平成 31年度

滋賀県立大学
情報ネットワークシステム借入

要求仕様書

平成 31 年 3 月

公立大学法人滋賀県立大学

-目次-

添付資料

別紙 1	現行 SPINS 構成
別紙 2	次期 SPINS 構成案
別紙 3	エッジスイッチ仕様
別紙 4	アクセスポイントの設置位置（既存）
別紙 5	アクセスポイントの設置位置（新規）
別紙 6	syslog の転送元一覧（既存）
別紙 7	死活監視対象機器（新規）

1. 調達の概要

1.1 調達の背景および目的

滋賀県立大学情報ネットワークシステム（以下「SPINS」という。）は、本学教員および学生の学術研究のための情報交換・情報検索や外部機関と連携した教育・研究に資する活動のほか、e-learning 等の学内外に向けたインターネットサービスの充実に役立てられ、教職員の日常業務のためになくてはならないシステムである。今回 SPINS のリース満了に伴い、各種ネットワーク関連機器の更改を行い、現行のシステムから一層の利便性・安全性を向上させるとともに、将来を見据えた構内通信システムの構築や他教育機関との認証機能連携のほか、大学業務の継続に必要となる重要データの外部保存等をあわせて行うものである。

1.2 調達の基本方針

SPINS 既存システムの更新および新規システムの導入にあたり、必要となる全ての作業やライセンス、更新後の保守ならびにサポート業務が本調達に含まれる。既存システムの更新部分にあっては、これまでの SPINS で提供されてきたサービスが維持できるようにするとともに、後述の要求仕様を満たすシステムを構築すること。新規システムの部分については、既存システムと協調し、矛盾することなく動作するように設計すること。

1.3 SPINSの概要

1.3.1 全体の構成

現状の SPINS の構成は以下の通りである（別紙1を参照のこと）。学内 LAN は大きく以下の3つの接続部で構成される。主に外部のインターネット接続を担う「学外接続部」、各学部棟と A5 棟を結び学内通信を制御する「学内接続部」、各演習室間を結び演習室内通信を制御する「演習室接続部」である。

学内接続部には事務棟を中心に各事務室を結ぶ「事務ネットワーク」がある。学外接続部と学内接続部には、利用者がネットワークを円滑・安全に利用出来るようにするための「内部サーバ」が設置されている。これら学外接続部・学内接続部・演習室接続部の機器を円滑に運用管理する為の「運用支援設備」が設置されている。これらの機器のうち、特に重要な役割を担う機器については、「無停電電源装置」を設置する事により電気的障害から保護し、瞬間的な停電が発生しても継続して使用できるようにしている。

1.3.2 学外接続部

外部インターネットへの接続経路としては、SINET と商用インターネットの 2 つが存在する。 各ネットワークへは対外接続ルータである「SINET 接続ルータ」と「商用インターネット接続ルータ」を介して接続されており、静的な経路設定のみ用いて通信経路を決めている。また、各対外接続用ルータにはアクセス制御が設定されており、インターネットから学内ネットワークへの通信を制限している。

各対外接続用ルータの配下には、本調達の対象外で、CAI システム更新時に導入された不正侵入防御装置、本調達の対象となる帯域制御装置、回線負荷分散装置、ファイアウォール、L7 スイッチが接続されている。また、帯域制御装置と回線負荷分散装置、回線負荷分散装置とファイアウォール、ファイアウォールと L7 スイッチ間には冗長化用スイッチが接続されている。

不正侵入防御装置は、学外からの不正侵入防御のほか、学内からの情報漏えいを防止している。

帯域制御装置は、SINET および商用インターネット向け通信の帯域量を制限している。

回線負荷分散装置は、SINET および商用インターネットの両接続回線をマルチホーム化し、効率的な回線使用や回線に障害が発生した場合に互いに有効活用できる設定を行っている。

ファイアウォールは、SINET および商用インターネット、DMZ、トラストネットワークを分離している。(以下、DMZ は「SINET DMZ」および「商用 DMZ」、トラストネットワークは「全学ネットワーク」および「演習室ネットワーク」という。)

DMZ に繋がるサーバについてポート数が不足しているため L2 スイッチ(以下、「DMZ スイッチ」)を導入している。なお、ファイアウォールには侵入検知・防御をするための IPS 機能があり、それぞれの DMZ およびトラストネットワークへの不正侵入を防いでいる。また、ファイアウォールの脅威についてレポーティングするファイアウォールレポーティングサーバを導入している。

