

教務情報システムの基盤構築・保守一式
調達仕様書

令和4年1月
放送大学学園

目次

1	調達案件の概要に関する事項	1
1.1	調達件名	1
1.2	調達の背景	1
1.3	目的	1
1.4	業務・情報システムの概要	2
1.5	構築、賃借及び運用保守契約期間	2
1.6	作業スケジュール	3
2	調達案件及び関連調達案件の調達単位、調達の方式等に関する事項	4
2.1	調達案件及びこれと関連する調達案件の調達単位、調達の方式、実施時期	4
(1)	調達案件名	4
(2)	調達の方式	4
(3)	実施時期（予定）	4
(4)	補足（用語の定義等）	5
2.2	調達案件間の入札制限	5
3	作業の実施内容に関する事項	6
3.1	作業の内容	6
(1)	設計・構築・テスト	6
(2)	運用保守	10
(3)	留意事項	13
3.2	成果物の範囲、納品期日等	14
(1)	成果物	14
(2)	納品方法	15
(3)	納品場所	15
(4)	支払条件	16
(5)	満たすべき要件に関する事項	16
(6)	作業の実施体制・方法に関する事項	16
(7)	作業の実施に当たっての遵守事項	18
(8)	成果物の取扱いに関する事項	19
(9)	入札参加資格に関する事項	19
(10)	再委託に関する事項	20
(11)	附属文書	21

別紙一覧

- 別紙① 次期システム WAKABA 基盤の作業範囲
- 別紙② 周辺機器一覧
- 別紙③ 学習センター住所一覧
- 別紙④ 導入台数一覧
- 別紙⑤ クラウド要件一覧
- 別紙⑥ 要件定義書

1 調達案件の概要に関する事項

1.1 調達件名

教務情報システムの基盤構築・保守 一式

1.2 調達の背景

放送大学学園(以下「本学園」という。)は、社会人や女性の学び直しの学修機関として、また高齢者が主体的に学んだ結果を社会参画・社会貢献に繋げられるような学生相互のコミュニティの形成支援や活動支援等を行う機関としての果たすべき役割も大きく、女性、社会人、高齢者等、生涯現役・全員参加型社会への転換に貢献すべく社会人等がより学びやすい環境の整備に取り組んできたところ、今後も継続的に当該環境の整備や発展に取り組むことを必要としている。

これまで様々なニーズに応えるため、本学園は、オンライン授業への柔軟な対応、各種電子化の推進、学習センター等間の情報の共有化、スマートフォンの普及に代表される急速に発展した ICT 技術への対応などを積極的に進めていくこととし、環境変化への適用強化や業務の変容に柔軟に対応すべく、平成 30 年 3 月末までに現在の教務情報システム(以下「システム WAKABA」という。)を新たに開発した。

平成 30 年 4 月から運用を開始した現在のシステム WAKABA は、毎年適宜改修をしながら業務への対応を図ることにより本学園の業務の遂行に一定の貢献を果たしてきたところであるが、昨今の ICT 技術の動向を踏まえ、セキュリティやユーザビリティの更なる向上等を目的とした更改開発を令和 5 年 4 月 1 日からの運用開始に向けて進めている。

一方、現在のシステム WAKABA が稼動しているハードウェア(各学習センターに配置したプリンタ等含む)(以下「システム WAKABA 基盤」という。)については、令和 5 年 3 月末をもって貸借の期限を迎えるため、新たなシステム WAKABA 基盤(以下「次期システム WAKABA 基盤」という。)を調達する必要がある状況である。

1.3 目的

次期システム WAKABA 基盤には、変容する本学園の業務に対応する拡張性、職員、教員及び学生が快適に操作できる性能、高度化するセキュリティ脅威への対応の実現が必要である。また、システム WAKABA は、長きに渡り安定的に使用できるシステムであることを目指していることから、その基盤である次期システム WAKABA 基盤について、昨今のデジタル技術等の動向を踏まえ、クラウド上に構築することを本調達の目的とする。

さらに、稼動開始後の安定運用の実現を本調達の目的とする。

1.4 業務・情報システムの概要

次期システム WAKABA 基盤の概要は図 1 のとおりである。

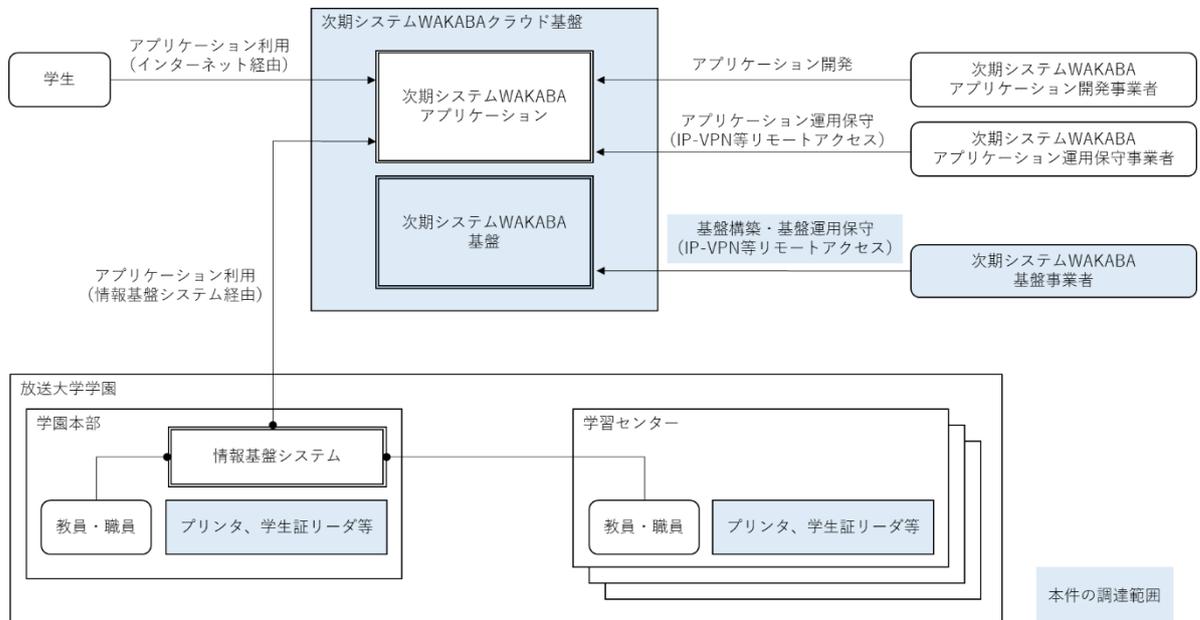


図 1 次期システム WAKABA 基盤の概要

1.5 構築、賃借及び運用保守契約期間

構築期間 : 契約締結日 ~ 令和 5 年 3 月 31 日

賃借及び運用保守期間 : 令和 5 年 4 月 1 日 ~ 令和 10 年 3 月 31 日

1.6 作業スケジュール

作業スケジュールは図2のとおりである。

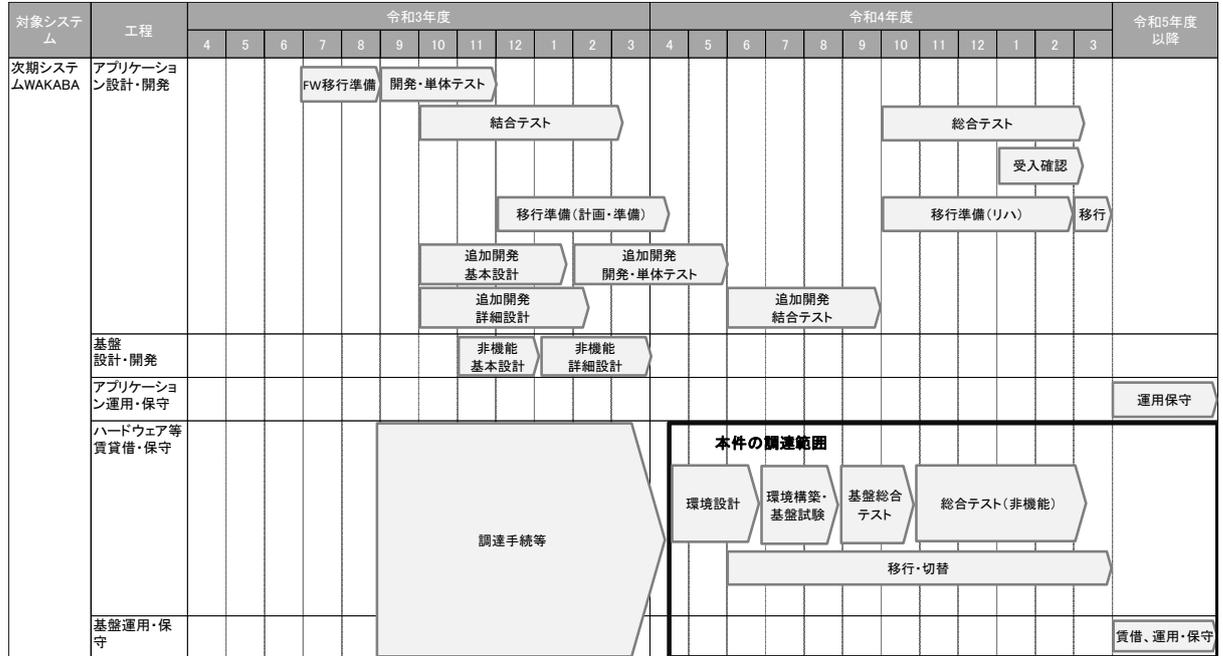


図2 作業スケジュール

2 調達案件及び関連調達案件の調達単位、調達の方式等に関する事項

2.1 調達案件及びこれと関連する調達案件の調達単位、調達の方式、実施時期

関連する調達案件の調達単位、調達の方式、実施時期は表1のとおりである。

表1 関連する調達案件の調達単位、調達方式、実施時期

No	調達案件名	案件開始	案件終了	補足
1	教務情報システム のアプリケーション 更新開発に関する 調達一式	令和3年 6月22日	令和5年 3月31日	次期システム WAKABA のアプリケーションを開発。株式会社エヌ・ティ・ティ・データが受託。
2	教務情報システム のアプリケーション 運用保守に関する 調達一式	令和5年 4月1日	令和10年 3月31日	No1にて開発したアプリケーションの運用及び保守を実施。

上記各調達案件の受託者は、本書において以下のとおり呼称する。

- ・上表 No1 の受託者：「AP 開発事業者」
- ・上表 No2 の受託者：「AP 運用保守事業者」

(1) 調達案件名

教務情報システムの基盤構築・保守 一式

(2) 調達の方式

一般競争入札

(総合評価落札方式(技術点と価格点の配点割合を1:1とする加算方式))

提案書等の審査要領は本学園にて別途定める。

(3) 実施時期(予定)

意見招請：令和3年11月上旬～11月下旬

入札公告：令和4年1月下旬～令和4年3月中旬

開札：令和4年4月上旬

(4) 補足（用語の定義等）

用語の定義は表 2 のとおりである。

表 2 用語の定義

用語	用語の説明
現行システム WAKABA	職員、教員、学生を支援し、教務情報を管理する現在のシステム。平成 30 年 4 月から運用している。
次期システム WAKABA	令和 5 年 4 月の運用開始に向けて開発が進められている、現行システム WAKABA の更改システム。
情報基盤システム	学園内ネットワーク、事務及び学生用 PC、LDAP 認証基盤、SSO 認証基盤を有する各種業務の基盤となるシステム。

2.2 調達案件間の入札制限

相互牽制の観点から相互に入札制限の対象とする調達案件は無い。

3 作業の実施内容に関する事項

3.1 作業の内容

(1) 設計・構築・テスト

① 設計・構築・テスト実施計画書等の作成

受託者は、本業務を遂行するにあたり、設計・構築・テストにおける実施計画書等を作成し、本学園に報告・協議・修正の上、速やかにキックオフ会議を開催し、本学園から実施計画書等の承認を受けること。

② 設計

受託者は本調達仕様書に基づき、次期システム WAKABA を動作させるために必要となるサービス及び機器等を技術提案に基づき発注し、当該サービス及び機器等についての環境設計（環境定義書及びシステム管理台帳の作成）を行い、本学園に報告して承認を受けること。また、発注するサービス及び機器等に基づき、次期システム WAKABA 基盤を運転するための具体的な運用マニュアルを整備すること。

環境については、クラウド環境を採用すること。クラウド環境を採用する条件は、別紙⑤「クラウド要件一覧」に記載の条件を満たすこと。

発注するサービス及び機器等は、現行システムのハードウェア、ソフトウェア、ネットワーク要件等に準じ、本調達仕様書に示すクラウド、周辺機器要件（別紙②「周辺機器一覧」、別紙③「学習センター住所一覧」、別紙④「導入台数一覧」）及び要件定義書（別紙⑥「要件定義書」）を満たすもので、次期システム WAKABA 稼動開始後から継続して5年間保守サービスを提供できるものを基本とする。5年間保守サービスを継続できない等、要件と異なるサービス及び機器等を選定する場合は、当該サービス及び機器等を選定する必要性、保守サービスを受けられないことへの対策等を検討の上、本学園へ説明し、承認を受けること。

なお、AP 開発事業者から非機能要件に関する詳細設計書が提示される。受託者が選定を検討したサービス及び機器等が、当該詳細設計書に示された事項を満たせることを確認し、問題がある場合は AP 開発事業者と協議した上で、対策を検討し、本学園へ報告・協議の上、対策を実行すること。また、受託者は、本学園からサービス及び機器等に関する設定情報の変更要望を受けた場合は、必要に応じて協議の上、環境定義書の更新を行うこと。

③ 環境構築・基盤テスト

受託者は、本調達仕様書に示すクラウド要件及び要件定義書に示す要件を満たす回線を準備した上で、発注したサービス及び機器等の搬入、設置、ラッキング、信号ケーブル・電源ケーブル接続及び関連する各種調整を実施すること。ま

た、環境定義書に基づき、各種ソフトウェアをインストール・設定して、次期システム WAKABA 基盤の環境を構築すること。なお、令和 4 年 9 月末までに学園本部とデータセンター間及びデータセンターと AP 開発事業者拠点間の回線を開通させること。ただし、AP 開発事業者拠点に設置するネットワーク機器及びデータセンターと AP 開発事業者拠点間の回線は受託者が準備する。

構築した環境について、環境定義書のとおり設定されていること並びにハードウェア及びソフトウェアが単体で正常に動作することを確認するため、基盤テストを実施すること。基盤テストにおいては、環境定義書に基づき、テスト観点、テスト項目、合否判定基準等を定めたテスト項目表を作成し、本学園の承認を受けた上でテストを実施し、品質評価として不具合の件数、発生理由及びその対応状況等の結果を本学園に報告すること。テスト結果が合格とならなかった場合は、適切な対策を検討して本学園へ報告し、指定された期限内に合格となるよう問題を解決すること。

また、システム基盤制御機能の開発として、AP 開発事業者が作成した非機能要件に関する詳細設計書に基づき、システム基盤制御を効率化するために必要なシェルプログラム（起動・停止、ログローテーション、バックアップ等）のプログラム設計、製造、単体テストを実施すること。

④ 基盤総合テスト

受託者は、システム基盤として必要な機能（監視機能、バックアップ機能等）を確認するため、基盤総合テストを実施すること。さらに、次期システム WAKABA のアプリケーションプログラムを本調達範囲内の必要な機器へインストール・設定すること。なお、次期システム WAKABA アプリケーションのインストール・設定に際し、本学園及び AP 開発事業者と協議の上、AP 開発事業者よりパラメータ及び次期システム WAKABA アプリケーションプログラムを受領すること。令和 4 年 10 月末までに次期システム WAKABA アプリケーションプログラムの動作確認を完了させ、基盤環境のバックアップを取得した上で、AP 開発事業者が利用可能な状態として引き渡しを行うこと。ただし、AP 開発事業者からの次期システム WAKABA アプリケーションプログラムの提供が遅れる場合の期日についてはこの限りではない。なお、動作確認の内容については AP 開発事業者と調整の上、対応することとし、AP 開発事業者の指定する代表的なシナリオ試験を実施することを想定する。

