基幹ネットワークシステム構築及び運用保守に係る業務委託仕様書

2025 年 7 月 31 日

公立大学法人　横浜市立大学

目次

【別紙資料】

別紙資料 1　現状機器一覧
別紙資料 2　基幹ネットワークシステム構成図
別紙資料 3　サーバ構成図
別紙資料 4　学生数・教職員数一覧
別紙資料 5　認証連携一覧表
別紙資料 6　基幹 NW 既存 L2･L3 スイッチ拠点別一覧
別紙資料 7　無線 AP 設置場所一覧
別紙資料 8　端末設置場所概要図
別紙資料 9　導入アプリケーションソフト一覧
別紙資料 10　キャンパス間回線とデータセンター構成図
別紙資料 11　キャンパス平面図
別紙資料 12　ネットワーク配線図（電子データのみ）

1. 導入の方針等

1.1 導入の趣旨

公立大学法人 横浜市立大学（以下「本学」という。）は、国際教養学部、国際商学部、理学部、データサイエンス学部、医学部の 5 学部、都市社会文化研究科、国際マネジメント研究科、生命ナノシステム科学研究科、生命医科学研究科、データサイエンス研究科、医学研究科の 6 研究科を横浜市内 5 キャンパスに展開し、附属 2 病院を擁する総合大学であり、「国際都市横浜と共に歩み、教育・研究・医療分野をリードする役割を果たすことをその使命とし、社会の発展に寄与する市民の誇りとなる大学を目指す」というミッションのもと、多角的に物事を考える力を養う教養と特色ある高い専門性を兼ね備えた、豊かな人間力を有する人材を育成することを教育ポリシーとしている。

この教育ポリシーに基づいた教育・研究・医療を提供するため、より「利便性」「安全性」「可用性」「運用性」が高い基幹ネットワークシステムが求められている。しかしながら、令和 7（2025）年度現在、本学で提供している情報基盤について表1のような課題があると認識しており、システム更新によってそれらの解消を図りたいと考えている。

表 1 現状の基幹ネットワークシステムの課題と対応策

重点項目	認識される課題	想定している対応策
通信量増加への対応	・研究データ量やクラウド環境利用の増加 ・学内 LAN/学外 WAN 回線への通信量増加でネットワークが逼迫傾向にある	・現時点の逼迫を解消する最低限の帯域増強 ・今後 6 年間での拠点単位での途中増強が容易な学外回線選定・構成変更
セキュリティ対策	・攻撃手法の高度化（ランサムウェア、サプライチェーン攻撃） ・攻撃対象の多様化（リモート環境、クラウド環境）	・事務用ファイルサーバ（3 拠点共用）や主要管理サーバの防御に重点を置いたセキュリティ強化や、管理者側機能の強化
DX・生成 AI への対応	・DX（デジタルを活用した業務変革）や生成 AI 活用による業務負荷軽減・コスト削減・付加価値創出への期待と需要の高まり	・Microsoft365 を活用してDXや生成 AI 利用を進めるうえで前提となる、アカウント情報の管理や連携の強化・整備

1.2 本学および基幹ネットワークシステムの現状

1.2.1 基幹ネットワークシステムの概要

これから更新を検討すべき基幹ネットワークシステムの現状を参考までに示す。構成する機器については別紙資料1「現状機器一覧」、構成については別紙資料 2「基幹ネットワークシステム構成図」、各種サービスを提供しているサーバ構成は別紙資料 3「サーバ構成図」の通りである。

これらの更新にあたり、表1に示した重点項目の改善を図り、課題を解消できるようなシステム構成となるよう設計すること。

1.2.2 大学における利用者人数等

本学における学生数・教職員数とその推移については、別紙資料 4「学生数・教職員数一覧」を参照のこと。これらの人数には大きな変化がないものとして、容量、性能等の設計をすること。

1.2.3 システム間連携

基幹ネットワークシステムにおいて、ユーザ認証関連のデータは、学内の他の情報システムと連携しており、別紙資料 5「認証連携一覧表」に記載した関係となっている。これらの連携関係は、システム更新後も継続するものとする。

2. 調達内容

2.1 基幹ネットワークシステムの構成

今回更新対象とする基幹ネットワークシステムの範囲を以下のように定義する。各システムの構成物については「4 基幹ネットワークの要求仕様」に詳述する。

表 2 基幹ネットワークシステムの構成

基幹ネットワークシステム	基幹ネットワーク、認証システム、アカウント管理システム、教育実習室システム、事務ネットワークシステムの総称。
基幹ネットワーク	本学内のネットワークインフラを構成し、基本的なネットワークサービスを提供するシステム。 以下の機材、サービスを含む。 ・学外データセンターへのサーバ機器ハウジング、ネットワーク接続 ・キャンパス間接続回線 ・基幹 L3 スイッチ ・サーバスイッチ ・学外接続用 L3 スイッチ ・キャンパス L3 スイッチ ・建屋 L3 スイッチ ・建屋内フロア L2 スイッチ ・認証スイッチ ・ファイアウォール ・無線 LAN 装置(コントローラ、アクセスポイント) ・VPN 接続サービス ・ネットワーク配線（居室の情報コンセントや無線 AP まで） ・仮想化基盤サーバ ・ユーザ管理システム（ActiveDirectory サービスを統合管理） ・DHCP サービス ・DNS サービス ・NTP サービス ・外部公開 Web サービス ・メールセキュリティサービス ・メール中継サービス ・ログ管理サービス ・ネットワーク監視サービス ・Active Directory サービス ・ファイルサービス
認証システム	端末機器の基幹ネットワークへの接続制御を行うシステム
アカウント管理システム	人事給与システムと連携してアカウントを管理できる仕組み。
教育実習室システム	実習室用 PC 貸出 PC 実習室用プリントサービス PC にインストールするソフトウェア一式 上記 PC の管理システム UNIX 演習サービス 並列計算機サービス
事務ネットワークシステム	事務領域のセキュリティサービス 資産管理エージェント ※事務領域とは、事務部門が使用するネットワークで、教育研究用とはアクセス制限等が異なる。

更新の対象となる拠点は以下のとおり。

	対象拠点	キャンパスマップ（以下の所在地は全て横浜市内）
1	金沢八景キャンパス	金沢区瀬戸 22-2 https://www.yokohama-cu.ac.jp/access/hakkei_campusmap.html
2	福浦キャンパス	金沢区福浦 3-9

		https://www.yokohama-cu.ac.jp/access/fukuura_campusmap.html
3	本学附属病院（以下「附属病院」という。）	同上 （福浦キャンパス同一敷地内）
4	舞岡キャンパス	戸塚区舞岡町 641-12 https://www.yokohama-cu.ac.jp/access/maioka_campusmap.html
5	附属市民総合医療センター(以下「センター病院」という。)	南区浦舟町 4-57 https://www.yokohama-cu.ac.jp/access/urahp_map.html
6	鶴見キャンパス	鶴見区末広町 1-7-29 https://www.yokohama-cu.ac.jp/access/tsurumi_campusmap.html
7	みなとみらいサテライトキャンパス	西区みなとみらい 2-2-1　横浜ランドマークタワー7 階 https://www.yokohama-cu.ac.jp/access/satellite_campusmap.html

※附属病院及びセンター病院の医療情報システム用のネットワークシステムは今回の調達対象ではない。
※鶴見キャンパス内は独自ネットワークのため、キャンパス間回線を当該ネットワークに繋ぐところまでと、当該ネットワークと連携してキャンパス内に敷設された基幹ネットワークの無線 LAN と事務 LAN を今回の調達対象とする。

2.2 調達の範囲

今回の調達では表2に示した基幹ネットワークシステムとそれに含まれるサブシステムのほか、以下の業務の履行を含める。

(1) システム構築及び関連業務
- ア　システム構築から運用開始(サービスイン)までのプロジェクトマネジメント業務
- イ　必要なハードウェア、ソフトウェア、その他機材の提供、台帳等の作成
- ウ　機器の設置、設定、動作テスト
- エ　ソフトウェアのインストール、最新パッチ等の適用
- オ　データセンターへのサーバ機器設置
- カ　データ移行、必要な範囲での補正等
- キ　必要に応じてネットワーク配線工事(居室の情報コンセントまで)、電源工事、機器取り付け工事
- ク　運用開始(サービスイン)前後での運用支援
- ケ　利用者用操作マニュアル、システム管理者用運用マニュアル作成
- コ　本学システム管理者への操作説明
- サ　不要となった機材（撤去した旧機器、付属品）及び納入機器類の梱包資材の廃棄
- シ　既存のネットワークに係る LAN 配線図、ポート接続構成図、ポート収容表等の更新

(2) 保守・サポート業務
- ア　教育実習室システムについては令和 8 年 4 月 1 日から運用開始、それ以外のシステムについては、令和 8 年 10 月 1 日から運用を開始すること。
- イ　保守・サポート業務期間は令和 8 年 4 月 1 日から令和 13 年 3 月 31 日とする。この期間の保守・サポートに係る費用を含めること。
- ウ　基幹ネットワークシステムを構成する機材の点検、障害対応、保守
- エ　教育実習室システムの端末のメンテナンス作業（OS のアップデート作業、ウィルス定義ファイルの更新、パッチ適用等）
- オ　定期処理(統計データ集計のバッチ処理、データバックアップ、計画停電対応など)
- カ　ドキュメントのメンテナンス

更新対象機器の詳細については、別紙資料 1「現状機器一覧」、別紙資料 2「基幹ネットワークシステム構成図」を参考に設計を行うこと。追加を想定している機器等については「4 基幹ネットワークの要求仕様」以降に示す。

2.3 導入のスケジュール等

全体の導入スケジュールは表3のとおりである。システムによって運用開始の時期が異なるため、分割して検収を行う。

情報教育実習室システムは令和 8 年 4 月 1 日を運用開始とする。

基幹ネットワークシステムは令和 8 年 10 月 1 日を運用開始とする。

表 3 基幹ネットワークシステムの導入スケジュール

2.4 システム構築プロジェクトで想定する工程

以下のフェーズ、もしくはこれらに相当するフェーズを実施する。最初のフェーズを除き、次のフェーズを開始する前には、原則として必ず、チェックポイントとして本学と受託者共同で前工程のレビューを行い、問題がないこと、あるいは課題等が生じていることなどを、確実に共有してから次フェーズに進むこと。

(1) 導入スケジュール調整
- ア　プロジェクト実施計画の作成
- イ　WBS（Work Breakdown Structure：作業分解構成図）の作成

(2) 概要設計
- ア　システム全体設計
- イ　システム基盤基本設計（セキュリティ基本設計を含む）
- ウ　ネットワーク基本設計
- エ　アプリケーション基本設計

(3) 詳細設計
- ア　システム基盤詳細設計
- イ　ネットワーク詳細設計
- ウ　アプリケーション詳細設計

(4) 導入およびテスト
- ア　アプリケーション作成
- イ　単体テスト
- ウ　結合テスト
- エ　システム基盤への組込・整備
- オ　システムテスト（システム単体、システム間接続、外部機器との接続等）
- カ　運用・シナリオテスト
- キ　受入テスト（本学職員によるテスト）

(5) システム導入および移行
- ア　アプリケーション導入、データ移行
- イ　システム管理者向け研修
- ウ　ユーザ研修

(6) システム保守・運用管理
- ア　システム保守・運用監視・障害対応

イ　運用サポート
ウ　ドキュメント管理・更新

2.5 成果物に関する事項

(1) 成果物の作成においては、様式、体裁、装丁、語句の表記方法等の統一を図るとともに、その質を監査する為の要員を配置し、十分な品質管理を行うこと。
(2) 成果物のデータファイルに設定されるタイトル、作成者名、会社名といった属性情報については、あらかじめ案を用意したうえで本学に確認すること。
(3) 成果物のうち、本学が要望する機能要件を実現するために、受託者が個別に対応（カスタマイズ）した部分を含む機能の実現に関する情報が記載されたシステム設計書、データベース定義書等については、その箇所が識別できるような措置を講じておくとともに、その個別対応に及んだ背景やシステム機能実装上の制約事項等、ソフトウェア保守の際に重要となる関連情報について、保守要員が容易に把握できるように追記・明示して納品すること。
(4) 文書等の成果物を電子ファイルで納入する場合、当該ファイルや格納ディレクトリ（フォルダ）の作成にあたって、以下の基準を順守すること。
　ア　電子メールにファイルを添付する場合があることを念頭において、ファイル名等に半角カナ文字の他、①、Ⅰ、㈱等の機種依存文字を含めないこと。
　イ　ファイル名等に半角または全角の空白文字を挿入しないこと。
　ウ　ファイル名等の命名はソート順を意識すること。
(5) 導入に必要な機器及びソフトウェアの納入において、製品に添付されるマニュアルや DVD／CD-ROM（以下「インストールメディア」という。）、保証書等の同梱品の扱いについては以下のとおり作業を行うこと。
　ア　インストールキーや製品シリアル番号等、マニュアルやインストールメディアに製品個々の独立性を表意する情報の印刷・刻印等がなされている場合は、インデクスシールを貼付してまとめること。特に、機器管理番号等との関連を明記した一覧表のファイルを必ず作成し、どの製品に付随したマニュアル、インストールメディアかどうかわかるようにしておくこと。
　イ　前項とは異なり、製品個々による独立性を表意する情報が添付されていないマニュアルやインストールメディアについては、同種類を一様にまとめて整理するか、本学と協議のうえで廃棄可能なものは一定部数のみ保存し、他を廃棄処分とするなど、適切な措置を講じること。
　ウ　ソフトウェア製品の開梱に伴う廃棄物が発生する場合は、受託者の負担・責任において処分することとし、業務履行場所に廃棄物をそのまま放置してはならない。
(6) 設計に係る成果物は次に掲げるドキュメントを基本とし、成果物の構成や様式等の詳細については作業着手前に本学と協議し、本学の同意を得ること。
　ア　開発工程表及び開発体制表
　イ　システム概要図（各システム・サーバの関連・全体構成を図示）
　ウ　すべてのハードウェアの設置場所が確認できる配置図面（ラックマウント図、教育実習室端末の設置図を含む）
　エ　システム設計書（機能、定義、インタフェース、データベース、モジュール、その他カスタマイズ部分も含む設計に係る事項の記載）
　オ　ハードウェア設計書（仕様、構成、設定、デフォルト値とチューニング後の初期値、その他設計に係る事項の記載を含む）
　カ　ネットワーク設計書（構成、設定値一覧、パラメータシート、VLAN 割り当て、ポート接続状況、その他設計に係る事項を含む）
　キ　IPアドレス管理表（NW 機器、サーバ類、クライアント端末類の一覧）
　ク　ソフトウェアのライセンス一覧（有償・無償・ライセンス数の判別が可能であること）
　ケ　テスト実施計画書
　コ　本番稼働計画書
　サ　システム移行計画書
　シ　研修実施計画書
　ス　研修で使用した全ての資料

セ　インストール手順書（サーバ、端末等全て）
ソ　各種検討報告書
タ　協議に関する記録等
チ　各システム及び機器間の接続要件仕様書
ツ　機器の設置作業等による施工計画書
テ　施工工事写真、施工報告書
ト　各種 LAN 配線図、ポート接続構成図、ポート収容表等（本学で所有するドキュメント一式に対して、今回の導入内容を反映すること）
ナ　その他、システム管理上必要と考えられるものについては、本学と別途協議すること。

(7)　運用・保守に係る成果物は次に掲げるドキュメントを基本とし、様式・詳細に関する協議は前項で掲げたとおりとする。
ア　保守体制表
イ　運用手順書（サーバ管理手順、運用スケジュール、メンテナンス手順、バッチ処理手順、他システムとの相互依存、連絡体制図、その他運用上必要な手順等を含む）
ウ　保守関連手順書
エ　ネットワーク管理等手順書（運用管理方法、監視装置関連操作方法等含む）
オ　障害時の事故管理等手順書（障害時の対応、連絡体制、復旧方法、動作確認方法等含む）
カ　データバックアップ等手順書
キ　機器管理番号を含むハードウェア一覧表、構成図等
ク　利用者向け操作マニュアル
ケ　システム運用マニュアル（通常時、イレギュラー対応時、管理機能と操作手順、権限設定方法等含む）
コ　サービスレベル記述書（対象となるサービスの内容と範囲、サービスレベル指標と水準等）
サ　受託者が運用保守するうえで使用する ID と当該 ID に付与された権限の一覧
シ　運用に関する報告書（ネットワークトラフィック、リソース使用状況、アカウント利用状況、障害対応状況、問い合わせ対応状況等、運用保守フェーズで必要となる報告書に必要な情報の詳細・フォーマットは事前に確認のうえ、システムからの出力設定に反映すること）
ス　その他、システム管理上必要と考えられるものについては、本学と別途協議すること。

3. システム全般に関わる基本要求

本システムの更新にあたり、基本的な要求事項を以下に示す。

3.1 システムの利便性・操作性・運用性

(1) やむを得ずスクラッチで開発しなければならないプログラム等を除き、一般的に入手できるハードウェア、ソフトウェアで構成し、学生や教職員が直接使用するものについては、使用・運用において特別な知識やスキルを必要としないこと。使用において、特別な操作が必要な場合は、GUI ベースで操作できること。

(2) 標準化された規格を採用すること。ただし、将来性のある最新技術も、信頼性、保守性、経済性を確認できれば積極的に導入することを検討するので、採用する場合は事前に本学と協議すること。

(3) ネットワークのレスポンスや、実習室システムの応答時間がユーザにとってストレスのない範囲であること。そのための目標とするレスポンス又はスループットを設定し、客観的な測定と、この目標を実現するためのシステムのチューニング（ネットワークの整備も含む）を実施すること。また、データの増加などによりシステム性能が低下しないよう、負荷分散方式やコンパクション処理の自動実行等を適宜検討に盛り込むこと。

(4) ネットワークの稼働状況やシステムの利用状況などは、機器側にエージェントを設定し可視化できるツールを提供し、本学の職員でも容易に状況が把握・確認でき、対策がとれるようにすること。また緊急性の高い事象の発生に対しては、アラートを発する仕組み、自動停止、システム管理者への自動発報等の仕組みを搭載すること。

(5) 障害や不具合により運用継続ができなくなることでシステム全体の可用性に致命的な影響を与える主要部分については冗長化し、故障してもサービス全体が停止しない構成とすること。

(6) アプリケーションソフトウェア、パッケージソフトウェアについては本学の指定がない限りは安定している最新のバージョンで導入すること。

(7) ハードウェアのコンフィグレーションや、各種ソフトウェアを本学の運用に合わせてカスタマイズする場合、その後の設定変更やチューニング、機能拡張等に備え極力、追加費用等を生じさせることなく容易な変更ができるよう十分配慮し、事前にその仕様等について本学と協議すること。

3.2 システムの拡張性・柔軟性

(1) システムを構成するソフトウェア、ハードウェア（CPU、メモリ、ストレージ等）について、十分な拡張性、柔軟性を有すること。

(2) 利用者やデータの増加等に対応できるようスケーラブルな構成とし、システムの停止や長時間のリビルド等を必要とせずに拡張できるよう考慮すること。

(3) 業務システムとのデータ連携は、標準的なインタフェースを使用し、連携仕様を提示できるようにすること。また、業務システムの更新や新規連携の際には、システム変更や修正をせずに容易に接続できるようにすること。

3.3 システムの信頼性・可用性

(1) 設備の長時間にわたる停電などの場合を除き、サーバリソースは 24 時間 365 日の安定した連続運用が可能であること。

(2) ネットワーク障害、システム障害などの各種障害が発生した際に、復旧のための原因特定が可能となるよう適切なログの採取を考慮したシステムとすること。ログ収集によるシステムのパフォーマンスへの影響が懸念される場合を除き、ログを収集していなかったことで障害原因の究明が出来ないような事態に陥らないよう、デフォルト値でログ出力をしないような項目がないかは十分確認すること。

(3) 定期的なバックアップと、本学が承認した障害時のリカバリ手順を明確にすること。

(4) リカバリ手順や所要時間は本学と協議し承認したものとすること。

(5) サーバ機器およびネットワーク機器に対しては、常時監視ができるようにし、異常時にはシステム管理者等へ警告を発する仕組みを考慮すること。

(6) 障害もしくはネットワークの許容量を超えるような利用の可能性を想定し、自動的な負荷分散やプロトコルに応じて帯域制御、優先制御等行うことで、サービス停止を回避するような仕組みを用意すること。

3.4 システムのセキュリティ

(1) 機密情報や個人情報の保護のため、使いやすさを維持しつつ適切なアクセス制御ができる仕組みを備えていること。
(2) ユーザ管理など重要なデータへのアクセス、及び、学外からのリモートアクセスについては、アクセスした利用者、アクセス先の情報、時間、端末、件数等を特定できる履歴(アクセスログ)を蓄積し、その解析をシステム管理者が随時かつ容易に行えること。
(3) 資産管理システムなどと連動して、ネットワーク接続端末の適正管理が実施できるよう考慮すること。
(4) 外部からの通信をモニタリングする仕組みを整備し、通信記録をログとして保存し、アクセス状況を解析可能とすること。その保存期間は原則 1 年以上とし、システムごとに本学と協議のうえ決定すること。
(5) サーバへの不正侵入に対する検知、阻止ができる仕組みを導入すること。

3.5 システム容量および性能

(1) 容量、性能は、年間増加率を考慮し、最低 6 年間は機器の増設や刷新なしで運用できるよう考慮すること。
(2) システムごとにあらかじめ設定した閾値を超えた場合に、自動的にシステム管理者に通知・発報ができるような構成とすること。
(3) リソースの利用状況を常時確認できるようにし、長期未使用者や退職者等のリソースを容易に再使用できるようにすること。

3.6 電源・LAN 配線等の設備について

基幹ネットワークの更新において、光ケーブル、LAN 配線、情報コンセント、ネットワーク機器収納ボックス、電源コンセントは既設の基盤を極力流用することとし、不足するもの、もしくは仕様・性能を満たさず変更が必要なものについては、事前に必要数を算出したうえで、増設、変更工事を行うこと。

