等の閉域網回線を利用すること。
	リモート操作時の接続方法	リモート操作の必要時のみ接続すること。
サポート体制	保守契約（ハードウェア）の種類	ハードウェア保守については、定額保守（オンサイト）とすること。[16]
	保守契約（ソフトウェア）の種類	ソフトウェアが法改正等によるバージョンアップした場合には、アップデートを事業者が実施すること。
	ライフサイクル	本システムのライフサイクル期間は、５年とする。

[15] クラウド利用時は記載不要です。
[16] クラウド利用時は記載不要です。

	期間	
	一次対応役割分担	一次対応については、すべて事業者が実施とすること。
	事業者側対応時間帯	一次対応における対応時間は、平日９時～17 時とすること。
	定期報告会実施頻度	運用の定期報告は、月１回程度実施すること。
	報告内容のレベル	保守の定期報告は、障害報告に加えて運用状況報告を行うこと。
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は、事業者のコールセンターにて行うこと。

6.5.4. 移行性[17]

要素		要件
移行時期	システム移行期間	既存システムから新システムへの移行期間は、１年未満とすること。
	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、利用の少ない時間帯（夜間など）とすること。
	並行稼働の有無	システム移行時の並行稼働期間は、XX ヶ月とすること。
移行対象（機器）	設備・機器の移行内容	現行システムで利用している、移行対象設備・機器のシステム全部を入れ替えること。
移行対象（データ）	移行データ量	現行システムから新システムへ 10TB 未満のデータを移行すること。
移行計画	移行のユーザ/事業者作業分担	現行システムから新システムへのデータ移行作業は事業者が実施すること。

6.5.5. セキュリティ要件[18]

要素		要件
前提条件・制約条件	順守すべき規程、ルール、法令、ガイドライン等の有無	本システムは、「〇〇県情報セキュリティポリシー」及び「「教育情報セキュリティポリシーに関するガイドライン」に準拠するよう構築すること。
セキュリティリスク分析	リスク分析範囲	システム開発実施において、セキュリティリスク分析を実施する範囲は、「〇〇県情報セキュリティポリシー」における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。
セキュリティ診断	Ｗｅｂ診断実施の有無	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。
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の適用は、定義ファイルリリース時に実施すること。
アクセス・利用制限	管理権限を持つ主体の認証	本システムの認証方法は、ＩＤ／パスワードによる認証とする。

[17] 現行の統合型校務支援システムからの移行が発生する場合のみ記載してください。
[18] 各自治体のセキュリティポリシーに照らして見直しを行ってください。

要素		要件
	システム上の対策における操作制限度	本システムの操作は、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。
データの秘匿	伝送データの暗号化の有無	伝送データの暗号化は、認証情報についてのみ実施すること。
	蓄積データの暗号化の有無	蓄積データの暗号化は、認証情報についてのみ実施すること。
不正追跡・監視	ログの取得	利用者のログイン・ログアウトや、重要なデータに対する操作を証跡として記録し、不正なアクセスに対する分析・調査が行えるようにすること。
	不正監視対象（装置）	ログを取得する装置の範囲は、「〇〇県情報セキュリティポリシー」における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。
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	Web アプリケーション特有の脅威、脆弱性への対策としてセキュアコーディングや Web サーバの設定等を講じることにより、安全性・信頼性を確保すること。
	ＷＡＦの導入の有無[19]	WAF（Web Application Firewall）の導入は行わない。

6.5.6. システム環境・エコロジー

要素		要件
システム制約/前提条件	構築時の制約条件	システム構築時には〇〇〇〇[20]に準拠すること。
	運用時の制約条件	システム運用時には、〇〇〇〇[21]に準拠すること。
システム特性	クライアント（端末）数	本システムで利用するクライアント（端末台数）については、本調達仕様書「5.2.ユーザの規模及び場所」を参照すること。
	特定製品の採用有無	（各自治体の調達方針に従って記載する）
適合規格	規格取得の有無(安全性)	（各自治体の調達方針に従って記載する）
	規格取得の有無（有害物質）	（各自治体の調達方針に従って記載する）
環境マネージメント	グリーン購入法対応度	（各自治体の調達方針に従って記載する）

[19] 外部ネットワークとの接続が発生する場合には導入を検討してください。
[20] 環境配慮のための規格等、各自治体で準拠すべき事項がある場合に記載してください。
[21] 運用にあたり各自治体で準拠すべき事項がある場合に記載してください。