業務用電子計算機システム借上げ
及び運用保守業務
要件定義書

令和7年
独立行政法人　大学入試センター

目次

第 1 章　概要

1.1. 名称

業務用電子計算機システム借上げ及び運用保守業務

1.2. 目的

(1) 本システムは，主として大学入試センター内の利用者に向けてサービスを提供するものであり，メール・グループウェア機能及びファイル共有システム等のサービスを提供している。およそ 220 台のクライアント端末が稼働しており，職員数（ユーザ数）は 180 名程度である。

(2) ネットワークとしては，不正の防止及び発生時の影響範囲を限定するため，外部との通信を行うサーバ装置及び通信回線装置のネットワークと，内部のサーバ装置，端末等のネットワークを分離し，さらに業務目的，所属部局等に応じて内部のネットワークを分離している。

1.3. 構成

(1) 基本構成はオンプレミスで構築しつつ，OPEN 環境とそこで使用するサービスについては受注者の判断により，大学入試センターと協議のうえで，クラウドサービスを利用して構築することも可能とする。

(2) サーバ，ストレージ及びネットワーク等のハードウェア機器は，仮想化が適さないものを除き，仮想化技術を用いて集約すること。

(3) ハードウェアリソース（CPU，メモリ，ディスク容量，ネットワーク回線等）及びシステムリソース等を可視化し容易に再分配することに加えて，一元的に管理することでリソース配分の最適化，システム運用業務の負荷軽減，増築等に伴う設定変更の簡素化を図る。

(4) 障害時における業務継続性を向上させるため，物理障害のポイントを削減し，各サービスの特性を踏まえた冗長化構成，バックアップ体制を講じる。

(5) ハードウェアリソース逼迫時，障害時，災害時における各サービスの業務継続性の向上のため，論理構成及び物理構成を実装する。

(6) 昨今及び将来のサイバー攻撃に対応すべく，より強固なセキュリティ対策として，ゼロデイ脆弱性や既知及び未知の脅威に対しても常に最速，かつ，確実な検知・遮断，対応等を実現するために，最新の技術を適用したふるまい検知，ログ分析，監視等を導入し，侵入防止及び侵入後における適切な対策によるセキュアな環境を構築する。

(7) 職員は，次期システムを利用するにあたり，利便性とセキュリティ性に優れたシンクライアント端末を利用する。

(8) 無線 LAN 環境においては IEEE802.1x 認証を導入し，セキュリティを確保する。

第 2 章　情報システムの要件（調達物品に備えるべき技術的要件）

2.1. 基本要件

■ 全般要件

(1) 提案する本システムの構成について，構成品一覧を提示すること（メーカー型番が分かる品目表を必ず提出すること）。
(2) 本調達機器等及びその構成・配置については，運用環境を考慮して，可能な限り実績のある最新の技術を採用すること。
(3) 本調達機器等について，特に定めないものは，JIS 等の国内規格，ISO 等の国際規格又はそれと同等の規格に適合する品質優良なものを使用すること。
(4) ハードウェア及びソフトウェアは，製品の動作が保証又は確認されたものであること。
(5) 納入期限までに発見された本調達機器等の不具合については，受注者の責任と負担で迅速に対応すること。

■ 導入要件

(1) センターネットワークに組み込むために必要となる設計・設定・テスト作業等を必ず実施し，センターネットワーク及び大学入試センター業務に何ら支障をきたさないようにすること。
(2) 本システム以外で利用しているネットワーク機器やサーバが問題なく動作するための結合／総合設計・設定・テスト作業等を実施すること。
(3) 現行システムと新システムとで併設する期間，業務に影響のない形で併設することとし，現行システムの設定変更が必要な場合には，現行事業者と調整の上，受注者の責任と負担において作業すること。

■ ハードウェア要件

(1) 同一の種類の機器に関しては，用途に応じて型番・スペックを最適化し，用途に応じて機器を統一すること。
(2) 本調達機器等に係る製品候補においては，契約期間中の保守が可能なものを選定すること。
(3) 原則として，特定調達品目として指定されている製品については，国等による環境物品等の調達の推進等に関する法律（平成 12 年法律第 100 号）（グリーン購入法）に基づく環境物品等の調達の推進に関する基本方針に規定された基準及び配慮事項を満たす製品であること。
　(ア) 環境（3R:リデュース／リユース／リサイクルの 3 つを含む）に配慮した設計・製造がなされている
　(イ) 使用済後も，引取り・リユース／リサイクル・適正処理がなされている
　(ウ) 環境に関する適切な情報開示がなされている
(4) 機器等の製造工程において，意図しない変更が加えられないよう適切な措置がとられていること。また，大学入試センターが求めた際，当該措置を証明する資

料を提出すること。

(5) 受注者が提示した機器リストの中に，大学入試センターにおいてサプライチェーン・リスクがあると判断した機器等がある場合には，受注者は，別の機器等（同等品）と交換すること。（政府調達におけるサプライチェーン・リスク対策のため）

(6) 本調達機器等は，機械的及び電気的に人体に危険がないものであること。

(7) 電源容量計算等の諸元（電源のコンセント形状，定格電圧，定格電流）を提案書に記載すること。

(8) ネットワーク機器については， IPv6 に対応済み，若しくは，将来的にソフトウェアのバージョンアップ等により IPv6 に対応できる機器であること。

(9) ネットワーク監視ソフトウェアによる死活監視に対応するために，サーバ及びネットワーク機器については，ping に対する応答が可能なこと。

■ ソフトウェア要件

(1) ソフトウェアは，バージョンを統一すること。また，原則日本語版であること。

(2) ソフトウェアのバージョン確定に当たっては，大学入試センターと協議すること。また，バージョン確定後から納入期限までにバージョンアップのあることが確認された場合には，動作確認が済んでいるものに限り，大学入試センターの承諾を得た後に最新バージョンを導入するものとする。

(3) ソフトウェアのライセンスを本調達に含めること。また，納入期限までに指摘されている脆弱性(ぜいじゃくせい)の有無を確認し，これを大学入試センターに書面にて報告し，大学入試センターと協議の上で納入期限までに修正モジュールの導入等適切な対策を施すこと。

(4) クラウドサービスを使用する場合，原則として ISMAP に登録されているサービスを利用すること。また，保管するデータセンターは国内に限ること。また，想定される利用料についても本調達に含めること。

■ セキュリティ要件

(1) システム構築に当たっては不正操作から保護するための対策を講ずること。

(2) 各種管理画面等へのアクセスに当たってはセキュリティ強化のため，多要素認証を実装すること。なお，知識要素（ID・パスワード等）及びネットワークによる制限で実装してもよい。

(3) DNS/Proxy/メール等の内部通信は，暗号化通信とすること。また，大学入試センターから指示した外部／内部通信に係るサーバに対し，SSL 証明書の適用を行うこと。
ただし，障害通知の SMTP/SMTPs 通信も発生するため，設定は，暗号／平文の両方が通信可能な設定とすること。

(4) システム環境構築完了後に，情報セキュリティを担保するため，セキュリティ診断とペネトレーションテストを実施すること。不備が発見された際は，修正し，再度ペネトレーションテストを実施し，安全性を確保すること。実施後には報告書

（実施方法や確認方法など，実施した内容が分かる資料含む。）を提出し，成果物として納めること。

■ 信頼性要件

(1) 各種災害（地震等）対策等を十分に考慮し，安全かつ信頼性のあるシステムを構築すること。無停電電源装置(UPS)を使用した安定的な電源の供給やデータ保護，外部媒体又はクラウド環境へのデータバックアップ等の措置を講ずること。
(2) 将来におけるハードウェア・ソフトウェアの増強・ネットワークの拡大・接続機器の増設及び拡張のため，互換性・移植性・接続性を確保でき柔軟に対応できるよう標準化が考慮されていること。
(3) 直接的にユーザサービスに関わる機器は，二重化構成とし，単一障害点（SPoF）がない設計とすること。

2.2. ネットワーク接続機器に関する要件

2.2.1. 基本要件

別紙「主なネットワーク配線及びスイッチ配置の概略図」を参照し適切なネットワーク機器を配置し，ネットワークを構築すること。

(1) 各EPSに設置するスイッチは，ケーブルの破損を防ぐため収納可能な EIA 規格準拠した 19 インチラックの情報コンセントボックス等に収納すること。
(2) コアスイッチから各フロアスイッチ・サーバ室内に設置のサーバまでは 10Gbps 以上の回線を接続すること。
(3) EPS 内に設置する各フロアスイッチからエッジスイッチ及び端末までは 1Gbps 以上で接続すること。

2.2.2. セキュリティ要件

ネットワークの構築に当たっては以下のセキュリティ要件を満たすこと。インシデント等の発生時には管理者への通知と関連するログを保存すること。

(1) 構内ネットワークにおいて許可のない端末の接続及び許可されないプロトコルの通信（不正アクセスや異常な通信）をブロックする機能を有すること。
(2) ウィルス，スパイウェア，マルウェア等の不正プログラムの侵入を防ぐとともに，内部で感染を広げないために不正な通信を防ぐ機能を有すること。
(3) DoS/DDoS 攻撃を防御する機能を有すること。

2.2.3. 対外接続用 L3 スイッチ（2 台）及び装置間接続用 L2 スイッチ（7台）

以下の仕様を満たす対外接続用 L3 スイッチ及び装置間接続用 L2 スイッチを用意すること。

■ 一般機能

(1) ループ防止機能により，ネットワークでのケーブル誤接続によるループ構成を自動的に検出し，該当ポートを切り離すことが可能なこと。
(2) VLAN（Port VLAN，Tag VLAN）機能を有しており，マルチサポートしているこ

と。
(3) トラフィック解析のためポートミラーリング機能を有すること。

■ ハードウェア要件
(1) EIA 規格準拠 19 インチラックに搭載可能なこと。
(2) 対外接続用 L3スイッチ(2 台)は，以下の要件を満たすこと。
(ア) 1GbE インタフェースを 4 ポート以上備えていること。
(イ) 10GbE に対応したインタフェースを 4 ポート以上，SFP/SFP+インタフェースを 4 ポート以上有し，いずれかで排他制御できること。
(3) 装置間接続用 L2 スイッチ(7台)は，以下の要件を満たすこと。
(ア) 1GbE インタフェースを 4 ポート以上備えていること。
(イ) 10GbE に対応したインタフェースを 4 ポート以上，SFP/SFP+インタフェースを 4 ポート以上有し，いずれかで排他制御できること。
(4) SFP インタフェースは，IEEE802.3 規格に準拠した 1000BASE-SX/LX に対応していること。
(5) SFP/SFP+の 10Gbps ポートを 4 ポート以上有すること。なお，接続先インタフェースに合わせて 10GBASE-SR もしくは 10GBASE-LR から選択可能なこと。

■ セキュリティ要件
(1) 不正な DHCP サーバの接続を防止できること。
(2) システムの機能設定情報をパスワード等で保護する機能を有すること。

■ 管理要件
(1) シリアル接続等のコンソールポートを有すること。
(2) セキュアなリモート・コンソール機能を有すること。
(3) NTP または SNTP クライアント機能を有し，一貫したタイムスタンプを刻むことが可能なこと。
(4) Syslog サーバにメッセージを送信可能なこと。
(5) SNMPv1/v2c/v3 による管理機能を有すること。
(6) コマンドや再起動により作成した設定を反映できること。