その費用については受託者が一定額を見込んで本調達に含めるものとする。

3.7 データセンター

現行のサーバ機器はデータセンターに設置している。更新するサーバ機器もデータセンターに設置し、そこで運用することを調達の範囲に含める。その要件は以下のとおりとする。

(1) 耐震性、給電性能、入室セキュリティなど、一般的なデータセンターとしての要件を備えていること。
(2) SINET と接続できること。また、SINET L2VPN 接続サービスを利用できること。
(3) キャンパス間を接続するために必要な回線もデータセンター内に収容できること。
(4) 設置する機材がすべて格納でき、かつ収納後 6U 以上の別の機器が搭載可能なラックスペースと、機材設置に必要なパッチパネル、パッチケーブル、ラックマウント用レール、ボルト等あわせて用意すること。
(5) 運用開始後、リセットボタンの押下や、稼働状況を示す表示ランプの確認など、やむを得ずサーバ機器を物理的に操作・確認しなければならない事態が生じた場合は、「11.3 保守」で定義する保守要員(サポート要員)が行うこと。
(6) 現行のラックに大学側の機器を搭載しており、システム更新後も継続利用する。更新に伴い異なるラックを利用する場合は、これらの機器を搭載可能なラックスペースを含めること。また、機器の移設作業も本調達に含めること。

3.8 回線

各キャンパスとデータセンターを接続する回線を調達範囲に含めている。構成については別紙資料 10「キャンパス間回線とデータセンター構成図」を参照すること。要件は以下のとおりである。

(1) 必要な帯域が保証されていること。
(2) 広域イーサーネット型のサービスにてキャンパス間の通信が直接行えること。

(3) 常時監視がされ、瞬断や故障時には、本学システム管理者に通知・説明がなされること。
(4) 受託者自身が自営で敷設している通信回線を提供することを必須とはしないので、通信事業者が提供する通信回線サービスを別途契約によって組み込む形も可能とする。また、ネットワーク障害が生じた際に受託者と協働して一刻も早く復旧に向けた対応を行うことが可能な体制とすること。
(5) マルチキャストパケットが透過できること。
(6) トラフィックレポートが利用できること。
(7) 網内の往復遅延の目標値は 4mmsec 以内と定めること。

3.9 システム連携

「1.2.3 システム連携」で示したシステム間の連携について、今回の基幹ネットワークシステム更新後もこれらの関係を維持できるよう考慮すること。原則として、連携先のシステムの機能追加や設定変更を行わずに更新が行えるよう配慮すること。

3.10 機器設置関連

(1) 設置場所
ア 基幹ネットワークシステムを構成するサーバ機器は、教育実習システムに関するものを除いて、原則としてデータセンターへ設置すること。
イ スイッチ等の新規設置については、必要に応じて現地調査を行ったうえで、必要な配線や電源の工事も行うこととし、本調達に含めるものとする。
(2) 電源設備
ア システムの移行に伴い、旧システムと新システムを平行稼働することを想定する場合は、金沢八景キャンパスにおいて並行稼働中に利用可能な電源容量は 30A×2 である。また、福浦キャンパス A205 において並行稼働中に利用可能な電源容量については、分電盤に現在空き系統が存在しないため、必要に応じて設備を用意すること。なお、並行稼働期間は 1 か月間とする。移行の方法は別途本学と協議し、それ以上の必要な電源容量は本調達の中で用意すること。
イ 原則、最寄りの分電盤より分岐して電源をとるなどして対処すること。また、これと異なる電圧、周波数の電源で稼働する装置は、電圧変換、周波数変換等の設備を用意すること。
ウ 設置する機器が設置済みの空調設備以上の冷房能力を必要とする場合、また特殊な冷却設備が必要な場合はその設備を用意すること。
エ 電源コンセントの形状により変換アダプタが必要な場合は用意すること。
(3) 電源管理
ア データセンター以外に設置するサーバ類には、停電時に正常かつ安全なシャットダウンプロセスで停止できるよう、無停電電源装置(UPS)を提供すること。
イ UPS は、接続したサーバが、停電時に正常かつ安全にシャットダウンできるまでの十分な電源容量を確保することとし、運用開始前にそのテストも必ず行っておくこと。
ウ バッテリ等の消耗品の交換は、運用保守契約に含めるものとする。
(4) 搬入・据付・配線・調整
ア 機器の搬入・据付・配線・調整等に関しては、事前に搬入経路や配管を確認し、本学と調整のうえ作業方法を決定すること。当該作業開始前において本学が求める期限までに、作業者、利用する車両の情報、駐車場利用時間等を本学に提示すること。
イ 搬入や工事に関しても作業工程表を作成し、本学の承認を得ること。なお、工程表には工程名称、期間、目的、報告予定日などを明記すること。
ウ 本学が用意した一次側電源設備から各機器への配線も行うこと。
エ 更新対象としていない既設ネットワークとの接続について障害が発生した場合は原因の分析を早急に行い、受託者の作業に起因する障害については迅速かつ真摯に対処すること。
オ 必要に応じて LAN 情報コンセントを設置すること。その際には、形式を統一すること。
カ 本学の施設内に設置する全ての機器について、盗難防止措置及び安全のための転倒防止措置を講じること。

キ　ネットワーク機器や新設する LAN 情報コンセントについては、不正な接続を防止するために、機器本体やポートに鍵を付けるなどの措置を講じること。

ク　八景キャンパスサーバ室、福浦 A205 室、福浦看護実習室のラックは全て既設（EIA 規格に準拠した 19 インチラック）を流用とする。ラックのスペースが不足する場合には、新たなラックの導入も本調達に含めるものとする。

ケ　構築業者は導入計画書に、構築から移行までのラック搭載計画を記載すること。

コ　導入する全サーバの操作に必要なディスプレイ、キーボード、マウス等の操作デバイスを提供すること。複数サーバを集約して共用のディスプレイ、キーボード、マウス等で操作することも可能とするが、その場合は切替機を用意すること。

サ　その他設置に必要なケーブル類は全て提供すること。

シ　設置されるハードウェアについて、機器管理番号や IP アドレス、サブネットマスク、VLAN の ID 等のネットワーク定義情報を明示し、原則として着脱可能なマグネットシールやタグ等を貼付すること。特に、これらの準備及び貼付にかかる一切の費用は受託者の負担とする。なお、明示する情報の内容については、本学と別途協議すること。

(5)　バックアップ

ア　機器故障や誤操作によるデータの消失回避のため、各サーバの復旧用イメージ及びデータのバックアップを取得すること。保存先はデータセンター内の別媒体とすること。

イ　導入サーバについて、2世代のフルバックアップを取得すること。ファイルサーバと認証システムについては、日次の差分も保存できること。

3.11 導入・テスト・研修

(1)　プロジェクト体制

ア　導入・構築を行うプロジェクトマネージャが、下記のいずれかの資格を保有していること。

（ア）　情報処理推進機構実施の情報処理技術者試験「プロジェクトマネージャ」

（イ）　米国プロジェクトマネジメント協会（PMI）本部認定「PMP 国際資格」

（なお、以降情報処理技術者試験資格は「情報処理(PM)」、PMP 国際資格は「PMP」と略記する。）

（ウ）　特定非営利活動法人　日本プロジェクトマネジメント協会「プロジェクトマネジメント・スペシャリスト」

イ　各作業担当者は基幹ネットワークシステムの更新に当たり、本学のネットワーク環境を十分把握したうえで業務を行うこと。

ウ　プロジェクトマネージャは、構築期間中は本プロジェクトの専任とすること。

エ　設計・構築要員とテスト要員は、各々別の人物を充てること。

オ　システムの構築及び付随する業務の遂行にあたっては、作業分担、編成時期等を明確にした組織（要員）管理計画書を作成すること。

カ　分担した作業ごとにプロジェクトチームを編成し進捗管理を行うこと。また、マルチベンダ構成によるチームを編成する際には、受託者が総責任者となる組織（要員）管理体制とすること。

キ　プロジェクトの体制を変更する場合には、その事由と新体制について事前に本学に説明し、協議したうえで実行すること。

ク　作業担当者を交代する場合は、業務一切の引き継ぎを確実に行い、それにより業務に支障が生じないようにすること。

ケ　プロジェクトマネージャは各作業担当者に、個人情報の取り扱い、本学のルール及び倫理・道徳・社会常識について指導をすること。

コ　定期的（月次・週次）に進捗報告会議を実施し、スケジュールに係る課題が発生した場合は本学と協議のうえ解決すること。またその会議で共有する資料は、内容について受託者の担当者間で齟齬のないよう、受託者内部で十分なレビューや査閲を行ったうえで、会議前日までにはデータで本学に送付すること。

サ　進捗報告会議にはプロジェクトマネージャが必ず参加すること。なお、会議の形態は WEB 会議でも構わないが、少なくとも月に 1 度は対面にて会議を実施すること。

シ　「2.4　システム構築プロジェクトで想定する工程」に示す各プロセスの終了時には、受託者内部で十分なレビューを実施し、そのレビュー結果を本学に提示すること。なお、本学が不要と判断しない限りは、

原則としてプロセスごとに本学と共同レビューを実施し、承認を得ること。

ス　進捗会議、レビュー会議における議事録は受託者が作成すること。

(2)　テスト

ア　全てのテストにおいて、テスト仕様書/結果報告書を提示し承認を得ること。テスト項目・パターンに漏れがないか事前に本学に確認すること。

イ　単体・結合テストは受託者保有の機器、製品を使用して実施すること。

ウ　システムテストは、本番機器の導入後であれば、実機を使用すること。また、既存システムの環境を用いてテストを実施する場合には、事前に本学と協議し、その指示に従うこと。

エ　運用・シナリオテストは、受託者が事前に本学の運用について詳細にヒアリングしたうえで、テストパターン(シナリオ)を用意すること。

オ　受入テストは本学が実施主体となり行うが、受託者は、必要な設定等の作業支援を行うこと。

カ　受入テストの実施にあたって、運用・シナリオテストで使用したテスト仕様書、テストデータ、テストシナリオを全て本学に提示すること。

キ　受入テストに使用するテストデータについては、受託者が作成すること。

ク　受入テスト期間中、受託者は本学職員からの問合せを受けられる体制を確保すること。

ケ　受入テスト後の修正にあたってはデグレードしないように細心の注意を払うこと。

コ　テスト時に使用した不要なデータ、ユーザ ID、プロセス、サービスはテスト完了時にシステムから完全に削除すること。

サ　冗長構成によるシステム切り替え等については実機によるテストを確実に実施し、想定した通りの暫定運用ができること、及び復旧手順を確認すること。

シ　本番環境の動作制限が生じたり、外部に影響するようなテストは、少なくとも実施の 1 ヵ月以上前にその内容やスケジュール等の概要を本学に提示して調整を図ること。

(3)　導入

ア　ネットワークやサービスの停止を伴う作業については、原則として土日、夜間に実施することを想定し、詳細は本学と別途調整すること。

イ　特に附属 2 病院については 24 時間体制で運営されている公的病院であるということを踏まえ、騒音の有無に関わらず、工事等を行う場合は診療業務に支障をきたさぬよう実施日、時間帯、場所等について本学と事前に十分調整すること。また、本業務の履行にあたって患者等に不快感を与えることのないよう、その挙止や身なり、対応、発言等について十分注意を払うこと。

ウ　各作業担当者は自らの所属等を証明するものを常時携帯するとともに、一般に目視できる位置に名札等を着用すること。

エ　各作業担当者が本学内各室に立ち入って作業を行う際は、原則として、事前に本学の許可を得たうえで作業を進めること。

オ　本業務に関わる機密事項や本学で知り得た学生情報、職員情報、患者情報等を取り扱うにあたって、受託者は、本業務に携わる者以外にこれら一切の情報が漏洩しないよう、十分に配慮すること。

(4)　移行

ア　原則、既存システムの全てのデータを、新システムへ移行することを想定しているが、その範囲・方法等については本学と協議のうえ決定することとする。

イ　新システムへの移行については、移行計画書としてまとめ、本学の承認を得たうえで実施すること。

ウ　現在運用しているシステムから、今回調達するシステムへ円滑な移行が可能であること。またその際、必要な条件等については事前に本学と協議すること。

エ　移行に伴う停止期間を最小限にし、かつ運用開始当初から安定したサービスが提供できるよう移行計画書を作成すること。

オ　システムの移行については、本学教職員の負担が最小となるよう考慮したスケジュールとすること。

カ　ID・パスワード、ファイルサーバ上の各データ(エンドユーザのデータ)は、原則として現状のデータ及びアクセス権を保持して移行すること。ただし、場合によっては、一部そのデータのメンテナンスを行う可能性もあることは認識しておくこと。

キ　移行に際してエンドユーザの負担となる作業が発生する場合は、エンドユーザへのサポートを行うこと。
ク　現行のユーザ管理システムからのデータの抽出は、本学職員の立ち合いのもとで作業を行うこと。
ケ　移行後のデータが、新システムで正しく登録できていること、また正常に動作することを確認すること。
コ　移行作業は原則として全てのサーバ系導入機器に必要であるほか、移行にり、本調達に含まれない既設の LAN 機器の設定変更がやむなく必要な場合も、受託者がその作業を請け負うこと。
サ　本案件の移行にかかる全ての費用は本調達に含まれるものとする。

(5)　展開支援
ア　認証システムやネットワーク機器更新に伴う利用者パソコンの設定変更に関して、展開支援を行うこと。
(ア)　キャンパス毎など期間を区切り、支援要員を配置したうえで切替え作業を行うこと。
(イ)　1か月程度で作業が完了する作業要員数を確保すること。
イ　展開支援要員として、以下要件のいずれかを満たす者を確保すること。
(ア)　ICT インフラ関連業務に 2 年以上従事していること。
(イ)　今回更新する本学のネットワーク環境を熟知していること。
ウ　展開支援要員のマネジメント要員として、以下要件のいずれかを満たす者を 1 名以上確保すること。
(ア)　PMP、情報処理(PM)のいずれかを保有していること。
(イ)　ITIL ファウンデーション以上を取得していること。
(ウ)　情報処理(SC)、情報処理(NW)のいずれかを取得していること。
(エ)　本調達の全体プロジェクトマネージャとの兼務であってもよい。
エ　展開作業は令和 8 年 7 月～9 月の間に実施するが、詳細な期間は本学と検討のうえ決定する。

(6)　研修
ア　基幹ネットワークシステムの導入研修としては以下を想定している。
(ア)　ユーザ研修:ユーザ(教職員)に対して研修を行う。
(イ)　システム管理者研修
(ウ)　条件:本学内の研修室(定員:30 名～60 名)を利用可能
イ　講師及び研修資料の準備をすること。研修資料は事前作成し、本学の承認を得ること。
ウ　研修の際には、実際の運用に使用できるレベルのデータを準備すること。

3.12 瑕疵担保及び著作権の取扱いについて

(1)　業務アプリケーションの稼働に必要となる各種ソフトウェア及びハードウェアの稼働については、受託者がそれらの製造者や販売者となっているかどうかを問わず、公開されていない他社製品における根本的なバグ等不具合を除き、受託者がトータルシステムとして最終的な稼働の責任を負うこと。
(2)　今回調達するシステムで採用する、あるいは、構築作業に関連して利用する、OS・ミドルウェア・フリーソフト(ソフトウェア)等について、ベンダが既に公表していた不具合等のリリースノートを確認せず、必要な対処を怠ったことによって生じた障害や不具合の責任については、受託者が負うこと。
(3)　受託者の関連会社又は協力会社が開発作業に参画する体制を採用することも可能とするが、その場合は受託者が責任をもって契約上及び実行上の品質確保要件を盛り込み、それらに従って関連会社・協力会社の監督をすること。また、それら関連会社・協力会社に対し、本章等の業務遂行にかかる要件の周知徹底を十分に図ること。
(4)　成果物として納品されるものに、第三者が権利を有する著作物を含める場合または第三者が所有する知的所有権を利用する場合は、それらの利用に必要な一切の負担や事務手続きを本学に代わって行うこと。また、受託者は事前に本学にその旨を通知したうえで、その承認を得ること。
(5)　受託者の責めに帰すべき事由により本契約に定める義務に違反して委託者に損害を与えた場合、受託者が負担する賠償責任は、原則として受託者の責めに帰すべき事由に起因して委託者に直接発生した通常かつ現実の損害に限定されるものとし、逸失利益などを含め特別な事情による損害については賠償責任を負わないものとするが、受託者の故意または重過失による損害については、別途協議とする。

4. 基幹ネットワークの要求仕様

基幹ネットワークを構成する機器及びシステムの要件を以下に示す。原則、以下に記載されている構成で実現することを想定しているが、他の構成や機器を用いた方がより効率的に導入・運用ができると受託者が考える場合や、システムの要件を満たすために、必要と考える機器や数量の増減がある場合は、必ず本学と協議したうえで構築すること。

なお、有線 LAN でのインターネット接続については、配下での大容量のデータダウンロード時を除き、各キャンパススイッチ直収端末にて下り常時 200Mbps 以上の速度で接続できることとし、それを下回る場合は原因調査のうえ、スペック向上等の必要な対策を講じること。

4.1 データセンターに関する要件

本学の運用を支える基幹システムを安定的に稼働させることを目的として、受託者が保有する、又は推奨するデータセンターと契約のうえ、そこに、原則として今回更新・導入するサーバ群及びコアネットワーク機器を配置することとする。受託者自身がそのデータセンターの保有者でない場合でも、保有していると同等のサービスが提供されるようにすること。

4.1.1 基本要件

(1) 「3.7 データセンター」の要件を満たすこと。
(2) 高密度ラックに耐えられる荷重／電力供給であること。
(3) クラウドサービスとの連携が可能であること。
(4) 一般の商用停電時でも、概ね最低5日間以上、非常用発電装置により電力供給が可能であること。
(5) 空調や粉じん対策のための空気還流などの対応ができていること。
(6) 災害（地震・津波・液状化等）の影響を生じさせない立地条件にあること。
(7) 運用に関する公的資格（ISMS、SOC 等）の認証を取得している、もしくは同等の取り組みを行っていることを公式な WEB ページ等で公表していること。
(8) 横浜市内からの通信回線利用料がリーズナブルな範囲に収まる距離にあること。
(9) 将来の拡張を考慮した IaaS とハウジングサービスの一体の運用が可能であること。

4.1.2 ファシリティ要件

(1) 高潮浸水想定区域外、かつ、土砂災害警戒区域外にあること。または、そのための対策が施されていること。
(2) 液状化の危険性がない立地に建てられていること。又は、そのための対策が施されていること。
(3) 自治体等により洪水や高潮、及び津波の危険性が指摘されている場所に建てられていないこと。又は、その対策が施されていること。
(4) 半径 100 メートル以内に、消防法における指定数量以上の危険物製造施設や高圧ガス製造施設がないこと。
(5) 管理運用の観点から、金沢八景キャンパスから公共交通機関を利用して概ね片道 120 分以内でアクセスできること。
(6) 建物は、震度7の地震に耐える耐震構造、免震構造、制震構造の何れかであり、建築基準法に規定する耐火性能を有すること。
(7) 避雷設備、火災報知設備、消火装置、非常照明設備、避難施設備、空調設備等の建築設備が設置されていること。
(8) 建物入口、エレベーターホール、入退館受付、サーバルーム及びデータ保管庫入口等には、有人によるセキュリティ監視、又は屋外・屋内の場所に応じた多数の監視カメラを設置し、24時間365日の監視を行うこと。
(9) 入退館については24時間365日有人による対応を行うこととし、許可を受けた者以外が容易に侵入できないこと。

(10) 機器設置室への入室に関しては、生体認証装置等による本人認証の管理及び記録が実施されていること。さらに、アンチパスバック機能及び共連れ防止の措置がなされていること。
(11) サーバルームにおいては、無死角の監視カメラが常時稼働していること。
(12) 入室の許可された者だけしかサーバルームへ入れないように、データセンターの入口からサーバルームまでセキュリティ対策が施されていること。
(13) サーバエリア電源容量、運用機器電源容量、施設・設備電源容量等を充分にまかなえ、かつ、電気系統の定期点検時に支障のない容量を確保できること。
(14) 受電設備の法定点検や工事等は、システム機器を停止せずに行うことができること。
(15) 100V、200Vの電力を供給可能であること。(ラック内で混在も可能)また、電源の経路については複数系統が提供できること。
(16) データセンターに設置する全ての機器をラックマウントするのに必要となる19インチフルラックサイズ(42U以上)を、必要ラック数用意すること。また、棚板も必要枚数用意すること。
(17) サーバ室の空調については冗長化されていて、24時間365日稼働し、安定的に供給できること。
(18) 空調設備については漏水対策が施されていること。
(19) 今後の回線冗長化なども考慮し、通信事業者を限定しないこと。
(20) 運用に関する以下の公的認証を取得していること。
    a. プライバシーマーク、又はそれに相当するセキュリティポリシーを社全体として明文化し、公式ページ等で公表していること。
    b. ISO/IEC27001(情報セキュリティマネジメントシステム)
    c. ISO22301(事業継続マネジメントシステム)、又はこれに相当する災害対策取り組み方針を社全体として明文化し、公式ページ等で公表していること。

4.2 キャンパス間接続回線

金沢八景キャンパス、福浦キャンパス、鶴見キャンパス、舞岡キャンパス、センター病院及びデータセンターを接続するために、ギャランティ型イーサネットサービスを調達する。なお、みなとみらいサテライトキャンパスについては金沢八景キャンパス経由でデータセンターに接続する現行構成を維持し、ベストエフォート型イーサネットサービスの既存回線を継続利用すること。

(1) 接続拠点及びアクセス回線速度は表 4-1 の通りとする。

表 4-1 キャンパス間接続回線の速度要件

拠点名	回線速度
データセンター	8Gbps 以上
金沢八景キャンパス	2Gbps 以上
福浦キャンパス	2Gbps 以上
鶴見キャンパス	1Gbps 以上
舞岡キャンパス	1Gbps 以上
センター病院	1Gbps 以上
みなとみらいサテライトキャンパス	1Gbps 以上

