

京都府立大学制御系システム刷新業務

仕様書

第1章 調達概要

1.1 件名

京都府立大学制御系システム刷新業務

1.2 目的

本業務は、本学が運用する学内制御系システムについて、老朽化および運用上の課題を解消し、クラウド基盤への移行により可用性、拡張性およびセキュリティの向上を図ることを目的とする。

1.3 背景

本学においては、学内情報基盤の更新計画に基づき、システムの段階的刷新を進めている。現行の制御系システムはオンプレミス環境で運用されているが、以下の課題を有している。

- 機器の老朽化および保守期限の逼迫
- システム拡張性の制約
- 運用管理負荷の増大
- セキュリティ対策の高度化への対応不足

これらの課題を解決するため、クラウド基盤を前提としたシステム刷新を実施する。

第2章 業務範囲

2.1 対象業務

本業務における作業は、以下のとおり。

- 「第4章システム要求事項」に示すシステム環境の提供と本学向け環境構築に掛かる作業
- 「第5章移行要件」に示すシステム移行・切替に掛かる作業
- 「第6章保守要件」に示す運用保守の準備に掛かる作業

2.2 対象システム

本業務において更新対象とする現行システムは、以下のとおり。

- DNS システム(二重化)
- DHCP システム(二重化)
- Active Directory(セカンダリ)

- 学内向け Web サーバ(2 系統相当)

(参考:既存システムの情報)

- DNS システム(二重化)
 - ◇ ゾーン数:1 (kpu.ac.jp)
 - ◇ レコード数:100
 - ◇ 想定クライアント数:6,000
- DHCP システム(二重化)
 - ◇ 管理アドレス数:8913(レンジ範囲のみ) ※セグメントのホスト数:9196
 - ◇ 想定同時接続数:3,000
- Active Directory(セカンダリ)
 - ◇ ドメイン数:1 (kpuecs.kpu.ac.jp)
 - ◇ ユーザ数:6,000
 - ◇ グループ数:30(セキュリティグループ数)
 - ◇ OU:5
 - ◇ ホスト数:148
- 学内向け Web サーバ
 - ◇ コンテンツ容量:100GB

2.2 対象外システム

以下のシステムは本業務の対象外とする。ただし、将来的な連携を考慮した設計を行うこと。

- ネットワーク監視システム
- 全学認証基盤
- 無線 LAN システム
- シンクライアント環境

第 3 章 基本方針

3.1 クラウド利用

本業務においては、パブリッククラウドまたはクラウドサービスの利用を前提とし、オンプレミス環境の新規構築は認めないものとする。

3.2 提案方式

本調達是一般競争入札により実施するが、事業者は入札前に本仕様書の要件を満たす本業務に係るスケジュール表、提案書及び要求事項確認表を提出すること。

3.3 重視事項

提供する構成においては、以下の観点を重視して設計・構築すること。

- 可用性
- セキュリティ
- 運用性
- 拡張性

第4章 システム要求事項

4.1 クラウド基盤要件

提供するクラウド基盤は、以下の要件を満たすこと。

- 冗長構成による高可用性の確保
- 適切なリージョンおよびゾーン設計
- バックアップおよびリストア機能の提供
- 監視およびログ管理機能の実装
- 将来的な拡張に対応可能な構成

また、本学と提供されるクラウド基盤(クラウドデータセンタ)の間は、専用回線で接続を行うものとする。

4.2 システム要件

4.2.1 システム全体要件

システム全体としては、本仕様書を満たす構成を提供すること。

(1) システム利用規模想定

- 端末数:6,000
- 教職員数:1,000
- 学生数:5,000
- 同時接続数:3,000

(2) SLA(Service Level Agreement)

- クラウドデータセンターの月間稼働率 99.9%以上
※ただし、データセンターの計画停止は除く
- 障害受付 24 時間 365 日

(3) バックアップ

- 日次バックアップ

- 保存世代:基本的に7世代(1週間)以上とする。
なお、システム毎のバックアップは設計時に調整する

(4) セキュリティ要件

- 通信暗号化
- ログ保存:基本的に5年間と考えるが、設計時にログ種類毎に調整する
- OSパッチ適用:ゲストOSおよびミドルウェアのパッチ適用は、2回/年(3月,9月)の適用を基本とし、緊急時には本学と協議のうえ対応方針を決定する
- クラウド基盤は定期的にISOやSOC等のグローバル監査を受けていること