基盤総合テストの実施にあたっては、非機能に関する詳細設計書、要件定義書に基づき、テスト観点、テスト項目、合否判定基準等を定めたテスト項目表を作成し、本学園の承認を受けた上でテストを行い、品質評価として不具合の件数、発生理由及びその対応状況等の結果を本学園に報告すること。テスト結果が合

格とならなかった場合は、適切な対策を検討して本学園へ報告し、指定された期限内に合格となるよう問題を解決すること。

なお、基盤総合テストに係るテスト項目表の作成にあたっては、AP 開発事業者が実施する総合テストとの重複を避けるため、本学園及び AP 開発事業者と十分に協議すること。

⑤ AP 開発事業者の総合テスト支援及び非機能要件に関わる総合テストの実施

受託者は、AP 開発事業者が実施する総合テストにおいて、AP 開発事業者と各種調整の上、AP 開発事業者が作成するテスト計画書やテスト結果報告書の作成支援を行うこと。AP 開発事業者が実施する各種総合テストについて、一時的な環境設定を変更する場合には環境の準備（設定作業の実施、変更内容の管理）、環境の戻し等を実施すること。また、AP 開発事業者が実施する各種総合テスト中に問題が発生した場合は、問題の切分け及び原因調査に協力すること。問題の原因が、受託者の委託範囲である場合は速やかに回復措置を講じること。

受託者は、性能テスト等の非機能要件に関わる各種総合テストを実施すること。また、テストの結果、設定変更及び対処が必要となった場合、チューニング等の対応を行い、環境定義書を修正すること。性能テストにおいては、AP 開発事業者と連携し、業務のロジックやデータベースの構成等を把握した上で、シナリオの作成や資材準備、テストを行うこと。

また、基盤総合テスト終了後からサービス開始前の期間においても、ウイルス定義ファイル、セキュリティパッチ等の適用、ハードウェア等の死活監視、障害発生時には環境設定情報、ログの取得、分析及び対処等の作業を行うこと。

⑥ 現行システム WAKABA から次期システム WAKABA への切替

受託者は、本学園及び AP 開発事業者と協議の上、データ移行及びシステム切替における、リハーサル及び本番システムへの切替計画（切替にあたって必要となる資材、切替手順、コンティンジェンシープラン等を含む）を策定し、本学園の承認を受けること。また、切替にあたって関連事業者（現行システム WAKABA の保守事業者及び連携対象システム保守事業者等）が実施する必要がある作業の内容、時期、頻度等を本学園へ報告するとともに、本学園が行う当該関連事業者との調整を支援すること。

受託者は、切替計画に基づき、切替リハーサル及び本番システムへの切替作業を実施し、リハーサル又は本番切替後に次期システム WAKABA が正常に動作することを、チェックリストで確認すること。（具体的なチェック項目は、次期システム WAKABA のアプリケーションが正常に画面表示されること等、基盤業者として確認できる程度の内容を想定している。）

切替リハーサルは、本番切替と同様の資材、切替手順にて実施し、問題が発生した場合は原因と解決策を検討し、切替計画を更新して本学園の承認を受けること。本番切替後は、切替計画通りに切替できたかどうか、問題発生件数、発生理由及びその対応状況等の結果を報告書として取りまとめて本学園へ報告すること。

関連事業者が実施する作業に要する費用は本調達の範囲外とする。次期システム WAKABA 及び関連事業者との接続、役割分担については別紙①「次期システム WAKABA 基盤の作業範囲」のとおりとする。

⑦ 学習センター設置機器の切替

受託者は、各学習センター及びサテライトスペース（以下「学習センター等」という。）の現地調査を行い、各学習センター等と協議して、機器設置レイアウト、機器交換の日程等の計画を作成し、本学園の承認を受けること。

なお、設置する機器の詳細、設置先、設置台数については、別紙②「周辺機器一覧」、別紙③「学習センター住所一覧」、別紙④「導入台数一覧」に示す。また、学習センター等に設置する機器の切替は、次期システム WAKABA への切替日と同日に実施する想定である。

また、受託者は各学習センター等及び本部に既設の端末ヘドライバソフト等のインストール作業を実施すること。インストール作業に必要な各種情報等については本学園より受領すること。

⑧ 運用リハーサルの実施

受託者は、本番システムへの切替後の運用に備え、「② 設計」において作成した運用マニュアルを用いて、本番運用と同様の運用リハーサルを実施し、運用マニュアルに不備があった場合は修正を行うこと。運用リハーサルの計画及び結果は、本学園へ報告し、承認を受けること。

また、受託者は次期システム WAKABA 基盤の構成情報を管理するため、システム管理台帳を作成すること。

⑨ セキュリティ診断及び脅威への対策

受託者は、本番運用の開始前に、第三者組織（※注）によるセキュリティ診断（アプリケーション、ハードウェア、ソフトウェア及びネットワークを対象とした診断）を実施すること。アプリケーションに係るセキュリティ診断については、AP 開発事業者からセキュリティ診断の対象を選定するための情報を受領し、特に重要と考えられる対象を検討・選定した上で本学園へ報告して承認を受けること。

受託者はセキュリティ診断の結果、脆弱性が指摘された場合は、必要に応じて AP 開発事業者と協議し、システムの環境変更や改修等への影響を見極め、必要となる対策を本学園に報告の上、対策を講じること。

(※注) 第三者組織は、受託者内、別業者を問わず、直接的に本業務の設計・構築業務に携わらない組織で、ISMS 適合性評価制度の認証を取得し、チームメンバー構成においては、システム監査技術者及び CISSP 有資格者をそれぞれ 1 名以上含むことを条件とする。

(2) 運用保守

① 通常時対応

ア. 運用保守計画の作成

受託者は、環境定義書を踏まえた上で運用保守期間全体に渡る実施計画書を作成し、本学園に報告して本学園から承認を受けること。また、本番運用開始時及び各年度の開始時に運用保守の年間計画（メンテナンスによるシステムの計画停止日時等を含む）を作成し、本学園に報告して本学園から承認を受けること。

イ. システム操作・稼動監視

受託者は、運用マニュアルに基づき、システム操作（システムの稼動監視、バックアップ取得・世代管理、ウイルス定義ファイルの更新確認、アクセスログの収集、システムカレンダーの更新、障害回復等）を実施すること。システムの稼動監視において、システム障害及びセキュリティインシデントの発生（又は見込まれる状況）を把握できる仕組みを導入し、システム障害及びセキュリティインシデントを検知した際は、運用保守における実施計画書に定められた関係者に通知すること。

ウ. 処理実績管理・監査

受託者は、運用マニュアルに基づき、システムのリソース使用状況やオンライン処理件数等の処理実績に関する情報の収集及び分析を行い、定期的にも本学園への報告を行うこと。また、不正ログインの有無等のセキュリティに係る監査を行い、定期的にも本学園への報告を行うこと。

エ. セキュリティパッチ等の適用

受託者は、自ら発注したハードウェア、ソフトウェア、ネットワーク機器等について、セキュリティパッチ等のリリース情報を定期的に確認した上で適

用の是非を検討し、本学園へ報告すること。本学園及び AP 運用保守事業者と協議の上、セキュリティパッチ等の適用が必要と判断された場合は、セキュリティパッチの適用タイミング・適用方法を検討した上で、本学園の承認を受けてセキュリティパッチ等の適用を実施すること。

なお、本番環境にセキュリティパッチ等を適用する前に、検証環境にて次期システム WAKABA アプリケーション等が問題なく動作することを確認すること。動作に問題がある場合は、本学園に報告した上で、対策を提案し、本学園の承認を受けてセキュリティパッチ等の適用を実行すること。また、セキュリティパッチ等の適用を実施する前には、必要に応じてシステムバックアップを取得し、パッチ適用直前の状態にリストアできるようにすること。パッチ適用により不具合が発生した場合でも速やかにサーバを正常稼働状態へ戻せること。

オ. 問合せ対応

受託者は、本学園及び AP 運用保守事業者からの次期システム WAKABA 基盤に係る問合せに対応すること。

受託者は、自らが発注した機器等について、問合せを受けた場合は、必要に応じて当該機器ベンダ等に連絡し、故障復旧、機器交換等の手配を行うこと。

また、学生証リーダー、学生証プリンタ、作業用プリンタ、証明書発行用プリンタの故障受付及び修理対応を可能とすること。

カ. 作業依頼等への対応

受託者は、次期システム WAKABA のアプリケーション仕様を変更する際に、本学園からの依頼に基づき、次期システム WAKABA 基盤に係る影響を調査し、本学園に結果の報告をすること。また、本学園から次期システム WAKABA 基盤に関する軽微な作業依頼（ログの取得依頼、運用ジョブのスケジュール登録・変更依頼、システムに関する設定情報の提供依頼等）を受けた場合は、対応すること。

キ. ハードウェア等の構成管理

受託者は、運用保守期間において、次期システム WAKABA 基盤の構成（サーバ、ソフトウェア、ネットワーク機器等）に変更が生じた場合は、最新の構成情報にて環境定義書及びシステム管理台帳を更新すること。また、受託者は、機器ベンダ等からの保守サービスを受けるために必要となるライセンスを管理（保守問合せ先の定期的な確認、保守サポート期限や内容の変更有無等を含む）して、運用期間において機器ベンダ等からの保守サービスを継続的に受けられるようにすること。

ク. セキュリティ診断対応

受託者は、第三者組織（9 ページの※注参照のこと）によるセキュリティ診断（アプリケーション、ハードウェア、ソフトウェア及びネットワークを対象とした診断）を年1回実施すること。

受託者はセキュリティ診断の結果、脆弱性が指摘された場合は、システムの環境変更や改修等への影響を見極め、必要となる対策を本学園に報告し、協議の上対策を講じること。

ケ. 運用保守作業報告

受託者は、運用保守期間において実施した作業について、報告書として取りまとめ月次で報告すること。また、運用保守作業を実施する中で改善すべき事項がある場合は、運用保守作業報告書において提案すること。

コ. 引継ぎ等における情報提供

受託者は、本学園の担当者の異動や、本学園が新たな関連事業者を調達した場合等において、情報提供等を依頼するので協力すること。また、本契約の終了後又は契約期間満了を待たずに、本学園が他の事業者と当該運用保守業務を契約した場合には、当該事業者に対し、作業経緯、残存課題等についての引継ぎを行うこと。

サ. 次期システム WAKABA 基盤の撤去作業

次期システム WAKABA 基盤の使用を終了すると本学園が決定した際は、当該機器の撤去作業を実施すること。この撤去作業に必要な費用等は、受託者にて負担すること。また、次期 WAKABA 基盤の使用を終了した際には、当該機器に含まれる全てのデータを確実に破棄または消去し、その証明を提示すること。

② 障害発生時対応

次期システム WAKABA に障害（情報セキュリティインシデントを含む）が発生した場合は、障害原因を調査し、一次切分けを行う。障害原因がアプリケーションに起因するものと切分けた場合は、AP 運用保守事業者へ連絡し、対応を依頼すること。障害原因が本調達範囲内のハードウェア、ソフトウェア、ネットワーク機器等によるものと切分けた場合は、以下のアからウに示す対応を行うこと。

なお、障害発生時等の緊急対応が行えるよう、本学園と連絡が取れるようにし、緊急性に応じて駆けつけ対応等を行うこと。また、大規模災害等の発災時には、本学園と協議の上速やかに運用継続に資する復旧作業を実施すること。

ア. 障害原因の特定と暫定対処

障害対応に当たって、発生した原因を特定し、復旧に向けた対策を本学園に報告し、承認を受けること。原因を特定した結果、恒久的な対処に時間を要する場合には、暫定対処を行い業務の再開を優先すること。

なお、障害の原因がアプリケーションに起因していると考えられる場合は、本学園及び AP 運用保守事業者と連絡して、対応について協議すること。

イ. 恒久対応の実施

受託者は、障害対応した事象が、将来にわたって発生する可能性がある場合には、恒久的な対応策を提案し、本学園及び AP 運用保守事業者と協議の上対処を実施すること。

ウ. 障害対応結果の報告

受託者は、障害の内容、発生原因、業務への影響、対処の内容、再発防止策等を本学園に書面で報告すること。

(3) 留意事項

① 設計・構築・テストにおける留意事項

- ・ 次期システム WAKABA 基盤の構築は、令和 5 年 4 月 1 日からの本格稼働を目途に行うが、並行して次期システム WAKABA のアプリケーション開発が実施されるため、受託者は AP 開発事業者と各種調整の上本業務を遂行すること。また、次期システム WAKABA が稼働する令和 5 年 4 月 1 日以降は、AP 運用保守事業者等と各種調整の上本業務を遂行すること。
- ・ AP 開発事業者が非機能要件に関する詳細設計を実施する。本業務の受託者は、非機能要件に関する詳細設計書を確認の上、AP 開発事業者と必要な調整を行い、本業務を遂行すること。また、選定する機器や環境定義が、詳細設計内容と整合しない場合は、AP 開発事業者と協議・調整の上で変更部分の詳細設計書、基本設計内容に影響が及ぶ場合は基本設計書を作成し、本学園の承認を受けること。
- ・ 受託者は、次期システム WAKABA の運用開始スケジュール等に影響を与えないよう、AP 開発事業者等と調整の上、作業を行うこと。また、AP 開発事業者がテスト工程やアプリケーション開発に係る仕様変更対応を実施する上で、次期システム WAKABA 基盤の環境に関する設定変更等の依頼を受けた場合は、対応すること。

- ・ 受託者は、次期システム WAKABA 基盤の実現に向けて、品質面、進捗面等で課題が生じた場合、速やかに対応策を検討し、AP 開発事業者及び関連事業者等と協力し、本学園の承認を受け、対策を講じること。なお、それにより発生した追加作業等については、受託者の責任と負担において実施すること。

② 運用保守における留意事項

- ・ 受託者は運用保守における通常時対応として、平日日中帯（9:00～18:00）により作業を実施すること。

3.2 成果物の範囲、納品期日等

(1) 成果物

① 設計・構築・テストにおける成果物

以下に示す成果物を、本学園と別途協議して決定する期日までに提出するとともに、次期システム WAKABA 基盤稼動開始後 1 か月以内に最終納品し、検収を受けること。

- ・ ハードウェア一式
- ・ ソフトウェア一式
- ・ 設計・構築・テストにおける実施計画書
- ・ 環境定義書（ハードウェア、ソフトウェア及びネットワーク構成、各種設定情報等を含む）
- ・ 運用マニュアル
- ・ 基盤テストに係るテスト項目表及びテスト結果（基盤テストの実施前後にそれぞれ提出する）
- ・ 基盤総合テストに係るテスト項目表及びテスト結果（基盤総合テストの実施前後にそれぞれ提出する）
- ・ 移行リハーサル及び本番システムへの切替計画書
- ・ システム切替結果報告書
- ・ セキュリティ診断結果報告書
- ・ 学習センター等設置機器のレイアウト、機器交換日程等の計画書
- ・ その他技術資料（議事録等）
- ・ 非機能要件に関する基本設計書（設計内容を変更した箇所）
- ・ 非機能要件に関する詳細設計書（設計内容を変更した箇所）

② 運用保守期間における成果物

以下に示す成果物を、本学園と別途協議して決定する期日までに提出すること。「①設計・構築・テストにおける成果物」のうち、運用保守期間中に更新したものについては、変更履歴を付した上で随時提出すること。また、運用期間中に作成・更新した成果物については、各年度末に納品し、検収を受けること。

- ・ 運用保守期間全体に渡る実施計画書
- ・ 運用保守の年間計画
- ・ 運用保守作業報告書（月次で報告する）
- ・ 障害対応結果の報告書（障害が発生した場合に作成する）
- ・ セキュリティ診断結果報告書
- ・ システム管理台帳
- ・ その他技術資料（議事録等）