(2) 既存回線からの移行にかかる全ての費用は本調達に含まれるものとする。
(3) 故障手配及び修理について、24 時間 365 日オンサイト保守が対応可能である回線サービスであること。
(4) インターネットを利用できるようにするため学術情報ネットワーク(SINET)に接続する回線については、回線機器を収容するためのハウジングラックも費用に含めること。
(5) 工事が必要な場合はその費用も本調達に含まれるものとする。

4.3　基幹ネットワーク機器類

以下の機器類を基幹ネットワーク機器類として、仕様を示す。

「基幹 L3 スイッチ」「サーバスイッチ」「学外接続用 L2 スイッチ」「キャンパス L3 スイッチ」「建屋 L2 スイッチ」「建屋内フロア L2 スイッチ」「認証スイッチ」「ファイアウォール」

4.3.1 基幹ネットワーク機器類の共通要求事項

本ネットワーク機器類は、学術情報ネットワーク(SINET)に 8Gbps 以上で接続されることを前提とするが、そのための要求事項は以下のとおりである。

(1) ネットワークは大学情報システムの基盤であることから、24 時間 365 日の安定した連続運用が可能である構成とすること。
(2) SNMP 機能等の利用により、機器やネットワークの稼働状況を把握できること。なお、トラフィック量を秒/分/時間での指定間隔で収集でき、その値を日および月単位でレポート出力可能であり、利用者からの大量のトラフィック送信を検知できる設計を行うこと。
(3) 本学の学生数・教職員数及び端末台数を考慮したうえで、十分な処理性能を有すること。
(4) 現在稼働している設定情報やデータなど、情報資産の移行が可能であること。
(5) EIA 規格に準拠した 19 インチラックマウントが可能であること。
(6) 冗長構成を組む機器については、自動、手動に関わらず本稼働前に切り替えテストを実施することを前提とし、その想定通りに動作することを保証できるものであること。
(7) ループ検知機能を設定し、設置時にその動作の確認を行うこと。
(8) 各スイッチは可能な限りカスケードしない構成となるようにポート数を考慮すること。
(9) 福浦キャンパスの A 棟(臨床研究棟)、B 棟(基礎研究棟)における現行の無線ネットワークでは IP アドレスが不足していることから、セグメント範囲を見直すこと。
(10) 八景キャンパスに設置されている一部のサーバでは、DC 側セグメントの IP アドレスが必要なため同一のネットワークアドレスを利用できるよう構成をとること。
(11) 鶴見キャンパスでは、キャンパス内での無線 LAN 環境を継続運用するため運用保守の対象に含めること。
(12) 保守運用を行ううえで必要となる適切な数量の予備機を調達すること。

4.3.1.1　レイヤ 3(L3)スイッチ共通要件

(1) スイッチング容量、最大パケット転送能力は搭載されたポートすべてでワイヤーレートの通信速度が出せる性能であること。
(2) 最大 MAC アドレス登録数は 64K 以上であること。
(3) レイヤ3機能が利用できルーディング(Static、RIP、OSPF)が利用できること。
(4) DHCP リレー機能を有すること。
(5) SNMP 機能を有すること。
(6) ケーブルの誤接続によりフレームを送信したポート又は同一装置の別ポートにフレームが戻ってくるループ構成になった際、ループを検知してポートを閉塞する機能を有すること。
(7) L2 ループを検出してポートを閉塞した場合に、当該ポートを自動で開放する機能有すること。
(8) 筐体は、19 インチラック搭載タイプで 1U 程度であること。
(9) RoHS 指令対応製品であること。
(10) 時刻同期が可能であること。
(11) IEEE802.1Q タグ VLAN 機能を有すること。
(12) 外部メディア(コンパクトフラッシュ、USB メモリ、SD カード)に構成定義情報、ファームウェア、ログを保存可能であること。
(13) 電源二重化が可能であること。
(14) マニュアルやリリースノートなどの技術情報は、原則として日本語で提供できること。
(15) Virtual Routing and Forwarding 機能を持つこと。

4.3.1.2　レイヤ 2（L2）スイッチ共通要件

(1)　スイッチング容量、最大パケット転送能力は搭載されたすべてのポートでワイヤーレートでの通信ができる性能であること。
(2)　1000BASE－X の規格で対応可能である機器であること。
(3)　SNMP 機能を有すること。
(4)　ケーブルの誤接続によりフレームを送信したポート又は同一装置の別ポートにフレームが戻ってくるループ構成になったときにループを検知してポートを閉塞する機能を有すること。
(5)　L2 ループを検出してポートを閉塞した場合に、当該ポートを自動で開放する機能有すること。
(6)　GUI またはコマンドでの管理が可能であること。
(7)　筐体は、19 インチラック搭載タイプで 1U 程度であること。
(8)　既存の LAN 配線環境を利用してよいが、不足する分については必要に応じて建屋 L3スイッチから各フロアまでの配線と各フロアスイッチから各部屋までの配線を行うこと。
(9)　RoHS 指令対応製品であること。
(10) 時刻同期が可能であること
(11) IEEE802.1Q タグ VLAN 機能を有すること。
(12) マニュアルやリリースノートなどの技術情報は、原則として日本語で提供できること。

4.3.1.3　基幹 L3 スイッチ

(1)　4.1 のデータセンターに設置すること。
(2)　2 台以上の冗長構成とすること。
(3)　10Gbase-SR 3 ポートを有すること。
(4)　SNMP 機能を有すること。
(5)　キャンパス間接続の回線は、最適なものを選定すること。
(6)　Virtual Routing and Forwarding 機能を持つこと。

4.3.1.4　サーバスイッチ

サーバ類の接続用のスイッチであり、データセンター及び、金沢八景キャンパスのサーバ室に設置する。データセンターで運用するサーバ、学内で運用するサーバ等の台数を考慮して必要なポート数のスイッチを提案すること。

(1)データセンター
ア　4.1 のデータセンターに設置すること。
イ　2 台以上の冗長構成とすること。
ウ　接続するサーバ等の数量に合わせたポート数を搭載すること。
エ　サーバ類は極力 10Gbps で接続すること。

(2)金沢八景キャンパス
ア　金沢八景（サーバ室）へ設置すること。
イ　接続するサーバ等の数量に合わせたポート数を搭載すること。
ウ　サーバ類は極力 10Gbps で接続すること。

4.3.1.5　学外接続用 L2 スイッチ

SINET との接続のために、必要であれば以下の要件を満足するスイッチをデータセンター内に設置すること。

(1)　2 台以上の冗長構成とし、フェイルオーバしても性能が変わらないこと。
(2)　SINET とは 8Gbps 以上で接続すること。
(3)　SINET と本学の基幹ネットワークとの接続に必要なインタフェースを備えていること。

4.3.1.6　キャンパス L3 スイッチ

(1) 金沢八景キャンパス、福浦キャンパス、センター病院、舞岡キャンパスに設置する拠点 L3 スイッチは、下位のキャンパス内スイッチ群の収容を兼ねる。
(2) キャンパス間接続の回線は、最適なものを選定すること。
(3) 八景キャンパスに設置する機種は、10GBase-SR 2 ポート、1000base-SX 12 ポートを有すること。
(4) 福浦キャンパスに設置する機種は、10GBase-LR 2 ポート以上を有すること。
(5) 必要台数、ポート数については、別紙資料 6「基幹 NW 既存 L2-L3 スイッチ拠点別一覧」を参照のこと。
(6) Virtual Routing and Forwarding 機能を持つこと。

4.3.1.7　建屋 L3 スイッチ

(1) 金沢八景、福浦キャンパスに設置する建屋L3スイッチは、建屋内の支線 L2 等の収容を兼ねる。
(2) 建屋間光配線用 1000base-SX 1 ポート、1000Base-T 24 ポート以上を有すること。
(3) 学術情報センターについては 48 ポート以上の 1000Base-T、及び 1 ポート以上の 1000base-SX を有すること。
(4) 必要台数、ポート数については、別紙資料 6「基幹 NW_既存 L2-L3 スイッチ拠点別一覧」を参照のこと。
(5) Virtual Routing and Forwarding 機能を持つこと。

4.3.1.8　建屋内フロア L2 スイッチ

(1) 産学共同研究センターは、1000base-SX 1 ポートを有すること。
(2) 学術情報センター(E 実習室)は、1000base-SX 1 ポートを有すること。
(3) 看護実習棟は、1000base-SX 1 ポート有すること。
(4) 先端医学研究棟 16 ポートスイッチ 1 台は、1000base-SX 2 ポート有すること。無線 LAN アクセスポイントの接続を考慮し、必要に応じて POE 対応とすること。
(5) ループの発生を検知し、ポートの shutdown ができること。
(6) 実習室以外のスイッチは、GUI での管理が可能であること。
(7) 製品購入から該当製品の出荷停止後5年間は、装置本体のハードウェア故障時に、無償にて代替品と交換すること。
(8) 必要台数、ポート数については、別紙資料 6「基幹 NW_既存 L2-L3 スイッチ拠点別一覧」を参照のこと。

4.3.1.9　認証スイッチ

(1) 建屋もしくは、キャンパス内に認証スイッチを配置すること。
(2) 認証機能は、「5. 認証システム」 を参照すること。
(3) 必要台数、ポート数については、別紙資料 6「基幹 NW_既存 L2-L3 スイッチ拠点別一覧」を参照のこと。

4.3.1.10　ファイアウォール

(1) 4.1 のデータセンターに設置すること。
(2) 19 インチラックに搭載可能であること。高さは、2U 以内であること。
(3) 100V/AC 電源で稼働すること。
(4) RoHS 指令対応製品であること。
(5) SINET からの接続部分に設置し、ファイアウォール機能を提供すること。さらに、冗長性を考慮した構成とすること。

(6) 10GBASE-SR を 2 ポート以上有すること。10／100／1000BASE-T を 8 ポート以上有すること。
(7) DMZ ネットワークを構成する機能を有すること。
(8) NAT（アドレス変換）／NAPT（IP マスカレード）をサポートしていること。
(9) アプリケーションレベルの防御する機能を有すること。
(10) IPS 機能を有すること。
(11) ポリシーで選択した通信のみ IPS を適用する機能を有すること。
(12) Winny 等の P2P プロトコルに対しても対策が実現可能である機能を有すること。学内教職員・学生数に対応した性能を有すること。
(13) 同時セッション（TCP）数は 6,000,000 以上であること。
(14) ファイアウォールの総スループットは 8Gbps 以上であること。なお、セキュリティ機能を動作させたうえでの性能とする。
(15) 各種通信ログ（不正通信など）のログ情報が、Syslog サーバへ送信可能であること。
(16) インターネット通信の総スループットは 8Gbps 以上であること。なお、セキュリティ機能を動作させたうえでの性能とする。
(17) 外部ネットワークからの侵入及び不正アクセス等を防ぎ、安全にインターネットを利用する環境を提供すること。
(18) ファイアウォールのフィルタ設定は送信元/送信先とアプリケーション名を元に処理可能であること。
(19) ネットワークセキュリティ毎にウィルス・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/無効に設定が可能であること。
(20) IPv4 通信に対して、脆弱性防御、アンチウィルス、アンチスパイウェア、URL フィルタリングといったコンテンツスキャニング機能が可能であること。
(21) PDF、Excel、WORD、PPT、ZIP 等のファイルタイプによる通信の可視化やフィルタリングが可能であること。
(22) HTTP/HTTPS、SMTP、POP3、IMAP、FTP 及び CIFS で転送されるファイルが解析可能であること。
(23) メールのスパム判定が可能なこと。また、脅威のあるサイトへのブロックは、ボットネット IP レピュテーション DB でのブロック機能を持ち合わせていること。
(24) DoS 攻撃(anomaly や flooding)に対し、HW 処理の防御機能を有すること。
(25) 不正通信および脅威と判断した端末検知し、自動的に遮断する機能を有すること。また、脅威と判定した端末についてはネットワークから隔離できるような仕組みを設けること。尚、ファイアウォールと連携した別ソリューションを導入してもよい。
(26) アプリケーション毎や通信先毎に優先・帯域制御が可能であること。
(27) 検知対象は本ネットワークシステムの全てとする。
(28) 脅威と判断した端末情報をシステム管理者にメール等で知らせる機能を有すること。
(29) システム管理者によってネットワークから隔離された、端末のネットワーク通信を許可する操作が可能であること。
(30) ホットスタンバイ機能、LAN 二重化機能、ゲートウェイ・フェールセーフ機能、アラート通報機能、ログ収納用ハードディスク機能を有すること。
(31) リアルタイム及び過去のネットワークアクティビティのレポート表示できる機能を有すること。
(32) 日本語 WebUI と CLI の両方での設定が可能で、CLI は telnet と SSH をサポートしていること。
(33) 保守専用に LAN ポートを有すること。
(34) SNMP 機能を有すること。
(35) Virtual Domain(VDOM)機能をサポートし、各 VDOM で独立したルーティングテーブルを持つことができること。
(36) インターネットサービスの IP アドレスデータベースを有し、Amazon、 Salesforce、Microsoft Azure、Microsoft Office 365、Box、Google Cloud を宛先に選択し、ルーティングできること。また、インターネットサービスの IP アドレスデータベースを管理者が更新することなく動的に更新される運用が可能なこと。
(37) インスペクションモードとして、トラフィックをバッファリングしコンテンツを再構築

してからセキュリティ上の脅威がないか検査する方式(プロキシベース)およびバッファリングされずパケットごとにペイロードを検査する方式(フローベース)の双方を有すること。

4.3.1.11 ファイアウォール用ログサーバ

(1) ソフト、OS、ハードが一体型のアプライアンス製品であること。
(2) 10/100/1000Base-T のインタフェースを 4 ポート以上有すること。
(3) ハードディスクは 12TB 以上搭載すること。
(4) RAID 構成(RAID0/1/5/10)が対応可能であること。
(5) 1 日のログ処理数が 200GB 以上であること。
(6) 最大 1 秒あたり 4000 ログレコード受信可能であること。
(7) 最大 200 デバイスのログ管理が可能なこと。
(8) ラックマウントに搭載可能でサイズは 1U 以内であること。
(9) 本調達のファイアウォール装置からのログを受信可能なこと。
(10) ログ通信は暗号化に対応可能であること。
(11) 本調達のファイアウォール装置からのログ受信は、リアルタイム送信とスケジュールによるバッチ送信に対応可能であること。
(12) レポート機能を有しユーザカスタマイズが可能なこと。
(13) 受信したログの内容情報から、アラート設定のカスタマイズが可能なこと。
(14) WebUI、CLI から設定管理が可能なこと。
(15) WebUI は日本語に対応可能なこと。
(16) SNMPv1,v2c に対応していること。
(17) SSH によるリモートアクセス管理に対応可能なこと

4.3.1.12 無線 LAN に関する要求事項

無線 AP は現行機種を利用継続するため、保守のライセンスを手配すること。なお、AP 設置台数や設置場所については別紙資料 7 「無線 AP 設置場所一覧」 を参照すること。

(1) 本システムは、Windows／Mac 端末、スマートフォン（iOS、Android）に対応していること。
(2) 無線 LAN コントローラは 4.1 のデータセンターに冗長化して設置すること。AP と連携して認証を行うこと。
(3) 学外のゲストユーザに対しては、インターネット接続のみが可能な環境を提供し、認証された学内ユーザ(学生、教職員)には学内ネットワークへの接続を提供する機能を有すること。
(4) IEEE802.11a/ac/ax/b/g/n をサポートしていること。また、それらを同時利用可能であること。
(5) IEEE802.11n/a/ac/ax と IEEE802.11n/g/b/ax の同時接続が可能であること。
(6) Web、SSH による AP 管理が可能であること。また、AP の集中管理が可能であること。
(7) 無線コントローラは 4.1 のデータセンターへ設置すること。また、コントローラは冗長構成とすること。
(8) 無線コントローラの設置に伴い、必要な機器及び什器等を用意すること。
(9) 無線 AP の給電は、PoE スイッチ、又は PoE 給電アダプタで実現すること。
(10) AP ごとの利用率の統計が容易に取得できること。
(11) 認証システムと連携して、APごとに、接続ユーザ、接続時刻のログを取得できること。
(12) 採取した各端末の利用時間情報(ログオン～ログオフ)を集計し、レポートが提示できること。レポート形式は本学と協議のうえ決定すること。
(13) 国立情報学研究所(NII)が提供している eduroam JP サービスが利用できるよう設定すること。
(14) 本学ユーザだけでなく、eduroam を経由して学内ネットワークにログインを許容する学外利用者について、アクセスしたユーザ名やログイン／ログアウト時刻、経由したノード等、本学と別途協議のうえで、必要なログを収集できるようにしておくこと。
(15) 次期システムではセグメント範囲を見直し、建屋内のフロア単位で分割すること。

(16) 将来ネットワークトラフィックが増えることにより帯域不足が発生しないように、無線コントローラに必要な性能を搭載すること。

4.3.1.13 リモートアクセス(VPN 接続)

学内専用のシステムについて、本学のアカウント所有者が学外からアクセスできるようにするサービスである。

(1) 学外からのリモートアクセスで学内のシステムが利用できること。
(2) 本学基幹ネットワークシステムの認証を用いて認証ができること。
(3) リモートアクセス方式は、VPN クライアントソフトを用いて SSL-VPN で接続すること。
(4) リモートアクセス端末として、Windows／Mac 端末に対応できること。また、タブレットなど、iOS や Android 端末からの利用も可能とすること。
(5) リモートアクセス端末は、認証サーバにて認証を受けたうえで、学内システム(電子ジャーナル、YCU ネット、UNIX 演習サーバ等)を利用可能とすること。
(6) リモートアクセスにより接続できるシステムを制限でき、学生と教職員それぞれで使用可能である学内システムを定義できること。
(7) 対応 OS については Windows11、MacOS については MacOS 12 以上とする。
(8) ネットワーク接続の際には、Micrsoft EntraID との SAML 認証によるシングルサインオンで認証すること。
(9) ゲストユーザ(学外ユーザ)のログインを禁止し、学内ユーザ(学生、教職員)のみにログインを許可させること。
(10) SSL-VPN スループットは 5Gbps 以上であること。
(11) リモートアクセス用機器は、データセンターのファイアウォールと兼用も可能とする。

4.3.2 基幹サーバ群

本サーバ群は、主にインターネット接続に必要な基本的なサービスを提供するサーバである。本システムの要求事項は、以下のとおりである。

(1) 各キャンパスからの各種サーバ増設要求などに柔軟に対応可能であるシステムであること。
(2) 情報漏洩などのアクシデント／インシデント発生のリスクを軽減可能であるシステムであること。
(3) ソフトウェアなどの資産管理及びライセンス管理を実現可能であるシステムであること。
(4) 個々のサーバの稼働状況等が容易に確認でき、リモートからの操作が可能であること。
(5) 現在稼働している設定情報やデータなどの情報資産の移行が可能であること。
(6) EIA 規格に準拠した 19 インチラックマウント可能であること。

仮想化基盤サーバ仮想サーバ群を稼働させるために、4.1 のデータセンターに仮想化基盤用物理サーバを設置する。仮想化基盤サーバは、それぞれ以下の要件を満たすこと。

(1) CPU はインテル Xeon プロセッサー相当以上 を 2 つ以上搭載すること。
(2) メモリは 96GB 以上を搭載すること
(3) ハードディスクは 10,000rpm 以上の SAS ディスクで構成し、RAID1 構成で論理容量 200GB 以上を提供すること。
(4) 通信用ネットワークインタフェースとして、10GBASE 2 つ以上を有すること。
(5) 保守用ネットワークインタフェースとして、1000BASE 1 つ以上を有すること。
(6) 電源は二重化され、ホットプラグに対応していること。
(7) 仮想化基盤ハイパーバイザーサーバとして、基盤ストレージ上にあるサーバ OS イメージを稼働させること。各仮想 OS のリソース配分は、各サブシステムの要件を参照すること。
(8) 仮想化基盤は HA 構成をとること。対象は、基幹サーバ、ネットワークサーバ、教室系サーバ群を対象とする。
(9) 全ての筐体に対して仮想マシンの移動が可能であるよう、OS 等のライセンスを手配すること。
(10) ファイルサーバと統合する場合は、適切な構成をとること。

4.3.2.1　基幹サーバ共通要求事項

(1) 4.1 のデータセンターへ設置すること。
(2) 全ての筐体(ノード)から以下の各項で指定する LAN(サブネットワーク)に 1000BASE 又は 10GBASE の性能で接続すること。
(3) 各システムの統計情報は、一括管理し、CSV 形式で出力できること。
(4) 統計情報(ディスク使用量、ジョブの統計情報等)を Web ブラウザ上の GUI にて表示できること。
(5) HDD はハードウェアコントローラによる RAID1などの冗長構成であること。また、HDD はホットスワップ対応であり、オンラインでのディスク増設が可能であること。
(6) データのバックアップ／リカバリ機能を有すること。
(7) ウィルス対策ソフトが実装可能であること。本学で提供するトレンドマイクロ ApexOne を利用してもよい。

4.3.2.2　ユーザ管理サーバ

基幹ネットワークシステムを構成する全てのシステムに対し、ユーザアカウント管理機能・認証機能を提供する。また、人事部門、学務部門から提供される教職員や学生等ユーザ情報の取り込み、調達範囲外のシステムを含むサブシステムへのプロビジョニング、PW 更新、ユーザ情報の変更や削除管理を行うため、データセンターに認証システムを設置する。

要求事項	要求仕様
数量	１式
ハードウェア	(1) 仮想化基盤サーバ上に構築し、CPU 2Core 以上、メモリ16GB 以上、HDD 100GB 以上を割当てること。なお、ユーザ管理システムの各機能が遅延なく利用できるようなリソースを追加すること。 (2) ユーザ管理システムが動作する OS を選定すること。
ソフトウェア及び制約条件	「7.ユーザ管理システム」に記載している要件を満たすこと。

