公立大学法人島根県立大学
統合学生情報システムの更新，及び，
運用保守に係る仕様書

2023（令和 5）年8月

公立大学法人島根県立大学

＜目次＞

第1章 業務の件名

公立大学法人島根県立大学
統合学生情報システムの更新，及び，運用保守 業務

第2章 業務の概要

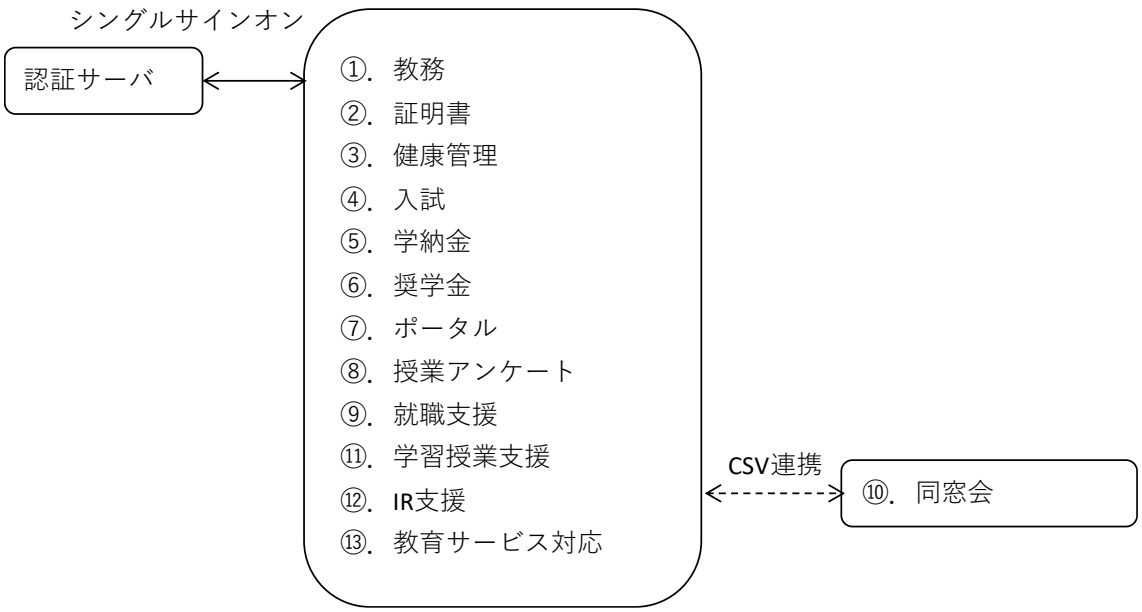
2.1 目的

2017（平成29）年度に更新した学生情報システムの賃貸借期間満了（6 年契約）に伴い，システムの機能強化，システム間連携の見直しを行うとともに，業務の効率化・省力化及び，学生・教職員へのサービス向上を図ることを目的にシステム更新を実施する。

(1) 既存システムの構成

(2) 現システムの構成及び更新範囲

現システムは下記の①～⑨システムに加え，2017（平成29）年度更新時から，⑪学習授業支援，⑫IR 支援，⑬教育サービス対応の 13 システムで構成され，①～⑨，及び，⑪～⑬システムは CSV ファイル連携の必要がない，1 つのシステムとして構成されるものとする。なお，⑩同窓会システムについては今回の更新対象外とし，既存のシステムを継続して利用する。また，既存システムと同様に，本学既設の認証サーバーを利用し，各サブシステム間の遷移は都度ログオンの必要のないシングルサインオンとする。



(3) システムの更新方針

①. 既存システムの賃貸借期間満了（2024（令和6）年 3 月末日）後の大学業務に支障がないよう，2024（令和6）年 4 月 1 日に確実にシステム全体を稼働させる。

②. 可能な限り，カスタマイズが不要なシステムを採用し，業務の標準化を行う。

③. スマートフォンやタブレットといったモバイル端末からの利用に対応し，情報を扱いやすくすることで業務の省力化を図る。

④. 大学 IR 機能等，一部の機能については，システム導入後に別途導入を検討する予定のため，システム導入後に大学 IR 機能等を付加できる汎用性のあるシステムに更新する。

⑤. システムの導入，テスト，教育，既存システムからのデータ移行，及び，稼働後の保守にかかる計画案作成と進捗管理については，授業や業務といった教職員本来の業務に支障をきたさぬよう，導入業者に主体となって発案，調整いただく。

⑥. ユーザーが新システムを効率よく，且つ効果的に利用できるよう，受託者は教職員への現地教育を定期的に行う。

⑦. 新システムは政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス上に構築を行うこと。障害発生からの復旧については，クラウドサービスの SLA を明示し，システムの可用性については別途協議とする。

⑧. 今後，本学が保有する別のシステムをクラウド化する際に，新システムと同じクラウド環境上に構築し，別の業者による保守を行うことができる環境とする。

⑨. 見積金額は新システムを稼働させるに必要なハード・ソフト，データ移行，構築作業，及び 6年間の保守費用等の経費すべてを含めた金額とする。すなわち，契約後からシステム稼働（2024（令和6）年 4 月 1 日）までの期間に，新たにシステム稼働のための追加作業が発生した場合の費用（電源工事など，建物に関する事象は除く）は，原則受託者負担とする。但し，大学事業拡大等の理由により，拡張が必要な場合はこの限りではない。