■ 信頼性要件
(1) 対外接続用 L3スイッチ(2 台)は，SINET データセンター文京ノード及び武蔵野ノードに接続し，冗長化すること。

2.2.4. リンク負荷分散装置(ロードバランサー)(2台)

負荷分散装置は 2 台用意し，リンク負荷分散及びサーバ負荷分散が可能な冗長化構成とすること。また，大学入試センターの指示に基づき，SSL 証明書の適用を行うこと。

■ 一般機能

(1) 大学入試センターで稼働しているシステム(試験情報システム, Web 会議(外部サービス), メール等)のサーバ負荷分散ができること(1 つのサーバや通信機器にかかる負荷を軽減し, 停止状態を防ぐ機能を有すること)。なお, これらシステムの負荷分散に当たっては, 試験情報用電子計算機システムの受注者及び大学入試センターと協議の上, その設定をすること。
(2) 業務に最適なサーバ振り分け(IPアドレス/ポート番号, HTTPヘッダ, URL等)を選択できること。
(3) 様々なアプリケーションやサービスの負荷分散(ロードバランサ)に対応できること。
(4) IPv6 に対応し, IPv6 環境でのサーバ負荷分散を実現できること。
(5) サーバの負荷状況を監視し, 負荷分散(ロードバランサ)を制御(負荷計測エージェント)可能なこと。
(6) 一連のトランザクションを同一サーバに転送(セッション維持)できること。
(7) セッションリカバリ機能があり, サーバ故障時でも別サーバとの通信が継続できること。
(8) SSL アクセラレーター機能を有し, 処理能力は 2,000tps 以上であること。
(9) IPv4, IPv6 ルーティング機能を有すること。
(10) IP アドレスとポート番号を対象とした負荷分散処理(レイヤー4ロードバランシング)が可能なこと。
(11) URI に応じてリクエストを特定のサーバ群に割り振る処理(レイヤー7トラフィック処理)が可能なこと。
(12) 100,000 セッション/秒以上の負荷分散処理性能を有すること。
(13) IP アドレスやポート番号, プロトコル, MAC アドレスによるフィルタリングが行えること。

■ ハードウェア要件

(1) 100BASE-TX/1000BASE-T のインタフェースを 4 ポート以上有すること。
(2) 10Gbps ポートを4ポート以上有し, 接続先インタフェースに合わせて 10GBASE-SR または 10GBASE-LR から選択可能なこと。
(3) 19 インチラック搭載型とし, 1U 以内に収納可能であること。

■ 管理要件

(1) セキュアなリモート・コンソール機能を有すること。
(2) Syslog サーバにメッセージを送信可能なこと。
(3) NTP または SNTP クライアント機能を有し, 一貫したタイムスタンプを刻むことが可能なこと。

■ 信頼性要件

(1) 2 台以上による冗長化構成を実現し, 片方に障害が発生しても, 自動的に切

替わり，もう一方により正常な運用が可能であること。
(2) 障害時の保守サービスを迅速に行うため，監視サーバから監視しその結果により運用保守対応が可能であること。

2.2.5. UTM 装置（統合管理装置を含む）（2台）

通信回線を介した不正を防止するため，不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。

将来，ネットワークが仮想化される可能性を見据え，対応可能な製品を 2 式用意し，冗長化すること。

■ 一般機能

(1) IPアドレスの変換機能を有し，ルーティング機能を有していること。また，プライベートアドレス（ローカルアドレス）を変換するための NAT 及び NAPT に対応していること。
(2) DoS/DDoS 攻撃防御機能を有すること。
(3) IEEE802.3ad リンクアグリゲーション機能を有すること。
(4) ファイアウォールのポリシー毎にウィルス・スパイウェア，URL フィルタリング等のコンテンツ検査機能を有効/無効の設定が可能であること。
(5) 脆弱性防御，アンチウィルス，アンチスパイウェア機能を有すること。
(6) 既知及び未知のあらゆる脅威に対する保護について。
(ア) 一般的な脅威回避技法が実装されているかに関わらず，エクスプロイト，マルウェア，スパイウェアを含む様々な既知の脅威をブロックできること。
(イ) ファイルや機密データの無許可の転送を制限し，大学入試センターのシステム及び業務とは関係ない Web の利用を制御できること。また，制御には，カテゴリごとの分類と，最新の URL 情報に基づくフィルタリング機能を有すること。
(ウ) 未知のマルウェアを識別して悪意ある動作について分析を行い，自動的にシグネチャを作成し更新時に配信できること。
(エ) クラウドシステムと連携するなど，早期に未知のマルウェアの発見と対策が可能な機能を有すること。
(7) ボットネット感染が疑われる端末をリストアップするボットネットレポート等の機能を有すること。
(8) Web UI 上で動的に表示を切り替えることができるリアルタイムレポート機能を搭載し，利用頻度の多いアプリケーション，URL カテゴリ，脅威をランキング形式で表示できること。
(9) IEEE802.1Q VLAN トランク機能を有すること。

■ ハードウェア要件

(1) 1000BASE-T インタフェースを 4 ポート以上，SFP+を 4 ポート以上有すること。
(2) 19 インチラック搭載型とし，2U 以内に収納可能であること。

■ 管理要件

(1) http 及び https 対応の Web インタフェースを有すること。
(2) ssh によるコマンドラインインタフェースを有すること。
(3) 複数台を一元管理が可能であること。
(4) ログの閲覧が可能であり，他のサーバに Syslog のログ出力が可能なこと。
(5) ログを保存するためのストレージとして，最適な RAID 構成で 10TB 以上の容量を有すること。なお，「2.5. ログ収集システム」に集約してもよい。

■ 信頼性要件

(1) ファイアウォール機能を有する装置で，冗長化構成が可能な製品であること。
(2) Active/Passive，Active/Active いずれかの冗長構成に対応していること。
(3) ファイアウォールスループットとしてIPv4ファイアウォールスループット 10Gbps 以上，アプリケーション制御スループット 10Gbps 以上以上処理能力を有すること。また，SSL インスペクション実行時にも安定的な運用が可能な処理能力を有すること。
(4) IPS，アンチウィルス，アンチスパイウェア機能を同時に使用した場合でも 3.0bps 以上の処理能力を有すること。

2.2.6. コアスイッチ（1式）

導入するコアスイッチは，制御ユニット・電源ユニット・ネットワークポート等の構成要素，またはコアスイッチ本体を冗長化可能な構成とし，いずれか一方に障害が発生した場合でも，ネットワーク機能を中断することなく継続運用できること。

■ 一般機能

(1) 全ての通信モードにおいて全二重通信の機能を有し，インタフェースが独立し，オートネゴシエーションにより全二重／半二重を自動的設定する機能を有すること。
(2) IPv4／IPv6 に対応できること。
(3) GEC（Gigabit Ether Channel:リンクアグリケーション）機能を有すること。
(4) QoS（Quality of Service）機能を有すること。
(5) ネットワークを介して，ファームウェアのバージョンアップ及びルーティング機能設定情報ソフトウェアをロードあるいはセーブ可能なこと。
(6) IPv4 パケット処理性能として 900MPPS(Packet per Second)以上を有すること。
(7) IPv4/IPv6 に対応し，1K 以上のルーティングエントリ数（スタティック）を有すること。
(8) 64,000 以上の MAC アドレス学習テーブル数を有すること。

■ ハードウェア要件

(1) 片系あたり，10Gbps 以上に対応した光インタフェースを 12 ポート以上有すること。また， 1000BASE-T/10GBASE-T インタフェースを 24 ポート以上有する

こと。
(2) コアスイッチからサーバ室内の各機器までの帯域は，10Gbps の帯域で接続すること。

■ セキュリティ要件
(1) システムの設定情報をパスワード等で保護する機能を有すること。
(2) パケットフィルタリング機能を有すること。
(3) IEEE802.1x 相当以上の認証機能を有すること。

■ 管理要件
(1) VLAN（Port VLAN，Tag VLAN）機能を有していること。
(2) SNMP，SSH をサポートしていること。

■ 信頼性要件
(1) 電源ユニットを筐体内で冗長化すること。
(2) VRRP 等の冗長化機能を有すること。
(3) 起動時，稼動中，トラブルシューティング時など，機器動作の信頼性を維持するための総合的な自己診断機能を有すること。自己診断機能は稼働中にも任意のタイミングで実行可能であること。

2.2.7. パッチパネル（2式）

ラックマウントタイプのパッチパネルを用意し，コアスイッチから各 EPS 等までの間の光回線を集約する。

■ ハードウェア要件
(1) ラックマウントタイプで1U であること。
(2) 適用コネクタは 24 心以上であること。

2.2.8. フロアスイッチ及びエッジスイッチ

L2 スイッチ単位で VLAN を構成し，IP アドレスが付番可能で，以下の仕様を満たす機器とすること。

なお，可能な限り機器を統一するものとし，設置場所のスペース等を踏まえ適切なものを用意すること。

■ 一般機能
(1) ポート数×1Gbps 以上のスイッチファブリックを実装する固定型の L2 スイッチ製品であること。
(2) ループ防止機能を有すること。
(3) IEEE802.1x に準拠した認証機能を有すること。
(4) IEEE 802.3ad リンクアグリゲーション機能を有すること。
(5) IEEE802.1p に準拠したパケット優先順位制御が可能なこと。
(6) 8 千以上の MAC アドレス学習テーブルを有すること。

■ ハードウェア要件

(1) フロアスイッチは，IEEE802.3 規格に準拠した 1000BASE-T インタフェースを有する機器を用意すること。
(2) コアスイッチと10Gbps で接続すること。
(3) 物理コンソールポートを有すること。
(4) EIA 規格準拠 19 インチラックに搭載可能なこと。

■ セキュリティ要件

(1) ポートごとに通信可能な MAC アドレス，又は MAC アドレス数を制限できること。
(2) 不正な DHCP サーバの接続や DHCP メッセージを使った DOS 攻撃を防止できること。
(3) システムの機能設定情報をパスワード等で保護する機能を有すること。
(4) QoS（Quality of Service）機能を有すること。
(5) パケットフィルタリング機能を有すること。

■管理要件

(1) Web ブラウザを使用して設定を行える機能を有すること。
(2) SSH によるリモート・コンソール機能を有すること。
(3) Web 設定画面や CLI 上のコマンド説明が表示できること。
また，コマンドや再起動により作成した設定を反映する機能を有すること。
(4) トラフィック解析のためポートのミラーリング機能を有すること。
(5) ソフトウェア及び設定情報を FTP 又は TFTP にてアップロード及びダウンロードが可能であること。
(6) NTP 又は SNTP クライアント機能を有し，一貫したタイムスタンプを刻むことが可能なこと。
(7) DNSを参照しIPアドレスの代わりにホスト名を使用できる機能を有すること。
(8) Syslog サーバにメッセージを送信可能なこと。
(9) SNMPv1/v2/v3 による管理機能を有すること。
(10) VLAN（Port VLAN，Tag VLAN）機能を有しており，マルチサポートしていること。