L7 スイッチは、SINET および商用インターネット向けの WEB 通信がプロキシサーバを経由するよう設定している。

さらに、SINET 接続ルータには、「財務会計システム」と「学務事務管理システム」が接続されている。

1.3.3 学内接続部

全学ネットワークは、L3 スイッチ(以下「全学コアスイッチ」という。)配下に接続される。全学コアスイッチは 1 台で機器の内部機能が冗長化されている。全学コアスイッチから光ファイバケーブルを用いて、各学部の L2 スイッチ(以下「学部コアスイッチ」という。)および内部サーバが接続する L2 スイッチ(以下「全学サーバスイッチ」)に接続される。全学サーバスイッチは 2 台で機器が冗長化されている。全学サーバスイッチから全学コアスイッチまでの配線は冗長化されており、通常時は負荷分散を行うが、障害発生時には片側の回線を使用して通信の確保を行っている。

各学部コアスイッチから各学部棟に設置される L2 スイッチ(以下「エッジスイッチ」という。)へ接続され、エッジスイッチから各室への配線がされている。ポート数の不足や配線先が遠方にある場合は、さらに L2 スイッチ(以下「支線スイッチ」という。)を介して各室への配線がされている。学部コアスイッチからエッジスイッチまでの配線は距離に応じて光ファイバもしくはメタルケーブルが使用されている。

講義棟・工学部・人間文化学部・事務局の一部や、図書情報センター、学生ホール、交流センター、食堂の一部には無線 LAN 設備が導入されている。無線 LAN は、複数のアクセスポイントを集中管理する無線 LAN コントローラ(以下「WLC」という。)および無線 LAN 運用管理装置を導入し

ており、アクセスポイントの管理は全て WLC にて行っている。WLC は冗長化構成を取っており、1 台が故障しても全ての無線 LAN を利用できるようにしている。

無線 LAN 運用管理装置はアクセスポイントの情報から電波の干渉状況を可視化することができるシステムである。1 台構成であり、故障した場合は利用できなくなる。

無線 LAN を利用する際には、事前登録された MAC アドレスのみ通信を許可する無線 LAN(「無線 MAC 認証」)と、利用の度に利用者がユーザ名とパスワードを入力して通信を許可する無線 LAN(以下「WEB 認証」という。)、証明書を利用した無線 LAN(以下「IEEE802.1x 認証」という。)がある。これらの認証を提供する認証システム(以下「Radius サーバ」という。)が導入されている。Radius サーバは冗長化構成を取っており、1 台が故障しても認証サービスを継続できるようにしている。一部の無線 LAN は WEB 認証、IEEE802.1X 認証の他に、PSK(事前共有鍵)認証を用いている箇所も存在する。

1.3.4 演習室接続部

演習室ネットワークは、ファイアウォールおよび全学サーバスイッチに収容され、その後 L3 スイッチ(以下「演習室コアスイッチ」という。)に接続される。演習室コアスイッチから L2 スイッチ(以下、「演習室スイッチ」および「演習室サーバスイッチ」という。)へ接続され、演習室スイッチから演習室の各機器に配線されている。

1.3.5 事務ネットワーク

事務ネットワークは、A5 棟学部コアスイッチ配下の A0 棟(以下、「事務棟」という。)エッジスイッチおよび支線スイッチを中心に構成されている。各学部の事務室は、ファイルサーバ等の資源を利用する為に全学ネットワークを経由して事務棟のネットワークへアクセスしている。

1.3.6 内部サーバ

現在はクライアントのプロキシ機能を提供するプロキシサーバを導入している。プロキシサーバは冗長構成を取っており 1 台が故障してもサービスの継続が可能となっている。プロキシサーバは WEB フィルタリング機能を提供しており、フィッシングサイトなどへのアクセスをブロックする機能を提供している。

また、クライアントからの要求に応じて IP アドレスを払い出す DHCP サーバを導入している。DHCP サーバは冗長構成を取っており 1 台が故障してもサービスの継続が可能となっている。IP アドレス情報の他に DNS サーバ設定情報をクライアントへ提供している。

スパム対策を実施するスパム対策システムを導入していたが、現在はクラウドサービスにて本機能を利用しているため、スパム対策システムは利用していない。

その他、様々な学内サービスを提供するサーバが接続されている。

1.3.7　運用支援設備

ネットワーク機器やサーバのログを集積するログサーバと、各種機器の状態を監視し、異常を発見した際にメールおよび警告灯で運用管理者へ通知するネットワーク監視装置が導入されている。これらは今回更新対象となる機器以外も監視対象としている。