2.2 業務の範囲

本調達業務は，以下①～④の業務を委託するものである。

①. 機能要件，非機能要件を満たす新システムの構築・テスト（「第 4 章 機能要件」，「第 5 章 非機能要件」，「第 6 章 テスト要件」参照）

②. 既存システムから新システムへのデータ移行（「第 7 章 データ移行要件」参照）

③. 利用者への操作教育（「第 8 章 教育支援要件」参照）

④. 新システムの運用保守／問い合わせ対応（「第 9 章 運用保守要件」参照）

2.3 納入期限及び保守委託期間

(1) 納入期限

2024（令和6）年 3 月 31 日

受託者は，本調達機器等の設計，構築及び環境設定，動作検証，教育等を納入期限まで

に完了し，翌日から本学にて運用可能な状態にすること。

(2) 保守委託期間

2024（令和6）年 4 月 1 日から 2030（令和12）年 3 月 31 日迄の 6 年間を対象とする。

2.4 提示物及び成果物

受託者は以下の書類を紙媒体及び電子媒体（CD-R 又は DVD-R）にて各 3 部提出し，本学の承諾を得ること。なお，電子媒体については，本学のクライアント PC にて読み取り可能な形式（本学においては，マイクロソフト社製品の Office 及び PDF を標準としている。）で提出すること。なお，成果物の著作権は本学に帰属するものとする。

No.	提示物／成果物	記載内容	提出期限
1	作業体制表	本業務を遂行するための窓口責任者，業務従事者，業務分担，連絡先，及び，エスカレーションルール等を示す体制図が記載されたもの	契約締結後 10 日以内。体制を変更する場合は，直ちに書面により通知すること。
2	情報セキュリティ確保のための体制表	本学より提供された情報資産の取扱を示す体制図，本学より提供された情報資産の管理方法が記載されたもの	契約締結後 10 日以内。体制を変更する場合は，直ちに書面により通知すること。
3	保有資格証明書及び業務実績	本業務に従事する要員が保有する資格証明，業務経歴が記載されたもの	契約締結後 10 日以内。
4	第三者認証証明書	提案するクラウドサービスが保有する以下の第三者認証証明書 ・ISO/IEC 27001 認証 ・ISO/IEC 27017 認証，または，CS シルバーマーク	提案時
5	全体計画書	本業務の実施にあたり，本業務全体（開発／テストテスト／移行／教育）の工程，スケジュール，作業分担が記載されたもの	契約締結後 10 日以内
6	開発計画書	新システムを開発（設計・構築）する上での工程，スケジュール，作業分担が記載されたもの	開発開始の 5 日以上前

7	設計書（システム設計）	新システムに関わる以下の設計が記載された資料 ①. 製品名及び数量の一覧（返却の要否について記載すること。） ②. システム構成図 ③. ソフトウェアのバージョン ④. ソフトウェアの設定値 ⑤. 利用するユーザー一覧 ⑥. セキュリティ機能・脆弱性対策 ⑦. その他本調達の中で変更した設定	2023（令和 5）年 12 月 31 日
8	設計書（機能設計）	新システムに関わる以下の設計が記載された資料 ①. 要件定義 ②. 業務フロー ③. カスタマイズ一覧 ④. 画面・帳票一覧 ⑤. データ項目定義（画面・帳票のレイアウトや項目を含む） ⑥. ジョブ一覧(バッチ処理仕様含む) ⑦. 外部インターフェイス仕様 ⑧. 各種コンフィグシート（環境設定定義書等）	2023（令和 5）年 12 月 31 日
9	開発物	パッケージやカスタマイズとは別に，個別に開発した実行プログラムのソースコード一式	2024（令和6）年3月 31 日
10	テスト計画書	単体テスト，結合テスト，総合テスト，受入テストの実施スケジュール，実施内容，合否判定基準，他関連システムの動作確認の手順及びスケジュール等，テストの実施要綱。	テスト開始の 5 日以上前
11	テスト結果報告書	各テスト計画書に基づき行ったテストの結果が記載された資料・品質評価報告書	2023（令和 5）年 12 月 31 日
12	移行計画書	移行スケジュール（移行リハーサル含む），移行データ，移行手順，移行結果確認項目，コンティンジェンシープラン等，移行の実施要綱。	2023（令和 5）年 12 月 31 日
13	移行結果報告書	移行計画書に基づき行った移行の結果が記載された資料	2024（令和6）年3月 31 日

14	教育計画書	利用者（教職員），及び，システム管理者に対しての教育を行う工程，スケジュール，役割分担を記載したもの	教育開始の 5 日以上前
15	運用手順書（システム担当者用）	本学情報システム担当者が，日々の運用やメンテナンス時，障害等発生時に参照可能な以下の手順書。各手順は初心者でも操作可能な手順とし，印刷時に A4 サイズとなるようレイアウトすること。 ①. 起動・停止手順 ②. バックアップ・リストア手順 ③. エラー等ログ確認手順（障害発生時の一次切り分けに利用できる内容であること。） ④. 障害発生時の対応手順（役割分担，連絡先等） ⑤. その他運用に必要な手順	2024（令和6）年3月31 日
16	運用手順書（教員用）	本学の教員が本システムを利用する際に使用する手順書。手順書は実際の業務シナリオ毎に作成すること。	2024（令和6）年2月28 日
17	運用手順書（職員用）	本学の職員が本システムを利用する際に使用する手順書。手順書は実際の業務シナリオ毎に作成すること。	2024（令和6）年2月28 日
18	運用手順書（学生用）	本学の学生が本システムを利用する際に使用する手順書。手順書は実際の業務シナリオ毎に作成すること。	2024（令和6）年2月28 日
19	メンテナンス作業報告書	保守業務のメンテナンス対応を実施した結果が記載された資料	保守業務委託期間中の年度末
20	課題管理表	受託者と本学との間で行われた問い合わせ対応や障害対応の内容，及び，対応状況を一元的に管理するもの	契約締結後 10 日以内
21	協議議事録	受託者と本学との間で行われた協議の内容がまとめられたもの	協議より 5 日以内
22	その他	本学との協議のうえ，必要と判断された成果物	適宜