■ 信頼性要件

(1) サーバ室に設置されない機器であるため，動作温度は，0℃～45℃に対応可能であること。
(2) 保管温度が 10℃～50℃に対応可能であること。
(3) VCCI クラス A に準拠していること。
(4) サーバ室でなく EPS 又は事務室に設置される機器であり，様々なノイズ源からの影響を受ける可能性が高いため，ノイズ規制 EN61000-3-2，

EN61000-3-3, EN300386 等に準拠していることが望ましい。

(5) パケット処理性能として 1,330MPPS（packet per second）以上を有すること。

2.2.9. メディアコンバータ(6 台)

スイッチのみで構成可能な場合は，不要。なお，SFP に適用可能な場合は，SFP を用いても良いものとする。

■一般要件

(1) オートネゴシエーションと 100Mbps Full-Duplex をモード切替する機能有すること。

(2) 回線は殆どがマルチモードで敷設しているが，マルチモードファイバー（MMF）／シングルモードファイバー（SMF）の両方に対応していることが望ましい。なお，SFP/SFP+を適用する場合は，1000BASE-SX 又は 1000BASE-LX のいずれかを選択できること。

■ハードウェア要件

(1) IEEE802.3 規格に準拠した 100/1000BASE-TX インタフェースを1ポート以上有すること。

■信頼性要件

(1) AC100V で動作し，動作環境は 0～50℃以上であること。

2.2.10. 無線LANアクセスポイント（20台）

大学入試センターが指定した場所に適切な台数を配置する。

■ 一般要件

(1) AutoMDI／MDI-X 機能を有すること。

(2) NTP 又は SNTP サーバ，クライアント機能を有すること。（コントローラにおける機能で実現可能でも構わない。）

(3) DHCP クライアント機能を有すること。

(4) Wi-Fi6 をサポートしていること。また，同時に二つ以上の周波数帯で利用可能なこと。

(5) 1 台あたり複数の SSID が設定可能なマルチ SSID 機能を有すること。

■セキュリティ要件

(1) 無線 LAN 端末の通信用インタフェースとアクセスポイント管理用インタフェースを物理ポートで分離することにより，高セキュリティな物理構成が取れること。

(2) パケットフィルタリング機能（アクセスコントロールリスト機能）を有すること。

(3) ハードウェアによる AES 暗号化機能を有すること。

(4) 脆弱性対策をした WPA2 認証，又は WPA3 認証に対応していること。

■管理要件

(1) Web ブラウザにより設定が可能なこと。

(2) コマンドの説明を CLI, Web ブラウザ上で表示できること。また，日本語のマニュアルが提供されていること。

(3) アクセスポイントのコントローラにより，コントローラから一元管理できる機能を有すること。

■信頼性要件

(1) ポートのペアを現用，待機として経路を冗長化する機能を有すること。

(2) 有線 LAN 障害時に無線 LAN 接続を自動的に切断する機能を有すること。

(3) 設定時の誤操作を防止するための機能を有すること。

(4) 給電インジェクタを有し，無線 LAN アクセスポイントに電源を供給できること。

2.3. サーバ等に関する要件

2.3.1. サーバの基本要件

大学入試センターサーバ室内にサーバを設置する場合，仮想化基盤，クラウドサービスの活用によりサーバ集約を図ること。また，以下の 2.3.1.1 から 2.3.1.4 に記述した内容を物理サーバ及び仮想サーバそれぞれの基本要件とする。

2.3.1.1. 時刻同期

NTP による時刻同期に対応しており，NICT にある NTP サーバと同期させること。

ただし，公開 NTP サーバは，これ以外にも提供されているので，同期させる公開サーバは，大学入試センターと協議し，決定すること。

2.3.1.2. ログレポート機能

ログレポート機能として，HTTP，Syslog，SNMP，SMTP メールに対応していること。

2.3.1.3. ハードウェアの特質，要件

各サーバにおいて個別の指定がある場合，そちらを優先とする。

(1) EIA 規格準拠 19 インチラックに搭載可能であること。

(2) CPU については，クロック周波数 2.5GHz以上で 6 コア以上を有し，8 コア以上拡張可能であること。なお，キャッシュメモリを 20MB 以上有すること。

(3) メインメモリについては，32GB 以上のメモリを有し，認識すること。また，拡張時には，512GB 以上まで拡張可能であること。

(4) 補助記憶装置は，次の仕様を満たすこと。なお，SSD 以外のストレージ（アプライアンス装置や Flash モジュール等）を適用する際には製品特性やメリット・デメリットについての資料を提示すること。

(ア) OS 格納用として記憶容量が 100GB 以上の SSD をミラーリングとして有すること。

(イ) ホットスワップをサポートしていること。
(ウ) データ格納用として，最適なストレージを使用し，最適な RAID で構成すること。
(エ) ホットスタンバイディスクを 1 個以上有すること。
(オ) ファイルサーバを除き DVD 光学ドライブを1台，内蔵していること。ただし，メディアのイメージを仮想ドライブとしてサーバ上にマウントできるのであれば，外付け DVD-ROM ドライブ3台の用意で構わない。

(5) IEEE802.3 規格に準拠した 1000BASE-T 以上に対応したネットワークインタフェースを 2 ポート以上有していること。

(6) キーボード，ディスプレイは，次の仕様を満たすこと。
(ア) ラックマウントタイプとし，ラック内に格納すること。
(イ) 日本語対応キーボードであること。
(ウ) 17 インチ（ワイド画面も含む）以上の TFT カラー液晶で 1280×1024 ピクセル以上の解像度の入力に対応していること。
(エ) 切替えスイッチ等を使用して，他サーバと共有も可とする。

(7) リモート管理機能として，次の仕様を満たすこと。
(ア) サーバ運用を補助するため，2.6. 監視システムと連携すること。
(イ) サーバの状態に関係なく，動作可能であること。
(ウ) サーバの状態に関係なく，遠隔からサーバ電源/リセット制御を行えること。
(エ) サーバの状態に関係なく，リモート管理機能又は監視システムにより，サーバ死活・温度・電源状態を監視する機能を有すること。
(オ) 異常の発生を管理者へ通知する機能を有すること。
(カ) 管理インタフェースとして，Web インタフェースを有すること。

(8) その他，次の仕様を満たすこと。
(ア) 24 時間×7 日間／週稼動可能な構成とすること。
(イ) 無停電電源装置(UPS)と接続し，停電時に安全に停止できること。
(ウ) OS 格納用のストレージをバックアップ/リストア可能な，バックアップ装置またはシステムを有すること。
(エ) データ格納用のストレージのデータ部分を複数世代，スケジューラで外部保管用メディア又はクラウド上にバックアップ可能であること。
(オ) 電源ユニットを二重化しており，ホットスワップに対応していること。
(カ) 情報漏出を防止するため，HDD 及び SSD の障害発生等で交換が必要になった場合，故障した HDD/SSD はデータ消去又は破砕すること。なお，交換した HDD/SSD は管理の上，データ消去又は破砕証明書を発行し，提出すること。
(キ) なお，サーバをクラウド上に構築するに当たっては，ISMAP に登録されているクラウドサービスを使用すること，及び使用するデータセンターは国内に限ること。

2.3.1.4. ソフトウェア要件

(1) OS は，マルチユーザ，マルチタスク，TCP/IP ベースのネットワーク機能及びグラフィカルユーザインタフェースを持つサーバ用オペレーティングシステムであること。なお，Windows OS の場合は，クライアントに必要なユーザ CAL(Client Access License)及びリモートアクセス CAL も調達すること。

(2) 「Microsoft Enterprise Agreement for Government Partners」等のソフトウェアの提供ベンダが用意する大学，独立行政法人を対象としたプログラムを適用し，ソフトウェアライセンス管理の負荷の軽減及び投資対効果の向上を図ること。

(3) UPS の管理機能により，停電を検出した場合には，システムを自動的にシャットダウンすること。

(4) バックアップ／リストア可能なソフトウェアを有すること。

(5) ウィルス対策ソフトウェアは，ウィルス対策ソフトウェア本来の機能に加え，マルウェア（ウィルス，ワーム，ボット等）による脅威に備えるため，マルウェア感染を防止する機能を備えるとともに，新たに発見されるマルウェアに対応するために機能の更新が可能であること。以下の機能・要素を用いたものを適用すること。

(ア) ウィルス対策
(イ) ファイアウォール機能
(ウ) 不正ソフト・マルウェア対策
(エ) フィッシング詐欺対策／Web 脅威のブロック
(オ) 脆弱性対策
(カ) 不正侵入防止機能

(6) ウィルス対策ソフトウェアは，履行期間中，最新のパターンファイルを適用すること。

(7) 不要な匿名接続を許可しないこと。

(8) 各サーバは，以下に記載するマルウェア対策，アクセス制御，証跡管理ができることが望ましい。且つ，統合管理（単一製品等）で実現できることが望ましい。

(ア) サーバに対する未知のウィルス・不正プログラム感染等への対策機能として，実行を許可するプログラムをホワイトリスト化し，ホワイトリストに存在しないプログラムの実行を防止できる機能を有すること。
(イ) 特権ユーザ(root)を含むシステム管理者であっても，特定のプログラムの実行を防止できる機能を有すること。
(ウ) 実行を許可したいプログラムを指定し，ホワイトリストに追加できる機能を有すること。
(エ) ホワイトリスト作成時にプログラムのハッシュ値を取得するなど，システムに負荷を掛ける手段は避けること。
(オ) サーバへのアクセスを業務上必要な者に限るために，全てのユーザ，プロセスに対して強制的にアクセス制御を実行できる機能を有すること。

(カ) サーバに対する不正アクセスを防止するために，システム管理者であっても，保護された領域へのアクセスを不可とすることができること。
(キ) ファイルの改ざんなどの不正操作をリアルタイムに検知できること。
(ク) セキュリティ事故による被害を最小化するため，サーバ管理者の権限を最少化させることができること。
(ケ) セキュリティ事故による被害を最小化するため，サーバ管理者であっても，サーバの重要なサービスや保護されたプロセスは，停止不可とすることができること。
(コ) セキュリティ事故による被害を追跡調査できるよう，ログの改ざん禁止を目的とし，ログに対して特権ユーザー(root)を含め，書き込みや削除の禁止設定をすることができること。
(サ) 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として，OS 機能では，残らない詳細ログ(OS コマンドレベル)を収集することができること。

(9) 攻撃に利用されたユーザやプロセス，マルウェアファイルなどを事後に調査するための詳細ログを収集することができること

2.3.2. 外部向け（DMZ）及び内部向けを一組とするサーバの共通事項

以下のサーバ（2.3.2.1～2.3.2.3）は，仮想化基盤により，外部向け，内部向けをそれぞれ構築し，冗長化構成とし，以下の要件を満たすこと。また，それぞれの機能に必要な CPU，メモリ，ストレージを以って構築すること。