③ 納品期日、媒体及び数量

①及び②に記載の期日までに、電子媒体で各 2 部提出することを基本とするが、詳細については本学園と協議して決定する。

(2) 納品方法

成果物は、全て日本語で作成すること。

情報処理に関する用語の表記については、日本工業規格（JIS）の規定を参考にすること。

電磁的記録媒体による納品について、Microsoft Office のファイル形式で作成し、CD-R もしくは DVD-R の媒体に格納して納品すること。

成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。

電磁的記録媒体により納品する場合は、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処すること。

(3) 納品場所

本学園の指定する場所

(4) 支払条件

賃貸借料には、ハードウェア、ソフトウェア、ライセンス調達、導入作業、クラウド利用、回線利用、運用支援作業及び保守等全ての費用を含めるものとする。

支払いは、賃借及び運用保守期間での月額（60ヶ月）によるものとする。

遠隔地バックアップに利用するクラウドストレージの利用料は本調達に含めるものとする。

(5) 満たすべき要件に関する事項

本業務の実施に当たっては、「本調達仕様書」の全ての要件を満たすこと。

(6) 作業の実施体制・方法に関する事項

① 作業実施体制

本業務の推進体制及び受託者に求める作業実施体制は図3のとおり想定している。受託者の体制については、遂行責任者を設置することを必須とするが、その他の詳細な体制は提案によるものとする。

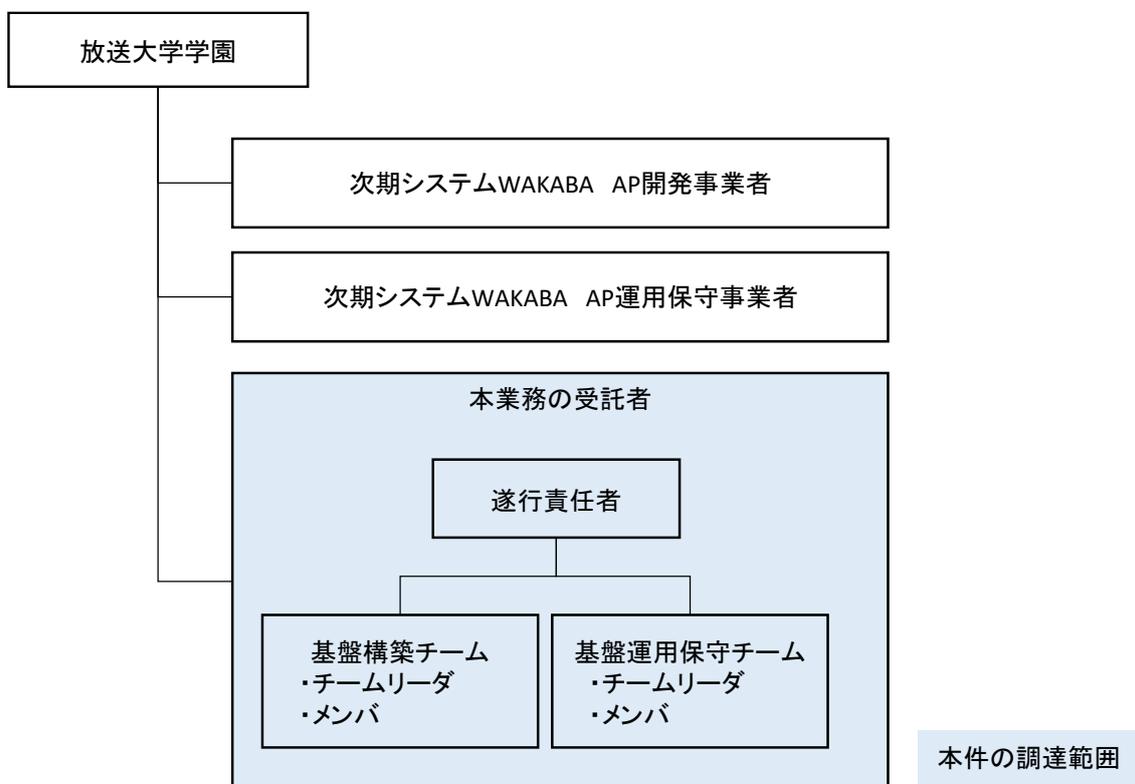


図3 本業務の推進体制及び受託者に求める作業実施体制

② 作業要員に求める資格等の要件

- ・ 遂行責任者は、独立行政法人情報処理推進機構 (IPA) による IT スキル標準 (ITSS) に基づき、プロジェクトマネジメント職種及び IT サービスマネジメント職種 (運用管理) レベル 5 以上の者であり、本システムと同規模以上の情報システムの設計・開発・運用・保守に係るプロジェクト管理の実務経験を 10 年以上有する者であること。
- ・ 遂行責任者は、以下のいずれかの資格を有する者であること。
 - ✓ 情報処理技術者 (プロジェクトマネージャ)
 - ✓ プロジェクトマネジメントプロフェッショナル (PMP)
 - ✓ プロジェクトマネジメント・スペシャリスト (PMS)
- ・ 遂行責任者の元で業務を実施する担当者には、独立行政法人情報処理推進機構 (IPA) が実施する情報処理技術者試験のうち、情報処理安全確保支援士の資格を有する者が含まれていること。

③ 受託者に求める資格等の要件

過去 3 年間に、全国 (各都道府県に少なくとも 1 か所以上) の拠点間をネットワークで結んだシステム基盤構築 (HW 設置/環境設計/構築/試験) 業務の実績を有していること。また、十万件以上の個人情報扱うシステム基盤構築業務、保守業務の実績を有していること。

④ クラウドセキュリティに関する認証等の要件

- ・ 政府情報システムのためのセキュリティ評価制度 (ISMAP) クラウドサービスリストに登録されていること。
- ・ クラウドセキュリティに関する次のいずれかの認証を取得していること。
 - ✓ ISO/IEC 27017 による認証取得
 - ✓ JASA クラウドセキュリティ推進協議会 CS ゴールドマーク
- ・ AICPA SOC2 及び SOC3 の監査フレームワークに対応し、所要の措置を適切に実施するとともに、第三者監査人の監査を受け、確実に実施されている旨の証明の提出が本システムの稼働開始以降の工程において対応できること。

⑤ 作業場所

本業務の作業場所及び作業に当たり必要となる設備、備品及び消耗品等については、受託者の責任において用意すること。また、必要に応じて担当職員が現地確認を実施することができるものとする。

⑥ 作業の管理に関する要領

受託者は、本業務を円滑に進めるにあたり、設計・構築・テスト期間及び運用保守期間における進捗管理、課題管理、リスク管理、品質管理、コミュニケーション管理、体制管理、変更管理、情報セキュリティ管理等を行うこと。また、管理状況（進捗、課題等）を取りまとめ、月次で報告すること。

受託者は、必要に応じて会議、打合せ等を設定し、円滑な業務推進に努めることとし、開催した会議については議事録を作成のうえ本学園へ提出し、承認を受けること。議事録の提出・承認期日については、別途本学園と協議して定める。

(7) 作業の実施に当たっての遵守事項

① 機密保持、資料の取扱い

- ・ 本学園が開示した情報、契約履行過程で生じた納入成果物（印刷した帳票を含む。）及び本作業の履行上知り得た一切の事項について、いかなる場合にもこれを本学園が開示することを認めていない第三者に開示又は漏えいしてはならないものとし、そのために必要な措置を講じること。また、本学園が提供した情報を第三者に開示する必要がある場合には、事前に本学園と協議し、了承を得ること。
なお、上記の開示又は漏えい防止及び本学園が提供した情報を第三者に開示する必要がある場合に本学園の了承を得ることについては、本作業の委託期間終了後も同様とする。
- ・ 本作業の実施に当たって、受領、作成及び出力した一切の情報について、本学園の許可なく作業実施場所から持ち出してはならない。
- ・ 本学園が提供する本作業に関連する文書等について、本学園が用意する場所に保管し、原則として、契約期間終了時まで返却又は裁断・溶解等の処分を行うこと。
- ・ プログラム及びデータは事前に許可した機器やディレクトリ・フォルダのみに格納すること。
- ・ プログラム、データ及びその他本作業の履行上発生した納入成果物については、本学園の許可なしに、作業実施場所から外部に持ち出したり、外部からアクセスできる状態に置いてはならない。
なお、本学園以外の物品等を作業実施場所へ持ち込み、又は本学園の物品を作業実施場所から持ち出す場合は、事前に本学園の許可を得ること。
- ・ 電子媒体によって運用するプログラム、データ及び文書等については、ウイルスチェックを実施すること。

② 著作権

- ・ 本件受託業務の作業により作成する納入成果物に関し、既に著作権を有しているものを除き、著作権法（昭和 45 年 5 月 6 日法律第 48 号）第 21 条、第 26 条の 3、第 27 条及び第 28 条に定める権利を含む全ての著作権を本学園側に譲渡し、本学園は独占的に使用できることとする。
なお、受託者は本学園に対し、一切の著作者人格権を行使しないこととし、第三者をして行使させないこと。また、受託者が本契約の納入成果物に係る著作権を自ら使用し、又は第三者をして使用させる場合、本学園と別途協議すること。
- ・ 納入成果物に第三者が権利を有する著作物が含まれている場合は、本学園が特に使用を指示した場合を除き、受託者は当該著作物の使用に関して費用の負担を含む一切の手続を行うこと。
なお、この場合、受託者は当該著作権者の使用許諾条件につき、本学園の了承を得ること。
- ・ 本件受託業務の作業に関し、第三者との間で著作権に係る権利侵害の紛争等が生じた場合、当該紛争の原因が専ら本学園の責めに帰す場合を除き、受託者は自らの負担と責任において一切を処理すること。

③ 契約不適合責任

- ・ 受託者は、本業務にて納入する全ての納入成果物について、契約不適合責任を負うものとする。契約不適合責任期間は本学園による検収後 1 年間とする。
- ・ 納入成果物に不備があった場合、関連する設計書、マニュアル等の納入成果物を修正の上、提出すること。

(8) 成果物の取扱いに関する事項

成果物の取扱いについては、「(7) 作業の実施に当たっての遵守事項」に定めたことのほか、別途締結する契約書に準拠すること。

(9) 入札参加資格に関する事項

① 入札参加要件

ア. 競争参加資格

放送大学学園契約事務取扱規程第 4 条及び第 5 条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。

全省庁統一資格において開札時まで令和 3 年度の関東・甲信越地域における「役務の提供等」の A、B 又は C の等級に格付けされている者であること。

イ. 公的な資格や認証等の取得

個人情報を取扱う情報システムの設計・開発、運用業務において JIS Q 27001 (又は ISO27001) を基準とした認証とプライバシーマーク及び品質マネジメント資格 (ISO9001) を取得していること。

② 入札制限

本調達に参加しようとする事業者に対し、本学園の他の調達を受託済みであることを理由とする入札制限の条件は設けない。

(10) 再委託に関する事項

① 再委託の制限及び再委託を認める場合の条件

- ・ 本業務の受託者は、業務を一括して又は主たる部分を再委託してはならない。
- ・ 受託者における遂行責任者を再委託先事業者の社員や契約社員とすることはできない。
- ・ 受託者は再委託先の行為について一切の責任を負うものとする。
- ・ 再委託先における情報セキュリティの確保については受託者の責任とする。

② 承認手続

- ・ 本業務の実施の一部を合理的な理由及び必要性により再委託する場合には、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性及び契約金額等について記載した書面を本学園に提出し、承認を受けること。
- ・ 前項による再委託の相手方の変更等を行う必要が生じた場合も、前項と同様に再委託に関する書面を本学園に提出し、承認を受けること。

③ 再委託先の契約違反等

再委託先において、本調達仕様書に定める事項に関する義務違反又は義務を怠った場合には、受託者が一切の責任を負うとともに、本学園は、当該再委託先への再委託の中止を請求することができる。

(11) 附属文書

① 事業者が閲覧できる資料一覧表

本業務に応札する事業者は、現行のシステム WAKABA 基盤に関する各種設計書、AP 開発事業者が作成した非機能要件に関する基本設計書、詳細設計書を参照できるものとする。その他の資料については、事業者からの申し出に基づき、本学園にて閲覧可否を判断した上で開示する。なお、本業務一式を遂行するためには、現行のシステム WAKABA 基盤及び次期システム WAKABA の非機能要件に関する設計について理解する必要があるため、本業務に応札する事業者は、資料閲覧を必須とする。

② 閲覧要領

ア. 閲覧場所

本学園の指定する場所とし、別途実施する入札説明会において説明する。

イ. 閲覧期間及び時間

別途実施する入札説明会において説明する。

ウ. 閲覧手続

本学園の指定する様式・方法で手続きすることとし、別途実施する入札説明会において説明する。

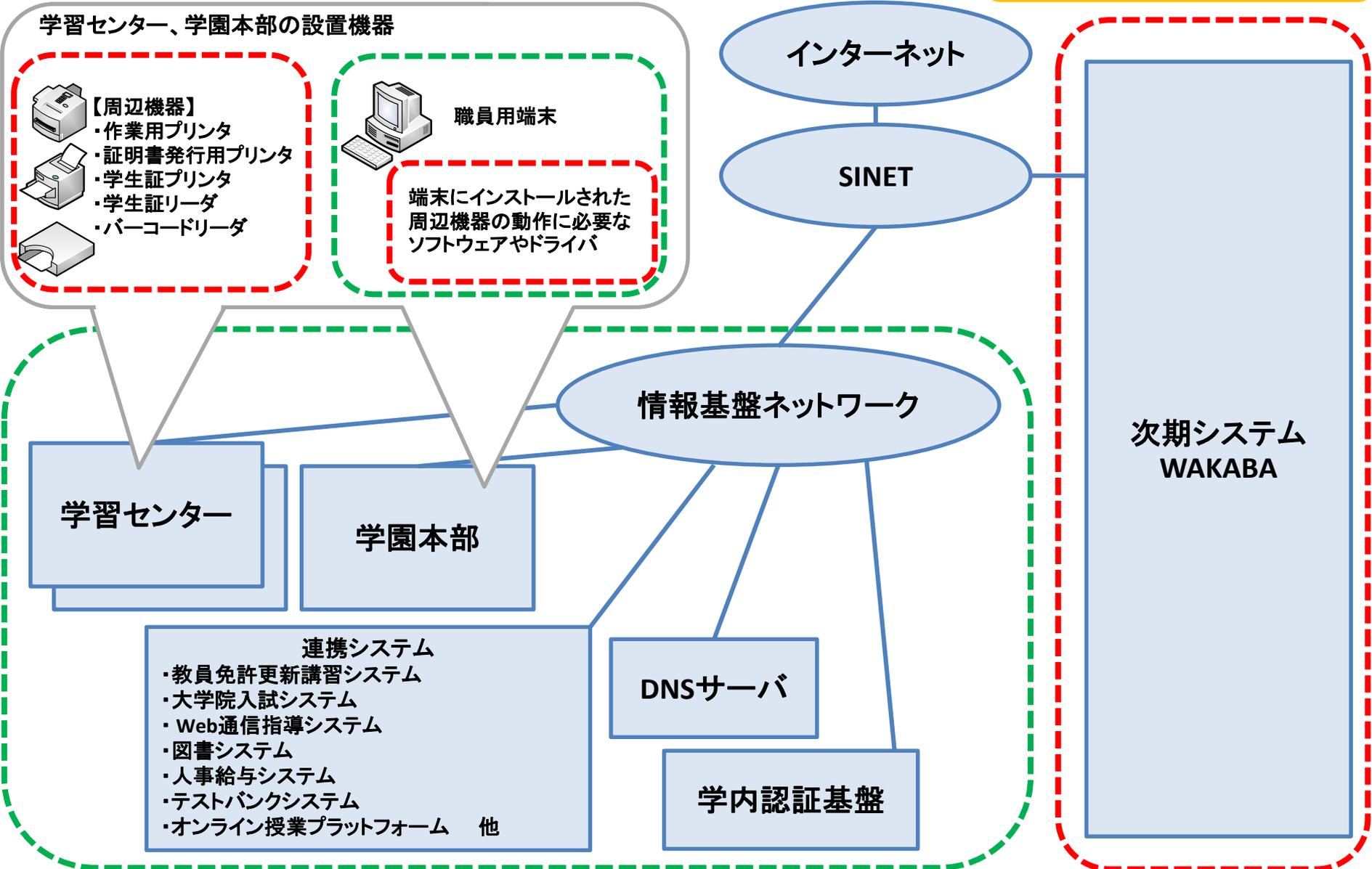
エ. 閲覧時の注意

閲覧にて知り得た内容については提案書作成の目的以外には使用できないものとする。

別紙① 次期システムWAKABA基盤の作業範囲

次期システム
WAKABA基盤の範囲

本学園の範囲



※図は例としてSINET回線を利用した構成としている

別紙② 周辺機器一覧

- ・以下に示す機器要件を満たす周辺機器(学習センター)を提供すること。
- ・項番1、項番4の機器について、定期交換部品を含み、平日日中帯にオンサイトで製品保守に対応すること。
- ・項番3、項番5、項番6の機器について、故障発生時に職員がセンドバックで機器を交換できる製品保守に対応すること。