第3章 業務要件

3.1 共通要件

(1) 受託者は，本調達業務を開始するにあたり，本調達業務全体の計画書（工程表，スケジュール，役割分担を明記したもの）を作成・提出し，本学の承認を得ること。

(2) 受託者は，各工程の作業を開始するにあたり，開発計画書，テスト計画書，移行計画書，教育計画書をそれぞれ作成・提出し，本学の承認を得ること。

(3) 各工程表については，成果物と対応させたガントチャート形式で作成すること。

(4) 各計画書等は，作業の進捗状況にあわせ随時内容の更新及び詳細化を図ることとし，更新後の計画書等は，定例会等の機会を利用して，本学に報告・提出すること。

(5) 各作業に関する打ち合わせ，納品物等のレビュー及び作業進捗確認のため，本稼働までの期間においては，原則として隔週，定例会議を行うこと。

(6) 毎回の定例会議の議事録を，遅くとも次回定例会議までに作成し提出すること。

(7) 定例会議では，計画上のスケジュールと実際の進捗状況の差を明らかにし，その原因と対策を明らかにすること。発生した課題については課題管理表にて対応状況を一元的に管理すること。

(8) 開発工程中における仕様変更については，変更を少なくするための方策を提案すると共に，各フェーズにおける変更不可となる時点についての考え方を示すこと。

第4章 機能要件

機能要件については，別添の「機能要件一覧」を参照すること。

第5章 非機能要件

5.1 インフラ要件

(1) データセンター

受託者は本システムを運用するための環境として，以下の要件を満たすデータセンターを提供すること。

①. 業務システムが稼働するデータセンターは，国内に設置され，学術情報ネットワーク SINET6（以下，SINET という。）と直結した SINET クラウド接続サービス（L2VPN サービス）を用いて構築すること。

②. 業務システムが稼働するデータセンターとバックアップデータ保存用のデータセンターは BCP の観点から 200km 以上離れており，且つ，別の都道府県とすること。

③. 第三者認証として ISMAP(政府情報システムのためのセキュリティ評価制度)に準じていること。

(2) クラウドサービス

受託者は(1)のデータセンター上に，以下の要件を満たすクラウドサービスとして本システムを提供すること。

①. 提案するクラウドサービスは，本学と同等（学生数 3,000 人規模）以上の構築および運用実績があること。

②. 提案するクラウドサービスは，マルチテナントでの提供とし，かつ，他のクラウドサービス利用者のデータ操作（閲覧・編集）に影響をうけないこと。

③. クラウドサービスは，サーバーサービス，ネットワークサービス，監視サービス，及び，バックアップサービスから構成されること。

[④ 削除]

④. 一部の機能については本学 3 キャンパス内からのみ利用できるよう，学内からの通信と学外からの通信を分けること。

⑤. プライベートアドレスとグローバルアドレスのどちらも利用できること。

⑥. データが格納されたストレージは多重化し，暗号化を行うこと。また，バックアップデータのアクセス制限や暗号化に関して，元のデータと同等のセキュリティレベルを提供できること。

⑦. データの所有権または利用権はクラウド事業者側には生じないことを証明する書類を提示すること。

⑧. アプリケーションや本仕様書で定義する各種サービス（サーバー，ネットワーク等）のログの所有及び利用権は本学にあるものとし，所有権がクラウド事業者にあるログ（操作ログ，アクセスログ等）は本学にも閲覧権があること。なお，ログは 1 年間分のログファイルを残すこと。

⑨. クラウド事業者が事業を終了する場合，2 年前には終了を告知すること。

⑩. ユーザーの都合により契約を終了する場合やクラウド事業者が事業を終了する場合，サービス利用終了前にユーザーがデータを完全な形（ダウンロード，物理媒体の提供等）で取り出すことが可能なこと。

⑪. 将来的に，クラウドサービスのサービス提供終了や，クラウドサービス料の高騰が発生した場合等に，オンプレミスの環境や他社クラウドに移行させることが可能なこと。

(3) サーバーサービス

サーバーサービスは，以下のアプリケーションサーバー，データベースサーバー，テスト環境サーバー，中継サーバーの機能を有すること。

①. サーバーサービスに必要なリソースは，論理的に独立した構成であること。

②. アプリケーションサーバー，データベースサーバーの OS は，製品ベンダによるサポートを受けられる OS とすること。

③. 「4.3 応答性要件」を確保するためのリソースとして，アプリケーションサーバー，データ

ベースサーバーに必要な CPU，主記憶装置の構成を提案すること。

④. 本学業務の繁忙期等において，アプリケーションサーバー，データベースサーバーのスペックを変更できること。

⑤. データベースサーバーで稼働するデータベース管理システムは，製品ベンダによるサポートを受けられるデータベースソフトウェアとすること。

⑥. アプリケーションサーバー，データベースサーバーは共に高可用性を有し，物理サーバーのシステム障害時には，すぐに別の物理サーバーで復旧できること。

⑦. テスト環境サーバーは，稼働前及び稼働後に，本番系のシステムに変更を反映する前の動作確認をするために用いる環境である。この変更とは，プログラムの修正や，機能追加に加え，OS やミドルウェアへのセキュリティパッチ適用，パラメータ設定変更を含む，本番系のシステムに対して行うすべての変更作業を指す。上記の動作確認を受託者の環境で用意し，動作を担保できる場合に限り，テスト環境サーバーを当該調達に含める必要はない。