なお，詳細なセキュリティ設定条件等は，大学入試センターと打ち合わせの上，決定するものとする。

2.3.2.1 プロキシサーバ

外部向け（OPEN 環境用）の Proxy サーバを用意すること。なお，セキュアな環境を維持するため内向け（CLOSED 環境用）にも Proxy サーバを用意すること。

(1) WEB/FTP Proxy システムを構築し，PROXY 機能を提供すること。
(2) OS は，Red Hat Enterprise Linux 9 と同等以上であること。
(3) http，https の通信に関して，Web プロキシ，キャッシュ及び URL フィルタリングを行うこと。
(4) アクセス制御，認証，ロギング，不正アップロードとウィルス付きコンテンツのダウンロード，HTTPトラフィック管理などとともに，不正確なサーバ証明書が実装されたサーバに対処できること。
(5) 管理者がカテゴリごとにフィルタリングの有効／無効を切り替えられること。
(6) フィルタリングは，ユーザのアクセスに対して，警告表示のみと遮断の 2 種類以上が利用する機能を有すること。
(7) 本機能，性能を満たす場合は，アプライアンス製品での提案も可とする。
(8) 外部向け Proxy サーバは冗長構成とするが，内部向け Proxy サーバはシン

グル構成とする。
(9) 外部向け Proxy サーバについてはクラウド上に構築してもよい。

2.3.2.2. DNS サーバ

外部向け，内部向けの DNS サーバを用意すること。
(1) OS は，Red Hat Enterprise Linux 9 と同等以上であること。
(2) DNS サーバの構築は，として BIND あるいはこれと同等以上の性能を有するソフトウェアを搭載し，DNS サーバとして機能すること。
(3) DNS サーバのアドレスを自動的に取得する設定とし，IP アドレス情報を取得し，ドメイン名とリンクさせること。
(4) ゾーンの動的更新を許可し，DNS のクライアント・コンピュータの名前と IP アドレスを，DNS サーバに動的に登録できること。
(5) 本機能，性能を満たす場合は，アプライアンス製品での提案も可とする。
(6) 外部向け，内部向けともに DNS サーバについてはクラウド上に構築してもよい。

2.3.2.3. メールサーバ

外部向け，内部向けのメールサーバを用意すること。
(1) OS は，Red Hat Enterprise Linux 9 と同等以上であること。
(2) ラックマウントタイプであること。ただし集約化が図られていればこの限りでない。
(3) Postfix あるいはこれと同等以上の性能を有する MTA(Message Transfer Agent)を搭載し，Mail サーバとして機能すること。
(4) スパムフィルター機能を有すること。
(5) メール詐欺を防ぐため DMARC/DKIM/SPF 機能を有すること。
(6) 外部向け，内部向けともにメールサーバについてはクラウド上に構築してもよい。

2.3.3. シンクライアントシステム（一式）

シンクライアントシステムの共通事項として次の条件を満たすとともに，2.3.3.1～2.3.3.4.に記載する要件を満たすこと。

■一般要件
(1) シンクライアント端末 180 台以上を管理する機能を有すること。
(2) シンクライアントシステムの方式としては，OPEN 環境及び CLOSED 環境においてユーザごとに独立した環境を設定できる仮想デスクトップ（VDI）方式とする。
(3) OPEN 環境 180 台及び CLOSED 環境 30 台が同時に運用可能なこと。CLOSED 環境は約 120 名の利用者が利用可能なこと。OPEN 環境及び CLOSED 環境は利用者ごとの環境を用意すること。
(4) 管理者がリモート操作からユーザ画面を表示することができ，操作が可能で

あること。
(5) ネットワークプリンタに対して印刷指示が可能であること。また，印刷環境を各利用者が個別に設定できる機能を有すること。
(6) 音声ファイルの再生やWEB配信動画の視聴の際，音声の聴取が可能であること。また，音声環境は，各利用者が個別に設定可能であること。
(7) シンクライアント端末全台から同時利用が可能であること。
(8) ウィルス対策ソフトウェアを搭載し，動作させること。ソフトウェアのライセンスは，受注者が用意すること。
(9) ウィル対策ソフトウェアは，履行期間中，最新のパターンファイルを適用すること。
(10) 2.3.3.1.のサーバは， Windows Server 2025 同等以上の機能，性能を持つOSを動作させること。
(11) OPEN 環境の 2.3.3.1./2.3.3.2./2.3.3.3.については，クラウド上に構築してもよいものとする。
(12) シンクライアントシステムの管理用画面は日本語の UI が提供されること。
(13) 日本語のマニュアルが提供されるだけでなく，管理画面上にもヒントボタンが提供され，設定方法や注意事項を UI 上でも確認できること。
(14) 仮想環境を構成する各サーバは，環境構築状況や問題の発生状況を正しく確認できるよう，UI 上に構成図として視覚的に表示されること。
(15) サーバの負荷が高い場合，仮想端末の同時起動数を制限することで，サーバ負荷集中による仮想端末不具合を防止できること。
(16) 仮想端末起動の集中によるサーバの負荷を軽減させるため，あらかじめ仮想端末を起動するスケジュールを設定できること。(曜日 / 時刻)
(17) 運用管理において，各仮想端末の利用状況を把握するため，仮想端末の操作画面を管理用画面で一覧表示する機能を有すること。また，ログオン/ログオン中(切断)/利用不可/ログオフ中/デスクトップ画面を表示する機能を有すること。

2.3.3.1. シンクライアントサーバ(一式)

■一般要件

(1) アプリケーションソフトウェアが遅滞なく動作すること。
(2) OS 及び各種アプリケーションの配信及びパッチの適用が速やかに実施可能であること。
(3) 一人のユーザに対して複数の環境を割り当てる機能を有すること。
(4) 座席移動等により，ユーザがある端末から別の端末へ引き継いだ場合でも，同一仮想デスクトップを移動前の状態から持続利用する機能を有すること。
(5) シンクライアント端末に接続された USB デバイスを仮想デスクトップ上で利用する機能を有すること。また，利用制限もできること。
(6) USB デバイス使用の許可/不許可を管理側で設定する機能を有すること。
(7) シンクライアント端末に接続されたイヤホン，マイク，カメラを仮想デスクトッ

プ上で利用する機能を有すること。また，利用制限もできること。
(8) 許可したデバイス以外をシンクライアント端末のパソコンに接続しても，ユーザが利用できない状態とすること。
(9) USB 接続するマウス及びキーボード等は，ヒューマンインタフェースデバイスとして USB のポリシー設定に影響されず利用可能とすること。
(10) ストレージのディスク消費を抑えるため，マスターイメージを共有利用する機能を有すること。
(11) パッチ適用やアプリケーションの配布といった，仮想デスクトップ環境展開後の変更においてもマスターイメージを更新することで適用させることが可能であること。
(12) マスターイメージ以外に仮想デスクトップ上で生じたデータについては，マスターイメージと分離されること。

■サーバ構築要件
(1) 複数の同構成のサーバが容易に運用できるよう，サーバイメージ原本取得/配付の仕組みを提供すること。
(2) CPU，メモリ使用率をホスト間で負荷分散が可能なこと。
(3) 物理サーバのメンテナンス時に当該サーバで稼働中の仮想デスクトップを停止する必要がないこと。

■セキュリティ要件
(1) OS のセキュリティパッチの適用及び OS のアップデートを管理者が自動的に行える機能を有すること。
(2) 画面転送の通信が暗号化可能であること。
(3) パソコンからの情報漏洩を防ぐため，パソコンに標準装備されたデバイスの遮断・許可，及び，不正なネットワークの利用を制限する機能を有すること。次のデバイスのポリシーを設定・変更する機能を有すること。
(ア) CD/DVD ドライブ
(イ) その他の記録メディア
(ウ) USB ポート
(4) 各ポリシー情報など，システムの設定情報は，暗号化されていること。
(5) 仮想デスクトップ環境の管理権限を分割できる機能を有すること。
(6) 仮想デスクトップ環境をユーザの部門，業務に応じてグループ単位で管理，展開が可能であること。
(7) パソコンをログオフした状態でも，パソコンに設定したポリシーが有効であること。
(8) ポリシーの設定・変更を行なうには，専用パスワードによる認証を必要とすること。
(9) ポリシーの変更等の操作は，OS ログイン時の利用者権限に依存せず，専用パスワードの保有者だけが行えること。

■管理要件

(1) 各ユーザの仮想デスクトップにインストールされているアプリケーションの一覧を取得する機能を有すること。
(2) 仮想デスクトップの展開，変更，追加/削除，ユーザーアサインなどの機能を GUI で提供していること。
(3) 仮想デスクトップ環境の状態を目視可能とする機能を有すること。
(4) 仮想デスクトップ環境は，コンピュータ名で画面に表示されること。
(5) 集中管理機能を利用した場合，各パソコンのポリシー登録・変更作業は，集中管理機能で定義されるネットワークパスワードによる認証でのみ利用する機能を有すること。

2.3.3.2. シンクライアントシステムストレージ(一式)

■一般要件

(1) HDD と SSD を併用する場合，I/O 処理の大部分を SSD で処理することで Read と Write の両面で高い I/O 性能を実現していること。
(2) 重複排除及び圧縮処理を実行し，SSD の容量空間を効率的に使用する機能を有すること。
(3) 2.3.3.1 シンクライアントサーバ及び 2.3.4 ファイルサーバと集約化してもよい。

■ハードウェア要件

(1) ハイブリッド HDD 又はオールフラッシュストレージのいずれかで構築すること。
(2) 実効容量 25TB 以上を有すること。また，圧縮機能の利用により 50TB 以上の実効容量を有すること。

■管理要件

(1) 仮想マシン単位で性能を可視化した管理用 GUI を採用していること。なお，Web ベース(HTML5)GUI を備えたストレージ管理ソフトウェアが利用できること。
(2) 各仮想マシン／仮想デスクトップの稼働状況をグラフィカルに表示できること。
(3) 装置で発生したイベント通知として Email，SNMP Trap，Syslog Server 等のいずれかで通知する機能を有すること。

■信頼性要件

(1) SSD 又は，HDD が独立した RAID6 相当以上で冗長化されていること。ただし，キャッシュとして利用される SSD はディスク障害によってデータロストが発生しない場合に限り，RAID 構成を不要とする。

(2) 仮想マシン単位でのスナップショット機能を有し，4 世代までをサポートすること。
(3) 日次・週次・月次のスケジュール，及び採取したスナップショット毎に保持期間を設定できること。
(4) 仮想マシン単位でのクローン機能を有すること。

2.3.3.3. 仮想デスクトップ環境

シンクライアントシステムを利用するユーザ（職員）の仮想デスクトップについて，以下の環境及び機能を有すること。

■一般要件

(1) 2vCPU，16GB 以上のメモリを搭載していること。
(2) C ドライブに 150GB 以上を割り当てること。また，ユーザプロファイルとして 50GB 以上を割り当てること。
(3) センターが指定する既存の各プリンタをシンクライアント環境にて利用できること。また，必要に応じて異なる機種の追加設定が行えること。
(4) 次のソフトウェアをあらかじめインストールし，ユーザが利用できること。
(ア) Microsoft Windows 11 Professional と同等以上のOS
(イ) Microsoft Office2024 と同等以上のオフィスソフトウェア
(ウ) セキュリティ対策ソフトウェア
(エ) 一太郎ビューア
(オ) 7Zips 等の圧縮・解凍ツールの最新版
(カ) IT 資産管理ソフトウェア
(キ) レーザプリンタ等の通常使用するプリンタドライバ（職員が使用できる状態に設定していること。）
(ク) 各ユーザが個別にインストールしているソフトウェアについては，大学入試センターとの協議の上，対応すること。