4.3.2.3　DHCP

(1) 4.1 のデータセンター内に、DHCP サービスを展開すること。実現機器及び実現方法 は任意であり、必要に応じ本調達に含めること。
(2) 本学では、クラス B のグローバルアドレスとプライベートアドレスを使用し、約 150 個のサブネットを構成しているが、今後 200 個程度まで増加することを見込んで対応できること。
(3) 2 台以上の冗長構成とすること。
(4) システム全体で 10,000 台接続できること。
(5) 静的／動的払い出しができること。
(6) DHCP オプションに対応していること。
(7) IP アドレス、MAC アドレスが GUI で一元表示可能なこと。

4.3.2.4　ファイルサーバ

情報実習室システム、事務システムの共有ストレージとする。なお、本サーバは NAS または SAN によるネットワークストレージを利用するものとする。実習室用と事務用とは論理的に分けて運用する。

情報実習室システムの UNIX 演習 サーバ、実習室等のユーザ端末における Windows 環境および、実行形式のファイルやコマンドスクリプトの共有収容領域として利用する。想定する同時利用者数は UNIX 演習 サーバから 100 ユーザ、Windows 環境におけるファイル共有 500 ユーザとする。なお、本サーバは NAS または SAN によるネットワークストレージを利用するもの

とする。

要求事項	要求仕様
数量	1 式
ハードウェア	(1) 10,000rpm 以上のSAS ディスクRAID構成と、必要なホットスペアディスクを提供すること。 (2) 通信用ネットワークインタフェースとして、10GBASE 2つ以上を有すること (3) 保守用ネットワークインタフェースとして、1000BASE 1つ以上を有すること。 (4) サーバダウンやフェイルオーバ等の特定イベント発生時に、通報が可能であること。
ソフトウェア及び制約条件	(1) 以下の用途ごとに、それぞれ指定した容量以上を指定したプロトコルで提供すること。 ・センター病院用：14TB,CIFS ・附属病院用：15TB,CIFS ・事務用：16TB,CIFS ・教育実習室用：10TB,NFS ・Proself用：1TB,NFS (2) Active-Directory と連動し、実習室用は利用者にホーム環境を提供すること。 (3) 現行のファイルサーバの内容を移行すること。 (4) ユーザ管理システムと連動して、ユーザの追加/削除に応じて、ホームの追加/削除及びクォータ設定が自動的に行われること。
その他	システム全般に関わる基本要求に準拠すること。

4.3.3 ネットワークサーバ群

4.3.3.1 共通要求事項

(1) 4.1 のデータセンターへ設置すること。
(2) 全ての筐体（ノード）から以下の各項で指定する LAN（サブネットワーク）に 1000BASE 又は 10GBASE の性能で接続すること。
(3) 主要機能は冗長化などにより、障害時のダウンタイムが極力少なくなる構成とすること。
(4) 複数機能を1機器で構成することで、操作性が統一できるなど、管理が容易な構成とすること。また、CUI だけではなく、Web 等の GUI でも操作可能とすること。
(5) 外部 DNS サーバはアプライアンスによる専用機で構成し、それ以外は汎用 OS による構成で可とする。
(6) サーバの稼働状況等が容易に確認でき、リモートからの操作が可能であること。
(7) 学内とインターネットを接続するうえで必要な機能としては、次項に記載するとおりと考えているが、他に必要不可欠な機器が漏れている場合は、導入前に本学と協議し、その合意に基づいて追加すること。

4.3.3.2 外部 DNS サーバ

要求事項	要求仕様
数量	2式 プライマリサーバ及びセカンダリサーバ機能を提供すること。
ハードウェア	(1) 筐体は 19 インチラックマウント型で、高さ 1RU 以内であること。
ソフトウェア及び制約条件	(1) DNS サーバ、を有すること。 (2) DNS ゾーン情報転送の暗号化を実現すること。 (3) 本学全ドメインの公開ホスト情報に対する回答を行い(コンテンツDNS)、SINET DNS セカンダリにこの情報を転送し(プライマリDNS)、学内全ネットワークからの本学以外のDNS情報の問合せをインターネットに対して実施

	する(キャッシュDNS)よう構築すること。 (4) JPNIC のレジストラ内容を変更しない事を制約として、DNS サーバの移行を実施すること。 (5) セキュリティホールが発見された場合、迅速に対応可能であること。
その他	システム全般に関わる基本要求に準拠すること。

4.3.3.3 内部 DNS、NTP サーバ

要求事項	要求仕様
数量	2式 プライマリサーバ及びセカンダリサーバ機能を提供すること。
ハードウェア	(1) 仮想基盤上に構築するか、もしくは筐体は19 インチラックマウント型で高さ1RU 以内であること。
ソフトウェア及び制約条件	(1) 学内及び学外公開ホスト情報に対する回答を行い(コンテンツDNS)、学内サブドメインDNS にこの情報を転送し(プライマリDNS)、学内からの本学以外のDNS 情報の問合せを外部DNS にフォワードする(キャッシュDNS)よう構築すること。 (2) 学内DNS クライアントの設定内容を変更しないことを条件として、DNS サーバの移行を実施すること。なお八景キャンパスの機器と福浦キャンパスの機器は異なるIPアドレスを参照している。 (3) NTPサーバ機能を備え、導入する全てのサーバ・パソコンについては本サーバと時刻同期を行うこと。
その他	システム全般に関わる基本要求に準拠すること。

4.3.3.4 外部公開 web サーバ

要求事項	要求仕様
数量	1式
ハードウェア	(1) 仮想基盤上に構築し、CPU 2Core 以上、メモリ4GB 以上、HDD 1200GB以上を割当てること。 (2) Web サーバを運用するうえで、必要なサーバリソース(メモリ、ディスク容量等)の追加は柔軟に対応可能であること。 (3) 提供されるWeb サーバは可用性を考慮し、冗長化されたものを用意すること。 (4) サーバOSは、Redhat Enterprise Linux v9相当以上を導入すること。
ソフトウェア及び制約条件	(1) Web サーバはApache2.2 又は2.4 相当以上とすること。 (2) 既存システムのWeb サーバのコンテンツ、URL 等の設定を、Web サイトにアクセスするユーザの閲覧性が変わらない条件で移行すること。新サーバへの更新切替時に、閲覧性が途切れないように対応すること。 (3) 各サイト担当者からWeb サーバへのアクセスはSFTP 接続を利用し、本学が指定するIP アドレスからのみ接続可能とする。 (4) サーバへのアクセスは、HTTPS でも行えるよう大学が発行するUPKIのSSL 証明書をサーバへインストールすること。 (5) HTTP 接続及びHTTPS 接続はいずれのネットワーク環境からも接続可能とすること。 (6) 容易にWeb サイトが更新できるCMS ツールの利用を新たに可能とすること。CMS ツールは、WordPress(Version 6.6 以上)に対応していること。 (7) WordPress の運用にかかるMySQL 等のアプリケーションをサーバにインストールし、利用可能である状態で提供すること。ライセンス費用として追加費用が生じないように考慮すること。 (8) WordPressは、各サイトの担当者が運用するWeb サイトにおいて、個別に利用できるようにすること。 (9) 各サイト担当者のWordPress管理画面へのアクセスはHTTPSを利用することとする。 (10) OS や導入アプリケーションのバージョンアップ作業は導入業者の責任におい

	て実施すること。作業実施の際は、本学と日時等調整を行い、了承を得たうえで実施すること。 (11) CGI の利用が可能であること。(Perl、PHP、Ruby) (12) カウンタ、フォームなど簡単なCGI プログラムが用意されること。それらはユーザにあわせてカスタマイズできること。 (13) CGI の実行に際してセキュリティが確保できること。 (14) ID とパスワード、IP アドレス・リモートホストによる制限などを利用するため、.htaccess の利用が可能であること。 (15) アクセスログ解析ツールが利用可能であること。 (16) セキュリティホールが発見された場合、迅速に対応可能であること。 (17) サーバのリソース使用量が設定した閾値を越えた場合は、ただちに本学のステム管理者へ連絡すること。 (18) web アクセス方法に変更がないことを制約として、web サーバの移行を実施すること。
その他	システム全般に関わる基本要求に準拠すること。

4.3.3.5 Web アプリケーションファイアウォール(WAF)

要求事項	要求仕様
数量	1 式
ハードウェア	(1) 仮想基盤上に構築し、CPU 2Core 以上、メモリ4GB 以上、HDD200GB 以上を割当てること。または、外部公開Webサーバと同一機器に導入する形としてもよい。 (2) Redhat Enterprise Linux v9 相当以上を導入すること。
ソフトウェア及び制約条件	(1) Webアプリケーションに渡されるデータをチェックし、攻撃とみなしたアクセスをブロックすること。 (2) 攻撃を検知するための最新の脆弱性対策パッケージ(ブラックリスト)を提供すること。PCI DSS要件6.5、6.6に準拠した機能を提供すること (3) 防御対象のWebサイトFQDN数は、2とする
その他	システム全般に関わる基本要求に準拠すること。

4.3.3.6 メール中継システム

要求事項	要求仕様
数量	1式
ハードウェア	(1) 仮想基盤上に構築し、CPU 2Core 以上、メモリ4GB 以上、HDD100GB 以上を割当てること。 (2) Redhat Enterprise Linux v9 相当以上を導入すること。
ソフトウェア及び制約条件	サブドメインへのメール配送や機器のアラートメール送信用に、内部メール配送サーバを4.1のデータセンターに設置する。内部メール配送サーバは以下の要件を満たすこと。 (1) サブドメインメールのSMTP 設定を変更させない事を制約条件として、内部DNS サーバのOS 上に構築すること。 (2) Internet とのメール中継配送を行うこと。 (3) 外部レンタルサーバやSaaS等からのメール配送も可能とすること。
その他	システム全般に関わる基本要求に準拠すること。

4.3.3.7 ネットワーク監視

要求事項	要求仕様
数量	1式
ハードウェア	(1) 仮想基盤上に構築し、CPU 2Core 以上、メモリ4GB 以上、HDD200GB 以上を割当てること。

	(2) Windows 2025 Server相当以上を導入すること。
ソフトウェア及び制約条件	(1) 学内に設置したスイッチングハブや、サーバ等各種機器の稼動状況を監視できること。 (2) 導入対象のサーバ機器に関して、ネットワーク負荷、CPU 使用率、メモリ使用率、HDD 使用率の状態を取得し、時系列のグラフ表示させること。 (3) 導入対象のネットワーク機器に関して、ネットワーク負荷の状態を取得し、時系列でグラフ表示できること。 (4) 導入対象のサーバ機器に関して、ICMP による死活監視を行うこと。停止を検知した際はメールによる通報を行うこと。 (5) 導入対象のサーバ機器に関して、CPU、メモリ、HDD について閾値監視を行うこと。閾値を超えた場合はメールによる通報を行うこと。 (6) 導入対象のネットワーク機器に関して、ICMP による死活監視を行うこと。停止を検知した際はメールによる通報を行うこと。 (7) 設定や監視が GUI で一括して行うことができること。 (8) イベントの種類や重要度を視覚的に判断しやすくすること。 (9) 不正なオペレーションの抑止のため、ツール自身の設定変更等の操作ログを取得できること。 (10) VLAN 情報を視覚化する等により、構成管理情報を容易に把握できる機能を有すること。 (11) 監視対象は SNMP の他に SMTP、HTTP、 DNS 等のサービス稼動状況も監視可能であること。 (12) データのバックアップ/リカバリ機能を有すること。
その他	システム全般に関わる基本要求に準拠すること。

4.3.3.8 ログ管理

要求事項	要求仕様
数量	1式 導入対象の各機器に関して、syslog にてログを収集すること。
ハードウェア	(1) 仮想基盤上に構築し、CPU 2Core 以上、メモリ 4GB 以上を割当てること。 (2) Redhat Enterprise Linux v9 相当以上を導入すること。 (3) 収集したログを 1 年分保持することが可能なディスク容量を備えること。
ソフトウェア及び制約条件	(1) 導入対象の Linux サーバのログを Syslog で受取り、ノード毎にファイルやフォルダを分けて保存すること。 (2) 導入対象のネットワーク機器のログを Syslog で受取り、ノード毎にファイルやフォルダを分けて保存すること。
その他	システム全般に関わる基本要求に準拠すること。

4.3.3.9 バックアップ

要求事項	要求仕様
数量	1式
ハードウェア	(1) 仮想基盤または物理サーバ上に構築し、CPU 4Core 以上、メモリ 16GB 以上を割当てること。 (2) Windows 2025 Server 相当以上を導入すること。
ソフトウェア及び制約条件	(1) 以下のバックアップスケジュール設定ができること。 ア 即時実行、繰り返し実行 イ 指定日時に1回のみ実行 ウ 指定時刻／時間帯に繰り返し実行 エ 毎日／毎週／毎月 指定 オ 曜日指定、第 n 週目指定 カ 一定間隔(時間、日、週、月) キ 失敗時の再試行設定(間隔／回数) ク スケジュールの一時停止／再開

	(2) フル(完全)バックアップ、差分又は増分又は累積バックアップのいずれかが取得できること。
その他	システム全般に関わる基本要求に準拠すること。

4.3.4 教室系サーバ群

4.3.4.1 共通要求事項

(1) 4.1 のデータセンターへ設置すること。
(2) 全ての筐体(ノード)から以下の各項で指定する LAN(サブネットワーク)に 1000BASE 又は 10GBASE の性能で接続すること。
(3) 統計情報(ディスク使用量、ジョブの統計情報等)を Web ブラウザ上の GUI にて表示できること。
(4) データのバックアップ／リカバリ機能を有すること。
(5) 個々のサーバの稼働状況等が容易に確認でき、リモートからの操作が可能であること。
(6) ウィルス対策ソフトが実装可能であること。本学で提供する、トレンドマイクロ ApexOne を利用してもよい。

4.3.4.2 ActiveDirectory (AD) サーバ

要求事項	要求仕様
数量	3式
ハードウェア	(1) 仮想基盤上に構築し、CPU 2Core 以上、メモリ4GB 以上、HDD100GB 以上を割当てること。ただし一部を物理サーバとして構築してもよい。 (2) Windows 2025 Server 相当以上を導入すること。
ソフトウェア及び制約条件	(1) ログイン認証が一斉に要求された場合、自動的に負荷分散を行う機能を有すること。 (2) 各実習室端末のユーザアカウントを本サーバで一元管理し、ログイン認証を行う機能を有すること。 (3) ユーザのアカウント、パスワードが本システムとWindows システム間において、同期できること。 (4) サーバからの指示で実習室内のパソコン端末の一括電源投入、シャットダウン機能を有すること。 (5) 現行のActive-Directory 環境を移行すること。 (6) 認証システムと連動して、ユーザの追加/削除、パスワードや各属性の変更が反映されること。 (7) 既設システムでは、一部機器の認証用にADと別途存在するLDAPサーバを使用していたが、次期システムでは廃止とし、ADサーバで認証を行う仕様に変更する。LDAPサーバで認証していた機器側の設定変更は本学で行う。変更にあたり必要な情報の提供を行うこと。
その他	システム全般に関わる基本要求に準拠すること。

4.3.4.3 UNIX 演習サーバ

要求事項	要求仕様
数量	1 式 UNIX 環境での演習を行うために、金沢八景キャンパスにUNIX 演習サーバを設置する。
ハードウェア	(1) 仮想基盤上に構築し、CPU 2Core 以上、メモリ4GB 以上、HDD 100GB以上を割当てること。 (2) Red Hat Enterprise Linux v9 相当以上を搭載すること。
ソフトウェア及び制約条件	(1) 別紙資料9「導入アプリケーションソフト一覧」に示す現状のソフトウェアに対応し、最新版を適用すること。 (2) X11R6 以上のマルチウインドウシステムを有すること。

	(3) 両キャンパスのホーム領域にNFS 接続し、ログインしたユーザに提供すること。 (4) 利用者のWeb 公開用に、バーチャルホスト対応したWeb サーバを稼働させること。
その他	システム全般に関わる基本要求に準拠すること。

4.3.4.4 並列計算機サーバ

要求事項	要求仕様
数量	1式 講義や卒業研究に用いるデータ分析用サーバを設置する。
ハードウェア	(1) 仮想基盤上に構築し、CPU 48Core 以上、メモリ64GB 以上、HDD 300GB 以上を割当てること。 (2) Red Hat Enterprise Linux 9相当を導入すること
ソフトウェア及び制約条件	(1) Active-Directoryと連動し、利用者にホーム環境を提供すること。 (2) アカウント管理システムと連動して、ユーザの追加／削除に応じて、ホームの追加／削除が自動的に行われること。 (3) 各ユーザのホームは、本サーバ上ではなく、マウントしたファイルサーバ上に作成すること。 (4) WEBサーバ機能(Apache2.2又は2.4相当以上)を実装すること。 (5) Jupyter Notebookをインストールすること。 (6) Python 3.13.2以上をインストールすること。 (7) R 4.4.3以上をインストールすること。 (8) サーバへのアクセスは、HTTPSでも行えるよう大学で発行するUPKIのSSL証明書をサーバへインストールすること。 (9) サーバへのアクセスは、学内いずれのネットワーク環境からも接続可能とすること。(教研LANと事務LANの双方) (10) VPN接続を利用したときのみ、学外ネットワーク環境からでも接続可能とすること。 (11) sqlite3をインストールすること。 (12) postgesqlをインストールすること。 (13) php8、php-cli、php-gd、php-xml、php-pgsql、php-mbstring、php-zipをインストールすること。
その他	システム全般に関わる基本要求に準拠すること。

4.3.5 移行サーバ

4.3.5.1 IdP サーバ基本要件

GakuninRDM および学認 LMS と連携するための Shibboleth サーバを vSphere 上の仮想マシンとして運用している。これらのサーバを仮想化基盤サーバ上に移行および運用支援を行うこと。現用中の仮想マシンは、RHEL9、4vCPU、8GB メモリ、100GBDisk で構成されている。移行先のインフラ上で RHEL を稼働させるためのライセンスの手配を含むこと。

4.3.5.2 学認 RDM 基本要件

GakuninRDM のクラウドストレージ(Wasabi100TB)および長期保管用に、アーカイブストレージ(TS-1232PXU-RP-4G-EX144T)及びアーカイブ管理サーバ(PowerEdge R360)を運用している。
これらのサービスを継続利用できるよう、調達するデータセンターのラック内へ機器を搭載し運用支援を行うこと。

5. 認証システム

ネットワークセキュリティ対策の一つとして、事前に登録されていない端末については、学外へは接続ができないよう制御する仕組みを導入する。ただし、本学が指定する業務システムや研究教育システムなどについては本機能の適用を除外することとし、詳細は別途、本学と協議すること。

5.1 認証システムに関する要求事項

(1) 本学内に接続されている有線・無線端末(Windows、Mac、Android、iPhone 等)の MAC アドレスでの認証を行う。
(2) 認証については本学基幹ネットワークシステムの認証を用いて認証ができること。
(3) クライアント OS 種別としては、Windows11、MacOS12 以上、Linux(CentOS、Ubuntsu)、Andoroid、iPad 等の iOS に対応すること。
(4) 認証を行うネットワークとしては、金沢八景キャンパス、福浦キャンパス、舞岡キャンパス、鶴見キャンパス(無線 LAN 環境のみ)、センター病院、附属病院、みなとみらいキャンパス、事務ネットワークとする。
(5) 端末の接続の際、初回は端末登録を必須とし、次回以降は自動的にネットワーク接続できること。
(6) システム管理者が、接続された端末のユーザ ID、IP アドレス、MACアドレスを把握できること。
(7) 認証システムに障害が発生した場合、3時間以内に仮復旧ができる対処を可能とする仕組みを提供すること。
(8) 認証の仕組みを利用するにあたって、ライセンスが必要な場合は、必要なライセンス数を用意すること。

5.2 端末登録システム

(1) 本システムは、有線・無線端末(Windows、 Mac、Android、iPhone 等)に対応していること。
(2) 初めて本学のネットワークに接続する端末は、端末情報登録画面で、本学基幹ネットワークシステムの認証システムと連携し、ID とパスワードを入力することにより、PC の MAC アドレスを自動で取得できること。登録前の端末が端末情報登録画面以外にアクセスした場合は、端末登録が必要なことが判り、端末情報登録画面へ誘導できること。その際のプロトコルは http、https のいずれも利用可能であり、無線 LAN 端末の場合は、認証成功後に SSID の切断及び再接続を行うことで、通信が可能となること。
(3) 本学内のクラス B のグローバルアドレスネットワーク、事務ネットワーク等のプライベートアドレスネットワークの何れの場所からのアクセスにおいても、本機能が利用可能なこと。
(4) 認証の条件として MAC アドレスが登録されているものとすること。また、登録された ID や MAC アドレスの情報を出力できること。
(5) 認証済端末についても 1 年に 1 度以上はユーザ ID による認証をさせるために、任意の対象レコードを一括で削除・登録できること(例:セグメント単位での削除等)
(6) 収集した MAC アドレスは、ネットワーク認証を実施するシステムに1分以内に引き渡し、MAC アドレス登録済み端末として、認証完了後にネットワーク利用を可能にすること。また、MAC アドレスを引き渡す際には、重複を排除する機能を有すること。
(7) 認証スイッチ台数が多いため、管理業務を円滑に行う為に除外情報の登録/削除等の管理は本システムで一元管理すること。
(8) 認証除外登録は、現行システムの登録情報を引き継ぐこと。

5.3 認証システム

(1) 端末登録システムにより、登録された端末は学外サイトへ接続する際および建屋内フロアL2 スイッチを跨ぐ接続をする際は、必ず認証を実施するネットワーク構成にすること。その実現方法については、手段は問わないが、運用保守を行っていくうえで簡便な方法で提供すること。なお、実現する手段として認証スイッチ等を導入する場合は、以下の仕様を満たすこと。
(2) 初回接続時は、端末情報登録画面で、ユーザが ID とパスワード入力することで Mac アドレス登録が完了すること。2 回目以降の接続は認証無しで接続できること。
(3) 1台の認証スイッチで 1,000 台の端末が同時に認証接続できること。また、システム全体で 15,000 台接