項番	分類	名称	機器要件	数量
1	周辺機器	作業用プリンタ	<ul style="list-style-type: none"> ・モノクロレーザープリンタ ・両面印刷が可能 ・A4 縦送りで片面印刷38ページ/分以上、両面印刷20ページ/分以上の性能 ・標準トレイにて A4 縦送り印刷時ファーストプリントが4.5 秒以下 ・データ処理解像度: 600dpi/400dpi/300dpi、プリント解像度: 1,200×1,200dpi、600×600dpi 以上 ・用紙サイズは、: A4、A5、A6、B5、レター、リーガル、エグゼクティブ、16K、ステートメント、封筒、郵便ハガキ、往復サイズ、カスタムサイズに対応 ・用紙種類として、普通紙、再生紙、ラベル紙、郵便はがき、往復はがき、封筒に対応 ・メモリを 512MB 以上搭載 ・インタフェースに、イーサネット(1000BASE-T/100BASE-TX/10BASE-T(TCP/IP)、IEEE802.11a/b/g/n)を装備 ・給紙容量は、セカンドトレイ含め860 枚以上 ・本体寸法は、387(W)×393(D)×252(H)mm以下 ・本体重量は、13.5 kg以下であること。(本体のみ、消耗品を含む) ・対応 OS は、Windows 10、Windows 8.1、Windows 8、Windows Server2012 R2、Windows Server2012 (導入場所については、「別紙③ 学習センター住所一覧」、「別紙④ 導入台数一覧」を参照のこと) 	2
2		プリンタラック	<ul style="list-style-type: none"> ・作業用プリンタ 2 台を上下に設置できるラックを1 台 	1
3		証明書発行用プリンタ	<ul style="list-style-type: none"> ・カラーLEDプリンタ ・デジタル4連LEDフルカラー乾式電子写真方式 ・両面印刷が可能 ・用紙サイズは、: A3、A4、A5、A6、B4、B5、B6、B6ハーフ、B7、B8、リーガル13インチ、リーガル13.5インチ、リーガル14インチ、タブロイド、レター、エグゼクティブ、16K、8K、ステートメント、フォリオ、Banner、封筒、郵便ハガキ、往復ハガキ、インデックスカード、Photo Size (4" x 6", 5" x 7") (100 x 150mm, 125 x 175mm)、カスタムサイズ: 幅 55-297 mm x 長さ 90-1321 mmに対応 ・用紙種類として、普通紙、郵便ハガキ、ラベル紙、封筒に対応 ・連続プリント速度が、A4(横) カラー 36ページ/分、モノクロ 36ページ/分、A3 カラー 20ページ/分、モノクロ 20ページ/分、自動両面: A4(横)カラー 27ページ/分、モノクロ 27ページ/分、自動両面: A3カラー 18ページ/分、モノクロ 18ページ/分以上 ・ファーストプリントが、フルカラー、モノクロ共に6.3 秒以下(A4 横送り) ・解像度が、600×600dpi/600×1200dpi/600×600 dpi (4階調)/LEDドットピッチ: 600 dpi に対応 ・標準給紙量が 320 枚以上 ・標準給紙のほかに、580 枚以上の増設トレイを搭載 ・本体寸法は、449(W)×552(D)×360(H)mm 以下 ・本体重量は、40kg 以下 (本体のみ、消耗品含む) ・騒音は、稼働時 54db(A)以下、待機時32db(A)以下 ・メモリは、1GB以上 ・対応 OS は、Windows 10、Windows 10 x64、Windows 8.1、Windows 8.1 x64、Windows 8、Windows 8 x64、Windows Server 2016、Windows Server 2012 R2、Windows Server 2012、macOS 10.13、macOS 10.12、OS X 10.11、OS X 10.10 (導入場所については、「別紙③ 学習センター住所一覧」、「別紙④ 導入台数一覧」を参照のこと) 	66
4		学生証プリンタ	<ul style="list-style-type: none"> ・フルカラー(5色(YMCKO))印刷が可能 ・印刷解像度が300dpi以上。また、設定で600×300dpi(YMCKO)、1200dpi×300dpi(K)に切り替え可能なこと。 ・USB・イーサネットインタフェースを有し、パソコンと接続可能 ・カードエッジまでの全画面印刷が可能 ・印刷スピードがフルカラー印刷時 210 枚/時以上 ・ドライバは、Windows 8.10に対応 ・印刷用のアプリケーション「CardPAS」を用意し、次期システムWAKABA からの印刷指示と連動して印刷が可能 ・既存導入システムと連携仲介する「CardPAS」との動作確認が済 ・適応カードタイプは、PVC、合成 PVC、PET、ABS、つやありプラスチックカード ・カードのサイズ仕様は、ISO 規定 CR-80 のカードを利用可能 ・カードの厚みは、0.25mm から1.25mm が印刷可能であり、カード厚調整ゲージが附属 ・カードフィーダー容量は、100 枚以上(0.76mm 厚のカードの場合) ・JIS II 磁気エンコーダが附属 ・本プリンタ 1 台につき、フルカラー印刷が可能となるカラーリボン(300 枚印刷可能)を各2 巻用意 ・カードプリンタ本体サイズが、高さ247mm×長さ205mm×奥行381mm 以内 ・オプションで両面印刷対応にアップグレード可能 ・接触・非接触 IC エンコーダを容易に装・脱着可能 (導入場所については、「別紙③ 学習センター住所一覧」、「別紙④ 導入台数一覧」を参照のこと) 	117
5		学生証リーダー	<ul style="list-style-type: none"> ・手動式磁気カードリーダー ・USB(キーボード)インタフェース ・カード動作速度は、100~1200mm/s ・寿命は 50 万パス以上 ・表示機能は、READY/OK/ERROR インジケータ対応 ・電源は、USB(BUS POWER)対応 ・学生証プリンタで発行した学生証の磁気ストライプ(JIS II)を読み取り可能 (導入場所については、「別紙③ 学習センター住所一覧」、「別紙④ 導入台数一覧」を参照のこと) 	68

別紙③ 学習センター住所一覧

北海道学習センター	〒060-0817 北海道札幌市北区北17条西8丁目 (北海道大学札幌キャンパス情報教育館内)
旭川サテライトスペース	〒070-0044 北海道旭川市常磐公園 (旭川市常磐館内)
青森学習センター	〒036-8561 青森県弘前市文京町3 コラボ弘大7階
八戸サテライトスペース	〒039-1102 青森県八戸市一番町1-9-22 (八戸地域地場産業振興センター〔ユートリー4階〕)
岩手学習センター	〒020-8550 岩手県盛岡市上田3-18-8 (岩手大学構内)
宮城学習センター	〒980-8577 宮城県仙台市青葉区片平2-1-1 (東北大学片平キャンパス金属材料研究所内)
秋田学習センター	〒010-8502 秋田県秋田市手形学園町1-1 (秋田大学手形キャンパス地方創生センター2号館4階)
山形学習センター	〒990-8580 山形県山形市城南町1-1-1 (霞城セントラル10階)
福島学習センター	〒963-8025 福島県郡山市桑野1-22-21 (郡山女子大学内)
いわきサテライトスペース	〒970-8023 福島県いわき市平鎌田字寿金沢22-1 (東日本国際大学5号館5階)
茨城学習センター	〒310-0056 茨城県水戸市文京2-1-1 (茨城大学キャンパス環境リサーチラボラトリー棟内)
栃木学習センター	〒321-0943 栃木県宇都宮市峰町350 (宇都宮大学峰キャンパス附属図書館内)
群馬学習センター	〒371-0032 群馬県前橋市若宮町1-13-2
埼玉学習センター	〒330-0853 埼玉県さいたま市大宮区錦町682-2 (大宮情報文化センター8・9・10階)

別紙③ 学習センター住所一覧

千葉学習センター	〒261-8586 千葉県千葉市美浜区若葉2-11 (放送大学本部敷地内)
東京渋谷学習センター	〒150-0043 東京都渋谷区道玄坂1-10-7 五島育英会ビル1階
東京文京学習センター	〒112-0012 東京都文京区大塚3-29-1
東京足立学習センター	〒120-0034 東京都足立区千住5-13-5 (学びピア21内)
東京多摩学習センター	〒187-0045 東京都小平市学園西町1-29-1 (一橋大学小平国際キャンパス国際共同研究センター棟3階)
神奈川学習センター	〒232-8510 神奈川県横浜市南区大岡2-31-1
新潟学習センター	〒951-8122 新潟県新潟市中央区旭町通1番町754 (新潟大学旭町キャンパス医歯学図書館)
富山学習センター	〒939-0311 富山県射水市黒河5180 (富山県立大学計算機センター3階)
石川学習センター	〒921-8812 石川県野々市市扇が丘7-1 (金沢工業大学内)
福井学習センター	〒910-0858 福井県福井市手寄1丁目4-1 (AOSSA 7階)
山梨学習センター	〒400-0016 山梨県甲府市武田4-4-37 (山梨大学構内)
長野学習センター	〒392-0004 長野県諏訪市諏訪1-6-1 (アーク諏訪 3階)
岐阜学習センター	〒500-8384 岐阜県岐阜市藪田南5-14-53 (OKBふれあい会館第2棟2階)
静岡学習センター	〒411-0033 静岡県三島市文教町1-3-93 (静岡県立三島長陵高等学校2階)

別紙③ 学習センター住所一覧

浜松サテライトスペース	〒430-0916 静岡県浜松市中区早馬町2-1 (クリエート浜松2階・4階)
愛知学習センター	〒466-0825 愛知県名古屋市昭和区八事本町101-2 (中京大学センタービル4階)
三重学習センター	〒514-0061 三重県津市一身田上津部田1234 (三重県総合文化センター内)
滋賀学習センター	〒520-2123 滋賀県大津市瀬田大江町横谷1-5 (龍谷大学瀬田キャンパス内)
京都学習センター	〒600-8216 京都市下京区西洞院通塩小路下る東塩小路町939番地 (キャンパスプラザ京都3階)
大阪学習センター	〒543-0054 大阪府大阪市天王寺区南河堀町4-88 (大阪教育大学天王寺キャンパス中央館内6・7階)
兵庫学習センター	〒657-8501 兵庫県神戸市灘区六甲台町2-1 (神戸大学六甲台キャンパスアカデミア館6・7階)
姫路サテライトスペース	〒670-0012 兵庫県姫路市本町68-290 (イーグレひめじ地下2階内)
奈良学習センター	〒630-8589 奈良県奈良市北魚屋東町 (奈良女子大学コラボレーションセンター3階)
和歌山学習センター	〒641-0051 和歌山県和歌山市西高松1-7-20 (和歌山大学松下会館内)
鳥取学習センター	〒680-0845 鳥取県鳥取市富安2-138-4 (鳥取市役所駅南庁舎5階)
島根学習センター	〒690-0061 島根県松江市白潟本町43 (スティックビル4階)
岡山学習センター	〒700-0082 岡山県岡山市北区津島中3-1-1 (岡山大学津島キャンパス文化科学系総合研究棟5階)
広島学習センター	〒730-0053 広島県広島市中区東千田町1-1-89 (広島大学東千田キャンパス東千田総合校舎内)

別紙③ 学習センター住所一覧

福山サテライトスペース	〒720-0812 広島県福山市霞町1-10-1 (まなびの館ローズコム3階)
山口学習センター	〒753-0841 山口県山口市吉田1677-1 (山口大学吉田キャンパス大学会館内)
徳島学習センター	〒770-0855 徳島県徳島市新蔵町2-24 (徳島大学新蔵キャンパス日垂会館3階)
香川学習センター	〒760-0016 香川県高松市幸町1-1 (香川大学幸町北キャンパス研究交流棟内)
愛媛学習センター	〒790-0826 愛媛県松山市文京町3 (愛媛大学城北キャンパス総合情報メディアセンター棟内)
高知学習センター	〒780-8072 高知県高知市曙町2-5-1 (高知大学朝倉キャンパスメディアの森内)
福岡学習センター	〒816-0811 福岡県春日市春日公園6-1 (九州大学筑紫キャンパスE棟4,5階)
北九州サテライトスペース	〒806-0021 福岡県北九州市八幡西区黒崎3-15-3 (コムシティ3階)
佐賀学習センター	〒840-0815 佐賀県佐賀市天神3-2-11 (アバンセ4階内)
長崎学習センター	〒852-8521 長崎県長崎市文教町1-14 (長崎大学文教キャンパス内)
熊本学習センター	〒860-8555 熊本県熊本市中央区黒髪2-40-1 (熊本大学黒髪キャンパス附属図書館南棟2F)
大分学習センター	〒874-8501 大分県別府市北石垣82 (別府大学別府キャンパス39号館2階)
宮崎学習センター	〒883-8510 宮崎県日向市本町11-11
鹿児島学習センター	〒892-8790 鹿児島県鹿児島市山下町14-50 (かごしま県民交流センター西棟4階)
沖縄学習センター	〒903-0129 沖縄県中頭郡西原町字千原1 (琉球大学 地域国際学習センター棟内)

別紙④ 導入台数一覧(予定)

No.	場所	作業用 プリンタ	証明書発行用 プリンタ	学生証 プリンタ	学生証用 リーダー
1	北海道 SC	0	2	2	0
2	旭川 SS	0	0	0	0
3	青森 SC	0	1	2	1
4	八戸 SS	0	0	0	0
5	岩手 SC	0	1	2	1
6	宮城 SC	0	1	2	0
7	秋田 SC	0	1	2	0
8	山形 SC	0	2	2	1
9	福島 SC	0	1	2	1
10	いわき SS	0	0	0	0
11	茨城 SC	0	1	2	1
12	栃木 SC	0	1	2	0
13	群馬 SC	0	1	2	0
14	埼玉 SC	0	2	2	4
15	千葉 SC	0	1	3	2
16	東京渋谷 SC	0	0	4	8
17	東京文京 SC	0	2	4	10
18	東京足立 SC	0	1	2	2
19	東京多摩 SC	0	0	2	2
20	神奈川 SC	0	2	4	4
21	新潟 SC	0	2	2	2
22	富山 SC	0	1	2	1
23	石川 SC	0	1	2	2
24	福井 SC	0	1	2	1
25	山梨 SC	0	1	2	0
26	長野 SC	0	1	2	0
27	岐阜 SC	0	2	2	0
28	静岡 SC	0	1	2	1
29	浜松 SS	0	0	0	0
30	愛知 SC	0	2	2	2
31	三重 SC	0	1	2	1
32	滋賀 SC	0	1	2	1
33	京都 SC	0	1	3	2

34	大阪 SC	0	2	3	4
35	兵庫 SC	0	1	2	2
36	姫路 SS	0	0	0	0
37	奈良 SC	0	1	2	0
38	和歌山 SC	0	1	2	0
39	鳥取 SC	0	1	2	0
40	島根 SC	0	1	2	1
41	岡山 SC	0	2	2	0
42	広島 SC	0	1	2	1
43	福山 SS	0	0	0	0
44	山口 SC	0	1	2	1
45	徳島 SC	0	1	2	0
46	香川 SC	0	2	2	0
47	愛媛 SC	0	2	2	1
48	高知 SC	0	1	1	0
49	福岡 SC	0	2	2	0
50	北九州 SS	0	0	2	0
51	佐賀 SC	0	1	1	0
52	長崎 SC	0	1	2	0
53	熊本 SC	0	2	2	0
54	大分 SC	0	1	2	0
55	宮崎 SC	0	1	2	0
56	鹿児島 SC	0	2	2	0
57	沖縄 SC	0	1	2	0
58	本部	2	3	8	8
	合計	2	66	117	68