2.3.3.4. シンクライアント端末の設定（180 式）

シンクライアントシステムに接続するための端末に必要となる設定を行うこと。シンクライアント端末及び接続するディスプレイ，キーボード，マウス等については，大学入試センターが別途用意するので，受注者はそれに対して必要となるソフトウェアのインストール及び各種設定等を行うこと。

なお，用意する PC は Windows11Pro がインストールされたノート PC を想定している。

■一般要件

(1) シンクライアントシステムで実行された画面情報を表示すること。
(2) USB メモリ等の外部媒体の利用について管理者が有効／無効を設定する機能を有すること。
(3) 管理者が遠隔によりパソコンごとに電源のオン／オフの切替え，ストレージに対する環境復元の操作（環境復元モードの ON/OFF）ができること。

また，再起動，スタンバイへの移行，ログオン／ログオフ，メッセージ表示およびコマンド実行による任意のプログラム起動などをスケジュール実行できること。

(4) PC のストレージへの書込みを行っても元の状態に復元する機能（環境復元）を有すること。ただし，パッチの適用やウィルス対策ソフトウェアのパターンファイルは，最新を維持できること。

(5) 端末のみで（仮想デスクトップ環境に接続せずに）Webex・Zoom が接続可能なこと。

(6) 2.3.3.5. のとおり機能により大学入試センター外から仮想デスクトップに接続可能なこと。

(7) 端末本体は，再起動により設定した初期状態に復帰すること。また，本体端末に設定することなく，設定情報の集中管理が可能であること。

(8) 端末本体起動時には，端末本体の OS へのログイン操作を必要とせずに仮想デスクトップへのログオン画面を表示させること。

(9) 2.3.9 ウィルス対策 DB サーバ，2.3.10WSUS サーバからの配信を受けられること。また，自宅へ持ち出した場合には，各サービス事業者からインターネットを介して直接配信を受けられること。

2.3.3.5. リモートアクセス

■一般要件

(1) 大学入試センター敷地外からも OPEN 環境の仮想デスクトップに接続可能なこと。

(2) 最大同時に 180 台が接続可能であること。

(3) 2.3.3.4.で設定したシンクライアント端末からのみリモートアクセスを可能とすること。

(4) リモートアクセスの際には多要素認証を行うこと。ID ・パスワードの他に端末固有情報およびデジタル証明書での認証を行うこと。

2.3.4. ファイルサーバ(一式)

■一般要件

(1) 各端末に対して，ファイルサーバとして動作すること。OPEN 環境用と CLOSED 環境用の2つの環境分を用意すること。

(2) 共有領域として，Active Directory に登録されたグループ及びユーザ毎にフォルダ単位で書き込み，参照のアクセス権を個別に設定すること。格納するデータは，各部署等において共有する文書，表計算，画像，音声及び各種アプリケーションで作成したファイルである。

(3) ユーザが一斉に移動プロファイルをクライアントにダウンロードすることを想定した構成であること。

(4) 職員全員が同時に接続できるサーバライセンスを有しており，かつデータの読み込み，書き込みが遅滞なく行えることを想定した構成であること。また，日

本語のフォルダ名及びファイル名が不具合なく使用する機能を有すること。

(5) 個別に利用できる領域として個人領域ファイルサービスを行うこと。格納するデータは，各個人のメール，文書，表計算，データベース，画像，音声，及び各種アプリケーションで作成したファイルである。また，ユーザごとに使用量の制限を行うこと。なお，ユーザごとの使用量については次項（ハードウェア要件）に示す範囲内で，当センターと協議の下に決定する。

(6) 構成される機器は，電源ユニットを二重化しており，ホットスワップに対応していること。

(7) 格納するデータは利用者が意識することなく自動的に暗号化して記録する機能を有すること。

(8) システムを正常にかつ自動的にシャットダウンする機能を有すること。

(9) ウィルス検索及び駆除等が可能であること。

(10) 共有領域に対してアクセスログを採取すること。

■ハードウェア要件

(1) 実効容量として OPEN 環境用を 20TB 以上，CLOSED 環境用を4TB 以上利用可能なこと。

(ア) OPEN 環境用 20TB のうち4TB を，各職員の個人領域及び移動プロファイル用の領域，残りの 16TB は共有フォルダ及びスナップショット用の領域とすること。

(イ) CLOSED 環境用4TB のうち1TB を，各職員の個人領域及び移動プロファイル用の領域，残りの3TB は共有フォルダ及びスナップショット用の領域とすること。

(ウ) ストレージは，ホットスペアストレージを1本以上含めること。

(エ) 容量の拡張が可能で，RAID6相当以上で構成すること。

■信頼性要件

(1) ファイルサービスを行うサーバあるいはノードが，複数台で構成され，障害対策として両現用クラスタ構成(Active/Active)であること。ただし，十分なパフォーマンスが提供できる機器ならば，Active/Standby も可とする。

(2) 動的に容量増減を可能とするファイルシステムであること。

(3) 故障したストレージ装置の交換を行う際には，ファイルサーバの運用を停止することなく，交換が可能であり，短時間で利用可能な領域に組み込めること。

(4) 停電発生時に備え，ディスク装置上のキャッシュデータを保護する機構を備えること。

(5) スケジュールバックアップが実行でき，実行時点におけるボリューム内データブロックのマッピングテーブルが作成できるスナップショット機能を有していること。

(6) 常にサーバ及びストレージ等の状況を監視し，ハードウェアの障害が発生した場合は，メールによる通報を行えること。

(7) サーバ等構成機器の動作状況及び管理，保守は，全てネットワーク経由で行えること。

2.3.5. ファイルサーバ監視システム（一式）

■セキュリティ要件

(1) ファイルサーバへのアクセスログを収集する機能を有すること。
(2) ログは，以下の種類を取得可能なこと。
(ア) 選択，読み込み，書き込み，コピー，作成，削除，名前変更，印刷
(イ) フォルダ作成，フォルダ削除
(ウ) ログオン，ログオフ，ログオン失敗
(エ)ドメインログオン，ドメインログオン失敗，アクセス拒否
(3) ファイルの持出し有無を検知するため，ファイルの読み込みとファイルのコピーを分類する機能を有すること。
(4) あらかじめ指定した条件に一致するアクセスがあった場合，管理者へのアラート通知機能を有すること。

2.3.6. 振る舞い検知管理サーバ

外部攻撃者から大学入試センターネットワークへの標的型サイバー攻撃を検知した場合，直ちにシステム管理者に通知可能なシステムであること。

■一般要件

(1) DHCP 及び固定 IP について，設定を変更せずに導入できること。
(2) マルウェア検知対象端末にエージェント（ソフトウェア）をインストールすることなく，導入・運用できること。

■セキュリティ要件

(1) マルウェアを検知した場合，直ちに感染端末の全ての通信を自動的に遮断できること。
(2) マルウェアの検知を実施するネットワークセグメントごとに監視できること。（セグメントは 20 以上を想定）
(3) マルウェア検知の事象は，メールや SNMP トラップによる通知が行えること。通知先のメールアドレスは複数指定できること。
(4) システム管理者に加え，マルウェア感染端末の利用者にもマルウェア検知について通知できること。
(5) マルウェア検知時には，感染端末，攻撃対象端末，及び C&C サーバの情報が採取できること。また，攻撃のパターンや攻撃に使用されたツールの情報も採取できること。
(6) 監視するセグメントのスイッチに接続し，監視できる VLAN 構成数は，20 セグメント以上有していること。
(7) 禁止アプリケーションの利用端末の検知と自動遮断する機能を有すること。
(8) 不正な通信を発信している端末をネットワークから切り離し不正な接続を遮断

できる機能を有していること。

(9) 持ち込み PC など，登録されていない機器を検知・遮断する不正接続防止機能を備えていること。

(10) ファイアウォール等と連携が可能な場合は，連携しマルウェア感染疑義端末を自動検知できること。

2.3.7. IT 資産管理システム

■一般要件

(1) コンピュータ名や OS バージョンなどの情報を自動取得・管理可能なこと。

(2) 利用されているソフトウェアの情報を自動取得し台帳化する機能を有すること。

(3) ソフトウェア辞書を活用しライセンス違反を把握する機能を有すること。

(4) Windows アップデートの適用状況を把握し，デバイスを適切な状態であるかを確認する機能を有すること。

2.3.8. AD/DHCP サーバ（一式）

ドメインコントローラ機能を有し，ディレクトリ DB，主体認証と承認，グループポリシーによる利用者，端末を制御する役割設定すること。OPEN 環境用と CLOSED 環境用の2環境分を用意し，障害発生時の対応のため冗長構成とし，障害発生時には自動的に切り替わること。

■ 一般要件

(1) OS は Windows Server 2025 相当以上であること。

(2) MS Windows Server 2025 に搭載される Active Directory と同等以上のドメイン管理が可能なこと。

(3) ユーザの利用者情報，ドメイン管理，アクセス管理等が可能であること。

(4) ユーザが利用するパソコンのIPアドレスは，執務室に定めた VLAN 構成単位下のアドレスを動的に付与する DHCP 機能を持つこと。また，管理者によって事前定義されたマッピングに基づいて，端末の識別子に応じて IP アドレスの発行ができること。

(ア) DHCP サーバで管理している IP アドレス情報は，リリース時間（解放時間（28H 想定）：協議の上設定する）を設定すること。

(イ) サーバレベル及びスコープレベルのポリシーベースのアドレスの割り当て機能を可能にすること。

ただし，重複する DHCP オプション設定の場合は，スコープレベルを優先する設定とする。

(ウ) DHCP サービスの継続的な可用性を実現する機能として，DHCP フェールオーバー環境を構築すること。

(エ) パケットフィルタリングにより正規の DHCP サーバ以外からの offer，acknowledgement メッセージを遮断（Untrusted に設定されたポートから offer，acknowledgement メッセージを遮断）することで，不正な DHCP サーバを防止すること。

(5) 正規のクライアントになりすまし，MAC アドレスを適当なものに変更しつつ DHCP サーバに対して IP アドレスを要求することで IP アドレスが枯渇する事態を防ぐため，アドレスプールの枯渇を防止する機能を有すること。
(6) ユーザの端末に DHCP サービスを提供し，Mac アドレス固定で IP アドレスを付与できる機能を有していること。
(7) 機能管理者があらかじめ設定した範囲の IP アドレスや DNS サーバのアドレスなどの情報を端末に自動的に割り当てできる機能を有すること。
　なお，サーバやプリンタ及びプロジェクター等の周辺機器及び指定する機器・装置等は，固定 IP アドレスを割り振ること。