⑧. テスト環境サーバーは，「4.3 応答性要件」を満たす必要はない。但し，テスト環境サーバーへの負荷により，本番環境サーバーが応答性要件を満たさなくなることがない構成とすること。また，本番系のアプリケーションサーバー，データベースサーバーとは別の IP アドレスで構成し，それぞれに対してアクセス制御をかけられること。

⑨. 実運用に影響がないと判断される場合は，テスト環境サーバーを 1 台構成としてもよい。ただし，実運用に影響がないことを示す根拠資料を提案時に提出すること。

⑩. リモートメンテナンス用に中継サーバーを用意すること。原則として，OS やミドルウェアをメンテナンスする際は，各サーバーに直接アクセスするのではなく，中継サーバーを経由してアクセスするものとする。

⑪. 不正プログラム（ウィルス，ワーム，ボット等）の感染を防止するために，大学が保有するエンドポイントセキュリティ対策ソフトウェアを，すべてのサーバーに導入すること。なお，大学が保有する対策ソフトウェアを導入できない場合は，受託者にて適切なソフトウェアを用意すること。

(4) ネットワークサービス

ネットワークサービスは，以下の条件を満たすこと。

①. SINET からクラウドサービスへの接続は閉域網で接続すること。

②. SINET からクラウドサービスまでのネットワークは 100Mbps 以上の帯域保証型のネットワークを用意すること。なお，契約期間の中で，帯域保証の幅の増減を検討している。増減にかかる費用は当該調達に含める必要はないが，違約金なく変更ができるようにすること。

[③ 削除]

③. 学内からクラウドサービスへの接続は，SINET 網以外のネットワークを経由しないこと。ただし，インターネットに公開する機能へのアクセスは例外とする。

④. SINET 網内は，VLAN で論理的にネットワークが分離されていること。また，学内に設置

するクラウドサービス接続用の機器は，タグ VLAN が利用できること。

[⑥ 削除]

⑤. ファイアウォールの機能を持ち，送信元及び送信先 IP アドレス，送信元及び送信先 TCP ポート番号，送信元及び送信先 UDP ポート番号全ての組み合わせによって，クラウドサービスに対する通信の許可，拒否を設定することができること。

⑥. 大学とクラウドサービス間の通信を IPSec による AES256 形式で暗号化・復号化する機能を有し，セキュアな通信を行うこと。ただし，大学とクラウドサービス間を通るすべての通信プロトコルが暗号化されている場合に限り，IPSec による暗号化を不要とする。

なお，本業務の関係機器を本学のネットワークに接続する際は，本学の指示する方法で行うものとし，必要な UTP ケーブルや光ファイバは，受託者が準備すること。なお，新たに敷設する UTP ケーブルはカテゴリ 6A 以上のケーブルとすること。

(5) 監視サービス

以下の監視設定を行う機能を有すること。

①. 本クラウドサービスの死活状況，CPU 使用率，メモリ使用率，ディスク使用率，及び，ディスクキューまたはディスクビジー率を監視すること。

②. 上記①にて一定の閾値を超えた場合，本学より指定されたメールアドレスに通知メールを出すこと。なお，閾値は，本学情報システム担当者と協議の上決定すること。

(6) バックアップサービス

以下のシステムバックアップ／リストア，及び，データバックアップ／リストアを行う機能を有すること。

種類	要件
システムバックアップ／リストア	①. OS の状態，ネットワーク設定，ソフトウェアのパッチ等，日々更新が発生しないシステム上の設定を取得することを目的とする。 ②. システムバックアップ／リストアについては，本学情報システム担当者が手動で実行し，結果を確認できること。 ③. バックアップデータを，3 世代以上保管できること。
データバックアップ／リストア	①. アプリケーション上の各種データ，運用スクリプト，ログファイル等，日々更新が発生するデータを取得することを目的とする。 ②. バックアップで取得したファイルは，データセンター内及び，バックアップデータ保存用のデータセンターにコピーを行うこと。 ③. バックアップを実行する際，アプリケーションの停止を行う必要がないこと。 ④. バックアップは日次で自動的に実行され，バックアップの結果

	をメール等で本学情報システム担当者に通知すること。 ⑤. バックアップは原則夜間に実施し，翌日業務開始時刻までにバックアップ処理が完了すること。 ⑥. バックアップデータを，7 世代以上保管できること。 ⑦. リストアの際は，任意の世代のバックアップデータから必要なファイルのみを復元することができること。

5.2 信頼性要件

(1) 計画停止を除いたサービス稼働率は 99.9%以上であること。

(2) 計画停止は年に 4 回までとし，夜間（18 時～6 時）の間に実施すること。また，計画停止は大学における 10 営業日以上前に，本学情報システム担当者に電子メールで通知すること。

5.3 応答性要件

(1) 通常期の同時利用ユーザー数を 50 人，繁忙期の同時利用ユーザー数を 300 人とし，ともに以下の要件を満たすこと。

①. オンライン処理の応答時間は，全ての業務シナリオにおいて，クラウドサービス上での応答時間が 2 秒以内であるか，ネットワーク伝送時間を含めた応答時間が 5 秒以内であること。

②. データ量の多い日においても，バッチ処理の全体処理時間は 6 時間以内とすること。

5.4 拡張性要件

(1) 導入後，データ量の増加によりサーバースペックを拡張することになっても，プログラムやファイル等の改修なく対応できるようにすること。

(2) アプリケーションの構成は，データ管理部分，業務ロジック，ユーザーインタフェースを分離・分割し，相互の独立性を高めることにより，機能追加や保守作業に対する影響範囲を局所化でき，システムの改変に対する柔軟性が確保できるように配慮すること。