※注1：SCは「学習センター」、SSは「サテライトスペース」の略

※注2：各SC等への配置台数は現時点の予定であるため、配置するには本学園に再確認すること。

※注3：本部用の学生証プリンタ、学生証用リーダーには、センドバックによる故障対応用の台数を含む。

別紙⑤_クラウド要件一覧

- ・業務サービスを提供するサーバ及びネットワーク機器等を構築するにあたり、以下の要件を満たすクラウド環境を採用すること。
ただし、遠隔地バックアップに関してはその限りではない。

項番	分類	項目	要件
1	データセンタの立地	-	日本国内に設置されていること。
2	データセンタの立地	-	受託者の開発及び運用保守拠点等から鉄道等の公共交通機関を使用し、かつ徒歩の時間も含めて90分以内に到着できる距離にあること。
3	データセンタの立地	-	ハザードマップ(液状化・浸水等)にて危険度が低い地域となっていること。
4	可用性	サービス時間	要望に沿ったサービス時間、メンテナンス時間が設定できること。
5	可用性	計画停止予定通知	原則、計画停止の1か月以上前に通知可能であること。
6	セキュリティ	監査	監査による情報提供に協力可能であること。
7	セキュリティ	ディスク破壊	クラウド環境のディスクの処分が必要になった際は、データセンター外へ持ち出さずデータセンター内での破壊が可能であること。また、ディスク破壊証明書が発行可能であること。
8	セキュリティ	データの格納先	個別対応によって、データの格納先を特定可能であること。
9	セキュリティ	閉域環境	インターネットアクセスのない閉域環境を構築可能であること。
10	セキュリティ	安全保障	外国法や外国資本の影響を受けないこと。また、契約の解釈が日本法に基づくものであること。
11	移行性	機器持ち込み	必要に応じて、本学園が保持する物理機器をデータセンターに設置することが可能であること。
12	移行性	将来的な他環境への移行	他環境への移行が容易であること。
13	運用・保守性	トラブル報告書の提出	トラブルが発生した際の報告書を提出できること。必要に応じて、個別説明を行うことができること。
14	運用・保守性	駆け付け対応	駆け付けが可能であること。
15	運用・保守性	パッチ適用タイミング	適用タイミングについて、調整可能であること。ただし、緊急性のあるパッチに関しては強制的に適用するものとする。
16	品質安全規格	使用機器リストの開示	使用機器リストの開示が可能であること。

(別紙⑥)

教務情報システムの基盤構築・保守 一式
要件定義書

令和4年1月

放送大学学園

目次

1	システム方式に関する事項	1
1.1	情報システムの構成に関する全体の方針	1
(1)	全体方針	1
(2)	非機能特性ごとの方針	1
1.2	次期システム WAKABA 基盤の全体構成	2
2	規模・性能に関する事項	4
2.1	利用ユーザ数	4
2.2	オンライン処理性能設計	4
2.3	バッチ処理性能設計	4
2.4	帳票出力性能設計	5
2.5	スパイク負荷対応	5
3	信頼性に関する事項	6
3.1	可用性に関する事項	6
(1)	可用性に係る目標	6
(2)	可用性に係る対策	8
3.2	完全性に関する事項	10
(1)	ログ管理方針	10
4	拡張性に関する事項	11
4.1	拡張範囲	11
(1)	拡張範囲	11
4.2	拡張性	11
(1)	拡張性確保方針	11
(2)	リソース毎の拡張方針	11
(3)	拡張性確保方針	11
4.3	拡張対策	12
(1)	仮想マシン拡張方式	12
4.4	拡張方式	13
(1)	拡張方式（処理）	13
(2)	拡張方式（機器）	13
5	上位互換性に関する事項	13
5.1	パッチリリース管理	14
(1)	パッチリリース情報の提供	14
(2)	パッチ適用方針	14
(3)	パッチ検証の実施有無	14

(4) リリース作業の自動化.....	14
(5) パッチ適用タイミング.....	14
6 中立性に関する事項.....	15
7 継続性に関する事項.....	15
7.1 バックアップ/リカバリ.....	15
(1) バックアップ方針.....	15
(2) リカバリ方針.....	18
7.2 大規模災害対応.....	20
(1) 災害対策範囲.....	20
(2) 復旧方針.....	20
(3) 保管場所分散度、保管方法.....	20
8 情報セキュリティに関する事項.....	21
8.1 情報セキュリティに関するコンプライアンス.....	21
8.2 セキュリティリスク分析.....	21
8.3 セキュリティ診断.....	22
8.4 セキュリティリスクの見直し.....	22
8.5 セキュリティパッチ適用.....	22
(1) セキュリティパッチ適用範囲.....	22
(2) セキュリティパッチ適用方針.....	22
(3) セキュリティパッチ適用タイミング.....	22
8.6 認証機能.....	23
(1) システム管理者権限を持つ主体の認証.....	23
(2) システム管理者権限を持たない主体の認証.....	23
8.7 操作制限.....	23
(1) システム上の対策における操作制限.....	23
(2) 物理的な対策による操作制限.....	23
8.8 管理方法.....	23
(1) 管理ルールの策定.....	23
8.9 データ暗号化.....	23
(1) 伝送データの暗号化の有無.....	23
(2) 蓄積データの暗号化の有無.....	23
(3) 鍵管理.....	23
8.10 不正監視.....	24
(1) ログの取得.....	24
(2) ログ保管期間.....	24
(3) 不正監視対象（装置、ネットワーク、侵入者・不正操作等）.....	24

(4) 検知と自動通知	24
8.11 ネットワーク制御	24
(1) 通信制御	24
8.12 不正検知	24
(1) 不正通信の検知範囲	24
8.13 サービス停止攻撃の回避	24
(1) ネットワークの輻輳対策	24
8.14 マルウェア対策	25
(1) マルウェア対策実施範囲	25
8.15 Web 実装対策	25
(1) Web サーバの設定等による対策の強化	25
8.16 セキュリティ強化	25
9 次期システム WAKABA 基盤環境に関する事項	26
9.1 運用保守用端末等	26
9.2 ソフトウェア構成	26
9.3 ネットワーク構成	27
(1) SINET 接続	28
(2) 本学園本部と SINET 接続ポイント間回線	28
(3) 運用保守拠点とクラウド環境間回線	28
(4) 本学園本部とクラウド環境回線	28
(5) クラウド環境とインターネット間接続回線	28
9.4 各環境の位置づけ	29
(1) 本番環境	29
(2) 検証環境	29
9.5 設備要件	30
(1) 環境マネージメント	30
10 教育に関する事項	30
10.1 教育対象者の範囲、教育の方法	30
10.2 教材の作成	30
11 運用・保守に関する事項	31
11.1 運用・保守要件	31
(1) メンテナンス作業役割分担	31
(2) オペレーション体制	31
(3) 運用・保守期間	31
(4) 定期保守	31
(5) 活性保守	31

(6) 予防保守	31
(7) リモートオペレーション.....	31
(8) マニュアル準備レベル.....	31
(9) オペレーション訓練.....	32
(10) 定期報告	32
(11) サービスデスクの設置有無.....	32
11.2 保守対応要件	32
(1) 保守サポート（ハードウェア、ソフトウェア）	32
(2) 保守部品確保レベル.....	32
(3) 保守時間	32
(4) サポート要員.....	32
11.3 システム監視方針.....	33
(1) システム監視方針.....	33
(2) 監視内容	33
(3) 監視結果通知方法.....	33
11.4 運転管理方針	33
(1) 運用時間	33
(2) 運用の自動化.....	34
(3) 時刻同期設定の範囲.....	34
11.5 運用故障対応	34
(1) 運用故障対応方針.....	34

別紙一覧

別紙⑥－1 運用保守用端末等一覧

別紙⑥－2 ソフトウェア一覧

1 システム方式に関する事項

受託者は以下に示すシステム方式に関する事項を満たすこと。

1.1 情報システムの構成に関する全体の方針

(1) 全体方針

- ・ システムのトータルコストの削減を図る。無駄をなくし、非機能要求レベルとの最適なバランスをとる。
- ・ 約9万人の学生が快適に利用できるようにするための性能を確保する。
- ・ 学修環境の変化等に合わせて業務を変化させていく必要があり、業務の変化に対応できるようクラウド化することで、拡張性を確保する。
- ・ 個人情報を多く保持することから、悪意ある者からの攻撃を防ぐため、網羅的・多層的なセキュリティ対策を行う。

(2) 非機能特性ごとの方針

表 1-1 非機能特性ごとの方針

項番	特性	方針
1	可用性	過剰なレベルとならないようにすること。コスト面も踏まえて可用性を確保する。
2	性能・拡張性	9万人の学生が利用することから、同時に快適に利用できるようにするため、レスポンス性能を確保する。 業務の変化に対応する必要があることから、柔軟にリソース提供できるようにするため、リソース拡張性を確保する。
3	運用・保守性	職員、教員が行っている手動作業の負荷軽減のため、必要に応じて作業の自動化を実施する。
4	セキュリティ	個人情報を狙った攻撃が増えていることから、情報資産を守るため、NISC や IPA の推奨するセキュリティ対策を実施する。
5	システム環境・エコロジー	法令及び規約を遵守する。

1.2 次期システム WAKABA 基盤の全体構成

次期システム WAKABA 基盤の構成を図 1 に示す。構成の変更を提案する場合には、変更の根拠を示すこと。受託後、関係事業者等と協議した上で、本学園の承認を受けること。

クラウド環境とインターネットとの接続回線は受託者が用意すること(図 1 では例として SINET 回線を利用した構成としている)。

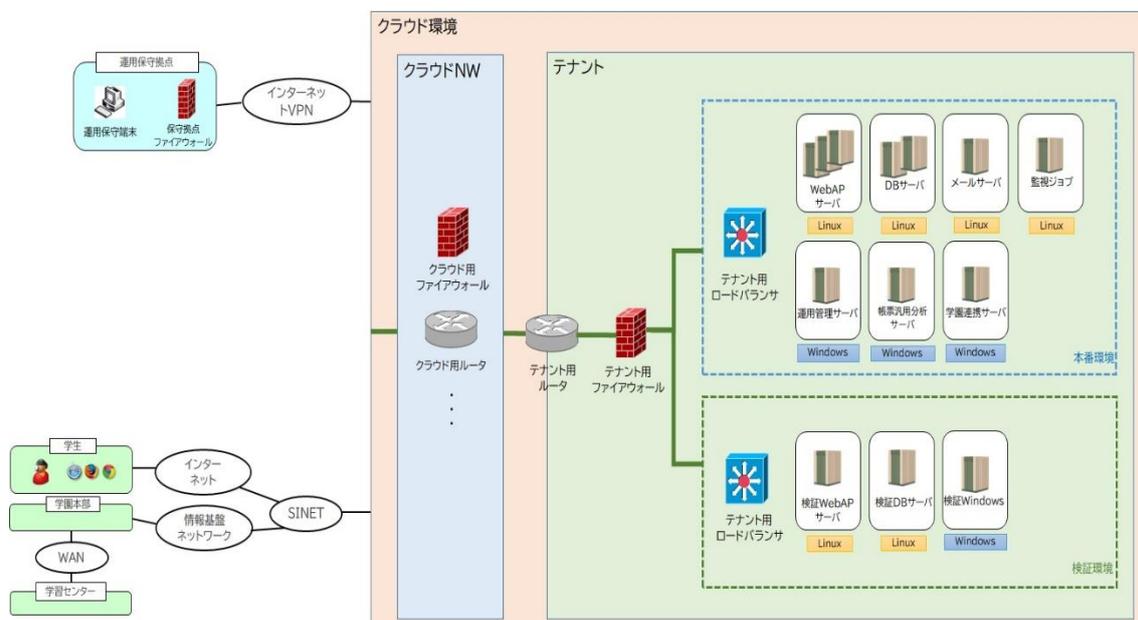


図 1 次期システム WAKABA 基盤の全体構成

補足として、図 1 における各種サーバの要件について以下に示す。

表 1-2 各種サーバの要件

項番	構成要素名	説明
1	WebAP サーバ	学生、職員、教員からの Web リクエストを受け付けて業務処理を行う、システムの基幹となるサーバ。CPU：4 コア、メモリ：54GB 以上のサーバを 3 台提供すること。
2	帳票・汎用分析サーバ	帳票の作成及び汎用分析(次期 WAKABA の DB データを用いてデータ分析を行う業務)を行うサーバ。CPU：4 コア、メモリ：15GB 以上のサーバを 1 台提供すること。

項番	構成要素名	説明
3	メールサーバ	メールを送信するためのサーバ。CPU：2コア、メモリ：4GB以上のサーバを1台提供すること。
4	学園連携サーバ	関連外部システムと連携するためのサーバ。CPU：2コア、メモリ：5GB以上のサーバを1台提供すること。
5	運用管理サーバ	保守拠点からのリモート接続先となるサーバ。CPU：2コア、メモリ：8GB以上のサーバを1台提供すること。
6	監視・ジョブサーバ	各種サーバやネットワーク機器、サービスの監視を行うためのサーバ。また、ジョブ（夜間バッチやバックアップ等）の実行・管理を行うためのサーバ。CPU：2コア、メモリ：6GB以上のサーバを1台提供すること。
7	DBサーバ	データベースを担うサーバ。クラスタリングソフトウェアにより Active-Standby 構成（HA 構成）で可用性及び性能を担保すること。CPU：4コア、メモリ：63GB以上のサーバを2台提供すること。
8	WebAPサーバ （検証環境）	検証を行うための WebAP サーバ。CPU：2コア、メモリ：67GB以上のサーバを1台提供すること。
9	DBサーバ （検証環境）	検証を行うための DB サーバ。CPU：2コア、メモリ：26GB以上のサーバを1台提供すること。
10	Windowsサーバ （検証環境）	ウイルス対策ソフトの管理や検証を行うための Windows サーバ。CPU：2コア、メモリ：4GB以上のサーバを1台提供すること。

2 規模・性能に関する事項

受託者は以下に示す規模・性能に関する事項を満たすこと。ただし、次期 WAKABA アプリケーション機能に伴う不具合による影響は除く。

2.1 利用ユーザ数

次期 WAKABA の利用ユーザ数は下記を想定している。参考とすること。

- ・ 学生は 9 万人を想定すること。
- ・ 教職員数は下記を想定すること。
 - ✓ 職員数：約 260 名
 - ✓ 期間業務職員等：約 550 名
 - ✓ 専任教員：約 90 名
 - ✓ 客員教授等：約 2,500 名(客員教員及び非常勤教員含む)
 - ✓ 特任教授(学習センター所長)：50 名

2.2 オンライン処理性能設計

次期 WAKABA のピーク時の同時アクセス数は 8000 ユーザとし、スループットは 99.9TPS としている。

業務性能要件一覧（オンライン処理）は表 2-1 のとおり定義しているため参考とすること。なお、本要件はピーク時に縮退構成（Web AP サーバが全台で動作していない状態）となった場合を除くものとする。

表 2-1 業務性能要件一覧（オンライン処理）

項番	項目	代表業務	レスポンスタイム要件
1	定型的な 検索処理	学生番号を指定した 学生検索	・システム内* 平均 5 秒以内 (90%ile)
2	参照系処理	学籍照会	・システム内* 平均 5 秒以内 (90%ile)
3	更新系処理	学籍設定	・システム内* 平均 5 秒以内 (90%ile)