■ セキュリティ要件
(1) ワンタイムパスワード機能を有していることが望ましい。
(2) トラップアカウントを設け，当該アカウントを用いた攻撃のためのログイン行為を検知すること。
(3) セキュリティに関する設定については，大学入試センターと協議の上決定すること。

2.3.9. グループウェアサーバ
グループウェアサーバは冗長化構成とし，以下の要件を満たすこと。
■ 一般要件
(1) 納入されるグループウェアソフトウェアが推奨する動作条件以上の処理能力を有すること。
(2) グループウェアソフトウェアは，現在使用しているソフトウェア（サイボウズガルーン 6.0 の最新版 ）同等以上であり，以下の機能を有すること。
(ア) ポータル
(イ) リンク集
(ウ) スケジュール
(エ) 社内メール
(オ) 掲示板
(カ) ファイル管理
(キ) メモ
(ク) To Do リスト
(ケ) メール
(コ) 通知一覧
(サ) ワークフロー
(シ) グループメール・メーリングリスト
(3) 現行のグループウェアソフトのデータ移行については，業務に支障を来たすことなく移行し，引き渡し後直ちに運用できること。
(4) 各端末やサーバにソフトウェアのインストールを必要としないこと。
(5) メールについては，1ユーザ当たり2GB の容量を管理できること。

■セキュリティ要件

(1) ユーザ名別にファイルの書き込み，作成，コピー，名前変更，削除，フォルダの作成及び削除のログを採取すること。

(2) 収集したログは，データベース形式で保存し，日時，曜日，時間帯等の複数の条件を指定して，アクセスログの検索が可能であること。

(3) 収集したログは，CSV 形式で自動的にエクスポートが可能であること。

■ハードウェア要件

(1) OS 領域を除き，提供できる実効容量として 800GB 以上を有すること。

(2) ログの保存が1年間可能なハードディスク容量を有すること。

■信頼性要件

(1) グループウェアサーバは冗長構成とすること。ただし，クラウドサービスを使用する場合は除く。

2.3.10. ウィルス定義 DB サーバ

OPEN 環境用と CLOSED 環境用の2つの環境分を用意し，以下の要件を備えたウィルス対策定義サーバを用意すること。

■ 一般要件

(1) 必要となるウィルス対策ソフトウェアのライセンスを用意すること。

(2) 430 台以上（OPEN 環境用／CLOSED 環境用仮想デスクトップ及びクライアント端末）に対応してウィルス定義ファイルを提供する機能を有すること。

(3) ウィルス対策ソフトウェアの動作状況及び更新状況を一括管理するための統合管理機能を有すること。

(4) ウィルス対策ソフトウェアのウィルスパターン定義情報をインターネット経由で取得し，所内 LAN に接続された端末が起動された際には，自動的に最新のウィルスパターン定義情報を反映させること。

(5) 大学入試センターが管理するファイルサーバ等についてスケジュールされたウィルススキャンを定期的に実行可能なこととし，短時間で処理できるよう設計すること。なお，ウィルススキャンの実行時間の短縮のため仮想スキャンサーバを複数構築しても構わない。

2.3.11. パッチ管理サーバ

OPEN 環境用と CLOSED 環境用の2つの環境分を用意し，以下の要件を備えたパッチ管理サーバを各 1 台用意すること。なお，2.3.10.のウィルス対策定義 DB サーバと兼用しても構わない。

■ 一般要件

(1) 430 台以上（OPEN 環境用／CLOSED 環境用仮想デスクトップ及びクライアント端末）に対応して Windows 更新プログラムや脆弱性のある修正パッチ等を

提供する機能を有すること。
(2) 更新プログラムやパッチ等をインターネット経由で取得できること。
(3) 本サーバから所内 LAN に接続されたパーソナルコンピュータへの配信は，スケジュール機能により，設定した日時に配信可能であること。
(4) 任意のグループごとに複数に分けて，設定した日時に配信できること。
(5) 本システムで管理する端末の Windows 系 OS の脆弱性パッチ（修正プログラム）を受信／配信できること。

2.3.12. Microsoft License 管理サーバ

WindowsOS，MS Office 等の Microsoft 製品における総合的なライセンス管理を行うため，以下の要件を備えた KMS サーバを1台用意すること。

■ 一般要件

(1) 統合的なライセンス管理・ライセンス認証ができること。
(2) ライセンス認証の状態を保つため，クライアントは定期的にアクティベーションを更新できること。

2.3.13. メールセキュリティシステム

以下の要件を備えたメールセキュリティシステムサーバを 1 台用意すること。

■ 一般要件

(1) MTA 及び外部データベースとの同居が不要であること。
(2) 管理 GUI は Web ブラウザ上で日本語にて操作可能であること。
(3) レポート機能を有し，当日分ランキング/送受信結果や，月/日/時間別メール流通量の確認，レポート結果 CSV 出力が可能なこと。
(4) 送信メールを即時送信せず，一時保留可能なこと。一時保留の時間を指定できること。保留時間設定箇所は，宛先が組織内か組織外かで分かれており，組織内外時間差配送が可能なこと。
(5) 大容量の添付ファイル付メールを添付しても，自動的にメール本文と添付ファイルとに分割し，添付ファイルのみをセキュアなファイル転送サービスで転送可能であること。
(6) 複数のルールを組み合わせ一つのセットとして管理し，有効/無効の切替えが可能であること。また，利用者全体やグループごとなど，任意の利用者単位でルールのセットが適用可能であること。
(7) 添付ファイルのパスワード通知先を任意に指定可能なこと。

■ セキュリティ要件

(1) メーラーで送信した添付ファイル付きのメールは自動的に「メール本文」と「添付ファイル」を分離し，メール本文はそのまま送信できること。一方，添付ファイルは自動的にファイルが取得できる URL を受信者に通知すること。
(2) SMTP／SMTPs，POP3／POP3s，IMAP4／IMAP4s の全てに対応しており，平文と暗号化通信の両方に対応していること。

(3) ユーザが意識することなく，宛先ドメインごとに送信メールの添付ファイル自動暗号化ルール適用を実現できること。
(4) SMTP 認証（SMTP-Auth）に対応していること。
(5) 暗号化は ZIP 形式や AES(Advanced Encryption Standard) 256bit 形式で行えること。あわせて，添付ファイル暗号化時の拡張子やファイル名を指定可能なこと。

■ ハードウェア要件
(1) OS 領域を除き，提供できる実行容量として2TB 以上を有すること。

2.4. バックアップサーバ（1 台）
■ 一般要件
(1) 本調達におけるグループウェアサーバ，プロキシサーバ，DNS サーバ，メールサーバ，ウィルス対策定義 DB サーバ等に対するバックアップ機能を有すること。
(2) Windows/Linux 等の OS 混在環境であってもバックアップ可能であること。

2.5. ログ収集システム（1台）
■ 一般要件
(1) 本調達に係る全てのネットワーク機器，サーバ，ストレージのログを一元管理することができること。
(2) ログ収集システムから出力されたファイルが暗号化されていること。また，出力され暗号化されているファイルを再度読み出しが可能なこと。
(3) 不正な改ざんを防止するため，ログに対するアクセス制御及び改ざんを検出する機能並びにログを保護する機能を備えていること。
(4) 収集したログを自動的に圧縮する機能を有すること。
(5) 表示したレポートを csv 形式，pdf 形式で保存可能なこと。
(6) 次のとおり分析を実施する。
(ア)ウイルス・セキュリティリスク検知件数
(イ)プロキシブロック検知件数
なお，詳細については，別途，協議の上で決定することとする。
(7) WEB ブラウザ経由で，ログの検索，分析，レポート表示，レポート出力ができること。
(8) 検索結果に基づいたアラートの通知，アクション実行が可能なこと。
(9) ログレポート機能として，HTTP/HTTPs，Syslog，SNMP，SMTP/SMTPs 等に対応していること。
(10) 別のシステムでもログ収集システムを利用するため，ログ収集システムにおいてクライアントライセンスが必要な場合には，18 ライセンス分を上乗せして調達すること。
(11) ログ収集システムについてはクラウド上に構築してもよい。

■ ハードウェア要件

(1) OS 領域を除き，提供できる実行容量として 20TB 以上を有すること。

2.6. 監視システム（1台）

物理サーバのリモート管理機能，無停電電源装置(UPS)等を監視対象とする監視システムを構築すること。

■ 一般要件

(1) ネットワーク上の SNMP 情報を元に監視対象のデバイスを検出する機能を有すること。
(2) IP アドレスの範囲をスキャンして監視対象のデバイスを検出する機能を有すること。
(3) 監視対象のデバイス同士の接続をグラフィカルに表示する機能を有すること。
(4) 監視対象の障害の有無が視覚的に確認する機能を有すること。
(5) SNMP にて取得した情報をグラフィカルにモニタリングする機能を有すること。
(6) デバイスのネットワーク I/F 毎に通信状況を監視可能なこと。
(7) 監視対象にて障害が発生した際に，Email，Web アラーム，Windows ポップアップ，外部プログラム，SMNP トラップでのいずれかで通知する機能を有すること。
(8) 障害発生時/復旧時に Email にて通知する機能を有すること。
(9) デバイスの稼働状況のレポートを出力する機能を有すること。
(10) リモート端末のドライブをサーバのデバイスとして利用する機能を有すること。
(11) リモートからの電源制御(電源投入/強制再起動)によりサーバを操作する機能を有すること。
(12) 電源 ON/OFF を伴うサーバのスケジュール運転の設定できる機能を有すること。ただし，UPS の機能で実現できるのであればこの限りではない。
(13) 故障・異常箇所を確認する機能を有すること
(14) サーバ監視で取得した情報を定期的に保存可能で，過去のサーバ情報を参照し現在の状態と比較できること
(15) Web インタフェースは，日本語の表示ができること。
(16) 振る舞い検知システムとの連携を想定し，機種選定・設計・設定を行うこと。また，既存システムを組み込むうえで，必要となる作業，ネットワーク機器やサーバにおける設計・設定・検証作業を行うこと。

2.7. 無停電電源装置(UPS)（一式）

導入するサーバ等の諸元に基づき，容量を算出し，必要な無停電電源装置（UPS）として，以下の仕様を満たす装置を用意すること。

■ 一般要件

(1) 本システムでデータ消失等の可能性のあるサーバや重要なネットワーク機器等は，安全性を考慮し，UPS に全て接続すること。

(2) 導入するサーバ等から算出し，必要な容量の UPS を設置すること。なお，諸元情報は提出すること。ただし，5,000KV 以上の UPS は設置しないこと。
(3) 管理 OS からゲスト OS をシャットダウンさせるために，仮想マシンの自動停止機能を設定できること。
(4) 障害予防策として，電源の状態をモニタリングし，電源障害を検知できること。また，信頼性の向上策として，停電を検知した際にネットワーク接続している端末等に同報メッセージの通知が可能なこと。
(5) バッテリー寿命を監視し，交換時期をLED点灯で判断できること。点灯時，バッテリーを交換すること
(6) 計画による停止することが可能なこと。