続できること。
(4) MAC 認証成功後，当該端末の通信が一定時間確認されない場合に MAC 認証成功状態を強制的に解除する機能を有すること。
(5) 認証に関係するログ情報を、認証の成功または失敗に係らず Syslog サーバへ送信する機能を有すること。
(6) マニュアルやリリースノートなどの技術情報は、原則として日本語で提供すること。
(7) 認証の実施にあたっては、クライアント端末への特別なソフトウェアのインストールが不要なこと。
(8) 端末登録システムより、登録された MAC アドレスが存在確認できていない場合は通信不可とする。
(9) 認証不可と判定された場合に、本学が特別許可する端末は除外設定を設けることができる機能を有すること。
(10) MAC アドレス登録後の 2 回目以降の接続時において、認証にかかる時間は 10 秒以内であること。
(11) 計画停電時には、全ての端末が認証せずにネットワーク接続できるように簡単に設定できること。
(12) 認証システムは、筐体を提供し、Active/Standby で冗長稼働させること。1 台のサーバの障害時にユーザが意識することなくもう 1 台に切り替わり動作可能なこと。
(13) クライアント OS の 種別としては、Windows11、MacOS 12 以上、Linux(CentOS、Ubuntsu)、Andoroid、iPad 等の iOS に対応すること。
(14) ログ情報として、結果だけではなく、ユーザ名、IP アドレス、MAC アドレスの紐づけができること。
(15) 上記ログに対応した端末情報(ユーザ名、IP アドレス、MAC アドレス)も表示可能なこと。
(16) ログ情報は、Syslog サーバへ送信可能なこと。
(17) 採取した各端末の MAC/ユーザ ID の情報を集計しレポート提示すること。レポートの内容については本学と協議のうえ決定すること。
(18) 次期システムでは現行の仕組みを見直し、端末の MAC アドレスを登録後、学生の端末は教研ネットワークのみ、教員と職員の端末は教研ネットワークと事務ネットワークの両方に接続可能とする仕組みを設けること。

5.4 資産管理

本学内に接続されている有線・無線端末の情報を一元的に管理する。
「9 事務ネットワーク」に接続する事務端末については、ソフトウェアのインベントリを行う管理エージェントを導入し、それが稼働しているもののみネットワーク接続を許可する運用とする。

5.4.1 資産管理に関する要求事項

(1) 大学内の機器に対して、ユーザ名、IP アドレス、MAC アドレス、OS 情報が収集できること。ただし、OS 情報については Mac アドレス情報の登録時に、本人による入力でもよい。
(2) クライアント OS の種別としては、Windows11、MacOS12 以上に対応すること。
(3) 資産管理のためのサーバはアプライアンス製品を導入するか、仮想基盤上に構築すること。
(4) アンチウイルスソフトが必要な場合は、本学がライセンス保有しているトレンドマイクロ ApexOne を使用してもよい。
(5) 本学の学内LANに接続されている PC の台数等が把握できること。
(6) ログによりPCの台数を学生と教職員とに分けて集計し、OSの種類ごとの台数が集計可能なこと。
(7) 資産管理サーバはデータも含めて一元的に管理できること。
(8) 収集した資産情報データを CSV により入出力できる機能を有すること。

5.4.2 ソフトウェアインベントリ（事務端末）

(1) 事務端末は、アプリケーションを資産として管理できること。（福浦キャンパス、舞岡キャンパス、鶴見キャンパス、附属病院、センター病院の事務端末も含む）
(2) クライアント OS の種別としては、Windows11、MacOS12 以上に対応すること。
(3) 事務端末がネットワークに接続する際、エージェントがインストールされていない場合は、管理者へ通

知する機能を有すること。ウイルス対策ソフトがインストールされていない端末は事務ネットワークには接続させないこと。

(4) 管理のためのサーバが必要な場合は、アプライアンス製品を導入するか、仮想基盤上に構築すること。

(5) アンチウイルスソフトが必要な場合は、本学がライセンス保有しているトレンドマイクロ ApexOne を導入してもよい。

(6) 取得したソフトウェア情報を GUI 操作で CSV 出力できること。

6. 教育実習室システム

本システムは、学生の教育又は実習に供されるシステムであり、PC 群と PC を維持・管理するための管理システム、認証のための ActiveDirectory、オンデマンドプリント管理システム、ファイルサーバ、UNIX 演習システムを含む。教育実習用システムの要求事項を下記に示す。

6.1 管理システム等の要求事項

(1) 利用者の利便性を考慮し、サーバ上に OS イメージを格納してクライアントに配信するシステムであり、多台数のクライアント環境を構築できること。
(2) クライアント配信システム用サーバは、以下要件を満たす構成（サイジング）にて、金沢八景キャンパスに設置すること。ただし、性能を担保するため各キャンパスに設置することも可とする。またその際どのサーバも冗長構成とすること。
(3) 各キャンパスからの各種端末増設要求などに迅速に対応可能なシステムであること。
(4) 情報漏洩などのインシデント発生のリスクを軽減可能なシステムであること。
(5) 端末の維持管理コスト及びオペレーションコストを軽減可能なシステムであること。
(6) クライアント端末の OS は Windows11 を想定しているが、チャネルについては構築段階で決定する。そのため General Availability Channel と Long Term Servicing Channel の両方での導入が可能であり、サポートも可能なシステムであること。
(7) イメージ配信やクライアント起動時のトラフィックがネットワークに不必要な負荷を与えないよう、柔軟に帯域制限できるシステムであること。
(8) ソフトウェアなどの資産管理及びライセンス管理を適正に実現可能となるよう考慮すること。
(9) 実習室端末は、同一環境の保持や更新の容易さなど運用面を考慮すること。
(10) システムの管理画面は、Web ブラウザからアクセス可能であること。
(11) システムの管理画面は、日本語表示に対応していること。
(12) CBT などを考慮し、特定のタイミングやユーザが指定した時間に、起動する OS イメージや世代を切り替えられること。
(13) クライアントの利用時間に関するログを収集し、CSV 形式のテキストファイルで出力する機能を有すること。
(14) クライアントの利用状況を表示する機能を有すること。
(15) 利用者に開放している PC 教室において PC の空き台数を学生のスマートフォン等から確認できる機能を有すること。
(16) クライアント単位又は管理クライアント内の同時起動数によるアプリケーションの起動制御をおこなう機能を有すること。
(17) アプリケーションの利用回数・利用時間を統計情報として収集し、CSV 形式のテキストファイルで出力する機能を有すること。
(18) 経年によって起動が遅くなる等の性能劣化を防ぐ機能又は仕組みを有すること。
(19) 現状では金沢八景キャンパスの一部の実習室で、建屋間帯域 1Gbps に 100 台近いノードが接続されるなど、潤沢な帯域が確保できていない為、帯域使用を削減する運用、ソリューションを提供すること。
(20) 金沢八景、福浦両キャンパスにて端末を検証するための環境をつくり、本番稼働開始前までに、大学が選定する利用者に評価利用させる期間を 1 週間設け、評価利用で受けた指摘の修正、管理系機能及び各実習室での一斉起動試験を完成させること。
(21) 各キャンパス端末設置に関して、レイアウト変更、台数削減を行う。現行システムの撤去、本学による什器類レイアウト変更、新規システムの設置（UTPや電源配線を含む）を考慮して稼働開始が 4 月 1 日となるよう本学とスケジュールを調整し、実習室システムの設置展開を行うこと。また、そのすべての費用を含むこと。
(22) 既存の実習ソフト（SPSS 等）管理用ライセンスサーバ環境を新環境に移行すること。

6.2　デスクトップ端末に関する要求事項

(1)　別紙資料8「端末設置場所概要図」に示す必要台数を設置すること。
(2)　実習室の端末台数を考慮し、講義等で使用した際に十分な性能が得られること。
(3)　アプリケーション管理やOS のバージョン管理が「6.1管理システム」にて効率的に行えること。
(4)　共通要求事項を満たしたシステムにて管理運用すること
(5)　看護棟実習室に設置する端末には、語学実習用のマイク付きのヘッドフォン計114台を設置すること。
(6)　講義という利用形態、及び、使用するソフトウェアの動作上、ストレスなく使用できる性能以上を有すること。
(7)　筐体は、設置スペースを考慮し本体と液晶ディスプレイが一体化されている液晶一体型又は、コンパクトタイプの筐体でディスプレイにマウントし設置が可能なこと。
(8)　AMD Ryzen 5 5600GE相当以上を搭載すること。メモリは16GB 以上を搭載すること。16GB搭載した状態で、メモリスロットに空きがあること。
(9)　Disk容量はSSD：512GB 以上を提供すること。
(10) Bluetooth が利用可能であること。
(11) web カメラとマイクが内蔵されていること。
(12) LCD は21 インチ以上とすること。
(13) マスター作成、検証用兼、予備機としてノートパソコンを2台、デスクトップパソコン3台用意すること。
(14) 盗難防止対策を取ること。
(15) 金沢八景実習室E、福浦看護実習室の2つの実習室において、教卓PCの画面を学生卓に設置した中間モニタに表示させる中間ディスプレイシステムを設置する。中間ディスプレイシステムおよび既存のアナログからデジタル配線の変更も本調達に含める。
(16) 特に実習室Eのスペースに余裕がないため、電源アダプタなど設置について考慮すること。
(17) 運用中のアップデート作業を含めること。アップデート実施の頻度は半年に1 度を想定すること。

6.3　貸出し用ノート端末に関する要求事項

(1)　貸出用ノート端末 として、学術情報センター3台、医学情報センター3台を設置すること。
(2)　CPU はインテル プロセッサー Core i5 相当以上 を搭載すること。
(3)　メモリは16GB 以上を搭載すること。
(4)　ディスク容量はSSD:500GB 以上を提供すること。
(5)　USB接続の外付けDVDドライブを10個用意すること。
(6)　ネットワークインタフェースとして、1000BASE-T 1つを有すること。
(7)　液晶サイズは15 インチ以上であること。
(8)　OS やアプリケーションについて実習室端末と同等の設定を行い配布すること。
(9)　運用中のアップデート作業を含めること。アップデート実施の頻度は年に1 度を想定すること。
(10) デスクトップ端末と同一の管理システムにて管理運用すること
(11) 無線LANアダプタを内蔵していること。

6.4　機能等に関する要求事項

(1)　既存の実習室においては、プロジェクタとスクリーンが設置されているが、実習室Eや看護棟実習室などでは2 台あたり1 台の中間モニタを設置すること。なお、必要なディスプレイ、切替機、ケーブル及びその設置、設定作業を、本調達に含める。
(2)　Microsoft Edgeのお気に入り、マイドキュメント、デスクトップ、などの設定は、パソコンを再起動しても初期の環境に戻らず、そのユーザのログオフした時の状態が維持されるようにすること。
(3)　どの実習室においても、実習室内の全クライアントに一斉に電源を投入してから1分以内に、全クライアントでログイン画面を表示させるようにすること。運用中この水準を維持するため、その仕組みに関しては別途本学に提示すること。

(4) 1 台ずつ及び複数のクライアントに対する一斉リモート操作として、電源ON／OFF／再起動、Windows へのログオン／ログオフ操作ができる機能を有すること。
(5) クライアントにログオンしているユーザ（アカウント）の一覧を表示することができること。
(6) クライアントの利用ログ（OS の開始／終了、ユーザのログオン／ログオフ情報）を収集する機能を有すること。
(7) クライアントから収集した情報を基に利用状況を分析し報告すること。
(8) 管理者が指定する一定時間経過後に、自動的に端末をシャットダウンする機能を有していること。
(9) 管理者がリモート操作で電源OFF/再起動、ログオフ操作を行う場合、管理者の指定する文字を「利用中の利用者端末の画面」に対して表示することが可能であること。
(10) 電源のON/OFF、ログオン/ログオフ、アプリケーションの起動/終了のログを取得する機能を有すること。
(11) 採取した端末毎の利用時間情報(ログオン～ログオフ)を集計し、月次でレポート提示すること。レポートの形式は事前に本学と協議のうえ決定すること。

6.5 ソフトウェアに関する要求事項

(1) 導入するソフトウェアは、別紙資料9「アプリケーションソフト一覧」に示すソフトウェアを導入すること。なお、既設環境の記載となっているため、数量については、別紙資料8 「端末設置場所概要図」に合わせること。
(2) ソフトウェアのバージョンについては構築期間中に本学と協議し、本学からの特別な指定がない限り最新バージョンを導入しその費用も含めること。
(3) 学術情報センターの貸出用ノート端末、その他に設置される端末は、現状の実習室Eと同様のソフトウェアに対応し、最新版を適用すること。
(4) 医学情報センター、センター病院に設置される端末、医学情報センターの貸出用ノート端末は、看護棟実習室と同様のソフトウェアに対応し、最新版を適用すること。
(5) 維持管理コスト及びオペレーションコストの負担軽減のための最適なライセンス形態を採用すること。
(6) 各製品上可能な限りアップデート権を提供すること。運用中のアップデート作業を含めること。アップデート実施の頻度は半年に1 度を想定すること。
(7) 福浦キャンパスで年一回実施されているCBT テストがあり、CBT の利用及びCBT クライアントソフトのバージョンアップに伴うイメージ更新を行うこと。
(8) CBT 試験実施時に外部回線と遮断し、専用のCBT サーバー（本学で用意済み）に接続し、CBT 用クライアントソフトを稼働させること。

6.6 プリンタに関する要求事項

6.6.1 プリンタ管理システム

(1) 実習室のオンデマンド印刷を実現するために、金沢八景、福浦にプリント管理システムを設置する。プリンタの台数については、別紙資料8 「端末設置場所概要図」を参照すること。
(2) 利用者は、印刷指示をしたのち、同一キャンパス内の任意のプリンタに併設したタッチパネルからID を入力し、プリントの取り出しが可能なこと。
(3) 金沢八景プリント管理システム障害時は、福浦プリント管理サーバを利用して印刷できること。
(4) 学生のBYOD端末向けにWebプリントが可能なこと。
(5) 福浦プリント管理システム障害時は、金沢八景プリント管理のサーバを利用して印刷できること。
(6) 利用者ごとに印刷枚数の上限が設定できること。上限に達した利用者は印刷不可となり、管理者側の操作がなければ印刷可能に戻せないように出来ること。
(7) 利用者ごとの印刷枚数の累計は、両キャンパスでの合計でカウントされること。
(8) プリンタごとの印刷枚数を集計し、月次でレポート提示すること。レポート形式の詳細は事前に本学と協議のうえ決定すること。
(9) 各プリンタにはそれぞれ、ID 入力用のタッチパネルを設置すること。

(10) モノクロ、カラープリンタは手差し印刷が可能なこと。
(11) 実習室の端末台数を考慮し、講義等で使用した際に十分な印刷性能が得られること。
(12) 要求事項を満たすための、管理サーバが必要な場合は、その機器・ソフトも含めること。
(13) 講義等で実習室端末全てからの利用上、十分な性能を持つこと。
(14) A4・A3 普通紙が印字できること。
(15) 専用の設置台を備えること。

6.6.2 モノクロプリンタ

(1) 片面印刷時にA4 ヨコ:32 枚/分、A3:17 枚/分 以上の印刷性能を有すること。
(2) 両面印刷時にA4 ヨコ:21.4 ページ/分、A3:12.2 ページ/分 以上の印刷性能を
    1. 有すること。
(3) 手差しトレイに100 枚の紙を搭載可能なこと。

6.6.3 カラープリンタ

(1) 片面印刷時にA4 ヨコ:カラー30 枚/分、モノクロ30 枚/分、A3:カラー17 枚/分、
    1. モノクロ17 枚/分 以上の印刷性能を有すること。
(2) 両面印刷時にA4 ヨコ:カラー21 ページ/分、モノクロ21 ページ/分、A3:カラー
    1. 10 ページ/分、モノクロ10 ページ/分 以上の印刷性能を有すること。
(3) 手差しトレイに100 枚以上の用紙をセットすることが可能なこと。
(4) 金沢八景キャンパス講師控室に設置のカラープリンタに関しては既存機器をそのまま継続利用し、オンデマンド及びプリンタ管理システムの対象から除外する。

6.7 端末空き状況表示システムに関する要求事項

(1) 金沢八景キャンパス内で、実習室が満室になった際に別の実習室の空き状況が把握できるように、空き端末表示Web システムを設置する。
(2) 金沢八景キャンパスのE実習室、G実習室、福浦キャンパス看護棟実習室、医学情報センターの端末空き状況を収集し、Web 表示させること。
(3) Web アクセス要求は学内外から行われることを想定し、必要なライセンス提供を行うこと。
(4) Windows11、MacOS12以上、Andoroid、iPad等のiOSを搭載した端末に対応すること。
(5) 教室レイアウトをベースにした図面による空き表示画面と、各実習室の空き台数を文字表示する画面を有すること。
(6) 端末の使用状況は電源ON/OFF ではなく、ログオン/ログオフで判定すること。利用者が端末の電源を突然切断しても空きを認識出来ること。

6.8 WEB カメラに関する要求事項

(1) 金沢八景キャンパスのサーバ室、福浦キャンパス A 棟 205 室の既設カメラを本学が保有するネットワークカメラに入れ替えること。
(2) 入れ替え後のカメラは録画対象として既設レコーダーに追加登録すること。入れ替え台数は別紙 8「端末設置場所概要図」を参照すること。
(3) ネットワークカメラを入れ替える際、LAN ケーブルは既存のケーブルを流用すること。

7. ユーザ管理システム(アカウント管理システム)

本学のユーザ管理システム(アカウント管理システム)は図 7.1 のような仕組みで構成されている。以下にユーザ管理システムの基本要求仕様を示す。

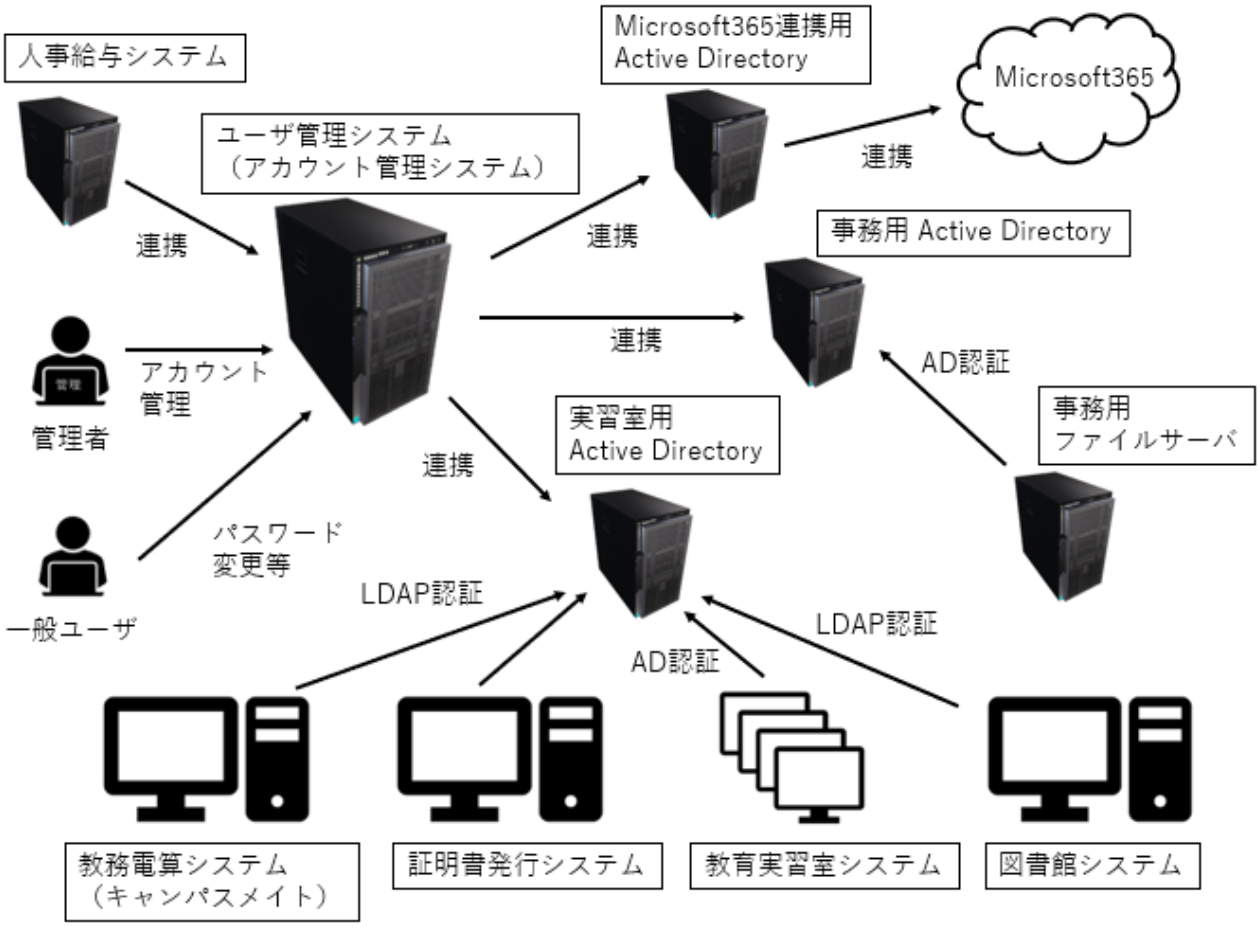

図 7.1 現在のアカウント管理の仕組み

7.1 システム構成基本要件

本システムは、本学構成員のユーザ情報を一元管理する ID 管理システム、ユーザ認証・ディレクトリサービスを行なう認証サーバ、利用者のホームディレクトリ・ファイルを保存するファイルサーバで構成する。

ユーザ管理システムの構成基本要件は以下の通り。

(1) ユーザ管理システムとして仮想環境上に1台以上のサーバで構成すること。
(2) CPU 2コア以上、メモリ 16GB 以上、ディスク領域 100GB 以上を割り当てること。なお、後記の各機能が遅延なく利用できるよう必要なリソースを追加すること。
(3) 稼働する OS は問わないが、以下に続く要求事項を満たすハードウェア、ソフトウェアを具備すること。
(4) サーバの稼働状況等が容易に確認でき、リモートからの操作が可能であること。