(注) * レスポンスタイムはネットワーク、クライアントネットワーク、クライアント画面表示時間を含まない。

2.3 バッチ処理性能設計

次期 WAKABA のバッチ処理性能は下記のとおり定義している。

- ・ 通常時とピーク時においては、下記のように定義する。
 - ✓ 日次バッチが午前 0 時～午前 6 時までに終了すること。

- ✓ システムの正常稼働に必須のバッチの場合、再実行の時間を確保すること。
- ・ 縮退時は下記のように定義する。
 - ✓ 日次バッチが午前 0 時～午前 6 時までに終了すること。
 - ✓ ただし、再実行の時間は確保しない。

2.4 帳票出力性能設計

次期システム WAKABA の帳票出力性能は下記のとおり定義している。
業務性能要件一覧（帳票処理）を表 2-2 に示す。

表 2-2 業務性能要件一覧（帳票処理）

項番	項目	代表業務	レスポンスタイム要件
1	帳票作成・CSV 出力 処理	学生番号を指定した 単票出力	・システム内* 平均 5 秒以内 (90%ile)

(注) * レスポンスタイムはネットワーク、クライアントネットワーク、クライアント画面表示時間を含まない。

2.5 スパイク負荷対応

同時トランザクション数の制御機能に加えて、同時トランザクション数を超えた場合、次期システム WAKABA の利用者向けに Sorry 画面を表示すること。

3 信頼性に関する事項

受託者は以下に示す事項を満たすこと。

3.1 可用性に関する事項

(1) 可用性に係る目標

① 運用スケジュール

- ・ 次期システム WAKABA は 24 時間 365 日の運転を原則としているため、単一故障によるサービス停止とならないよう必要なハードウェアについては二重化を図り、可用性を確保すること。24 時間 365 日稼働であるが、計画停止時はシステムを停止することができる。
- ・ 運用時間における次期システム WAKABA の計画停止は、本学園と調整の上、実施可能とすること。なお、クラウド事業者による計画停止についても、計画停止の情報を把握次第、関係者と調整を行うこと。
- ・ 計画停止の時間帯については、ユーザの利用が比較的少ない時間帯を想定すること。
- ・ 計画停止時には次期システム WAKABA の利用者向けに Sorry 画面を表示できること。

② 稼働率

次期システム WAKABA の稼働率は 99.9%以上を確保すること。なお、24 時間 365 日の運転における停止可能時間は、年間 8.76 時間である。

次期システム WAKABA の稼働率の対象となる業務は以下の業務となる。

- ・ 次期システム WAKABA アプリケーションのポータル機能から学生及び教員が利用できるサービス・業務
- ・ 次期システム WAKABA アプリケーションのポータル機能から職員が利用できる業務（ただし、汎用分析機能は含まない）
- ・ 次期システム WAKABA と連携する外部システムとの連携機能
- ・ 次期システム WAKABA アプリケーションの業務バッチ処理（異常終了することで、オンライン処理に影響を与えるもの）

③ RPO、RTO、RLO

RPO、RTO、RLO を定義する。

(a) RPO (目標復旧地点)

- ・ 業務データ
 - ✓ 原則、1 営業日前の状態に復旧すること。
- ・ 業務データ以外のデータ (システムデータ、ログ等)
 - ✓ 原則、バックアップを最後に取得したタイミング (前日やシステム変更時等) の状態に復旧すること。
 - ✓ 目標復旧地点のレベルを確保するように、データの耐障害対策を行うこと。

(b) RTO (目標復旧時間)

年間平均での目標復旧時間を 4 時間とする。クラウド事業者で対応するべき障害内容を除き、原則 4 時間以内の復旧を行うこと。ただし、遠隔地バックアップを伴う障害への復旧時間については、1 営業日以内の復旧を目標とすること。

(c) RLO (目標復旧レベル)

業務停止を伴う障害が発生した際の復旧においては、稼働率の対象となる全ての業務とサービスが正常に利用可能な状態となっていること。

④ 復旧作業

- ・ 手順書、スクリプト及び復旧製品を用いて短時間で確実な復旧ができること。
- ・ 稼働率を考慮して可能な限り作業手順を自動化すること。
- ・ 業務停止となる障害が発生した際の復旧方法を事前に明確にし、その動作をテスト等で確認しておくこと。
- ・ クラウド事業者提供範囲における障害についても、机上での確認を行うこと。

(2) 可用性に係る対策

サーバ可用性確保方針は表 3-1 のとおり。

想定できる障害（例えばハードウェアの故障等により業務が一時的に中断するケース等）に対して、対策を施すこと（例えば冗長構成による切り離しなど）により、業務再開までに要する時間は、10分未満であること。

表 3-1 サーバ可用性確保方針

区分	サーバ等	故障箇所	二重化	対処など
1	WebAP サーバ (仮想)	ノード	○	縮退運転
		N I C	—	仮想マシンのため、故障を想定しない
		ディスク	—	仮想マシンのため、故障を想定しない
		電源装置	—	仮想マシンのため、故障を想定しない
2	DB サーバ (仮想)	ノード	○	ホットスタンバイによる待機系への切替
		N I C	—	仮想マシンのため、故障を想定しない
		ディスク	—	仮想マシンのため、故障を想定しない
		電源装置	—	仮想マシンのため、故障を想定しない
3	メールサーバ (仮想)	ノード	○	仮想マシンホストの HA クラスタによる切替
		N I C	—	仮想マシンのため、故障を想定しない
		ディスク	—	仮想マシンのため、故障を想定しない
		電源装置	—	仮想マシンのため、故障を想定しない
4	帳票・汎用分析サーバ(仮想)	ノード	○	仮想マシンホストの HA クラスタによる切替
		N I C	—	仮想マシンのため、故障を想定しない
		ディスク	—	仮想マシンのため、故障を想定しない
		電源装置	—	仮想マシンのため、故障を想定しない
5	学園連携サーバ(仮想)	ノード	○	仮想マシンホストの HA クラスタによる切替
		N I C	—	仮想マシンのため、故障を想定しない
		ディスク	—	仮想マシンのため、故障を想定しない
		電源装置	—	仮想マシンのため、故障を想定しない
6	運用管理サーバ(仮想)	ノード	○	仮想マシンホストの HA クラスタによる切替
		N I C	—	仮想マシンのため、故障を想定しない
		ディスク	—	仮想マシンのため、故障を想定しない

区分	サーバ等	故障箇所	二重化	対処など
		電源装置	—	仮想マシンのため、故障を想定しない
7	監視・ジョブサーバ (仮想)	ノード	○	仮想マシンホストの HA クラスタによる切替
		N I C	—	仮想マシンのため、故障を想定しない
		ディスク	—	仮想マシンのため、故障を想定しない
		電源装置	—	仮想マシンのため、故障を想定しない
		電源装置	—	仮想マシンのため、故障を想定しない
8	WebAP サーバ (検証環境) (仮想)	ノード	○	仮想マシンホストの HA クラスタによる切替
		N I C	—	仮想マシンのため、故障を想定しない
		ディスク	—	仮想マシンのため、故障を想定しない
		電源装置	—	仮想マシンのため、故障を想定しない
9	DB サーバ (検証環境) (仮想)	ノード	○	仮想マシンホストの HA クラスタによる切替
		N I C	—	仮想マシンのため、故障を想定しない
		ディスク	—	仮想マシンのため、故障を想定しない
		電源装置	—	仮想マシンのため、故障を想定しない
10	Windows サーバ (検証環境) (仮想)	ノード	○	仮想マシンホストの HA クラスタによる切替
		N I C	—	仮想マシンのため、故障を想定しない
		ディスク	—	仮想マシンのため、故障を想定しない
		電源装置	—	仮想マシンのため、故障を想定しない

3.2 完全性に関する事項

受託者は以下に示す完全性に関する事項を満たすこと。

(1) ログ管理方針

① ログ管理設計方針

- ・ 各サーバ上のログファイルは、日次で共有ストレージのバックアップ領域へ転送すること。(各サーバ上のログを一元管理することで、ログ管理作業の効率化をはかること。)
- ・ 共有ストレージへ転送が完了したログファイルは、1週間分サーバ上に保持すること。
- ・ 1週間を過ぎたものは各サーバ上から削除すること。
- ・ ログ管理実施対象全機器の全てのログを管理対象とはせず、システム運用、障害解析、セキュリティ対応における重要性や必要性を考慮して管理対象のログを選定すること。
- ・ 管理対象ログは、特性や用途に応じて以下の分類で選定すること。
 - ✓ OS ログ
 - ✓ ミドルウェア、ソフトウェアログ
 - ✓ 業務 AP ログ
 - ✓ その他ログ

② ログ保存期間

セキュリティに関するログの保存期間は 5 年間とすること。その他ログの保存期間は、ログの特性やディスク容量を考慮して決定すること。

なお、クラウドストレージの使用を終了すると本学園が決定した際は、クラウドストレージに保管されたログの直近 3 年分を取り出し、外部メディアに格納して本学園へ提供すること。当該外部メディアの調達についても、本調達範囲に含むものとする。

4 拡張性に関する事項

次期システム WAKABA 基盤の構成は、本項の方針に基づき定義している。

4.1 拡張範囲

(1) 拡張範囲

業務量の増加や機能の拡張性を考慮し、サーバ等の各種リソースについては拡張が可能であること。ただし、検証環境におけるサーバ等の各種リソースについては、業務量の増加や機能の拡張性を考慮しないものとする。

4.2 拡張性

(1) 拡張性確保方針

業務量の増加や機能の拡張性を考慮し、サーバ等の各種リソースについてはソフトウェアの改修を行うことなくスケールアップ又はスケールアウトが可能であること。

(2) リソース毎の拡張方針

リソース毎の拡張方針を表 4-1 に示す。

表 4-1 リソース拡張方針

項番	リソース	想定する拡張方針
1	CPU	時間平均で CPU 利用率 80%未満を目標とすること。 80%を超えた場合、拡張の検討を実施すること。
2	メモリ	時間平均でメモリ利用率 80%未満を目標とすること。 80%を超えた場合、拡張の検討を実施すること。
3	ディスク	ディスク利用率 80%未満を目標とすること。 80%を超えた場合、拡張の検討を実施すること。

(3) 拡張性確保方針

業務の拡大に備えて、仮想マシンの拡張性確保方針は以下とする。

- ・ サーバ処理能力の増強方法については、サーバ特性と拡張用途に応じて柔軟に対応すること。
- ・ スケールアップ及びスケールアウトともに、増強に必要なリソースを事前に確保しておく必要はないが、リードタイムを考慮した増強計画を立てること。

4.3 拡張対策

(1) 仮想マシン拡張方式

① リソース割り当て増強による拡張

リソースが不足した場合は、既存仮想マシンに CPU、メモリの割り当てを増強させることで処理能力の拡張を行う。

WebAP サーバにおいては、処理能力が不足する可能性があるため、仮想マシンのスケールアウトによる拡張を行う。

② 仮想マシン単位の拡張

負荷分散構成をとる仮想マシンにおいては、仮想マシン単位での増設を行う。増設の手順を以下に示す。

- ・ 増設する新仮想マシンの環境構築を行う。
- ・ 新仮想マシンを起動する。
- ・ 新仮想マシンを負荷分散構成に組み込み、振り分け対象に含める。

4.4 拡張方式

(1) 拡張方式（処理）

① オンライン処理、バッチ処理

サーバ処理能力の増強方法については、サーバ特性と拡張用途に応じて柔軟に対応すること。

スケールアップ及びスケールアウトともに、増強に必要なリソースを事前に確保しておく必要はないが、リードタイムを考慮した増強計画を立てること。

② 帳票出力処理、汎用分析処理

仮想ホスト上で動作する帳票汎用分析サーバは、スケールアップによる拡張を基本とすること。仮想ホストのリソースの空きがない場合、もしくは仮想マシンの割り当て上限に達している場合は、スケールアウトによる拡張を検討すること。

(2) 拡張方式（機器）

機器毎に拡張方式は表 4-2 のとおりとなる。

表 4-2 拡張方式

項番	サーバ	CPU	メモリ	ディスク	備考
1	WebAP サーバ（仮想）	CPU 利用率が目標とする80%を超えた場合、拡張を検討する。	メモリ利用率が目標とする80%を超えた場合、拡張を検討する。	ディスク利用率が目標とする80%を超えた場合、拡張を検討する。	空きリソースの割り当てが難しい場合、もしくは仮想マシンの割り当て上限に達している場合、スケールアウトを行う
2	帳票汎用分析サーバ（仮想）				
3	学園連携サーバ（仮想）				
4	メールサーバ（仮想）				
5	運用管理サーバ（仮想）				
6	監視・ジョブサーバ（仮想）				
7	ストレージゲートウェイ				
8	DB サーバ（仮想）				
9	WebAP サーバ（検証環境）（仮想）	確保しない	確保しない	確保しない	機能確認を目的としているため、拡張性を考慮しない
10	DB サーバ（検証環境）				
11	検証 Windows サーバ（検証環境）				

5 上位互換性に関する事項

受託者は、以下に示す上位互換性に関する事項を満たすこと。

5.1 パッチリリース管理

(1) パッチリリース情報の提供

パッチリリース情報を取得した場合は、可能な限り速やかに本学園及び AP 開発事業者もしくは AP 運用保守事業者を含む関係者へ周知すること。

(2) パッチ適用方針

パッチ適用方針は以下を考慮して、本学園及び AP 開発事業者もしくは AP 運用保守事業者を含む関係者と協議、調整の上、必要なパッチを適用すること。

- ・ 緊急性
- ・ 重要性
- ・ 次期システム WAKABA 基盤の動作への影響
- ・ アプリケーション改修・試験への影響

(3) パッチ検証の実施有無

本番環境への適用前に検証環境で現業務・サービスへの影響度を十分に検証した後、実施をすること。

(4) リリース作業の自動化

作業ミスを低減するため、サーバ・運用端末への更新ファイルの配布作業を可能な限り自動化すること。自動もしくは手動で配布したのち、更新処理を手動で実行して、パッチをリリースすること。

(5) パッチ適用タイミング

パッチ適用のタイミングは定期保守時とすること。また、障害発生時や緊急性の高い脆弱性発見時には、必要に応じて臨時でパッチ適用を行うこと。

6 中立性に関する事項

受託者は、以下に示す中立性に関する事項を満たすこと。

- ・ 特定の事業者や製品、クラウド環境に依存することなく、他者に引き継ぐことが可能なシステム構成であること。

7 継続性に関する事項

受託者は以下に示す継続性に関する事項を満たすこと。

7.1 バックアップ/リカバリ

(1) バックアップ方針

① 共通方針

(a) バックアップ対象

バックアップは業務データ（データベース、データベース外の業務ファイル等）、システム基盤データ（ログ、OS、ミドルウェア、ネットワーク機器など）、について行う。

(b) バックアップ取得間隔

データ種別に応じて以下から取得方式を選択すること。

- ・ 日次バックアップ
スケジューラを使用し日次でバックアップを取得すること。
- ・ 毎時バックアップ
スケジューラを使用し毎時でバックアップを取得すること。
- ・ 非定期バックアップ
任意の日時にバックアップを取得すること。

(c) バックアップ取得先

通常時は共有ストレージにバックアップを行うとともに、大規模災害に備えた遠隔地バックアップを行うこと。クラウド環境を利用したオンラインストレージ（以下、「クラウドストレージ」）を活用する場合は、データの保管場所が日本国内となるサービスを利用すること。また、インターネットから論理的に分離されたプライベートストレージ領域に保管すること。

通常時バックアップの対象、取得先を表 7-1 に、遠隔地バックアップの対象を表 7-2 に示す。

表 7-1 通常時バックアップの対象

項番	バックアップ対象	取得先
1	業務ファイルデータ	クラウド上の共有ストレージ
2	外部システムからの連携データ	
3	DB データファイル	
4	DB アーカイブログ	
5	DB 制御ファイル	
6	DB 初期化パラメータファイル	
7	OS ログ・ミドルウェアログ	
8	業務 AP ログ	
9	システムバックアップ（仮想マシンの OS・ミドルウェア）	クラウド上の共有ストレージ
10	システムバックアップ（ネットワーク機器、共有ストレージ及びサーバ機器の構成情報）	