5.5 セキュリティ要件

(1) 本調達機器に対し，以下のセキュリティ機能を具体化し，実装すること。

①. 本調達に係る情報システムへのアクセスを業務上，必要な者に限るための機能。

[② 削除]

②. 本調達に係る情報システムにおけるセキュリティ事故及び不正の原因を事後に追跡するための機能。

(2) 本調達機器に対し，以下の脆（ぜい）弱性対策を実施すること。

①. 構築する情報システムを構成する機器及びソフトウェア（ミドルウェア，ファームウェアを含む）の中で，脆（ぜい）弱性対策を実施するものを本学と協議の上で決定し，納入期限まで

に対策処理を施すこと。

②. 脆（ぜい）弱性対策を行うとした機器及びソフトウェアについて，公表されている脆（ぜい）弱性情報及び公表される脆（ぜい）弱性情報を把握すること。

③. 把握した脆（ぜい）弱性情報について，対処の要否，可否を判断すること。対処したものに関して対処方法，対処しなかったものに関してその理由，代替措置及び影響を納品時に本学に報告すること。

(3) 本調達機器で利用する管理者ユーザーに対し，以下のとおり対応すること。

①. 管理者ユーザーの一覧を完成図書に含めること。

②. 管理者ユーザーのパスワードを適宜変更可能なように，変更に伴う影響範囲，及び，変更方法を文書化すること。

第6章 テスト作業要件

6.1 テスト計画

実施する単体，結合，総合，セキュリティ等のテストについて，テスト方針，テスト工程毎にテスト計画書として提出すること。また，本学が主体となって実施する受入テストについて支援すること。テスト計画書に記載すべき事項を以下に示す。

①. 受託者のテスト実施体制と役割

②. テストに係る詳細な作業及びスケジュール

③. テスト環境（テストにおける回線及び機器構成，テスト範囲）

④. テストに関するツール類（開発するプログラムの概略仕様も含め）

⑤. テストデータ

⑥. 評価指標

なお，パッケージを提案の場合，パッケージ部分について単体，結合テストは不要とする。

6.2 テスト実施要件

(1) テスト工程共通要件

各テストの各テスト工程において共通する要件を以下に示す。

①. 受託者はテストの管理主体としてテストの管理を実施すると共に，その結果と品質に責任を負い適切な対応を行うこと。

②. 受託者は本学及び関連する他システムに係る業者等との作業調整を行うこと。

③. 本学に対し定期進ちょく報告及び問題発生時の随時報告を行うこと。

④. 各テストを行うため，一連のテストケース（入力，出力及びテスト基準），テストシナリオ（例外処理を含む。），テストデータ，テスト評価項目及びテスト手順を各テスト実施前に作成の上，提出すること。

⑤. 各テスト終了時に，実施内容，品質評価結果及び次工程への申し送り事項等について，本学と協議の上，テスト実施報告書を作成すること。

⑥. 他システムとの接続テストを実施する際には，本学職員，当該システム開発及び保守業者と十分な調整を図り，受託者の負担と責任において実施すること。

⑦. テストに必要なプログラム類の開発ないし用意を行い，進捗を報告すること。

(2) テストデータ要件

テストにおいて使用するテストデータに係る要件を以下に示す。

①. テストデータは，原則として受託者において用意すること（受入れテストのデータについては本学と協議する）。

②. 本学のデータを利用する場合，本学担当者と協議の上，匿名加工などのしかるべき対応をとること。

③. テストデータの管理は，受託者が責任を持って行うこと。

(3) テスト環境要件

テスト環境に係る要件を以下に示す。

①. 単体，結合，総合，セキュリティテストの各テスト工程に必要な機器等は，受託者の負担と責任において準備すること。

②. 受け入れテスト時の電力，実施する場所は本学が提供する。それ以外の一切の必要経費は受託者の負担とすること。なお，受入テストの場所は，3 キャンパスを想定している。

③. テスト環境における受託者のセキュリティ要件は第9章の記述に従うこと。

(4) 総合テスト要件

総合テストに係る要件を以下に示す。

①. ソフトウェアが仕様に適合し，かつ本番環境で利用可能であることを確認できる評価指標を設定した上で，テストを実施すること。

②. 性能及び負荷のテストにおいては，本番環境と同様の環境により相応の負荷等をかけ，問題が発生しないことを確認すること。

③. 総合テストでは，を満たすことを確認すること。以下の項目について確認を行うこと。

（ア）機能性

- システム機能が，正常系，異常系共に仕様書どおりに動作すること。
- 他システムとの業務連携処理が正常に機能すること。

（イ）信頼性

- 信頼性要件を満たしていること。
- 障害が発生した際の回復処理が適切であること（バックアップデータを用いた回復処理を含む）。

- 情報セキュリティ要件を満たしていること。

（ウ）使用性

- 要件及び説明書どおりに動作し，利用者が利用しやすいこと。

（エ）機能性

- オンライン処理，バッチ処理の応答時間，スループットが適切であること。
- システムの限界条件（データ量，処理量）下で，正常に動作すること。

(5) セキュリティテスト要件

セキュリティテストに係る要件を以下に示す。

①. 開発したソフトウェアについて，攻撃手法（バッファーオーバーフロー，SQL インジェクション等）として既知である入力があった場合にシステムのセキュリティに影響を及ぼさないことを確認すること。