7.2 基本機能要件

(1)本システムを利用する初期ユーザ数として、利用期限切れで未使用の削除待ちユーザを含め、22,000 ユーザ以上を扱えること。なお、初期利用者でエントリする主な利用者数は、次のとおりである(令和7年 6 月 10 日現在)。

ア　学生　7,500 人
イ　教職員 9,000 人（内：共同研究者や業務用 ID 等　2,300 人）
ウ　卒業生 4,000 人

本学への入学予定者と卒業生については、重複して登録される時期がある。また、教職員も入退職に伴う同様の時期が存在する。そのため、前述の初期利用者数に、入学予定者 1,300 人と入れ替わる教職員 700 人を加えた 24,000 人以上を本システムで扱うことができること。また卒業生については、毎年、メールの継続利用希望者 500 人程度が増える想定であり、これらの人数を扱えるようにすること。

(2) 本システムと連携する連携先のシステムとのインタフェースを原則として変更することなく、ユーザ情報を提供（統合された ID とパスワードで運用）できるようにすること。

7.3　各機能に関する技術的要件

7.3.1 ID 管理システム

(1) ID 管理基盤は利用者情報を管理し、ID の登録、更新、削除を可能にする ID 管理システムと、利用者情報を記録し他システムとのデータ連携を可能にするデータ連携システムで構成すること。ただし、機能要件を満たせば、統合された構成でもかまわない。
(2) 24,000 人以上の利用者情報を管理し、ID ライフサイクルを制御する機能を提供できること。
(3) ID 管理システムは Web インタフェースにより利用できること。なお、動作保証をするブラウザの種類、バージョンは、別途本学と協議のうえ決定すること。
(4) 文字コードは既存データからの移行を考慮して適切な方式を選択することし、別途、本学と協議のうえ決定すること。
(5) ID を使わない事情が生じた場合、フラグや利用期限等で利用を停止する形とし、当該 ID を物理的に削除しないようにすること。またその場合、履歴も追えるようにしておくこと。

7.3.2 ユーザ ID

(1) 利用者種別ごとにユーザ ID の体系を分けられること。
(2) 学生のユーザ ID は別途、教務部門等から指定された CSV による登録を行う。CSV に記載のものを利用できるとともに、ID 管理システムより個別に登録する場合は、本システムにて自動発番できるようにすること。
(3) 利用者の登録時に本学にて指定した文字列・文字数・文字種を用いて初期パスワードを自動生成できること。また生成した初期パスワードをユーザ ID とともに通知書として印刷できること。
(4) 通知書を印刷するプリンタは、本学が指定するプリンタに印刷できる設定を行うこと。
(5) 緊急事態等に備え、システム管理者が全利用者のパスワードを一括して初期化することが可能であること。
(6) パスワードポリシー（強度、変更サイクルの期間等）をシステム管理者が設定できること。
(7) パスワードは暗号化して DB に保存すること。

7.3.3 利用者の検索

(1) 検索条件を指定して画面から利用者が検索できること。
(2) ユーザ ID、氏名、所属、学籍番号、教職員番号、メールアドレス等を検索条件として想定している。なお、項目の詳細は、導入時に本学と協議のうえ決定すること。
(3) 検索結果から利用者を選択したうえで、当該ユーザ情報の編集／更新、利用権限の付与／停止処理ができること。

7.3.4 利用者の登録

(1) システム管理者による CSV 形式での一括処理及び Web インタフェースによる個別登録処理（利用者

情報の個別登録・更新・削除）が可能であること。その際、登録する項目は、個々に任意、必須の指定ができること。

(2) 学務システムから提供されるデータにより新入生アカウントを一括登録、卒業生アカウントを一括削除できること。

(3) 全学生、全卒業生及び全教職員が含まれるセキュリティグループを自動更新できること。

(4) 人事給与システムから提供されるデータにより、退職者アカウントの一括削除ができること。

(5) 利用者を新規登録する際に、指定するルールでメールアドレスを自動生成することが可能なこと。また、自動生成するかどうかを、処理モードとして選択できること。また、自動生成した文字列の修正が一定のルールの下、利用者自身で可能であること。

(6) システム管理者が利用者種別ごとに最長利用期間を設定できること。

(7) 利用者の情報を一括登録する際には、登録前に確認画面が出て、状況によっては登録をキャンセルすることができること。

(8) 一括登録の途中でエラーが発生した場合は、どのデータが何の理由でエラーになったかをログに残して元データの調査ができるようにすること。

(9) 利用者情報に対する全ての変更履歴（変更内容、変更者、変更日時）を画面上で確認できること。

7.3.5 管理者機能

(1) アカウントの利用停止と解除を行えること。

(2) アカウントには以下のステータスを用意し、管理者による操作、または、アカウントの有効期限等により状態遷移できること。

ア パスワード無効状態（認証不可、メール受信可、本人によるパスワード変更で復活）

イ アカウント有効期限切れ状態（認証不可、メール受信可、自動メール転送不可、延長申請で復活）

ウ 管理者利用停止状態（認証不可、メール受信不可、管理者操作で復活）

(3) 申請を受けた管理者が、GUI からアカウント有効期限の延長更新ができること。

(4) アカウント有効期限切れ状態の場合、及び、管理者が個別に指定した場合、そのアカウントを利用停止状態にできること。

(5) ディスク使用量を個人別に制限できること。ディスク使用量が既定値に近づいたユーザに自動的に通知する機能を持たせること。

(6) 学籍番号、教職員番号、氏名（姓・名）、メールアドレス、UNIX シェル、入学年度、学年、在学状態、所属、申請者情報等の基本情報を一元的に保管できる機能を有すること。

(7) 検索結果よりアカウントに対して、状態遷移の操作ができること。

(8) 管理者利用停止状態のアカウントは、管理者の CSV 投入、GUI 操作により、削除（プロビジョニング先データを含む全データの削除を行う）できること。

7.3.6 Active Directory 連携

(1) 画面から登録、変更された利用者情報の内容を Active Directory（以下「AD」という。）と連携すること。なお、AD は実習室用と事務用及び Microsoft365 連携用の3種類存在するものとする。

(2) 本学で設定するルールに基づき、ユーザ ID 毎にファイルサーバにホームディレクトリパスを生成し、ホームディレクトリの作成・権限付与・退避・削除を行うこと。また、アカウントの停止時に退避を行い、本学が指定する一定期間後に自動的に削除を行うこと。

7.3.7 教務システム連携

(1) 教務システムと実習室用 AD の認証連携に必要となる、かつ、教務システムの教職員ユーザ登録に必要となる基礎情報を日次で CSV 出力すること。

(2) CSV 出力する項目は以下を見込んでいるが、各項目は必要に応じて追加する可能性もある。

ユーザ種別
処理指示子（追加・更新・削除）

職員番号/学籍番号
氏名（漢字）
氏名（カナ氏名）
ユーザ ID
生年月日
所属コード
職員区分コード
退職年月日

(3) 職員番号が設定されていないユーザ情報は CSV 出力対象には含めないこと。

7.3.8 メールサービス連携

(1) 既存のメールサービス（Microsoft365）と連携するためのサーバ機能を有すること。
(2) 既存のメールサービスに対して利用者情報伝播を行うこと。また、利用者の登録処理時（登録、更新、削除）に個々のメールボックスの作成、削除を行うこと。

7.3.9 認証サーバ

(1) 認証サーバは、Microsoft Windows Server の、ActiveDirectory で構成すること。
(2) ID 管理システムと連携し、24,000 人以上の利用者情報を使用した認証機能を提供すること。
(3) 各認証クライアントからの同時認証に対して、ストレスなく処理できる構成とすること。
(4) LDAP/LDAPS（TLS）プロトコルで通信可能な機能を有すること。ただし、原則として本システムでは、LDAPS を利用すること。
(5) エントリのパスワード情報は、暗号化又はハッシュ化して格納する機能を有すること。
(6) エントリの最終更新日時を記録する機能を有すること。
(7) エントリの組織単位（OU）、属性値や操作内容に対してアクセス制御を行う機能を有すること。

7.3.10 卒業生への対応

(1) 卒業生は、Microsoft365 の Outlook 機能以外は利用できないこと。
(2) 実習室用 AD は、卒業に伴うアカウント情報削除後に、メール機能維持のため、バックスキャッタ対策用に、自動的にアカウントの再登録を行うこと。
(3) 所属学部の情報を失わないこと。
(4) 予め設定した期間（年数）の間に 1 度もログインされない放置状態の卒業生アカウントは、Microsoft365 上で完全に削除できること。なお、このルールは卒業生のみに適用させること。
(5) CSV 等による一括登録／削除及び個別登録など、一連の卒業生対応の処理が行えること。
(6) 卒業生がパスワード変更するためにユーザ管理システムにアクセスするにあたり、ライセンスが必要な場合は本調達に含めること。

7.3.11 利用者情報のバックアップ

(1) バックアップの対象は、本システムで用いるプログラム、設定ファイル、データベース、ログなど日次的に変化するものを対象とする。これらデータのバックアップを取得できる仕組みを有すること。日次的に変化しないデータなどについては、構築時もしくは定期点検時に必要なバックアップを取得できる仕組みを有すること。
(2) バックアップスケジュールをジョブ単位で設定できること。
(3) 障害のためにリストアを行う必要がある場合、バックアップデータからバックアップを行った状態に復元することができること。また、サーバ 1 台あたり 1 日以内に復元可能であること。
(4) システムの運用を中断することなく、定期的に自動で行うことができること。

(5) バックアップジョブの結果を電子メールで通知することができること。

7.4 データ移行に関する要件

7.4.1 データ移行

(1) 本学と協議のうえ、既存の ID 管理システム、認証サーバ、ファイルサーバから利用者の情報をパスワード情報含め移行すること。移行の際は、サービスの停止期間が最短となるよう十分に考慮すること。
(2) 本学と協議のうえ、移行の方法及びスケジュールを決定し実施すること。

7.5 非機能要件

7.5.1 セキュリティ

(1) 人事情報と密接に連携することから、データへのアクセスやエクスポートに対してログを取得するなどセキュリティ対策を考慮したシステム開発・構築を行うこと。
(2) データベース又はサーバに保持するデータに対し、不正なアクセス及び閲覧を防ぐためのアクセス制御機能を設けるとともに、必要な場合は、データを暗号化して保存できるようにすること。
(3) Web インタフェースに提供する機能については大学にて発行する UPKI の SSL 証明書にて暗号化すること。
(4) 不要なサービスや機能を停止又は削除し、想定しない通信やアクセス、許可されていないタスク・コマンドの実行などができないようにすること。

7.6 アカウント管理システム

電子情報システムに人事情報とデータを連携する形でアカウント管理システムを設ける。
なお、今回更新する電子情報システムが、以下に示すアカウント管理システムの要求仕様を満たせるのであれば、電子情報システムの中で実現してもよい。

7.6.1 アカウント

本学の様々なシステム利用のためのログイン用の ID であるとともに、メールアドレスとしても利用しているが、個人で所有するアカウントのほかに「業務用アカウント」を設け、特定の部署やグループで共有して使用できるようにすること。

また、個人所有のアカウントには「学生アカウント」、「卒業生アカウント」、「教職員アカウント」を設け、それぞれで利用できるサービスやアクセス可能な範囲を制限できること。さらに「教職員アカウント」の中でも、教員と職員とで一部制限を変えることができるようにすること。

7.6.2 アカウント管理

本学で使用している様々なシステムでは、ユーザ認証により利用させる方法を取っているが、認証方法がシステムごとに異なるため、複数の Active Directory サーバ等の認証サーバを用意している。
ユーザの利便性のため、同じアカウント名、パスワードであらゆるシステムを利用できるようにしているため、認証サーバ間でアカウント情報を共有させる必要がある。

ユーザ管理システムが、認証サーバ間でのデータの整合をとる役割を果たすとともに、ユーザや管理者に対して、アカウント情報の表示、設定のため Web ブラウザベースでのユーザインタフェース(以下、この章では「Web UI」という。)を提供すること。

7.6.2.1 システム管理者のアカウント管理業務

システム管理者のアカウント管理業務の概要は以下のとおりである。これらはユーザ管理システムで行

うものとする。

【学生アカウント/卒業生アカウント】

(1) 毎年4月に新入生のリストが教務部門から送付されてくるのでそのデータをユーザ管理システムに一括登録し、アカウントを作成する。作成したアカウント情報は、初期パスワードとともにプリントアウトし、教務部門経由で本人に渡す。

(2) 留学生などの受け入れ時は時期に関係なく教務部門よりリストが送付されてくるため、それをもとにアカウントを作成する。

(3) 卒業生については、教務部門より卒業生リストが送付されてくるので、それをもとに学生アカウントから卒業生アカウントに一括処理で移行させる。学生のアカウント名は原則、学籍番号をもとに作成され、修士課程／博士課程前期／博士課程後期への進学時など学籍番号が変わると新たなアカウントが付与される。

【教職員アカウント】

(1) 在籍者からの招待

(2) 業務用アカウントの申請

(3) 退職者については退職翌年度の 5 月初旬にアカウントを使用停止にした後、一定期間後に削除を行えるようにすること。

(4) 教職員アカウントの中には、職員番号を持たない人、人事給与システムに登録のない人もいるが、これらのアカウントには利用期限が設けられており、開始した時期に関わらず毎年 5 月初旬の利用期限が近くなると継続申請を促すことで、その継続申請があれば利用期限を延長することができるようにすること。

【学生・教職員共通】

(1) パスワードを失念した利用者に対しては、申請書を受理したうえで、パスワードを初期化し、初期パスワードを印刷して渡すことができるようにすること。

(2) アカウントが使用できないなどの問合せに備えて、ユーザ管理システムよりアカウントのステータスを確認できるようにすること。

7.6.3 アカウント管理システムで実現する機能

(1) 人事情報（人事給与システム）と連携したデータベースを保有し、アカウントとその利用者の最新の情報がユーザ管理システムに反映されている状態にする。

(2) 個人の識別を職員番号だけでは行わないようにする。

(3) 教職員の職員番号、職種、職員区分等の履歴が閲覧できる。

(4) アカウント情報の最新のものをユーザ管理システムに提供する。

(5) 利用者自身でパスワードの再発行や、利用期限の延長、業務用アカウント発行などの申請ができるインタフェースを提供する。

(6) 利用者が、職種や職位、所属など、任意に指定した単位ごとに一斉メールが送信できるインタフェースを提供する。

(7) アカウント管理者に対する管理用のインタフェースを提供する(アカウント検索、ユーザ情報の表示、職員番号の変更履歴表示、CSV 出力等)。

(8) ユーザ管理及びアカウント管理のデータベースで保有する利用者情報を、利用者ごとに 1 レコードで全項目 CSV 出力が可能なこと。

7.6.4 ハードウェア要件

(1) 1台以上のサーバで提供すること。

(2) 24 時間 365 日稼働する前提で機種選定を行うこと。

(3) 100,000 レコード程度のユーザ情報(後述)が登録できる容量があること。

(4) 毎日データをフルバックアップし、ハードウェアの故障時には、ハードウェアの復旧後、6 時間以内にデータ復旧できること。
(5) WEB サーバとデータベースサーバは分けること。
(6) 物理サーバ、仮想サーバのいずれの提供でも可とするが、データセンターに設置し、システム管理者がリモートでログインして作業ができるようにすること。

7.6.5 ソフトウェア要件

7.6.5.1 人事給与システムとの連携

(1) 人事給与システムから提供される CSV ファイルを毎日取得し、本システムに取り込むこと。提供方法は特定のファイルサーバにあらかじめ決められた名前のファイルが格納されているものとする。
(2) この一括取り込み時のログを残し、ファイルのフォーマットエラー、不正データの存在など途中でエラーが発生した場合は、どのデータが何の理由でエラーになったかをログに残して元データの調査ができるようにし、その旨をログに残すこと。また、取り込みが完了した CSV ファイルは別フォルダに退避して残すこと。
(3) CSV ファイルで提供されるデータの内容は以下の 3 ファイルを見込んでいるが、各項目は必要に応じて追加する可能性もある。

・ 職員基礎情報

人給 ID
職員番号
氏名
氏名カナ
旧姓使用フラグ
生年月日
性別
身分(職員区分)
人事職種コード
地位(職位)コード
職名コード
所属コード
採用年月日
採用事由
退職日
退職事由
更新日時

・ 機構情報(約 390 件)

所属コード
所属名称

・ コード情報(約 180 件)

コード
コード名称

(4)年度末にマスタ情報(機構情報及びコード情報)が変更される場合は、任意のタイミングで取り込みを一定期間停止できること。マスタ情報を更新後は、停止期間中の変更情報をまとめて取り込めること。
(5)何らかの理由により本システムが停止した場合は、その間に人事給与システムから出力された CSV ファイルは、後日まとめて取り込めること。

7.6.5.2　データ管理方法

(1)　「生年月日＋氏名カナ」で個人を識別し、キーとすること。これが等しい人物は同一人物とする。
(2)　キーに対してアカウントを紐づけること。
(3)　アカウント管理システムでは以下の項目を格納し、管理する見込みである。必要に応じて増減する可能性はある。
(4)　人事給与システム上では職員番号が変わる際は別レコードとして登録されるため、CSV ファイルで取り込んだ際に【生年月日＋氏名カナ】が同じ場合には同一人物とみなし、採用年月日が新しい職員基礎情報で上書きし、以前の職員番号の情報は履歴として残すこと。採用年月日が同一の場合には、変更日時が最新の情報で上書きすること。但し、人事給与システムの情報がすべて退職済みの場合は、職員基礎情報で上書きはしない。
(5)　【生年月日＋氏名カナ】が同一の別人がアカウント申請した場合には、問合せ等で発覚した後に本人に別人であることを確認するが、その後システム上で別人として管理ができるように、履歴として残しておいたデータを再利用できるようにすること。
(6)　人事情報との紐づけ有無をアカウントとの登録区分として区別できること（例.紐づけあり：人給）○○、紐づけ無し：申請）○○　など）
(7)　退職処理時に登録区分が「人給)○○」の場合は、「申請）○○」に変更すること。また、退職日となるまでは、変更前の WEB 機能の利用権限を維持できること。
※　登録区分は人事給与システムから連携されアカウントが紐づくと「申請)○○」から、「人給）○○」に変更されること。

7.6.5.3　データ出力

(1)　アカウント情報の新規登録、更新が発生するたびに、ユーザ管理システムに通知し、ユーザ管理システム側のデータを更新できるようにすること。
(2)　通知の方法は指定しないが、リアルタイム（3 分以内）にユーザ管理システムに登録、更新が反映されること。何らかの理由で反映できなかったときは、その旨をシステム管理者に通知されるようにすること。
(3)　通知するデータは以下の条件で抽出する。
ア　新規に追加されたレコード
イ　更新されたレコード

7.6.5.4　データ更新

共同研究者で作成されたアカウントが事務職員に変更された際、事務用ファイルサーバにログインができるように、事務用 AD にユーザ登録が実施できること。

7.6.5.5　管理者によるデータ検索、閲覧、更新機能

登録されたアカウント情報をシステム管理者が検索、閲覧できる Web UI を提供すること。
(1)　管理者は本システム内で特定のアカウントに管理者権限を設定できるものとする。
(2)　登録されている情報は全て閲覧できるものする。
(3)　個々のアカウントに対して、職員番号、所属、職種等、人事給与システム側で変更される可能性のある項目の履歴が一覧で参照できること。
(4)　CSV の出力機能を有すること。
(5)　アカウント情報を検索する際に、大文字/小文字の区別をしないこと。

7.6.5.6　利用者向けアカウント確認、設定画面

利用者が自身のアカウントの登録情報を確認でき、一部の項目について設定変更できる Web UI を設け、以下の要求仕様を満たすこと。

(1)　ユーザ ID でログインできること。
(2)　ユーザ自身に関する登録情報が閲覧できること。
(3)　パスワードを失念したときに再発行する際のメールの送付先が設定できること。
(4)　パスワードの変更ができること。
(5)　メール送信時の送信者名を自由に設定できること。

7.6.5.7　利用者による新規アカウント発行機能

アカウントの申請は、すでにアカウントを所有している職員番号を持った職員が、新規アカウントを必要とする利用者に招待メールを送付することで、申請フローを開始する。不用意に本学と関係のない人からの申請ができないようにするため、このような形とする。

申請フローは図 7.2 のとおりである。

図中の既存職員とは、すでに本学のアカウントを所有し、職員番号を持っている教職員である。新規アカウント利用者は、新たに入職した人、もしくは、研究員として本学のアカウントを必要とする人である。