表 7-2 遠隔地バックアップの対象

項番	区分	バックアップ対象	対象方針
1	業務	業務ファイルデータ	最新一世代
2		外部システムからの連携データ	
3	データベース	DB データファイル	最新一世代
4		DB アーカイブログ	
5		DB 制御ファイル	
6		DB 初期化パラメータファイル	
7	ログ	仮想基盤管理ソフトウェアログ	管理対象のログ を最長 60 か月分
8		OS ログ・ミドルウェアログ	
9		業務 AP ログ	
10		監査証跡ログ (セキュリティに係るログ)	最長 60 か月分

(d) バックアップ自動化の範囲

- ・ バックアップは極力業務に影響を与えないように実施すること。
- ・ 操作ミスなどによるバックアップの失敗を回避するために、バックアップは極力自動化すること。

② 対象ごとのバックアップ方針

バックアップ対象ごとのバックアップ方針を表 7-3 に示す。

表 7-3 対象ごとのバックアップ方針

項番	バックアップ対象	取得間隔	自動取得 or 手動取得
1	DB、外部システムからの連携データ、業務ファイルデータ	日次：フルバックアップ 毎時：更新ログ	自動取得（任意タイミングで手動取得可）
2	ログバックアップ	日次	自動取得（任意タイミングで手動取得可）
3	システムバックアップ （OS、ミドルウェア、ネットワーク機器）	非定期（システム変更時）	手動（可能な限り自動化）

(2) リカバリ方針

① 復旧作業

- ・ 可能な限り復旧用製品による復旧を実施すること。ただし、復旧専用製品である必要はない。（例：データベース製品のリストア機能など）
- ・ ネットワーク機器のように復旧用製品が対応していない機器については、ベンダー推奨の手順により手動復旧すること。

② リカバリ自動化の範囲

一部のリカバリ作業を自動化すること。ただし、リカバリは障害の範囲やケースによってリカバリ方法が大きく異なるため、全てを自動化することはない。

③ 外部データの利用可否

リカバリに使用するデータは、事前に取得したバックアップデータとし、外部データを利用しない。（外部データ：次期システム WAKABA の外部の連携先システムのデータ）

④ リカバリ対象外の範囲

以下についてはリカバリの対象外とする。

- ・ 遠隔地バックアップを含め、全てのバックアップを同時破損した場合
- ・ バックアップ取得後に共有ストレージ上のファイルシステムに実施された変更
- ・ バックアップ取得後に収集した監視・ジョブイベント情報
- ・ バックアップ取得後の OS・ミドルウェア設定ファイルへの変更

⑤ 目標復旧地点

通常時及び遠隔地バックアップにおけるバックアップ対象毎の目標復旧地点を以下に示す。

なお、遠隔地バックアップを用いたリカバリについては表 7-4 を対象とすること。

表 7-4 バックアップ対象と目標復旧地点

項番	バックアップ対象	目標復旧地点 (RPO)
1	DB バックアップ、外部システムからの連携データ、業務ファイルデータ	原則、障害発生から 1 営業日前時点
2	ログバックアップ	障害等解析用にバックアップ保管対象であるためリカバリは不要。
3	システムバックアップ (OS、ミドルウェア、ネットワーク機器)	直近のシステム変更時バックアップ取得時点

7.2 大規模災害対応

(1) 災害対策範囲

- ・ 災害対策を実施している設備を利用すること。
- ・ 以下に災害の例を記載する。
 - ✓ 地震
 - ✓ 瞬電・停電
 - ✓ 火災
 - ✓ 漏電
 - ✓ 雷
 - ✓ 水害
 - ✓ 電界・磁界
 - ✓ テロ

(2) 復旧方針

- ・ DR サイト（ディザスタリカバリサイト）は用意しない。
- ・ 東日本大震災と同等規模の地震が発生しても業務データは損失せず復旧できる対策を行うこと。
- ・ 災害後に業務を再開する場合は、災害の影響や業務再開の時期を考慮して、同一の構成又は稼働率の測定対象としている業務に必要な限定された構成でシステムを再構築する方針とすること。
- ・ 大規模災害時でも通常時と同じ目標復旧地点に戻せることが望ましい。困難な場合は、可能な限り直前までの復旧とする。

(3) 保管場所分散度、保管方法

以下のいずれかの対策を行い、災害時でもバックアップデータが損失しないようにすること。

- ・ 少なくとも 1 ヶ所以上の遠隔地にバックアップデータを保管すること。なお、クラウドサービスを利用したバックアップにおいて、拠点の所在が明らかにならない場合は、その安全性について本学園と協議の上で開発時に設計すること。
- ・ バックアップデータを複数の施設で、複数のデバイス・メディア上に、冗長的に格納し保管すること。

8 情報セキュリティに関する事項

受託者は以下に示す情報セキュリティに関する事項を満たすこと。

8.1 情報セキュリティに関するコンプライアンス

- ・ 次期システム WAKABA 基盤の開発時及び運用時は以下の規則を順守すること。
 - ✓ 放送大学学園情報セキュリティポリシー 基本方針
 - ✓ 放送大学学園情報セキュリティポリシー 対策基準
- ・ 個人情報保護に関して、以下を順守すること。
 - ✓ 個人情報の取扱いに係る事項については、本学園と協議の上十分なセキュリティ対策を行うことと。また、個人情報の適正な取扱いを図るための責任者を選任し、併せて報告すること。
 - ✓ 受託者が個人情報を複製する際には、事前に本学園の許可を得ること。ただし、複製の実施は必要最小限とし、複製が不要となり次第、その内容が絶対に復元することができないように破棄・消去すること。
 - ✓ 受託者が、本調達業務を履行する上で個人情報の漏えい等、個人情報の秘密保持に反する行為及び安全確保の上で問題となる事案等を把握した場合には、直ちに本学園に報告すること。
 - ✓ 受託者が、個人情報の取扱いにおいて、適正な取扱いをしなかった場合は、本調達業務の契約解除の措置を受けることがある。上記の規則に規定されている法令を順守すること。
- ・ 契約書の規定を順守すること。
- ・ 規則が競合した場合セキュリティ強度が強い方の規則を順守すること。

8.2 セキュリティリスク分析

次期システム WAKABA はインターネットに接続しており、ネットワークを通じた不特定多数の攻撃者からの脅威にさらされるため、セキュリティリスク分析を実施すること。なお、セキュリティリスク分析の範囲は、次期システム WAKABA の開発範囲とすること。守るべき資産を定義し、その資産ごとに発生しうるリスクや脅威を分析すること。

なお、セキュリティリスク分析は開発時点において AP 開発事業者が実施する。

8.3 セキュリティ診断

Web アプリケーション、サーバ、ネットワーク機器に対して第三者の専門技術者による以下の診断を行うこと。

- ・ 人手による擬似的な攻撃の実施
- ・ 脆弱性診断ツールを使用した網羅的なチェック

8.4 セキュリティリスクの見直し

受託者は以下のような想定イベントの発生有無を確認し、発生した場合に、システム全体に対するセキュリティリスクの見直しを行い、本学園と協議の上、対応方針を定めること。

- ・ 緊急性の高い脆弱性が見つかった場合
- ・ NISC（内閣サイバーセキュリティセンター）や IPA（独立行政法人 情報処理推進機構）等の対策ガイドラインが改訂された場合

8.5 セキュリティパッチ適用

(1) セキュリティパッチ適用範囲

セキュリティパッチ適用範囲は、次期システム WAKABA 基盤とすること。

なお、クラウド事業者が提供する機器についても対象範囲とすること。

(2) セキュリティパッチ適用方針

セキュリティパッチ適用方針は以下を考慮して本学園と調整の上、必要なセキュリティパッチを適用すること。

なお、クラウド事業者が提供する機器に対するパッチ適用方針についても同様に、以下を考慮して本学園と調整を行うこと。

- ・ 緊急性
- ・ システム動作への影響
- ・ アプリケーション改修・試験への影響
- ・ 環境や運用に対する脆弱性の該当状況
- ・ セキュリティリスク
- ・ セキュリティパッチの適用計画

(3) セキュリティパッチ適用タイミング

原則、システム計画停止時にセキュリティパッチを適用すること。ただし、セキュリティインシデントが発生した場合や緊急性が高い脆弱性が見つかった場合は、本学園と協議の上、必要に応じて臨時でパッチを適用すること。

8.6 認証機能

(1) システム管理者権限を持つ主体の認証

システム管理者権限の認証は、複数回の認証を行うこと。

なお、認証は ID/パスワードを想定すること。

(2) システム管理者権限を持たない主体の認証

- ・ ユーザ ID、パスワード入力によるログイン機能を有すること。
- ・ 本学園の統合認証基盤への対応を行うこと。
- ・ パスワードは入力内容を非表示とすること。

8.7 操作制限

(1) システム上の対策における操作制限

- ・ ユーザレベルの管理ができること。
- ・ グループまたは個人ごとの設定により、利用できる機能を制限できること。

(2) 物理的な対策による操作制限

ファシリティ（データセンター、運用保守拠点等の施設、建物）やサーバ機器等に対し、物理的なセキュリティ対策を実施すること。なお、クラウド事業者が提供する機器についても同様にセキュリティ対策を実施すること。

8.8 管理方法

(1) 管理ルールの策定

運用保守作業において、認証に必要な情報（ID/パスワード等）の追加、更新、削除、パスワード初期化、アカウントロック解除等のルール策定を支援すること。

8.9 データ暗号化

(1) 伝送データの暗号化の有無

インターネットを流れるデータについては、全て暗号化を実施すること。

教職員が使用するネットワークについては、暗号化の実施又はセキュアな通信経路を利用すること。どのようなセキュリティを確保するのかを提案すること。

(2) 蓄積データの暗号化の有無

データベースに格納された情報について、少なくとも重要情報について暗号化を行うこと。

(3) 鍵管理

鍵管理については、セキュリティを考慮し、適切な方式を採ること。

8.10 不正監視

(1) ログの取得

不正利用の状況をログから追跡出来るように利用者の全てのデータアクセスに対してログを採取できること。

なお、ブラウザを閉じる等を行った場合のログアウトのログは除く。

(2) ログ保管期間

ログの保管期間は、サービス開始から 60 か月（5 年）とすること。

(3) 不正監視対象（装置、ネットワーク、侵入者・不正操作等）

不正監視対象（装置、ネットワーク、侵入者・不正操作等）は、次期システム WAKABA 基盤全体とすること。なお、クラウド事業者の提供するハードウェア機器及びデータセンターについても監視を行うこと。

(4) 検知と自動通知

システムで検知可能なセキュリティインシデントが発生した際に、自動で通知できること。

8.11 ネットワーク制御

(1) 通信制御

- ・ 不要なプロトコル・通信ポートについては通信を遮断すること。
- ・ 本学園と調整の上、必要に応じて IP アドレスの通信制御を行うこと。
- ・ ネットワークの観点で、入口対策、出口対策、内部対策等の有効な対策が実施されていること。
- ・ 本調達で整備するウェブサイトにおいて、本学園より IP アドレスによる接続可否の制御を依頼(調達期間中、必要に応じて随時)することがあるので、受託者側で対応すること。

8.12 不正検知

(1) 不正通信の検知範囲

不正通信の検知範囲は、次期システム WAKABA の外部との接続部分（職員/教員/学生等次期システム WAKABA 利用者からの業務処理依頼等の接続の範囲、及び次期システム WAKABA と連携する外部システムとの接続範囲）とすること。

8.13 サービス停止攻撃の回避

(1) ネットワークの輻輳対策

サービス不能攻撃（DoS、DDoS 攻撃）について、影響を排除する対策、または低減する対策を実施すること。

8.14 マルウェア対策

(1) マルウェア対策実施範囲

マルウェア対策実施範囲は、原則としてサーバ等を設置するデータセンター内の機器及び運用保守拠点内の機器を対象とすること。

8.15 Web 実装対策

(1) Web サーバの設定等による対策の強化

データの漏洩、改ざんやシステムへの不正アクセスを防ぎ情報の機密性を高く保つために、Web サーバの設定等による対策の強化を実施すること。

8.16 セキュリティ強化

セキュリティ強化の観点から、入口対策、出口対策、内部対策等の有効な対策が実施されていること（Web 対策、ネットワーク対策、マルウェア対策等）。

9 次期システム WAKABA 基盤環境に関する事項

受託者は、以下に示す次期システム WAKABA 基盤の稼動環境に関する事項を満たすこと。

9.1 運用保守用端末等

次期システム WAKABA 基盤の運用保守用端末等について、「別紙⑥-1 運用保守用端末等一覧」に示す全ての要件を満たすこと。

9.2 ソフトウェア構成

次期システム WAKABA 基盤のソフトウェア構成について、「別紙⑥-2 ソフトウェア一覧」に示す全ての要件を満たすこと。

9.3 ネットワーク構成

クラウド環境とインターネットとの接続回線について、SINETを利用する場合は、以下の(1)から(3)に示す要件を満たすこと。また、SINETを利用しない場合は、以下の(3)から(6)に示す要件を満たすこと。

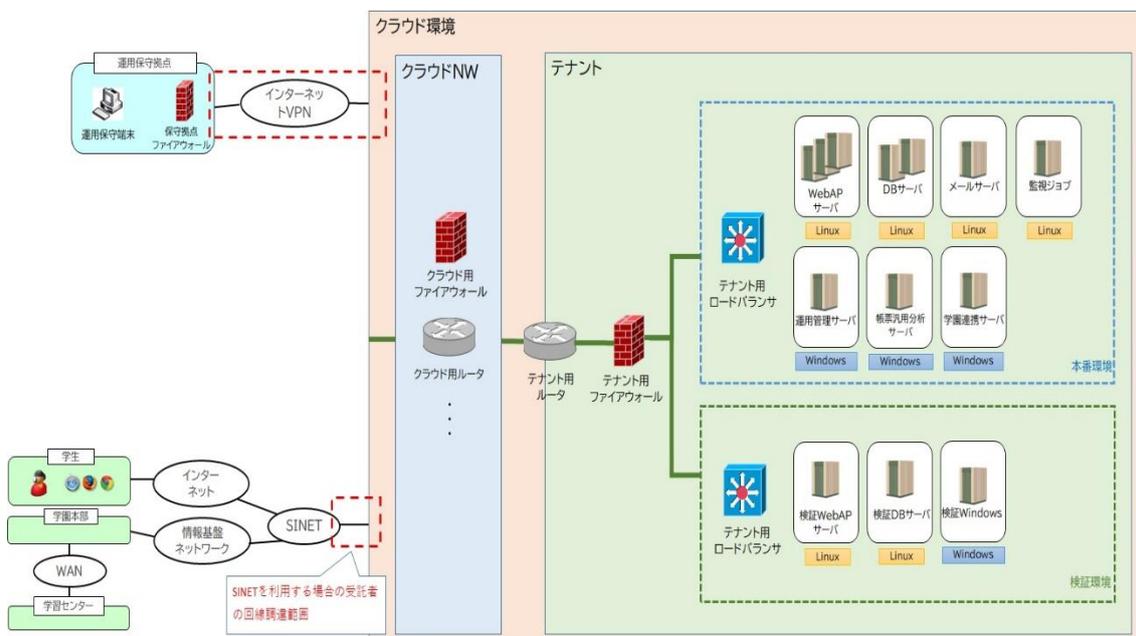


図 9-1 受託者の回線調達範囲 (SINET を利用する場合)