②. システムの動作環境又は動作前提であるハードウェア及びソフトウェアについて，既知の脆弱性が存在しないこと，及び既知の攻撃手法に対して脆弱な設定が行われていないことを確認すること。

③. ①及び②の確認は，適切なテストツールを選択して想定されるパターンを網羅的に行うこと。

④. セキュリティテストにおいて発見された脆弱性及び当該脆弱性に関して実施した対処について，テスト実施報告書に記載すること。

(6) 受入テスト支援要件

本学が主体となって実施する受入テストに係る要件を以下に示す。

①. 受入テストにおける具体的な手順及び結果を記入するための受入テスト手順書（案）を作成すること。なお，システム操作に精通していない職員でも分かりやすいテストとなるように工夫すること。

②. 受入テストは本学が主体となって行うが，本学の求めに応じて受入テストを支援するための要員を確保すること。

③. 受入テストで必要となるテストデータの準備を本学と協力し行うこと。

④. 受入テストで確認された障害について対応方針を提示し本学の承認を得ること。

⑤. 本学に承認された対応方針に従い，プログラム及びドキュメント等を修正すること。

第7章 データ移行要件

7.1 データ移行計画

以下を前提に移行計画書を作成し，それに基いて本学の了承を得ながら作業を進めること。

(1) 既存システムからのデータ移行は画像等の一部のデータを除き，原則として CSV 形式ファイル(テキストファイル)により行うものとし，CD-R 等のオフラインによるデータ交換を原則とする。データ移行においてはバッチ(一括)登録が可能であること。なお，既存システムからのデータ出力に関しては既存システム側で対応するため，本調達の範囲外とする。

(2) 現行システムからの情報・データの抽出に関しては，現行システム運用業者によって，一般的なファイル形式（フォーマット変換が必要な場合は受託者において作業を行うこと）にて抽出・提供までが行われることとする。現行システムからの移行対象データは原則すべてのデータとする。

(3) サービス系システムにおける「お知らせ機能」，「掲示板機能」，「スケジュール機能」等については別途大学側と協議のうえ移行範囲を決定するものとする。

(4) 受託者は，抽出されたデータを受領することを前提に，必要に応じ，本システムデータベースへの移行プログラムの設計・開発，移行後のデータに関する正当性確認プログラムの設計・開発等，移行にあたって必要となる各種作業を実施すること。

(5) 受託者は，(1)(2)のデータ・プログラムを前提に，現行システムで利用している情報データを新システムのデータベース等へ移行し，付随する各種作業を実施すること。

(6) 移行データ提供時期，回数は大学側と協議の上決定すること。

(7) 移行は，2024（令和 6）年 3 月 31 日までに実施すること。

(8) 本稼働後の数日間は本学にて稼働立ち合い，及び，障害対応を行うこと。

7.2 データ移行対象データ

(1) 移行対象データは，3 キャンパス合計で 9,930 人分程度であり，内訳は以下のとおりである。

キャンパス	在学生及び卒業生	2024（令和6）年度新入生
浜田キャンパス	5,400 人程度	250 人程度
松江キャンパス	4,500 人程度	200 人程度
出雲キャンパス	3,000 人程度	150 人程度

(2) 既存システムに登録されている学籍番号は以下の形式を使用しており，システムはこれらの形式を変更することなく管理できること。また，今後，桁数の増加やファルファベットを取り入れる形式に変更する可能性があるため，そのような形式にもプログラムを改修することなく管理できること。

キャンパス	既存システムから出力される様式
浜田キャンパス(～H19)	[学部コード][入学年度][通し番号]・・・・数字のみ 8 桁
松江キャンパス(～H19)	[入学年度][学科・専攻コード][通し番号]…数字のみ 5 桁
出雲キャンパス(～H19)	[入学年度] [通し番号] [学科・専攻コード] …左から5桁数字，末尾英字1文字　計6桁

全キャンパス共通(H20～)	[入学年度][学部・学科・専攻コード][通し番号] ・・・・数字のみ7桁

7.3 次期システムへのデータ移行支援

(1) 機器内の電磁的記録について，次期システムへの移行のために必要なものを大学指示に従い提出すること。

(2) 次期システムへの移行のために必要な技術情報の提供を行うこと。

第8章 教育支援要件

次期システムを本稼働するにあたり，利用者が不便なく操作できるよう，本稼働前後に十分な教育を行うこと。また，本稼働後も定期的に利用者教育を行うこと。回数や実施形式については大学と協議の上，決定すること。

(1) 情報システム担当者に対する教育

初回のみ，完成図書（設計書／運用手順書）について講習会を行うこと。特に，本稼働後に情報システム担当者が OS やミドルウェアを直接操作して，バッチを実行したり，ログを取得したりする必要がある場合は，手順書を作成した上で，説明を行うこと。

(2) 教員に対する教育

年 1 回集合研修。ただし初回は，本システムの操作を習得するために必要な教育を全てのキャンパスで行うこと。

(3) 職員に対する教育

年 1 回集合研修。ただし初回は，本システムの操作を習得するために必要な教育を全てのキャンパスで行うこと。

(4) 学生に対する教育

初回のみ，学生が利用する機能を教職員に対して，講習すること。

第9章 運用保守要件

9.1 共通事項

(1) 受託者は，本章に記載する，問い合わせや，変更要求，障害対応要求など，各種保守対応を無償で実施し，各種対応は，保守業務時間帯（「第 9 章 作業体制及び方法」に定義）の中で行うことを原則とする。ただし，障害対応等および本学が緊急かつ業務に支障を来すと判断した場合はこの限りではない。