(5) 回線要件

- 本学とクラウドデータセンタ間は専用回線で接続する
- 構築する各システムとの通信はインターネット経由ではなく、専用回線で接続する

4.2.2 システム全体要件

各対象システムにおいては、適切な構成・実装を提供すること。

(1) DNS システム

要求事項を以下に示す。

- 権威DNSと内部DNSを分離した構成とすること
- 権威DNSと内部DNSは別サーバとすること
- 内部DNSは再帰問い合わせを許可すること
- 権威DNSは再帰問い合わせを許可しないこと
- 権威DNS、内部DNSはそれぞれ冗長構成とすること
- 既存ゾーン情報を移行すること

(2) DHCP システム

要求事項を以下に示す。

- IPアドレス管理機能を有すること
- フェイルオーバー構成とすること
- 管理対象端末数は前述のシステム利用規模想定端末数とする

(3) Active Directory

要求事項を以下に示す。

- 既存セカンダリADを移行すること
 - ・既存GPOの移行
 - ・既存OU構成の移行
 - ・既存ユーザ情報の移行
 - ・既存DNS連携機能の維持
- 認証基盤機能を提供すること

- 将来的な統合認証システムとの連携を考慮した構成とすること
- 既存サーバ撤去まで並行運用可能なこと

(4) 学内向け Web サーバ

要求事項を以下に示す。

- 学内サービスを提供する基盤とする
- Apache 又は同等の互換性を有する Web サーバを提供すること
- セキュリティ対策を講じた構成とすること
- SSL、TLS に対応すること
- 本学が提供するサーバ証明書が利用可能であること
- ファイルのアップロードは FTP(または SFTP/FTPS)が利用可能であること

(5) 本学-クラウドデータセンタ間回線

要求事項を以下に示す。

- 導入する回線は受託業者で用意するものとし、これの導入及び運用に掛かる費用も本調達に含めるものとする
- 専用回線は 2 本用意すること
- 2 本の専用回線のいずれかに異常が発生した場合、もう 1 本の回線へ切替を行うことで運用を継続できるものとする
- 回線速度は、構築するシステムにおいて本学の通信必要容量が問題なく通信できる回線を準備すること
- 本学で必要となる通信容量は、受託業者にて提供するシステム構成から試算を行い、必要となる回線を手配すること

4.3 セキュリティ要件

セキュリティ要件を以下に示す。

- ネットワーク分離を考慮した構成とすること
- アクセス制御および認証の適切な実装を行うこと
- ログの取得および監査機能については、ゲスト OS、ミドルウェア、対象サービスおよびクラウド基盤が備える標準機能により対応することを基本とする
- 監査ログの対象には、ゲスト OS のシステムログ、認証ログ、管理者ログイン・管理操作ログ、DNS/DHCP/AD/Web サーバ等のサービスログ、および障害解析に必要なログを含むものとする
- 取得対象ログ、保存期間、保存方法、保存先および閲覧・抽出方法については、設計時に本学と協議のうえ明確化し、設計書に記載すること
- 外部接続に対する適切な防御対策を行うこと
- 管理者アカウントの権限制御を行うこと
- 通信の暗号化(TLS)を行うこと

- OS およびミドルウェアの脆弱性対策について、受託者はクラウド基盤として提供可能なセキュリティ機能および推奨設定を提示すること
なお、ゲスト OS 上のセキュリティ対策ソフト等が必要となる場合は、別途提案事項として提示すること
- セキュリティパッチの適用方針については、受託者はクラウド基盤側で提供可能な更新管理機能、通知情報および推奨運用を提示すること
なお、適用作業は本学と協議のうえ、必要に応じて別途実施範囲を定めるものとする
- 監査ログは、障害解析、運用確認および監査対応に必要な範囲で保存すること

4.4 性能要件

性能要件を以下に示す。

- 本学の利用規模に応じたシステム性能を確保すること
- 想定負荷に対する応答性能を確保すること
- 本学が必要とする通信が遅滞なく通信できる回線であること

4.5 クラウドサービス要件

クラウドサービス要件を以下に示す。

- 提供するクラウドサービスは、日本国内でデータ主権が確保され、外国法令の影響を受けない、またはその影響を最小化したソブリンクラウドであること
- 提供するクラウドサービスは、ISMAP (Information system Security Management and Assessment Program) に対応したサービスを提供することとし、ISMAPクラウドサービスリストまたはISMAP-LIUクラウドサービスリストに掲載されている、もしくはISMAPへの登録申請中であること
- データ保存先は国内データセンターとする
なお、クラウドサービス提供事業者は、利用するデータセンターの所在地を明示すること
- 高可用なクラウドサービスを採用する
- 初期導入時のシステムサイジングは将来の利用を考慮したものではなく、現在の利用に応じた最適なサイジングを行い、スケーラビリティに対応できること
- リソース(CPU、メモリ、DISK)は運用状況に応じて柔軟に増減できるものとする
- 学内ネットワークとクラウド基盤間の閉域接続については、安定した通信を確保するための適切な構成を提供すること
- 月額費用を事前に明確化できる料金体系とすること
クラウドサービスの料金は月額固定とする
- バックアップおよびリストア機能を有し、障害時にバックアップデータから復旧可能であること
- システムは 24 時間 365 日監視を行うこと