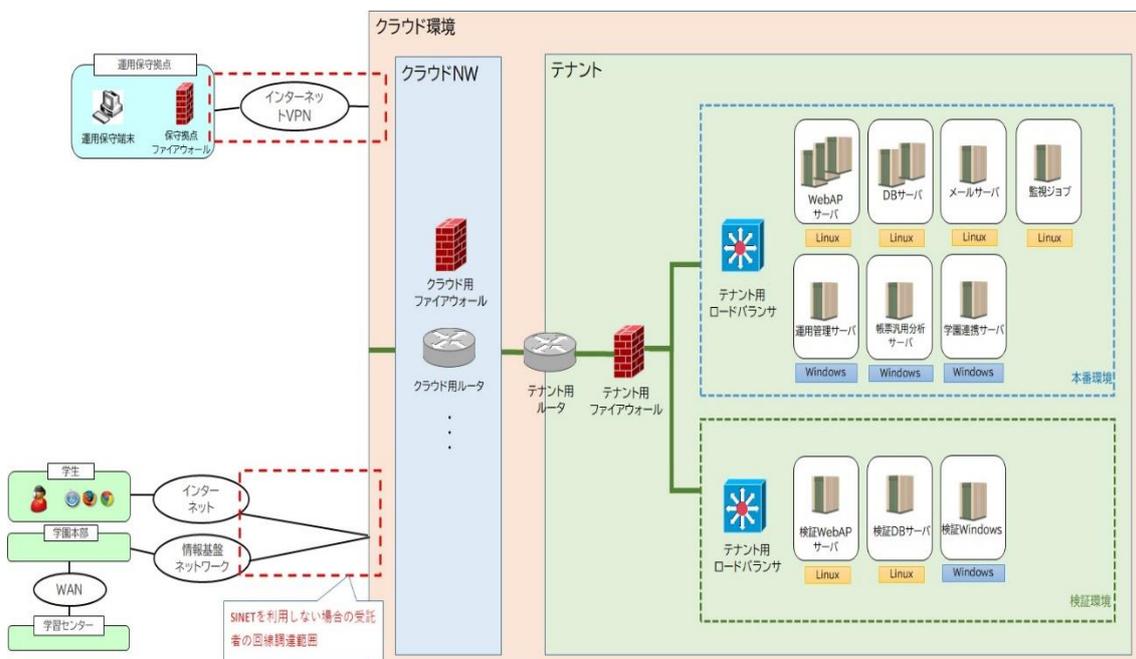


図 9-2 受託者の回線調達範囲 (SINET を利用しない場合)

(1) SINET 接続

クラウド環境及びインターネットと接続する回線は、SINET を利用すること。
SINET を利用する場合、受託者の回線調達範囲はクラウド環境及び SINET 間の回線とする。

- ・ 200Mbps 帯域保証回線とすること。
- ・ SSH/SCP、HTTPS 等の暗号化プロトコル用いた通信とすること。
または、事前に暗号化したデータを送受信すること。
- ・ 接続回線は、冗長化とすること。

(2) 本学園本部と SINET 接続ポイント間回線

本学園本部から次期システム WAKABA を操作する回線については本学園が用意する。受託者は本学園が用意した回線の貸与を受け、以下の要件を満たして利用すること。

- ・ SSH/SCP、HTTPS 等の暗号化プロトコル用いた通信とすること。

(3) 運用保守拠点とクラウド環境間回線

受託者が運用保守を行う場合は、必要に応じて運用保守拠点とクラウド環境を接続する回線を整備すること。通信は、暗号化プロトコルを用いた VPN 通信とすること。

(4) 本学園本部とクラウド環境回線

本学園本部から次期システム WAKABA を操作する以下の要件を満たす回線を提供すること。

- ・ 本学園本部とクラウド環境間を広域イーサネットまたは専用線で接続し、VPN 接続と同等のセキュリティを担保すること。
- ・ 50Mbps 以上の回線速度を保証すること。

(5) クラウド環境とインターネット間接続回線

クラウド環境とインターネットを接続する回線を提供すること。本回線は以下の条件を満たすこと。

- ・ 200Mbps 帯域保証回線とすること。
- ・ SSH/SCP、HTTPS 等の暗号化プロトコル用いた通信とすること。
または、事前に暗号化したデータを送受信すること。
- ・ 接続回線は、冗長化とすること。

9.4 各環境の位置づけ

次期システム WAKABA 基盤は、利用目的別に複数の環境から構成すること。各環境の位置づけを以下に示す。

(1) 本番環境

本学園の業務を行うために、各種サービスを提供するシステム環境とすること。

(2) 検証環境

次期システム WAKABA において、エンドユーザに安定したサービスと品質の維持・提供を続ける為に、表 9-1 に示すとおりとする。

表 9-1 検証環境の利用目的

項番	利用ユーザ	利用目的
1	・教員 ・職員	本番環境へ次期システム WAKABA アプリケーションをリリースする前の機能確認
2		操作が不慣れな教職員への研修
3		学生等からの問合せに関するシステム動作確認
4	・AP 運用保守業者 ・ハードウェア等運用 保守事業者	本番環境へ次期システム WAKABA アプリケーションをリリースする前の稼動・検証
5		OS やミドルウェアのバージョンアップやパッチ適用に関しての検証
6		その他、システムの安定稼動に必要な各種検証

9.5 設備要件

受託者は、以下に示す事項を満たすこと。

(1) 環境マネジメント

① 機材の運用・保守期間

機材の運用・保守期間は、サービス開始から 60 か月（5 年）とすること。

機材の運用・保守期間を満たせない製品を選定する場合は、選定の根拠を示すこと。

受託後、関係事業者等と協議した上で、本学園の承認を受けること。

10 教育に関する事項

受託者は以下に示す事項を満たすこと。

10.1 教育対象者の範囲、教育の方法

本学園の次期システム WAKABA 担当者及び AP 運用保守事業者の求めに応じて、業務上の役割、アクセス権限等を踏まえ、次期システム WAKABA 運用に向けた十分な教育、サポートを実施すること。

10.2 教材の作成

教育に用いる教材については、受託者において準備すること。

11 運用・保守に関する事項

受託者は、以下に示す事項を満たすこと。

11.1 運用・保守要件

(1) メンテナンス作業役割分担

次期システム WAKABA 基盤のメンテナンス作業全般及び障害対応全般を実施すること。

(2) オペレーション体制

運用・保守作業を行う際は、作業員・確認者の2名体制とする。

(3) 運用・保守期間

5年間（令和5年4月1日～令和10年3月31日）

(4) 定期保守

定期保守の頻度は年間2回を想定し、計画停止を計画すること。ただし、パッチ適用の必要性を考慮した上で、臨時保守の実施を検討すること。

(5) 活性保守

ハードウェアについて、可能な範囲で活性保守を行うこと。活性保守の対象がクラウド事業者提供の機器となる場合も同様とする。

(6) 予防保守

予防保守を行うこと。クラウド事業者提供のハードウェア機器についても、検出した予兆に応じて、クラウド事業者と連携して予防保守を行うこと。

(7) リモートオペレーション

運用性、保守性向上のため、遠隔地（運用・保守拠点）からのリモートオペレーション（リモート監視、リモート操作）を行うことができる。障害発生等により、遠隔地（運用・保守拠点）からのリモートオペレーションが困難となった場合は、駆けつけ保守を実施（対象機器を設置場所で直接操作してオペレーションを実施）すること。

また、汎用分析機能のメンテナンスのため、汎用分析サーバへのリモートオペレーションを、本学園の職員が汎用分析サーバ接続用専用端末を利用して本部から行うことができること。汎用分析サーバ接続用専用端末及び基本的なOSインストール、ウイルス対策ソフトウェアのインストールまでを本調達の対象範囲とするが、汎用分析サーバ接続用専用端末の情報基盤システム接続のための各種設定及び接続作業については本学園にて実施する。

(8) マニュアル準備レベル

システムの通常運用と保守運用のマニュアルを整備すること。運用期間中にシステム構成や手順の変更によりマニュアル修正が必要になった場合には対応すること。

(9) オペレーション訓練

保守・運用に関する訓練は、受託者が全て実施する。通常運用、保守運用に加えて、障害発生時の復旧作業に関する訓練を実施すること。訓練は年1回を目安に定期開催すること。

(10) 定期報告

本学園に対し、定期報告を四半期に1回実施すること。定期報告では、障害報告に加えて運用状況報告を行うこと。また、必要に応じて改善提案を行うこと。

(11) サービスデスクの設置有無

問合せ窓口として、周辺機器専用のサービスデスクを設置すること。

11.2 保守対応要件**(1) 保守サポート（ハードウェア、ソフトウェア）**

次期システム WAKABA 基盤を構成するハードウェア、ソフトウェアに対して、サポートを行う。

(2) 保守部品確保レベル

部品を提供するベンダーが、運用・保守期間の間、保守部品を確保すること。

(3) 保守時間

- ・ ハードウェア保守は、サービス停止を伴わないで保守作業が可能な機器（縮退運転等でサービスが継続）については、日中帯（9:00～18:00）オンサイトでの保守対応（土日祝日や年末年始等は含まない）を行う。ただし、サービス停止が発生する機器については 24 時間 365 日オンサイトでの保守対応を行う。
- ・ ソフトウェア保守は、サービス停止を伴わないで保守作業が可能なソフトウェアについては、日中帯（9:00～18:00）オンサイトでの保守対応（土日祝日や年末年始等は含まない）を行う。ただし、DBMS については 24 時間 365 日オンサイトでの保守対応を行う。

(4) サポート要員

- ・ 駆けつけ対応を行うサポート要員のスキルレベルは、システムの運用や保守作業手順に習熟し、ハードウェアやソフトウェアのメンテナンス作業を実施できるレベルとすること。次期システム WAKABA の必要な運用作業手順を理解していること。
- ・ サポート要員はオンコール待機とし、連絡があり次第駆けつけること。

11.3 システム監視方針

(1) システム監視方針

統合監視ソフトによる一元管理を実施すること。

(2) 監視内容

以下に示す監視を実施すること。監視間隔は、監視内容に応じて、秒間隔～分間隔の間で設定すること。

① 死活監視

対象のステータスがオンラインまたはオフラインの状態にあるかを判断する監視。

② エラー監視

対象が出力するログ等にエラー出力が含まれているかを判断する監視。また、次期システム WAKABA アプリケーションログから、どのモジュールでエラーが発生しているのかの詳細についても判断できること。

③ リソース監視

対象が出力するログや別途収集するパフォーマンス情報に基づいて CPU やメモリ、ディスク、ネットワーク帯域といったリソースの使用状況を判断する監視。

④ パフォーマンス監視

対象が出力するログや別途収集するパフォーマンス情報に基づいて、ディスク I/O、ネットワーク転送等のスループットについて判断する監視。

⑤ サービス監視

次期システム WAKABA アプリケーションの稼働状態を判断する監視。次期システム WAKABA アプリケーションの Web ページに http (s) リクエストを送信した応答結果で稼働状態を判断すること。

(3) 監視結果通知方法

障害検知時やリソース閾値超過時は、運用監視サーバ上の統合監視ソフトのクライアント画面に障害を通知すること。また、検知内容の緊急度や重要度に応じてメールによる障害通知も実施すること。

11.4 運転管理方針

(1) 運用時間

次期システム WAKABA は 24 時間 365 日稼働とすること。ただし、計画停止期間は除く。計画停止は年間計画によって確定し、年間計画は関係者間で十分に調整すること。ただし、脆弱性対応など緊急性の高い場合は、本学園及び AP 運用保守事業者を含む関係者と調整の上、直前の通知で次期システム WAKABA を停止する可能性がある。

(2) 運用の自動化

可能な限り自動運転を実現すること。

(3) 時刻同期設定の範囲

本調達内の機器について、NTP を利用して日本標準時と同期すること。ただし、全機器が本調達範囲外の NTP サーバと同期する必要はなく、代表機器のみ同期し、他の機器は、代表機器に同期してもよい。

11.5 運用故障対応**(1) 運用故障対応方針**

- ・ 故障対応を行うベンダーの営業時間内で故障対応を行う場合は、受託者は運用設計で想定する保守レベルの障害対応を実施すること。
- ・ 故障対応を行うベンダーの営業時間外で故障対応を行う場合は、受託者は可能な限り障害対応を実施すること。
- ・ 故障対応を行うベンダーが異常を検知してから数時間以内に保守員・SE が到着する。ただし、保守レベルがセンドバック保守の機器については、駆けつけ保守の対象としない。また、故障機器の代替機器をベンダーが事前に保有する場合は、速やかに代替機器を提供すること。

別紙⑥-1 運用保守用端末等 一覧

・以下に示す要件のスペック以上の物品を提供すること。

項番	分類	名称	要件	数量
1	NW機器	保守回線用ルータ	<ul style="list-style-type: none"> ・WAN側インタフェースとして、1000BASE-Tポートを2個以上有すること。 ・LAN側インタフェースとして、1000BASE-Tポートを14個以上有すること。 ・ファイアウォール機能を有していること。 ・IPsec VPN接続に対応していること。 ・IPsec VPNスループットが1Gbps以上であること。 ・機器故障時における可用性を高めるため、フェールオーバー機能を有すること。 ・本装置を机上に設置することが想定されるため、省スペースを考慮し、幅220mm、奥行き230mm程度の大きさであること。なお、EIA規格に準拠した19インチラックに搭載する場合は、棚板や専用金具などを用いて搭載するものとし、高さが1U以内であること。 	2
2	運用・保守用機器	運用・保守用端末	<ul style="list-style-type: none"> ・ノート型PC ・CPU インテル(R) Core(TM) i5-4310M相当 (2.7GHz - 3.4GHz/3MB)以上 ・メモリ 4GB以上 ・HDD 320GB以上 ・ディスプレイ 15.6インチ以上 ・指紋センサー ・日本語配列キーボード 	3
3		ディスプレイ	<ul style="list-style-type: none"> ・ディスプレイ(24型以上のフルHD液晶モニター) 	2
4	汎用分析機能メンテナンス用機器	汎用分析サーバ接続用専用端末	<ul style="list-style-type: none"> ・ノート型PC ・CPU インテル(R) Celeron(R) プロセッサ 3855U相当 (1.6GHz/2MB)以上 ・メモリ 4GB以上 ・HDD 320GB以上 ・ディスプレイ 15.6インチ以上 ・日本語配列キーボード 	1

別紙⑥-2 ソフトウェア一覧

- ・以下に示すソフトウェアを提供すること。
- ・提供するソフトウェアについて、次期システムWAKABAアプリケーションの動作に必須な製品を「◎」、推奨される製品を「○」としている。推奨される製品については、以下に示す製品と同等機能を有する異なるソフトウェアを選定することも可能とする。ただし、本選定に伴い、非機能設計、アプリケーションに影響が発生した場合は受託者の責において対応すること。

項番	ソフトウェア種別	製品名	数量(※)	製品指定
1	OS	Red Hat Enterprise Linux Server 8(仮想化ゲストOS ライセンス10台)	9	◎
2	OS	Microsoft Windows Server 2019 Standard (仮想インスタンス4台)	4	◎
3	OS	OS Microsoft Windows	4	○
4	Webサーバ	Apache 2.4	4	◎
5	Application Platform	WildFly 23.0	4	◎
6	データベース	Oracle Database Standard Edition 2 19c	3	
7	データベースクラスタソフトウェア	Pacemaker	1	○
8	帳票	SVF WebDesigner Limited 10.X	2	◎
		SVF Connect SUITE Standard Windows版 10.X	4	
		SVF PDF Enterprise Windows版 4コア 10.X	2	
		SVF WebDesigner Limited (HS) 10.X	1	
		SVF Connect SUITE Standard Windows版 (HS) 10.X	1	
		SVF PDF Enterprise Windows版 4コア (HS) 10.X	1	
9	データ連携	DataSpider Servista Basic Server Package 4.X	2	◎
		オプションアダプター(FTP) 4.X	2	
		追加Studio for Webクライアント	2	
10	アンチウイルス	McAfee Endpoint Security	16	○
		McAfee ePolicy Orchestrator	1	
11	監視・ジョブ	Hinemos Manager	2	○
		Hinemos Agent	16	
12	メール	Postfix 3.X	2	◎
13	学生証発行関連ソフト	CardPAS (L8110用)	115	◎
14	Office	Microsoft Office	3	○
15	SQLエディタ	SI Object Browser for Oracle(1クライアントライセンス)	1	○
16	SSL証明書	セキュア・サーバID	4	○
17	組み込みフォント	日本語True Type Font(HG正楷書体-PRO)	2	◎

※数量について、ライセンス数ではなくインストール対象のサーバ数である。