(2) 受託者は，依頼された保守対応について課題管理表にて案件管理を行い，最新の対応状況や対応内容を一元的に把握できるように努めること。

(3) 障害対応やソフトウェア適用など，対象装置への変更を行う際には，原則，検証を行った上

で，必ず事前に大学の承諾を得てから作業を行うこと。

(4) 受託者は，保守システムの設計，マニュアル等に変更が発生した場合，随時，完成図書への反映を行うこと。

(5) 受託者は，保守システムで利用するクラウドサービスに対する問い合わせも一元的に受け付け，保守対応を行うこと。

(6) 年一回程度，運用全体に係る定例会議を開催し，運用状況の報告及び改善提案等を行うこと。

9.2 問い合わせ対応／軽微な変更作業

(1) 本学担当者から対象装置に関する運用方法や技術的な問い合わせを受けた場合，過去実績や調査結果を基に，速やかに適切な応答をすること。

(2) 問い合わせに対する一次回答は 1 営業日以内とし，1 ヶ月以内の対応完了を目指すこと。

(3) 本学は，年に1回，休日における停電を予定している。当該日に障害が発生した際には，問い合わせを受け付け，必要に応じて，保守対応を行うこと。

9.3 障害対応

(1) 受託者は，対象装置に関する障害を受け付け，復旧に向けて適切かつ迅速な対応を行うこと。

(2) 障害発生時には，本学及び障害に関連する保守業者等と綿密な調整・連携を行い，受託者の責任と負担で保守作業を行うこと。

(3) 障害発生時の問い合わせの受付は，土日・休日を除く，平日 9 時～17 時を基本とする。

(4) 障害発生の問い合わせを受け，24 時間以内に一次回答を提示すること。

(5) 障害発生の問い合わせを受けてから，4 時間以上復旧が見込めない場合は，代替手段を本学と検討，適用し，本学の業務に支障が出ないよう対応すること。

(6) 復旧作業においては，本学と協議のうえ，取得済みバックアップデータからのリカバリや手動による縮退運転移行等の復旧操作を実施すること。

(7) 発生した障害に対して解析を行い，原因を究明し，復旧を行うこと。また，予防のための情報収集を行い，再発防止策を検討すること。

(8) 当該年度実施した障害対応について，作業報告書を作成し，本学に報告すること。

(9) すべての障害は1ヵ月以内に解消すること。ただし，障害の重要度に応じて大学と優先順位と対応期限を協議すること。

9.4 メンテナンス対応

(1) 対象装置に関してシステムが安定稼働するよう，4 ヶ月に1回以上，以下のメンテナンス対応を行い，本学と協議の上，原則として受託者にて実施を行うこと。

①. 機器のファームウェアアップデート

②. OS, ミドルウェアのアップデート
③. 納入したソフトウェアに対する修正パッチの適用
④. 不正アクセス, 重大エラーの有無の確認, 及び改善対応
不正アクセス及び重大エラーは, OS, ミドルウェア, アプリケーションそれぞれについて, 確認を行うこと。
⑤. ディスクの空き容量等の確認, 及び改善対応
⑥. ディスク, ネットワークトラフィック状態等の確認, 及び改善対応
⑦. 運用に影響を及ぼす恐れのあるセキュリティ情報の提供, 及び改善対応
⑧. 対象装置のシステムバックアップの取得

(2) 当該年度実施したメンテナンス対応について, 作業報告書を作成し, 本学に報告すること。なお, 改善対応を行わなかったものについては, 作業報告書にその理由, 代替措置及び影響を明記すること。

9.5 その他運用支援

(1) 対象装置について, 技術支援, 技術情報提供, 及び, システム全般にわたる運用支援を行うこと。

(2) 障害の切り分け等において, 本学やその他関係業者から協力を求められた場合には, 必要な協力を行うこと。

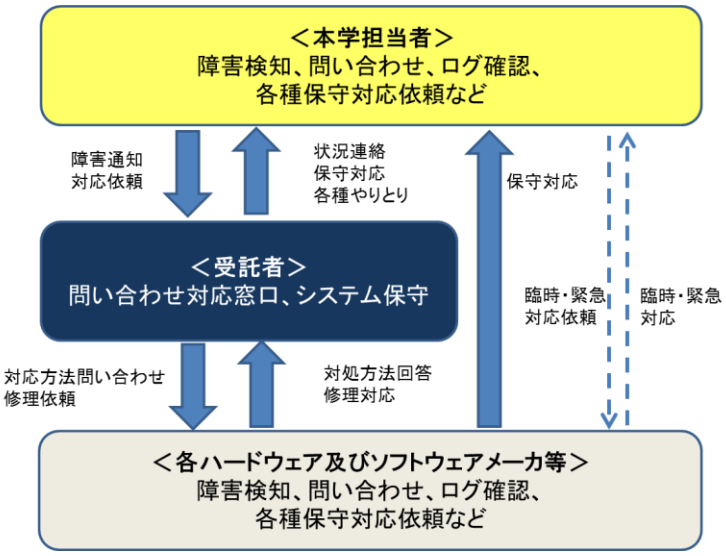
(3) 本学が指定する業務イベントの際には各キャンパスに担当者を派遣し現地で運用支援を行うこと。対象のイベントは, 新入生登録, 各種テストデータ取り込みを想定しているが, その他本学と協議のうえ, 必要と判断される場合は現地にて運用支援を行うこと

(4) 運用対象システムに対するセキュリティ監査において, 本学から以下に示すような指示があった場合は, それに従って支援を行うこと。
①. 監査人への資料の提示
②. 監査人によるヒアリングへの対応
③. 監査人による視察における立ち合い