- データセンター障害時の対応については、クラウドサービス提供事業者が公表するサービス仕様、SLA および障害情報に基づく対応を基本とし、受託者は本学への情報提供および連絡調整を行うこと
- 障害発生時には本学へ速やかに連絡すること
- 障害対応窓口を設けること
- 今後予定している全学認証システムおよびネットワーク監視システムとの連携を考慮した構成とする
- 契約終了時はデータの返却および完全消去が可能であること

第5章 移行要件

5.1 基本方針

現行システムから新システムへの移行は、業務への影響を最小限に抑えることを前提とする。

移行実施のうえでは、次の作業項目を含めること。

- 既存環境調査
- 移行リハーサル
- 切替計画
- 切戻し計画
- 移行後の動作確認

5.2 移行計画

DNS、DHCP、Active Directory、Web サーバ等の既存設定情報については、適切なエクスポートおよびインポート方式により移行すること。また、クラウド基盤における高可用性構成(HA 構成)を考慮した移行計画とすること。

なお、作業遂行においては以下の内容を含めた移行計画書を作成すること。

- 移行方式(段階的移行または一括移行)
- 移行スケジュール
- 並行稼働の有無および期間
- 切替手順
- 教育・引継ぎ
 - ・システム管理者向け説明会
 - ・運用手順説明
 - ・管理者教育

第6章 保守要件

運用保守要件を以下に示す。

- システム監視体制の確立
 - ・障害一次受付窓口を設けること
 - ・問い合わせ受付時間: 平日 8:30～17:15 とすること
 - ・障害発生時、重要な変更時または本学からの依頼時には、必要な情報を報告すること
- 障害発生時の対応体制の明確化
 - ・障害報告書を提出すること
- パッチ適用および更新管理
 - ・セキュリティパッチの適用方針については、受託者はクラウド基盤側で提供可能な更新管理機能、通知情報および推奨運用を提示すること
 - なお、適用作業は本学と協議のうえ必要に応じて別途実施範囲を定めるものとする
- バックアップおよび復旧手順の整備
 - ・バックアップ及び復旧の方針を示し、バックアップを取得すること
- クラウド基盤においては、24 時間 365 日の監視体制を整えること

また、保守時間は以下とする。

- 平日対応時間: 本学側の対応可能時間は平日 8:30～17:15 となる。このため、これ以外の時間における緊急対応は、以下のとおりとする。
- 緊急時対応: 緊急時においては、別途定める本学担当者へ連絡し指示を仰ぐこととする

第 7 章 プロジェクト管理

プロジェクト管理として、以下を明確にして提示すること。

- 実施体制および役割分担
- 進捗管理方法
- 課題管理方法
- 定期報告の実施
- 進捗報告および課題報告の実施

第 8 章 成果物と受け入れ

本業務における成果物は以下のとおりとする。

- 基本設計書
- 詳細設計書
- システム構成図
 - ◇ 論理構成図

- ◇ ネットワーク構成図
- ◇ 障害時の冗長構成図
- 運用手順書
- 移行手順書
- テスト報告書

設計には、取得対象ログ、保存期間、保存先、閲覧・抽出方法、監査ログ保全方針に関する設計内容を含むこと

なお、電子化された完成図書を本学検収後に提出すること。本図書は本学が加筆、修正、印刷できること。

また、構築完了後は成果物提出と共に本学による受け入れ試験を受けるものとする。

なお、受け入れ試験における合格判定基準は以下とする。

- システム設計後に本学が定める試験項目に合格すること
- 重大な不具合がないこと
- 課題は全て解決していること、もしくは解決のめどが立っていること

第9章 契約条件

契約条件は以下のとおりとする。

- 契約形態:業務委託契約

第10章 その他

- 本調達は、次年度の運用に伴う調達の採用を保証するものではない。
- 運用する環境構築に必要となる費用については全て本調達に含むものとする。
- 監査または情報提供依頼に応じて、クラウドサービス提供事業者が公開する SOC レポート、ISO 認証情報、サービス稼働情報等、クラウド基盤に関する公開情報または提供可能な情報を提示できること。

なお、本学固有環境に関する個別監査情報については、クラウドサービス提供事業者が提供可能な範囲に限るものとする。

- 業務の一部を再委託する場合は本学に申請し、その承諾を得ること。
- 本仕様書の記載事項について疑義が生じた場合は、本学と受注者との間で協議して定めるものとする。

以上