■ ハードウェア要件
(1) 1 台当たり 6U 以下のラックマウント型であること。
(2) センターの供給定格電圧及び定格容量を考慮し，10,000VA / 8,000W 以下に抑えた構成とすること。また，ステップダウントランスフォーマ等を活用し，100V 入力の装置に電力を供給することも可能な構築も可とする。
(3) 常時商用方式又はラインインタラクティブ方式であり，AC100V 又は AC200V 入出力であること。
(4) 入力端子形状は，並行 2 極アース付き（NEMA 5-15P/MEMA 5-30P/MEMA L6-30P）固定とすること。
(5) IEEE802.3 規格に準拠した 100BASE-TX/1000BASE-T の管理用ポートを 1 つ以上持つこと。

2.8. KVM スイッチ（一式）
2.3. ～ 2.7.の各装置のうちラックマウントタイプについて格納できること。
■ 一般要件
(1) 導入するサーバの台数に応じた複数台のサーバを接続可能な KVM スイッチ（Keyboard/Video/Mouse switch）を搭載し，未使用時 3U 以下の高さで収納できること。
(2) ラック搭載型のフラットディスプレイ（キーボード付き）を搭載し，対角 17 インチ以上で解像度 1280×1024 において 1677 万色以上表示可能な TFT 液晶ディスプレイを有していること。
(3) 日本語キーボード機能を有していること。
(4) ポインティングデバイスを有していること。
(5) 設置及びサーバの収納については，大学入試センターの指示に従うこと。

2.9. 財務会計システム（一式）
2.9.1. 会計システム管理サーバ（1 式）
■ 一般要件
(1) OS は VMware vSphere 7 と同等以上であること。ただし，使用するソフトウェア

やミドルウェア等が対応していない場合には，大学入試センターからの指示によりライセンスのダウングレードをすること。

(2) 財務会計向けとして

(ア) AP/DB サーバ用として，仮想 OS は Red Hat Enterprise Linux 9 相当を用意し，大学入試センターからの指示によりダウングレードが可能であること。なお，RHEL8系が使用可能なライセンスであること。

(イ) CPU：コア数 6 以上，メモリ：28GB，ストレージ：2.4TB 以上を割り当てること。

(ウ) SVF for PDF を用意すること。ただし，インストール作業は財務会計システム担当事業者が行う。

(3) 旅費精算向けとして

(ア) C/S サーバ用として，仮想 OS は Windows Server2022 相当であること。

(イ) CPU：コア数 4 以上，メモリ：12GB 以上，ストレージ（OS 含む）：1TB 以上を割り当てること。

(ウ) 必要なソフトウェアやデータベース（Oracle）のインストール作業は財務会計システム担当事業者が行う。

(エ) RMS-CAL 及びデバイス CAL は最低数（5 個）のライセンスを用意すること。

■ セキュリティ要件

(1) ウイルス対策ソフトウェアを有すること。

(2) ウイルス対策ソフトウェアは，履行期間中，最新のパターンファイルを適用すること。

(3) 各サーバは，マルウェア対策，アクセス制御，証跡管理を行うこと。

■ ハードウェア要件

(1) 内蔵は SSD で 600GB 以上のストレージ 4 本以上でホットスペアディスク1本以上を含む RAID1+0 若しくは RAID5 で構成し，提供できる実効容量として 4.2TB 以上を有すること。

(2) メモリは，42GB 以上有すること。

(3) DVD-ROM 機能を有するドライブを有すること。

(4) 1000BASE-T に対応したネットワークインタフェースを 2 ポート以上有していること

(5) ラックマウントタイプであること。ただし集約化が図られていればこの限りでない。

■ 管理要件

(1) サーバの状態に関係なく動作可能なリモート管理機能を有すること。

(2) リモート管理機能は，サーバの状態に関係なく，遠隔からサーバ電源/リセット制御を行えること。

(3) リモート管理機能又は監視システムにより，サーバの状態に関係なく，以下の項目が監視する機能を有すること。

(ア) サーバ死活
(イ) 温度
(ウ) 電源

(4) リモート管理機能は，異常の発生をリモートへ通知する機能を有し，管理インタフェースとして，Web インタフェースを有すること。

(5) 収集したログはデータベース形式で保存し，日時，曜日，時間帯等の複数の条件を指定して，アクセスログの検索が可能であること。

■ 信頼性要件

(1) UPS を有し，UPS からの停電信号を受けシステムを正常にかつ自動的にシャットダウンする機能を有すること。ただし，集約化されていれば個々に設置しなくともよい。

(2) 構成される機器は電源ユニットを二重化しており，ホットプラグに対応していること。

(3) 各サーバ内でデータをバックアップすること。

(4) ディスクドライブの診断を行うことにより，故障の予兆監視が可能であること。予防交換が必要と判断したディスクドライブについて，冗長性を維持した状態でホットスペアディスクドライブへデータを自動コピーし，コピー完了後に自動切替えを行う機能を有すること。

2.9.2. 会計システム管理用パソコン(1 台)

■ 一般/ハードウェア要件

(1) デスクトップ省スペース型パソコンであること。

(2) OS は，Microsoft Windows 11 Professional 相当以上を用意すること。

(3) CPU は，3.2GHz以上であること。

(4) システムメモリについては，32GB 以上のメモリを有すること。

(5) ストレージは 200GB 以上の容量 SSD 装置を内蔵すること。

(6) DVD ドライブを有すること。

(7) 15 インチ以上で解像度 1280×1024 において，1677 万色以上表示可能なディスプレイを有すること。

(8) JIS 配列若しくは OADG 配列準拠の 109 又は 109A 日本語キーボードを有すること。

(9) ポインティングデバイスとしてホイール付き 2 ボタンマウスを有すること。

(10) RS-232C D-SUB9 ピン(オス)のシリアルポートを 1 個以上有すること。

(11) インタフェースは，1000BASE-T 対応のポートを有すること。

(12) USB 3.0 準拠以上の USB ポートを 3 個以上有すること。

(13) マルウェア(ウィルス，ワーム，ボット等)による脅威に備えるため，マルウェアの感染を防止する機能を備えるとともに，新たに発見されるマルウェアに対応するために機能の更新が可能であること。

(14) アンチウィルスソフトウェアは，履行期間中，最新のパターンファイルを適用す

ること。

(15) Microsoft Office 2024 Professional と同等以上の日本語ワープロ，表計算ソフトウェア，データベースシステム，プレゼンテーションソフトウェアを含む統合オフィスソフトウェアの入手及びインストールを代行すること。

(16) 筐体は，横置きが可能であること。

(17) その他，次の仕様を満たすこと。

(ア) 製造事業者において，法人向け製品として製造・販売されていること。

(イ) 情報漏出を防止するため，HDD/SSD 障害発生時に当該 HDD/SSD を取り外し交換した場合，故障した HDD/SSD は破砕すること。なお， HDD/SSD の破砕証明書（破砕前後の写真含む）を発行し，提出すること。

(18) 環境配慮に関して，次の仕様を満たすこと。

(ア) 省エネ法に基づくエネルギー消費効率について，省エネ基準達成率が AA 以上であること。

2.9.3.無停電電源装置(UPS)（一式）

財務会計システム向けの無停電電源装置（UPS）として，以下の仕様を満たすハードウェアを納入すること。

■ ハードウェア要件

(1) 本システムでデータ消失等の可能性のあるサーバや重要なネットワーク機器等は，安全性を考慮し，UPS に全て接続すること。

(2) 3U 以下のラックマウント型であること。

(3) 常時商用方式であり，AC100V もしくは AC200V の入出力であること。

(4) 入力端子形状は，並行 2 極アース付き（NEMA 5-15P）固定とすること。

(5) IEEE802.3 規格に準拠した 100BASE-TX/1000BASE-T の管理用ポートを 1 つ以上持つこと。

(6) 導入機器の消費電力，接続形態，無停電電源装置のバッテリ容量を考慮すること。

2.10. ファットクライアント端末の設定（40 台）

各職員が執務室や会議室で利用するための端末。シンクライアントシステムへの接続は行わない。それ以外の OPEN 環境（ネットワーク含む）への接続・利用を可能とすること。ファットクライアント端末については，大学入試センターが別途用意するので，受注者はそれに対して必要となるソフトウェアのインストール及び各種設定等を行うこと。

なお，用意する PC は Windows11Pro がインストールされたノート PC を想定している。

■一般要件

(1) USB メモリ等の外部媒体の利用について管理者が有効／無効を設定する機能を有すること。

(2) 管理者が遠隔によりパソコンごとに電源のオン／オフの切替え，ストレージに

対する環境復元の操作（環境復元モードの ON/OFF）ができること。また，再起動，スタンバイへの移行，ログオン／ログオフ，メッセージ表示およびコマンド実行による任意のプログラム起動などをスケジュール実行できること。

(3) PC のストレージへの書込みを制限する機能（環境復元）を有すること。ただし，パッチの適用やウィルス対策ソフトウェアのパターンファイルは，最新を維持できること。

(4) 端末本体は，再起動により設定した初期状態に復帰すること。また，本体端末に設定をすることなく，設定情報の集中管理が可能であること。

(5) 2.3.9 ウィルス対策 DB サーバ，2.3.10WSUS サーバからの配信を受けられること。また，自宅へ持ち出した場合には，各サービス事業者からインターネットを介して直接配信を受けられること。

(6) 次のソフトウェアをあらかじめインストールし，ユーザが利用できること。
(ア) Microsoft Office2024 と同等以上のオフィスソフトウェア
(イ) セキュリティ対策ソフトウェア
(ウ) 一太郎ビューア
(エ) 7Zips 等の圧縮・解凍ツールの最新版
(オ) IT 資産管理ソフトウェア
(カ) レーザプリンタ等の通常使用するプリンタドライバ

2.11. データ移行

移行作業においては，業務系電子計算機システムの利用方法及び運用管理方法を考慮した上で，提案・入札及びシステム構築作業を行うこと。また，既存システムを継続利用しているので，これらの業務に影響しない形での構築作業及び移行作業を行うこと。

現行稼働中のシステムから下記のデータとサービスを引き継ぎ稼働させること。なお，移行の詳細範囲については，移行計画書を作成し，大学入試センターと協議し，指示に従うこと。

(1) ネットワーク機器の設定については，現行システムの設定を踏襲するものとするが，変更が必要な場合，事前に大学入学センターと協議すること。

(2) 現行利用者管理サーバにて保持しているユーザアカウント情報（200 名）

(3) 現行ファイルサーバにて保持している各部署の全てのデータ（約 8TB）

(4) 現行ファイルサーバ監視システムのデータを移行すること。ただし，現行の CLOSED 環境のファイルサーバにあるデータの移行に当たっては，大学入試センターの担当者と協議のうえ，移行先を決定すること。

(5) 現行のガルーンの掲示板文書データと全メールデータ，予定データをユーザアカウント毎に移行する。
ただし，掲示板文書データは，一旦全てバックアップし，直近の過去2年分を有効データとして移行する。（約1TB）

(6) ウィルス対策用パラメータやパターンファイルデータは，同一製品のソフトウェアの場合に限り，セキュリティ対策管理サーバよりウィルス対策サービスを移

行する。(1GB)