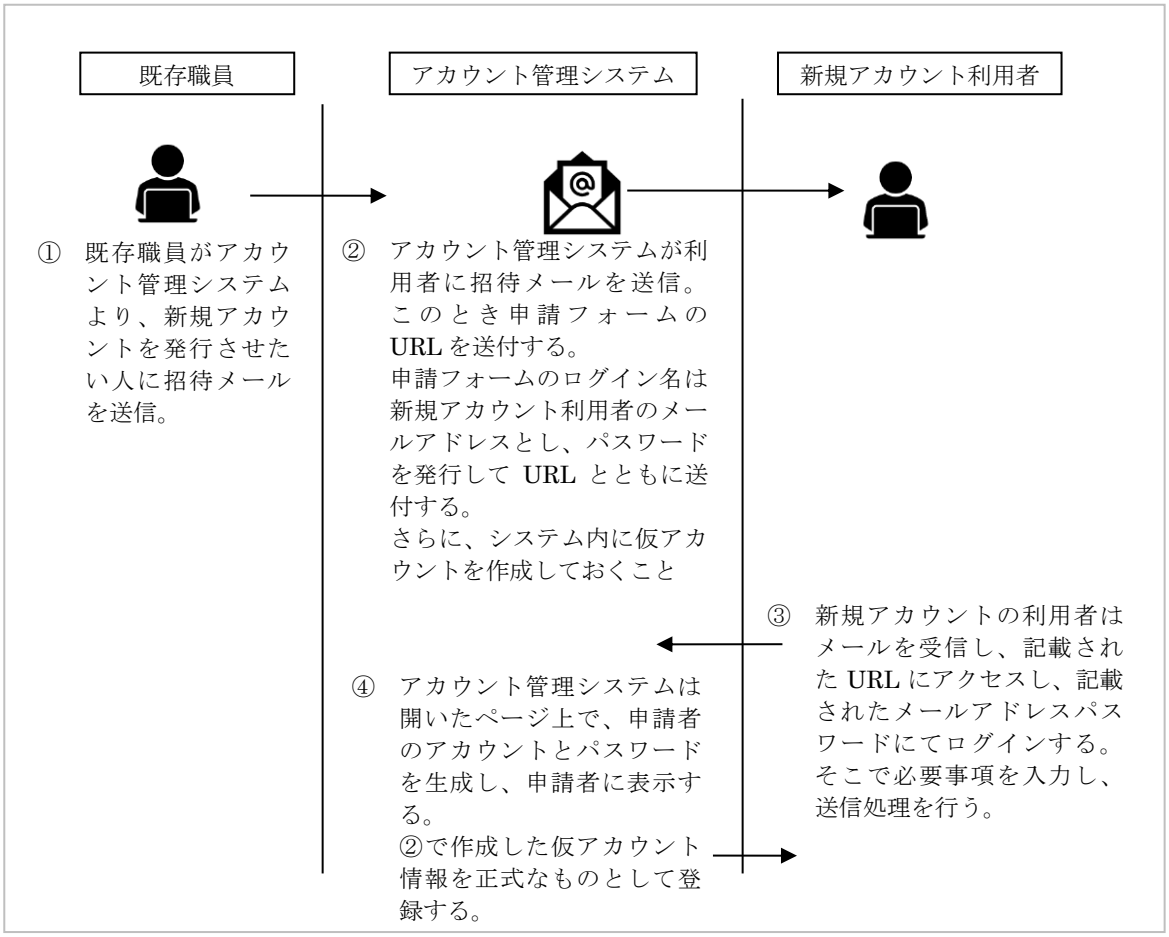

図 7.2 アカウント申請フロー

(1) 招待メール送信、アカウント申請用に、Web UI を設けること。
(2) 学外からの利用も可能とすること。
(3) アカウント申請は、教職員用と業務用の 2 種類を選択できること。

＜教職員用アカウント申請＞

(1) 職員番号をもった教職員のみが招待メールを送信できるものとし、氏名、所属、招待したい人のメールアドレスが入力できるものとする。氏名の前後にスペースが存在する場合は削除すること。
(2) 招待のキャンセルができること。
(3) 教職員用アカウントの申請ができる教職員は、あらかじめ指定しておいた人事給与システムの職員基礎情報（職員区分）によって制限できること。
(4) 招待を受けた人にメールを送信すること。
(5) 招待を受けた人が入力する申請フォームを Web UI で設けること。その際、招待を受けた人のメールアドレスをシステムのログインユーザ名とする。システムが発行したパスワードでログインできるようにすること。申請フォームには、氏名、氏名カナ、生年月日が入力でき、招待メールの差出人の氏名、所属、メールアドレスが表示されること。既に氏名カナと生年月日が一致するアカウントが登録済みの場合はアカウントが存在する旨を表示すること。
(6) アカウントは一定のルール（例. 氏名カナのローマ字など）に従って自動生成すること。
(7) 自動生成された文字列は、招待を受けた人が部分的な修正（修正文字数等の制限あり）が可能であること。
(8) アカウントの初期パスワードは自動生成し、利用者が申請画面に情報を入力した後、登録操作が完了した時点で画面に表示すること。
(9) 初回ログインで使用した招待を受けた人のメールアドレスは、パスワード再発行用の副メールアドレスとして保持され、使用できること
(10) 申請は学外からでもできるようにすること。
(11) 新規アカウント申請時に、すでに【生年月日＋氏名カナ】が同一の有効な別アカウントが存在した場合には、申請者に主となるアカウントを選択させ、それ以外のアカウントは、1 年毎の継続申請を必要とする人事給与システム外利用者アカウントとして扱えるようにすること。
(12) 一人の教職員が無制限にアカウントの申請（及び招待）ができないよう、人数の上限値を設けられるようにすること。
(13) 招待したい人のメールアドレスが既に既存利用者の副メールアドレスとして登録されている場合には、招待できないようにすること。ただし、卒業生が職員として採用されるケースに対応するため、学生アカウントの副メールアドレスは招待可能とする。同一の副メールアドレスへの招待は、上限値を設けられるようにすること。
(14) 大学ドメインのメールアドレスはサブドメイン含め招待を不可とすること、
(15) 招待したい人のメールアドレスには、招待メールを送信する教職員自身のメールアドレスは指定できないようにすること。

＜業務用アカウント申請＞
(1) 職員番号をもった教職員のみが業務用アカウントを申請できるものとすること。
(2) 業務用アカウントの申請ができる教職員は、あらかじめ指定しておいた人事給与システムの職員基礎情報（職員区分）によって制限できること。
(3) 申請画面は、アカウントの名称、アカウント文字列、申請理由が入力できること。さらに画面上に表示された申請ボタンを押下すると、承認者宛に承認依頼のメールが送信されること。
(4) 承認者はあらかじめ指定しておいた特定の管理者アカウントとしたうえで、本システムのその他の管理者が誰でも承認を行えること。
(5) 承認を行うため Web UI を設けること。この画面に業務用アカウントの申請者の情報が記載されており、承認するかどうかのボタンを設けること。
(6) 承認者のメールアドレスに承認用の Web UI の URL を添付すること。
(7) 承認者が承認した記録が残せ、承認がない場合は受け付けできない仕様とすること。
(8) 一連の申請内容は発生日時とともにログに残すこと。

7.6.5.8 登録用キーによる教職員アカウント一括発行機能

新規入職者へのアカウント招待業務の効率化を図るため、登録用キーの一括発行と、登録用画面を設ける。

これにより、現場の看護師長などが 100 名規模のアカウント発行を行う際、手動でのメール招待を繰り返すことなく、事前にキーを配布し、入職者自身がアカウント登録を行う運用を可能とする。

本機能はアカウント申請機能（メール招待方式）と併用可能であり、利用現場の運用に応じた柔軟な選択を可能とする。

登録用キーは、本人以外の不正利用を防止するために管理画面にて発行・削除等を制御し、使用済みかどうかをシステム上で判定できるようにする。

(1) 登録用キーを管理画面上で一括発行できること。
(2) 発行されたキーを一覧で管理でき、発行日や利用状況（未使用／使用済み）を確認できること。
(3) 発行済みのキーについて、使用前であれば削除できること。
(4) 登録用キーを PDF 形式で一括出力し、紙での印刷配布が可能であること。1 ページにつき 1 キーとする。
(5) 入職者が登録用キーを使用し、本人確認のうえ Web 画面からアカウント登録が可能であること。
(6) アカウント登録画面は、登録用キーにより一意にアクセス可能とし、管理者によるアクセス制御が行えること。
(7) 本機能により発行された登録用キー数も、アカウント発行上限数の算定対象とすること。
(8) 使用済みまたは無効なキーによるアカウント登録はエラーとなること。

7.6.5.9 ユーザによるパスワード再発行機能

Web UI での申請により迅速にパスワード再発行に対応できるようにする。本機能は学生、教職員とも利用できること。

また、学外からの利用も可能とすること。

(1) パスワード再発行用の Web UI を設けること。
(2) システムは申請を受けたらアカウント情報として登録済みの副メールアドレスあてに、仮パスワード再発行用の Web UI の URL を送付すること。副メールアドレスの登録がない場合は、従来通り紙の申請書を使って初期化申請を行うようメッセージを出力すること。
(3) 送付された URL の接続先である、仮パスワード再発行用の画面で新規パスワードを入力することによって、パスワードの再発行（更新）が行えること。
(4) 申請のログを残すこと。

7.6.5.10 ユーザによる利用期限延長申請機能

共同研究者など一部の利用者（人事給与システム外利用者）はアカウントの利用期限が設定されているため、期限前に延長申請をする必要がある。

(1) 利用期限延長申請を希望する利用者は、自身のアカウントでアカウント管理システムにログインできること。なお、利用期限を迎えた後でもログインできること。
(2) 利用期限延長申請用の Web UI を用意し、利用者が自身で延長申請できるようにすること。ただし、名誉教授の場合は延長申請できないようにすること。
(3) 申請画面は、氏名、氏名カナ、生年月日、延長理由が入力でき、承認者を選択できること。さらに画面上に表示された申請ボタンを押下すると、承認者に承認依頼のメールが送信されること。
(4) 承認者の選択肢はあらかじめ指定しておいた人事給与システムの職員基礎情報（職員区分）によって抽出される利用者であること。
(5) 承認者のメールアドレスに承認用の Web UI の URL を添付すること。
(6) 承認用の Web UI を提供すること。Web UI に利用期限延長の申請者の情報が記載されており、承認をするかどうかのボタンを設けること。
(7) 承認者が承認した記録が残せ、承認がない場合は受理できない仕様とすること。
(8) 申請を受理すると、アカウントの利用期限は、申請月日が 2/1 より前ならその年の 5/25 日、2/1 以降なら翌年の 5/25 まで期間を延長するよう設定すること。なお、この月日の設定は後で容易にシステム管理者が任意に変更できること。また、そのログを残すこと。
(9) 学外からの利用も可能とすること。

7.6.5.11　所属、職位、職名によるメール一斉送信機能

所属や職位でグルーピングした対象者に対して、その時点での最新の属性情報に基づいて利用者がメールを一括送信できるようにする。

(1)　所属、職種、職位などを単位にしたグループでメールの一斉送信ができること。
(2)　送付先のグループをドロップダウンで選択でき、選んだグループに属するメンバーにメールが送付できること。
(3)　送付先のグループは複数選択できるが、複数のグループに属する人に複数のメールが届かないよう、送付先の重複を排除すること。
(4)　退職日を過ぎたアカウント(退職者)もメール送信の対象に設定できること。
(5)　アカウントロック状態の場合は、送信対象から除外すること。
(6)　Web UI によりメール本文が入力でき、送信先を選択することで送信できること。メール本文は1,500 文字以上入力できること。
(7)　ファイルが添付できること。ただし、添付できるファイル数や、合計のデータ容量には一定の閾値を設け、それを超えた場合は警告を表示できるようにすること。またその閾値はシステム管理者が容易に変更できること。また、業務用アドレスを除く設定ができること。
(8)　送信サーバは本学に設置した SMTP サーバを使用してよい。
(9)　送付先のメンバーが送信前に全て確認でき、送信したくない人を個別に削除できること。
(10)　CC、BCC、Reply-To(返信先)の宛先も指定できること。
(11)　送信する前に、内容を確認し、入力した内容の修正ができること。
(12)　送信予約機能があること。(指定した時刻に送信)
(13)　メールの差出人は送信者のアカウントとなること。
(14)　利用者はシステムにログインして利用できるようにすること。
(15)　利用者はあらかじめ指定しておいた人事給与システムの職員基礎情報(職員区分)によって制限できること
(16)　学外からの利用ができないこと。但し、VPN 接続経由での学内ネットワークからの利用はできること。
(17)　送信のログ(選択条件、送信対象、件名など)を残すこと。

7.6.5.12　セキュリティグループの生成機能

Microsoft365 上のセキュリティグループや、事務 AD のグループの作成とメンバーの追加・削除メンテナンスを容易に行えるようにする。

(1)　所属、職種、職位などを単位として Microsoft365 のセキュリティグループが作成できること。
(2)　人事給与システムと紐づけがないアカウントも追加できること。
(3)　上記と同じメンバーで事務 AD 上にもグループが作成されること。
(4)　このグループを作成するための Web UI を設けること。
(5)　これらのグループ単位をメンバーの抽出条件としてドロップダウンで選択し、所属するメンバーを含んだセキュリティグループを作成し、その後、メンバーを個々に増減できること。
(6)　グループ名は任意に命名できること。
(7)　一度作成したグループのメンバーを変更できること。
(8)　一度作成したグループの抽出条件を保持し、以降所属の変更があったアカウントについては該当するセキュリティグループに対してメンバーの増減が行われること。
(9)　システム管理者のみが利用できること。

7.6.5.13　データ移行

(1)　本システムの運用開始時には、既存アカウントは文字列を変更することなく、人事給与システムとの紐づけを事前に行ったうえで、新システムで利用できるよう全て移行すること。その際、アカウントと

の紐づけできなくとも、できない状態で移行すること。

(2) 移行時に既存アカウントと紐づけできなかった人事給与システムのデータについては、ユーザ管理システムに通知する直前の状態として本システム上にデータを作成し、管理者によるデータ検索閲覧の対象とすること。その際、まだユーザ管理システムに通知されていない(アカウントとして正式なものとなっていない)ことが分かるようにすること。

(3) 移行後に上記データに合致する【生年月日＋氏名カナ】のアカウント申請があった場合には、ユーザ管理システムに通知されて正式なアカウントとして登録されること。

(4) 移行時に人事給与システムと紐づけできなかった既存アカウントについては、利用者自身による利用期限延長申請により【生年月日＋氏名カナ】が入力された際に、再度紐づけされるようにすること。

7.6.5.14 ログデータ保管期間

(1) システム上でのログデータ保管期間は 5 年とし、アカウント情報の履歴データの作成に関する経緯が追えるようにすること。

(2) 5 年を超えるログデータの扱いについては本学と協議のうえ、決定すること。

8. メールセキュリティ基本要件

メールによる外部からの攻撃に備える入口対策、情報漏洩を未然に防止する出口対策を実現するメールセキュリティ対策システムを構築する。

8.1 メールシステム

要求事項	要求仕様
数量	メールシステムについては全学で Micorsoft365 を利用しており、基幹ネットワークの更新後も継続して利用するものである。 Micorsoft365 のライセンスは大学側で調達したものを利用する。
ソフトウェア及び制約条件	基幹ネットワークシステムの更新後も、Microsoft365 の環境でのメールが滞りなく利用できるようにすること。 メールセキュリティ対策サーバと連携しセキュリティ強化を行うこと。
その他	なし

8.2 メールセキュリティ対策サーバ

メールセキュリティの強化を目的とする各種処理を実装するためのシステムを構築する。

要求事項	要求仕様
数量	2 式 メールセキュリティ対策基本ソフトウェアを動作させるためのサーバ
ハードウェア	(1)仮想基盤上に構築し、CPU 4Core 以上、メモリ 16GB 以上、HDD 200GB 以上を割当てること。 (2)Redhat Enterprise Linux v9 相当以上を導入すること。
ソフトウェア及び制約条件	(1)入り口対策(攻撃対策)機能 ア SPF、Sender-ID、DKIM の方式を利用し、認証結果や添付ファイルの有無などに応じて、配送や注意喚起文言の挿入、破棄などを行うことができること。 イ 受信した実績のない外部アドレスからメールを受信した場合にはじめて受信するアドレスであることをメール本文中に挿入し注意喚起を行うことができること。 ウ 返信等の送信した実績のない外部アドレスから添付ファイル付きのメールを受信した場合に、返信等の送信した実績のないアドレスであることをメール本文中に挿入し注意喚起を行うことができること。 エ 特定の IP アドレスやドメインメールアドレスから送信されるメールは、迷惑メールに分類されないようにホワイトリストとして管理できること。なお、リストは 5000 件の登録できること。及び、ユーザごとにホワイトリストを分割管理できること。 オ 送信メールサーバから受信メールサーバまでのメールの配送経路の通信を暗号化できること。 カ 相手サーバが TLS をサポートしていない場合には平文で送信することができること。さらに、相手サーバが TLS サポートを応答したにもかかわらず、相手の暗号スイートが古かったり、証明書が失効していたり、TLS のバージョンが古い場合にも、平文で配送し再送を繰り返したり配送不能にならないようにすることができること。 キ 特定のサーバ間の通信は暗号化を強制できること。 ク 社外からの特定の拡張子、ファイル種別が添付されたメールの受信を制限することができること。 ケ フリーメールから送信されたメールでメールアドレスのフレーズ部分の偽装対策として、Subject に### freemail ### のような文字列を挿入で

	きること。 コ　フリーアドレスからのメールなど特定のフィルタリング条件に合致するメールについて添付ファイルを PDF 化することでマクロやスクリプトを除去し攻撃を無効化できること。 (2)出口対策(誤送信防止)機能 ア　To、Cc に 10 件以上の宛先が含まれる場合、Bcc に変換して送信することでメール送信先間での送信先メールアドレスの漏洩を防ぐことができること。 イ　過去にやりとりのあるアドレスに、PW で保護されていないファイルが添付された場合、メール本文及び添付ファイルに指定するキーワード(秘密、機密、取扱注意等)が含有していないか判定できること。 ウ　上記でキーワードが含有していると判定した場合には、メールの送信を保留停止できること。 エ　上記でキーワードが含有していると判定した場合には、本文に以下のような内容を記載し、送信者に送信再確認のメールを返送できること。 (ア)　機密情報が含まれると判定され、PW 保護がないために差し戻された旨を記載 (イ)　送信先のアドレスのリストと宛先に間違いがないか確認を促す文言 オ　過去にやりとりのないアドレスに、PW で保護されていない添付ファイルが付与されているか検知ができること。 カ　上記で検知がされた場合には、メールの送信を保留停止できること。 キ　上記で検知がされた場合には、本文に以下のような内容を記載し、送信者に送信再確認のメールを返送できること。 (3)性能要件 ア　入口対策及び出口対策を考慮したうえで、下記スループットを満たすこと。 PDF 変換:メールサイズ 150KB で平均処理通数 80 通/sec その他機能:メールサイズ 150KB で平均処理通数 3000 通/sec (4)機能要件 ア　ウイルス検知や承認依頼メールなどの通知メールでは、日本語・英語やその他言語を併記することができるなど自由に文面を定義できること。 イ　ログによる監査が行えるよう、メールタイトル、添付ファイル名、添付ファイルサイズのログが出力できること。 ウ　組み込んだルールにどのくらいのメールが該当したかの有効性確認ができること。特定のフィルタリング事象発生時に個別のタグをつけたログを残すことで監査を容易に実施できること。 エ　新たに見つかったウイルスのパターンファイルが対応前に過去に内部に配送されていないかを確認できること。(ログに添付ファイルのハッシュコードを出力しておくことなどにより、確認できる手段を提供すること。) オ　フィルタ対象者(学生以外)が以下の前提条件に合致するメール送信を行った場合、メール送信を一時保留し、配送／破棄の判断を要求する通知メールを送信者に送信する。送信者が、通知メール本文にある承認 URL または否認 URL の何れかをクリックすることにより、保留メールの配送・破棄が実行される。※URL をクリックすると、WEB ブラウザ(HTTP or HTTPS)にて承認結果を表示する。 ※メール保留時間の既定値は 24 時間とし、時間経過後は自動破棄とする。 ＜前提条件＞ ・送信履歴なし／添付ファイルあり／添付ファイルのパスワードなし ・送信履歴あり／添付ファイルあり／添付ファイルのパスワードなし／機密情報あり カ　送受信履歴を 450 日保持する。 キ　HTML 形式のメール本文に含まれる画像や図表は添付ファイルと見

	做さないようにする。 ク　特定の内部ユーザアドレス(FROM)によるメール送信時、TO 及び CC に含まれるアドレスを BCC に自動変換処理しない条件動作を追加する。特定の内部ユーザは新規のアドレスリストで管理し、このリストのアドレスと合致する場合は BCC 自動変換処理を行わない。 ケ　外部アドレスから添付ファイル付メールを受信した場合、添付ファイルを Box に格納し、メール本文と通知メールを併せて 1 通のメールとして 利用者に送信する。 コ　FROMアドレスとTOアドレスの組み合わせ指定により、出口対策機能の適用を除外するホワイトリスト登録ができること。 サ　バックスキャッター対策として、AD 上に存在しないユーザを宛先としたメールは Reject すること。 シ　Bounce メールは、Bounce サーバを経由して送信すること。 ス　外部へのメール送信時に DKIM 署名を付与すること。 セ　送信時 DMARC 認証を実装すること。
その他	システム全般に関わる基本要求に準拠すること。

8.3 Bounce 対策サーバ

bounce メールの送信元アドレスは、NDR スパム等の影響により、外部サイトにおいてスパム判定スコア等が低下しブラックリスト入りする可能性がある。
このリスクの軽減策として、メールセキュリティ対策サーバの IP アドレスとは別の送信元として Bounce メール送出を行わせるためのサーバを別途構築する。

要求事項	要求仕様
数量	1 式
ハードウェア	(1)仮想基盤上に構築し、CPU 4Core 以上、メモリ 8GB 以上、HDD 100GB 以上を割当てること。 (2)Redhat Enterprise Linux v9 相当以上を導入すること。
ソフトウェア及び制約条件	(1)メールセキュリティ対策サーバからの bounce メールの送信を行うこと。 (2)運用中の IP アドレスが、外部でスパム判定を受ける等により運用に影響が出た場合、IP アドレスの変更が可能であること。
その他	システム全般に関わる基本要求に準拠すること。

8.4 ファイル配信サーバ

メールセキュリティ対策サーバで添付ファイルの連携先として利用するため、また、学外のユーザとのファイルのやり取りを行うため、https でファイル共有を行うサーバを構築する。

要求事項	要求仕様
数量	1 式
ハードウェア	(1)仮想基盤上に構築し、CPU 4Core 以上、メモリ 6GB 以上、HDD 100GB 以上を割当てること。 (2)Redhat Enterprise Linux v9 相当以上を導入すること。 (3)ファイル保存用領域として、1TB の領域を確保すること。
ソフトウェア及び制約条件	(1)Proself および Proself MailProxy オプションを導入すること。 (2)AD サーバと連携しユーザ認証が行えること。 (3)メールセキュリティ対策サーバと添付ファイル処理の連携を行うこと。
その他	システム全般に関わる基本要求に準拠すること。