第10章 作業体制等

10.1 作業体制

(1) 受託者は，以下に示す条件を満たす作業体制を構築すること。受託者は，本学情報システム担当者のほか，下図の関連業者と一体となって相互に協力しつつ本件業務を適切に行わなくてはならない。



(2) 受託者は，別紙「情報セキュリティ遵守に関する特記事項」を遵守するよう体制を整備すること。

(3) 受託者は，統括責任者，主任技術者，構築要員から成る業務体制を設けること。責任体制を明確にするため，担当者名，役割等を明記した業務体制図を本学に提出し，発注者の承認を受けなければならない。変更の際も同様とする。

(4) 統括責任者及び主任技術者は，受託業者内社員から選定し，責任を持って業務を遂行すること。

(5) 統括責任者は，契約の履行に関し，プロジェクト全体に渡りマネージメントを行うものとし，発注者に対する統括窓口としての役割を担う。運用保守期間も同様である。

(6) 原則として即時に責任ある答弁が可能な者を統括責任者とし，本学からの業務等に対する問い合わせに対し，速やかに対応すること。

(7) 統括責任者は業務の進捗状況全体を把握し，本学に対して内容及び結果を本学へ定期的に報告すること。

(8) 主任技術者は，発注者からの要望を聞き取り，分析の上，実装設計を行い，構築要員に作業内容の詳細指示を行う者をいう。また，統括責任者と情報共有を行い，緊急時で統括責任者不在の場合，統括責任者に代わり窓口応対を行うものとする。

(9) 本契約の履行に際し，受託者は，本学内での構築作業実施時に主任技術者又は統括責

任者を本学に常駐させること。

(10) 本仕様の質疑については，あらかじめ本学の指示を受けること。ただし，軽微でない事項については本学と協議し，両者合意の上，作業するものとする。

(11) 受託者は施工にあたり，法令に定められた手続きが必要な場合，関係各所に対し必要な手続きを行うこと。また，手続き完了後は本学に報告すること。

(12) 本件業務の体制を変更する場合は，変更する1週間前までに後任者の報告を行い，書面をもって本学の承諾を得ること。なお，担当者交代の際には，本件業務に支障を来たさないように十分な訓練を行った後，後任者に引継ぎを行い，本学に引継ぎ経過を報告すること。

(13) 本件業務の対象システムに受託者以外の製品が含まれている場合，製品に関する問い合わせや修理依頼は，受託者が窓口となって対応を行うこと。

(14) 本学と受託者において協議を行った際には，受託者より協議の結果を文書あるいは電子メール等にて2営業日以内に提出し，本学の承認を得ること。

10.2 作業者の実務実績・資格要件

(1) 構築作業及び保守，運用支援に従事する要員は，以下に示す実績・資格を有する作業者を配した作業体制とすること。

①. 本システムと同規模以上のシステムの構築作業及び運用管理支援業務に関与した経験を有すること。

②. 統括責任者または主任技術者は，本システムと同規模以上のプロジェクト管理経験を有する者であり，経済産業省情報処理技術者プロジェクトマネージャ保有者から選任すること。

③. 統括責任者または主任技術者は，本システムと同規模以上の構築経験を有する者であり，経済産業省情報処理技術者ネットワークスペシャリスト（テクニカルエンジニアネットワーク）から選任すること。

④. メンバー内に，セキュリティ設計担当者として，情報処理安全確保支援士試験（情報セキュリティスペシャリスト，テクニカルエンジニア情報セキュリティ）保有者を加えること。

⑤. 統括責任者と主任技術者は，同一人物による兼務は不可とする。なお，セキュリティ設計担当者は兼務可とする。

10.3 作業実施環境

(1) 作業及び保守を行う場所は，原則，本学内とする。なお，トラブルや問い合わせ受付業務など，上記の作業場所以外でも業務遂行が可能な作業については，受託者の負担により用意した，入退室管理，端末等の盗難防止策等の対策を行い，別紙「情報セキュリティ遵守に関する特記事項」を満たす場所で実施することも可能とする。

(2) 受託者が本業務を実施するために，本学の敷地内の作業場所を使用する場合は，作業場所を整理・整頓し，安全に留意して事故の防止に努めるとともに，労働基準法・労働安全衛生法を遵守して安全の徹底を図り作業すること。また，本学が用意する設備や環境を使用する

際は，十分な注意を払って適切に使用し，本件委託業務以外の目的に使用しないこと。

(3) 受託者は本業務を土日及び祝祭日を除く平日の 9:00～17:00，または本学及び受託者において協議・合意した実施日時に行うこと。ただし，障害対応等および本学が緊急かつ業務に支障を来すと判断した場合はこの限りではない。

(4) 本作業に必要な工具，ケーブル等は受託者の負担とし，導入のために機器等の追加が必要な場合は，受託者の負担において準備し，作業終了後に撤去すること。

(5) 既設建物(特に室内装飾)を汚損又は破損しないように細心の注意をもって行うこと。また，受託者の責めに帰す事由による構造物及び道路の損傷，土地の踏み荒らし等，第三者に与えた損害に対する費用等は全て受託者の負担とする。

10.4 その他

(1) 本仕様書に基づく作業に関し，第三者との間に著作権に係る権利侵害の紛争等が生じた場合は，当該紛争の原因が専ら本学の責めに帰す場合を除き，受託者の責任と負担において一切の処理をすること。

(2) 本仕様書に記載なき事項でも，本調達機器の構築・稼働・運用に必要な物品の納入，調整作業等については，受託者の負担において用意すること。