(7) 現行のシンクライアント環境(デスクトップ等)からの移行(80GB×160 台)

(8) ユーザ毎のブラウザのお気に入り情報

(9) 財務会計システムについては，当該システム担当者の指示に従い移行すること。

なお，移行作業は，あらかじめ協議のうえ，現行システムのインストール作業，データ移行等の作業内容を確認し，決定すること。また，移行後はシステムの動作検証をすること。

(10) シンクライアントシステムの移行に当たっては，以下の点を留意すること。

(ア) 各端末にアプリケーションソフトウェアの導入作業を実施すること。

(イ) アプリケーションの動作確認は，受注者側で実施すること。

(ウ) シンクライアント環境での動作をサポートしないソフトウェアについては，大学入試センターと協議の上，導入作業の対象から除外する。

(エ) Active Directory で登録されたユーザ名とパスワードでシンクライアントにログインさせること。

(11) 各職員は，管理者が特別に認めた場合を除き，アプリケーションのセットアップ制限やアクセス制限を受けた一般ユーザの権限で利用できること。

第 3 章　保守要件

3.1. 基本要件

本件は日常のヘルプデスク対応は行わず，運用管理事業者（ヘルプデスク）を支援するものである。運用管理事業者が一次切り分けや一次回答ができるようドキュメント等を整備すること。

以下の保守やサポートの実績については，翌月（営業日の3日まで）に報告書を提出すること。

なお，保守作業の内容（日時，担当，原因，調査，対策）や交換部品等が明記された作業完了報告書を都度提出するこ

と。また，サポートについては，日時別にまとめ，完了・未完了・完了予定等が判別できること。様式については，A4縦書式とし，Microsoft Office 2024（Word，Excel）以降で作成したものとする。

(1) 受注者は，次の(2)～(7)に示す条件を満たす保守体制を用意すること。なお，保守対応とは，問い合わせ受付窓口対応，システム保守対応，ハードウェア保守対応，ソフトウェア保守対応の総称を示すものとする。

(2) 保守期間は，履行期間が終了するまでとする。なお，保守期間中にハードウェア及びソフトウェアのサポート期間が終了しないこと。

(3) 受注者は，保守対応における責任体制を明確にするため，担当者名を明記した保守体制図を提出すること。なお，体制を変更する必要が生じた場合には，変更内容を記載した書面をもって報告し，大学入試センターの承諾を得ること。

(4) 障害発生時には，大学入試センター及び運用管理事業者と綿密な調整・連携を行い，受注者の責任と負担で保守作業を行うこと。

(5) 調達機器について，技術的サポートを行うこと。また，今後の運用中に調達機器と他の機器との接続及び別途調達したソフトウェアを大学入試センター又は運用管理事業者がインストールするような場合，大学入試センターと密接に連絡が取れる体制にあり，連絡があった場合は支援すること。

(6) サーバ及びネットワーク機器に障害が発生したときは，受注者は，大学入試センター又は運用管理事業者からの連絡を受けてから 4 時間以内に状況の確認，原因の調査を開始すること。なお，障害状況の確認後 4 時間以内にシステムを復旧させること。

ただし，復旧が困難な障害については，3営業日以内に解決を目指すこととし，それ以上時間を要する場合には，大学入試センターと協議の上，善後策を講じること。発生した障害が，大学入試センターの業務に支障を来す重大なものの場合には，暫定的な処置を施し，業務への影響を取り除いた上で，3営業日以内の解決を目指すこと。

(7) 保守対応は，日本語で実施すること。

3.2. 問い合わせ受付窓口対応

(1) 受注者は，大学入試センター及び運用管理事業者からの本システムに関する問い合わせや，各種保守対応依頼を一元的に受け付ける問い合わせ受付窓口を設け，大学入試センターに対して適切な回答ができるように，提案するシステム，稼動させるハードウェア，ネットワーク，セキュリティの環境，特性を熟知し，十分な技術支援，運用支援体制を有すること。

(ア) 電話，電子メール，FAX等による保守・運用に関する技術的問い合わせに対応する体制を有すること。

(イ) 受注者は，提案するシステムの機能修正，不具合対応等，運用に必要な情報を提供すること。

(ウ) 受注者は，連絡体制，担当保守員を含む保守体制を記載した資料を提出すること。

(エ) 大学入試センターにおけるサーバ及びネットワーク機器に障害が発生した際には，受注者の受付後 4 時間以内に保守員が到着し，状況の確認，原因の調査を開始すること。なお，システムの復旧は，障害状況の確認後 4 時間以内に実施し，報告書を提出すること。

ただし，復旧が困難な障害については，3 営業日以内に解決を目指すこととし，それ以上時間を要する場合には，大学入試センターと協議の上，善後策を講じること。発生した障害が，大学入試センターの業務に支障を来す重大なものの場合には，暫定的な処置を施し，業務への影響を取り除いた上で，3 営業日以内の解決を目指すこと。

(オ) 本システムのプログラムの不具合，システムの不具合によるシステム修正については，迅速に改修作業を行うこと。

(カ) 障害対応や不具合対応等に対応するため，導入するサーバ等機器，ミドルウェア及びソフトウェア等のサポート契約について本調達に含めること。

(キ) 提案するシステムの運用に，影響を及ぼす恐れのあるセキュリティ情報を速やかに提供すること。

(ク) 大学入試センターからの照会は，2時間以内に回答するよう努め，照会内容は全て記録（照会者，照会日時，電話・メール等の照会方法，完了の有無を含む）し，以下を網羅した内容の報告書を月初めに提出すること。

(2) システム保守の受付時間（24H／365 日）は，電話によるサポートを随時行うこと。

(3) 大学入試センターからの問い合わせをインシデントとして管理し，インシデントのクローズまで，対応を継続すること。

(4) 障害について対応したときは，障害報告書を作成し，大学入試センターに報告すること。

3.3. システム保守対応

(1) 本調達システムにおいて，運用開始後，障害発生時の一時切り分け及び運用管理支援については，運用管理事業者が行うこととする。なお，重大障害発生時や切り分け困難時等，本調達で納品されたハードウェア及びソフトウェアの各

製造元（メーカー）が単独では解決できない事象発生を想定し，受注者において，ハードウェア・ソフトウェアで構成されるシステム全体の保守を実施すること。

(2) 受注者は，対応依頼を受け付けた障害を解消するため，適切かつ迅速な対応を行うこと。必要に応じて，各メーカーと協力し，ハードウェア保守対応，ソフトウェア保守対応を行うこと。

(3) システム保守対応の対応時間は，問い合わせ受付窓口対応の受付時間に準ずる。ただし，対象製品の故障の重要度，緊急度が大きいと判断した場合，大学入試センターから要請した場合は，この限りでない。なお，対応時間外のシステム保守対応については，本調達に含まないものとする。

(4) 発生した障害に対して解析を行い，原因を究明し，再発防止策を検討し，対策を施すこと。

サーバ及びネットワーク機器等のシステムに障害が発生したときは，受注者の受付後2時間以内に状況の確認，原因の調査を開始すること。なお，障害状況の確認後，原則4時間以内にシステムを復旧させること。

ただし，復旧が困難な障害については，3営業日以内に解決を目指すこととし，それ以上時間を要する場合には，大学入試センターと協議の上，善後策を講じること。発生した障害が，大学入試センターの業務に支障を来す重大なものの場合には，暫定的な処置を施し，業務への影響を取り除いた上で，3営業日以内の解決を目指すこと。

(5) 年に1～2回程度，休日における停電作業を予定しているため，作業に伴い障害が発生した際には，保守対応を行うこと。特に，大学入試センターの業務に支障を来す重要な障害が発生した場合には，当日中に復旧させること。

ただし，当日中の復旧は暫定対応とし，3営業日以内の解決を目指すことでも構わない。なお，障害復旧に係る OS やバックアップデータのリストア作業は，運用管理業者が実施するため，本調達の範囲外とする。

(6) 大学入学共通テスト実施時期における障害発生等，不測の事態に備え，事前に協議の上，センター内で保守対応のため，16 日間程度の待機を要請する。

【内訳】本試験・追試験の実施日（4日間），採点期間（8日間），成績提供（4日間）

(7) 本調達内容に関する大学入試センター及び運用管理事業者からの問い合わせ，相談に応じること。なお，「実施要項(案) 別紙 2」の他業者と連携対応を含む。

3.4. ハードウェア保守対応

(1) 各ハードウェア障害時には，当該機器又はそれを構成する部品等の調達・交換・修理等を迅速に行う等，受注者の負担により常時正常な稼動を保証すること

(2) 本調達機器の保守に関して，メーカー等が提供するハードウェア保守サービスに準ずる安定したサポート及び保守サービス品質の維持を図ること。なお，サーバ及びネットワーク機器の保守サービスレベルについては，24 時間×7 日間／

週のオンサイト保守対応とすること。

少額部材等の場合には，提供しているメーカー等が提供している一般的な内容の保守を提供すること。

(3) 調達機器に障害が発生した場合，(2)の保守サービスレベルの範囲で，ハードウェア障害と判断された時点から，原則 4 時間以内に保守員を派遣し，障害装置の修復，故障部品の修理にあたるものとする。なお，賃貸借及び保守期間中は，必要な交換部品を必ず提供することが可能なこと。

(4) 受注者は，問い合わせ受付窓口対応の受付時間外における障害に備えるため，各ハードウェア及びソフトウェアのメーカー等へ，大学入試センター及び運用管理事業者から直接問い合わせが可能な窓口を用意すること。

(5) ハードウェアの修理又は交換を行う際に，ラックからの取り外しや，据え付け・調整作業が必要な場合は，実施すること。また，必要に応じて，大学入試センターと協議のうえ，設定内容の再投入等，設定作業を行うこと。

(6) 修理対応後，障害個所の修理又は交換後，機器が適正に機能するか動作確認すること。大学入試センター及び運用管理事業者と連携が必要な場合には，連携すること。

(7) 保守期間中，ハードウェアに対する修正ファームウェアの適用要否に関する情報を大学入試センターに対し提供すること。また，大学入試センターがファームウェアの修正が必要と判断した場合，受注者が適用作業を行うこと。大学入試センター及び運用管理事業者と連携が必要な場合には，連携すること。

(8) 本調達ハードウェアに搭載された HDD／SSD に障害が発生した際に，当該 HDD／SSD を取り外し交換した場合，故障した HDD/SSD は破砕すること。なお，HDD/SSD の破砕証明書（破砕前後の写真含む）を発行し，提出すること。

3.5. ソフトウェア保守対応

(1) 受注者は，ソフトウェア（OS 含む）に関する問い合わせ，セキュリティ情報等の提供，障害発生時における解決支援に対応すること。

(2) 納入したソフトウェアに対する修正パッチ及び修正モジュールがメーカーより提供された場合，大学入試センター又は運用管理事業者によるこれらの適用要否の問い合わせに対しては，対応を行うこと。

修正パッチ及び修正モジュールの適用については，運用管理事業者にて実施するものとする。なお，適用中に不測の事態が発生した場合には，大学入試センター又は運用管理事業者からの問い合わせに対しては遅滞なく対応すること。