9. 事務ネットワーク

事務ネットワークは教務システムや財務会計システムなどのシステムが接続され、主に事務職員が利用するものである。個人情報や非公開情報など機密性の高いデータを扱うことから、より高いセキュリティが要求され、他のネットワークとは物理的又は論理的に分離されている必要がある。

表 8-1 に事務ネットワークの必要な場所を示す。

表 8-1 事務ネットワークの必要な拠点

NO	拠点	場所	既設/新設	部署
1	八景キャンパス	本校舎 2 階	既設	総務部
2		本校舎 1 階	既設	研究推進部、グローバル推進
3		YCU スクエア	既設	教育推進課、アドミッション課
4		学術情報センター	既設	学術情報課
5		総研棟 1 階	既設	施設、ICT 推進
6	センター病院	研究棟 4 階	既設	診療情報管理担当
7		救急棟 5 階	既設	システム担当、診療情報管理担当
8		本館 5 階	既設	安全管理室、庶務担当、人事担当、労務担当、施設担当、経営企画担当、DPC 担当、物品管理担当
9		本館 3 階	既設	臨床試験管理室、臨床工学担当、地域連携担当、医療相談支援担当
10		本館 1 階	既設	医事管理担当、医事請求担当
11	附属病院	附属 4 階	既設	統括部、安全、システム、情報センター、看護部
12		附属 3 階	既設	CRC
13		附属 2 階	既設	医事課、地域連携・福祉相談など患者サポートセンター
14	福浦キャンパス	B 棟 2 階	既設	福浦学務
15		実習棟 2 階	既設	シミュレーションセンター
16		医学情報センター	既設	医学情報担当
17		先端研 4 階	既設	臨床試験管理室（治験）
18		先端研 5 階	既設	先端研
19		研修棟	既設	臨床研修センター
20		看護棟 2 階	既設	研究・産学連携推進
21		オープンイノベーションラボ	既設	臨床研究推進
22	鶴見キャンパス	鶴見	既設	鶴見キャンパス担当
23	舞岡キャンパス	舞岡	既設	舞岡キャンパス担当
24	みなとみらい	ランドマークタワー	新設	みなとみらいキャンパス担当

9.1 事務ネットワーク構成

事務ネットワークとして下記の機器の更新に必要な作業を行うこと。

また、現行の拠点設置 VPN 用対応ルータは撤廃したうえで、教研ネットワークと事務ネットワークを論理的に分割した構成を実現させること。

また、SINET L2VPN 接続サービスを利用し、外部のクラウドサービスを事務ネットワークとして利用できること。

9.2 レイヤ 3 スイッチ

(1) レイヤ3スイッチ機能として Static、RIP v1/v2、OSPF v2 をサポートすること。

(2) L2 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、L2 ループ防止機能を有すること。

(3) 障害発生時の迅速な復旧の為、外部メディア（コンパクトフラッシュ、USB メモリ、SD カード）に構成定義情報 、ファームウェア、ログを保存可能であること。

(4) スイッチのポート間でアクセス制限（通信の許可または禁止）を設定できること。

(5) 業務アプリケーション(プロトコル)単位でのグループ化が可能なプロトコル VLAN 機能を有すること。
(6) 冗長電源機能を有すること。
(7) 拡張スロット(10G×2 対応可)を 1 つ以上有すること。
(8) 10/100/1000BASE-T ポートを 24 個 以上有すること。うち 4 ポートは排他利用で 1000BASE-SX / LX ポートとしても利用可能なこと。
(9) スイッチ容量は 88Gbps 以上を有すること。
(10) DHCP リレー機能を有すること。
(11) MAC アドレス登録数は 16,000 以上可能であること。
(12) 時刻同期ができること。
(13) SNMP エージェント機能を利用できること。その際、SNMPv1/v2c/v3 を利用すること。
(14) IEEE802.1Q タグ VLAN 機能を有すること。
(15) RoHS 指令対応製品であること。
(16) Virtual Routing and Forwarding 機能を持つこと。

9.3 レイヤ２スイッチ

(1) レイヤ2スイッチ機能を有すること。
(2) L2 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、L2 ループ防止機能を有すること。
(3) スイッチのポート間でアクセス制限(通信の許可または禁止)を設定できること。
(4) 10/100/1000BASE-T ポートを 24 以上有し、スイッチ容量は 48Gbps 以上を有すること。
(5) 八景キャンパス YCU スクエアは、10/100/1000BASE-T 48 ポート以上を 4 台用意すること。スイッチ容量は 56Gbps 以上有すること。24 ポートスイッチは、1000BASE-SX 1 ポートを 1 台有すること。
(6) 八景キャンパス総合研究教育棟(サーバ室)は、1000BASE-SX 3 ポートを 1 台、1000BASE-SX 1 ポートを 1 台有すること。残り 1 台は 1000BASE-SX は不要。
(7) 八景キャンパス学術情報センターは、1000BASE-SX 1 ポートを 1 台有すること。
(8) MAC アドレス登録数は 8,000 以上可能であること。
(9) 時刻同期ができること。
(10) SNMP エージェント機能を利用できること。その際、SNMPv1/v2c/v3 を利用すること。
(11) IEEE802.1Q タグ VLAN 機能を有すること。
(12) RoHS 指令対応製品であること。

9.4 ＷＩＮＳ／ＡＤサーバ

要求事項	要求仕様
数量	2式
ハードウェア	(1) 仮想基盤上に構築し、CPU 2Core 以上、メモリ4GB 以上、HDD100GB 以上を割当てること。 (2) Windows2025 Server 相当
ソフトウェア及び制約条件	アカウント管理機能として、CSV形式のファイルに記述されたアカウント情報を一括でActive Directory へ反映し、CSV ファイルを編集することにより、アカウントの一括更新、削除を行うことが可能な機能を有すること。その際のアカウント数は500以上を管理できること。もしくは、基幹ネットワークシステムの認証サーバと連携できる仕組みにすること。
その他	システム全般に関わる基本要求に準拠すること。

9.5 管理用 PC

管理用 PC として下記の機能を提供できるノート型 PC を 2 台用意すること。

(1) CPU として Intel 社製 Core™ i5-1334U 以上を 1 つ以上有すること。
(2) メインメモリを 16GB 以上有すること。
(3) 物理容量が 500GB 以上の HDD を1つ以上有すること。
(4) 14 型液晶(解像度 1366×768 以上)を有すること。
(5) USB2.0/3.0 ポートを 4 つ以上有すること。
(6) 1000BASE-T/100BASE-TX/10BASE-T 自動認識ポートを 1 ポート以上有すること。
(7) OS は Microsoft 社製 Windows 11 Pro(64 ビット) 日本語版相当以上であること。
(8) Microsoft 社製 Office 2024 Professional 相当以上を有すること。

9.6 無線 LAN(事務)

(1) 教研ネットワーク用の SSID とは別に事務ネットワーク用の SSID を新設すること。
(2) AP 毎に SSID のステルス ON,OFF を設定できること。

10. ランサムウェア対策

DC 内の WindowsServer および保守端末はランサムウェア対策を実施すること。

(1) 全く未知の攻撃手法のマルウェア対策として効果が期待できること。

(2) マルウェアの検知・駆除をするのではなく、感染させないあるいは OS が破壊されることを防ぐ機能を有すること。

(3) シグニチャが不要であり、可能な限り、定義ファイルや AI エンジンのようなものに対するアップデート処理がなく、高頻度のフルスキャンが不要である運用を継続して行えること。

(4) マルウェアが自動実行される前、ファイルレスマルウェアなどでスクリプトが動いても、OS のコア設定（OS のプロセスやメモリ、レジストリレジストリ）への改ざん行為を阻止する機能を有すること。

(5) Microsoft Defender と併用し、且つシステム上干渉せずに共存できること。

11. 運用支援

11.1 導入時における運用支援

新システムの稼動直後の安定稼動を目的とし、令和 8 年 10 月を予定している基幹ネットワークシステムのサービスインの際、受託者は専任要員を以下のように確保し、本調達に含めて支援を実施すること。

(1) 利用者のサポートのため、サービスイン前の2週間を準備期間としてその間の準備作業、サービスイン後の1か月間を運用開始期間として運用支援を行うための常駐員を配備すること。その場所は八景キャンパスとは限らず、他のキャンパスや病院も想定すること。運用支援期間中は、発生する問い合わせに対して最低同時に3件は対応できる体制としておくこと。

(2) 現在本学の運用支援を行っている業者とは令和8年 9 月 30 日までの契約期間となっている。先行導入する教育実習室システムについては、既存システムと連携する必要があることから、安定稼働するまでの 1 ヵ月を目途に既存業者と連携し運用支援を行うこと。

(3) 新システムに移行する際、利用者が用いる端末の MAC アドレスの登録や設定変更が必要となる場合には、問い合わせや不具合対応、利用者に対する現地での作業支援を実施できるようにすること。

(4) 必要に応じて利用者向けのマニュアル作成及び改訂を行うこと。

(5) 作業範囲は以下を基本とし、詳細な対応方法については、サービスインの前に本学と受託者の間で別途協議する。

ア 利用者端末の MAC アドレス登録支援
イ 利用者端末の有線及び無線ネットワーク接続支援
ウ 事務ネットワーク接続用端末の資産管理エージェントのインストール及び設定支援
エ 事務ネットワーク接続者のファイルサーバ接続支援
オ 利用者端末設定変更、MAC アドレス登録の進捗状況等の管理者への報告
カ プリンタや部門で購入した NAS などの設定変更支援

11.2 システム運用

11.2.1 システム運用管理委託範囲

本学及びデータセンターを対象とし、基幹ネットワークシステムの運用管理を委託する。

本学の情報システム部門は、情報システム全体の技術調整役として、業務システムや部門ネットワークシステムを含めた全体最適を考慮し、運用することを業務としている。受託者は本学既設 LAN や、業務システム・部門ネットワークシステムとの連携について熟知したうえで情報の提供・支援を実施できること。

11.2.2 運用管理・オペレーション

(1) 基幹ネットワーク配下にあるネットワーク機器、サーバ機器、通信回線の運用監視・障害対応。※

(2) 今回導入するネットワーク機器、サーバ機器の本学からの依頼に基づく設定変更。※

(3) システムの監視による評価・改善の提案。

(4) 定期処理(データバックアップや利用状況のレポート作成等)の実施及びその支援。

(5) 端末・プリンタのメンテナンス(パッチ適用、アップデート、アプリケーションの追加インストール、検証作業)。

(6) 業務システム・部門ネットワークシステムとの調整の支援等。

※一部無線 LAN アクセスポイントについては、既存の装置を残している。それらも運用管理の範囲に含める。

11.2.3 システム運用管理方針

(1) 基幹ネットワークシステムは、24 時間、365 日稼動するものとして運用すること。

(2) ハードウェア障害へは 24 時間 365 日対応すること。
(3) サーバ機器については、データのバックアップを定期的、自動的に実施され、スケジュールは任意に設定できること。
(4) システム管理ツール等の利用により、容易に稼働状況を把握・監視ができるようにすること。
(5) 本学計画停電時の本学内に設置した機器のシステム停止対応（金沢八景 1 回、福浦 1 回の計 2 回/年。 PC、プリンタは対象外）を行うこと。
(6) ネットワークリソース、サーバリソースの利用状況を常に監視し、異常があれば本学と協議のうえ対処すること。また、本学の要求に応じて変更作業を行うこと。
(7) 学内外からの不正アクセスを監視し、異常があれば本学と協議のうえ対処すること。
(8) 運用に関する本学から問い合わせ、相談に対し、迅速に対応すること。
(9) 故意か否かに関わらず、受託者の作業の結果によって障害や不具合を生じさせ、それにより本学への影響が生じた場合、その復旧に向けて事情を問わず最優先に対応すること。本件がなければ生じなかった本学職員の作業負担分については受託者が補填することを想定し、本番環境の操作を行う場合は慎重かつ万全を期すこと。

11.2.4 システムの評価・改善の提案

(1) システムの構成や利用状況・負荷状況などを評価し、改善へ向けた提案を行うこと。
(2) 本学の情報基盤として全体最適を考慮し、業務システム・部門ネットワークシステムとの調整支援として、助言・提案を行うこと。また、今後のシステム導入などにおいても、積極的に助言・提案を行うこと。
(3) 今後、Microsoft365 や OneDrive と連携して独自システムを構築する可能性があり、Microsoft 社のクラウドサービスと本学システムの構成を十分把握して、的確な提案を行えること。

11.2.5 管理の省力化への考慮

(1) システムの運転は、バッチ処理、バックアップ処理等、原則、自動化する。
(2) システムは自動監視を行う。運転状況を自動監視し、障害や監視閾値異常の際は管理者等へメール連絡する仕組みを考慮すること。
(3) 安全を配慮した仕組みでのリモートメンテナンスにより、効率的な管理が実施できること。

11.3 保守

11.3.1 保守体制

(1) 保守要員（サポート要員）及びその統括責任者を確保すること。常駐かリモートでの対応とするかは問わないが、その責任者又は担当者が、隔週に1回以上は本学を訪問し、保守・運用に関わる業務を実施すること。詳細な内容については本学と協議のうえ決定すること。
(2) 保守要員（サポート要員）は、情報処理技術者試験「テクニカルエンジニア（システム管理）」相当以上のスキル、又は5年以上の実務経験を有していること。
(3) 保守要員はその責任・必要に応じて、直接、エンドユーザ対応を行い、結果を本学の管理者に報告すること。
(4) 保守サポート体制の範囲は、今回導入した製品と、既存の無線アクセスポイント及び福浦キャンパスオープンイノベーションラボの機器を範囲とする。本学既設 LAN との連携について熟知し、情報の提供・支援が行えること。
(5) 保守対応時間は原則として祝日、年末年始などを除き月曜日から金曜日の 8:30 から 17:30 までとする。ただし、予め週末や祝日などに行うイベントや、緊急性の高いメンテナンス適用の必要性などにより、教職員や学生に影響を生じさせない必要がある作業については、別途本学と協議のうえ、それ以外の時間でも対応すること。
(6) 支援体制図・人員体制表を提出し、本学へのサポート体制を明確にすること。
(7) 保守サポートの作業内容の詳細は、契約後に本学と協議のうえ決定すること。

11.3.2　基幹ネットワークシステム管理

(1) システムの稼働監視及び、セキュリティ対策を実施すること。
(2) 定期的なシステムバックアップ業務を実施すること。
(3) 施設拡張におけるネットワーク整備、及びその支援を実施すること。
(4) 本学からの要求により、DNS の登録作業を実施すること。
(5) 本学からの要求により、ファイアウォール制限解除設定を実施すること。
(6) 本学からの要求により、技術情報を提供すること。
(7) 本学からの要求により、リモートアクセスシステムへの追加設定を実施すること。(年 2 回を想定)
(8) 新バージョンのOSがリリースされた等の理由によりKMSのバージョンアップを必要に応じて実施すること。

11.3.3　ハードウェア保守

(1) ハードウェアの定期的なメンテナンスを実施すること。
(2) ハードウェア障害に伴い、システムの復旧が必要な場合、速やかに対応すること。
(3) 障害発生時、即時解決が出来ない場合、代替機を用意すること。
(4) 実習室については、端末の点検(ファンが回っているか等)及び清掃(ホコリ取等)を年1回以上行うこと。
(5) 定期的なメンテナンス時にハードウェア障害の発生が予測された場合は速やかに部品を交換し、障害予防対策を講じること。
(6) ハードウェアの使用状況を常時監視し、ハードウェアの障害発生予測及びディスク装置などの容量不足などを事前に把握し、計画的な資源プロビジョニングが実施可能であること。
(7) 保守時に機器を本学から搬出する場合には、代替機器を用意して、保守期間中もシステムの稼働を中断しないようにすること。
(8) 導入した製品のメーカーを問わず、すべての製品についてアフターサービス、定期点検、保守等に責任をもって対応すること。
(9) UPS、RAID コントローラのバッテリ交換は運用保守契約の中で実施すること。

11.3.4　障害対応

(1) 各部署における機器の障害時復旧作業の実施及び電話対応を実施すること。
(2) 障害発生時には、必要に応じて保守員を派遣し対応すること。
(3) 障害状況を整理し本学へ報告を行い、協議のうえ対策を講ずること。特に、受託者の作業の結果として生じたと想定される不具合や障害については、一刻も早く対応すること。
(4) 障害対応後、障害の発生時間や原因、対応作業、今後の予防措置などをまとめて、報告書として本学に提出すること。その原因が、受託者内のコミュニケーション・連携不足など人為的な要因にあると考えられる場合には、具体的にそれをどう是正するのかを必ず社内で協議のうえ、本学に再発防止策を示すこと。

11.3.5　ネットワーク機器の保守管理

(1) ネットワーク機器のチェックランプの点検やツールによる応答チェックなどを実施すること。
(2) 障害時におけるログの採取及び解析を実施すること。

11.3.6　ヘルプデスクサポート

(1) 本学のヘルプデスクと連携し、障害対応を行うこと。

(2) 本学のヘルプデスクからの要望がある場合、調達範囲外でも障害の一次切分け作業のサポートを行うこと。

11.4 運用

11.4.1 電源管理

(1) 基幹ネットワークシステムを構成する本学キャンパス内に設置してある機器及びシステムは、無停電電源装置に接続されること。
(2) 停電が一定時間を超えた場合には無停電電源装置から通知を受け、システムを正常かつ自動的に停止させる機能を有すること。ただし、通信機器については、この限りではない。
(3) 電力が復旧した際には、機器をもとの稼働状態に戻し、停電前の状態に戻ったことを確認すること。

11.4.2 構成管理

(1) サーバ及びハードウェア資源の利用状況や負荷情報の監視及び評価を行い、必要に応じてサーバの機能変更などの改善提案とその実施を行うこと。
(2) ソフトウェアのセキュリティ上の脅威が発見された場合は、本学と協議のうえ、早急に対応すること。
(3) 導入したソフトウェアのバージョンアップや新たなソフトウェアの導入による実習室等のユーザ端末群の環境再構築を、本学と協議のうえ、年 2 回程度実施すること。
(4) 運用手引書・システム構成図・ネットワーク構成図・ハードウェア／ソフトウェア一覧表などを作成し、常に最新構成を把握していること。

11.4.3 運用監視

(1) 基幹ネットワークシステムを構成する全ての機器及びシステムの運用状況を、本学が必要に応じて即時に把握できる環境を用意するとともに、受託者も同じ状況の把握が可能であること。
(2) また、定常運用時に発生した障害等について、即時に通報または通知が可能であること。

11.4.4 障害対策

(1) 受注者が設置する機器管理サーバにより、導入機器の障害情報を自動収集可能なこと。
(2) 重要障害が発生した場合、本学と協議のうえ、対策を講じること。
(3) 基幹ネットワークシステムを構成する機器のバックアップ、リストアを簡易な手順にて実施可能であること。
(4) バックアップ及びリストアの実現方法については問わない。なお、バックアップ不能な場合は、障害復旧手段を別途定めること。

11.4.5 セキュリティ監視

(1) ネットワークへの不正なアクセスを 24 時間監視し、不正なアクセスを検知した場合は、本学のシステム管理者に連絡すること。
(2) 学内外からの不正アクセスまたは重大なセキュリティ侵害事象を発見した場合には、発生場所を速やかに特定すること。
(3) 本学のネットワークに接続した端末の不正な動作を検知した場合には、その端末の IP アドレス、利用者を特定し、本学の管理者に通知し、対応を協議すること。
(4) 監視結果は監視報告書として取り纏めを行い、月次報告書として本学のシステム管理者に提出すること。
(5) 監視に必要なハードウェア、ソフトウェアを用意すること。

11.4.6　運用支援

(1) 安定した運用を維持するため、本学を会場とし、月1回の定期的な会議を開催すること。会議での協議事項等について報告書を作成し提出すること。
(2) 問い合わせ内容・受付日時・回答内容・対応状況等に関する作業記録を一元的に管理し、情報共有できるシステムを提供すること。
(3) システム作業実施のために作業手順書を作成し、実施承認及び実施確認を本学から受けること。
(4) 本学の運用に必要なシステムの開発、性能・機能向上に伴う作業、プログラムの移植及び機器の接続に関し、必要な技術情報を提供し、作業の支援を行うこと。
(5) システムの円滑な運用と有効利用を図るため、本調達システムに関して、システム管理者等に必要な講習を実施すること。
(6) ソフトウェアなどシステムの利用にあたっての重要な変更がなされる場合は、利用者向け説明会・講習会を行うこと。開催内容、時期については、本学と協議のうえ決定すること。
(7) 説明会・講習会は、利用者向けに同一内容で2回開催すること。
(8) 本学としての信用・信頼が失墜しかねないセキュリティ事故が生じた場合は、本学と受託者で別途協議のうえ、本学からの要請後連続する最大 5 日間は、この優先的対応を行うこと。

11.4.7　運用マニュアル

システムの運用やユーザサービスのため、製造元から供給されるハードウェア・ソフトウェアのマニュアルのほか、運用または操作に必要なマニュアルを作成・提供すること。

11.4.8　ハードウェア及びソフトウェアマニュアル

本学に提供するマニュアルはすべて日本語とする。日本語版のマニュアルがない場合には英語版に替えてもよいが、適切な日本語の参考文献を必要数納めること。

11.4.9　管理者・利用者用マニュアル

(1) 管理運用や一般的な利用に必要なマニュアルを作成し提供すること。
(2) 同マニュアルは一般的な形式のデータファイルで提供すること。
(3) 同ファイルは管理者及び利用者の便宜を図るため、本学で加筆・修正・印刷・配付することを認めること。

11.4.10　作業記録

(1) 障害対応や QA 対応等の対応事項は全て記録し、対応状況を管理すること。対応内容は原因等により適切に分類し、増減の傾向等がわかるようにして報告すること。
(2) 障害対応や QA 対応等の対応事項の記録を蓄積・分析し、運用管理のための対応作業を体系的に整理すること。
(3) 作業手引書(対応手順書)を作成し、特に定常的に発生する QA 対応などについては、対応マニュアルを作成すること。
(4) 重要障害については、本学の要請に応じて、過去に遡って報告書を速やかに提出できるようにしておくこと。