ログサーバが収集したログは NAS にアーカイブを行い、過去に発生したインシデントに備える体制を構築している。

1.3.8　無停電電源装置

電気的障害から保護が必要な機器として、次の機器が無停電電源装置に接続されている。

- 対外接続ルータ
- 帯域制御装置
- 回線負荷分散装置
- ファイアウォール
- L7 スイッチ
- 全学コアスイッチ
- 学部コアスイッチ
- 全学サーバスイッチ
- 無線 LAN コントローラ
- 無線 LAN 運用管理装置
- スパム対策システム
- Radius サーバ
- DHCP サーバ
- プロキシサーバ
- ログ管理装置
- ネットワーク監視装置
- NAS

2. 構成の要件

本調達に係る構成の要件を以下に示す。これらの要求要件は最低限の要求であって、全ての項目を満たしたとしても、最低限の基準を満たしたことにしかならないことに注意すること。

2.1 全般

(1) リース期間は 2019 年 9 月 20 日から 2025 年 9 月 19 日までの 6 年間とすること。

(2) リース期間において、必要となる機器、ライセンス、保守サービスを提供すること。

(3) 今回想定している学内 LAN の構成を別紙 2 に示す。本仕様書において必要な機能を述べるので、その機能を満たす構成を、請負者が提示すること。

(4) 既存システム、機器に設定されている項目は、原則、新システム、機器に引き継げるよう設計を行うこと。引き継げない場合は、本学と協議し、適正な設定を行うこと。

(5) 更新対象となるのは学外接続部・学内接続部・内部サーバ・運用支援設備・無停電電源装置であるが、財務会計システム、学務事務管理システム、事務ネットワーク、演習室ネットワークなど本システムに接続するシステムに極力、変更が生じないよう設計すること。

(6) 現行システムを変更する必要がある部分については事前調査を実施し、変更が必要な箇所・意図等を記した資料を提示すること。また、その費用も含むこと。業者決定後、変更が必要な箇所等について、本学担当者の許可を得ること。

(7) 機器仕様は 1 台あたりに求める要件とする。

(8) Windows および Mac の OS(オペレーティングシステム)を利用してシステムを構築する場合、本学が所有する包括ライセンスより提供することが可能である。
(ソフトウェア名： Microsoft 社 System Center Endpoint Protection)

2.2 配線

(1) 原則、建屋間や建屋内については既存の LAN 配線(I3-CS、C7・A7 棟については CAT-6)および光ファイバケーブルの流用を前提とすること。

(2) 業者決定後、経年劣化により既設配線の交換が必要と判断される部分は、箇所等を記した資料を提示すること。当該箇所については、試験器等を用いて測定を行い、試験結果を提出すること。

(3) 業者決定後、機器更新等に伴い配線の追加・変更・新設が必要と判断される場合は、箇所・意図等を記した資料を提示すること。当該箇所については、試験器を用いて測定を行い、試験結果を提出すること。

2.3 学外接続部

ここでは別紙２に示す学外接続部において必要とされる機能要件のみを述べる。この機能要件を満たすような学外接続部の詳細な構成および設計は請負者の責任において行うこと。なお、ここで述べる機能要件を実現するために、必ずしもそれぞれの機能に応じ

た機器を個別に準備する必要はなく、複数の機能を集約した機器を用いても問題はない。

2.3.1　対外接続ルータ(2 台)

SINET および商用インターネット接続用ルータを各々1 台ずつ用意すること。

現在、SINET 回線の速度は 1Gbps、商用インターネット回線の速度は 500Mbps であるが、将来的に商用インターネットを 1Gbps に増速することも検討しているため、この点を考慮した機器を選定すること。

(1) 19 インチラックに搭載および固定が可能であること。
(2) 通信速度は最大 1Gbps 以上の転送性能であること。
(3) WAN 側インタフェースは 10/100/1000BASE-T のポートを 1 個以上有すること。
(4) LAN 側インタフェースは 10/100/1000BASE-T のポートを 8 個以上有すること。
(5) スタティックルーティング、ポリシーベースルーティング、RIPv1/v2、RIPng、OSPFv2、OSPFv3 機能を有すること。
(6) 2.8.4 項 BCP バックアップシステムに対して、通信の振り分けが可能なこと。

2.3.2　帯域制御装置

本システムはリプレースを必要とせず、既存機器を本学指定の場所に収集すること。

2.3.3　回線負荷分散装置(2 台)

本学では学外インターネットへの接続回線として SINET 回線と商用インターネット回線を用意している。これら 2 つの回線をマルチホーム化し、効率的な回線使用を行うとともに、回線障害によるネットワーク停止のリスク低減するために導入する。インバウンド通信、すなわち学内に設置される学外向けサーバ等に対する通信について、両回線の負荷状況を確認し、負荷の低い方に通信を振り分ける機能および一方の回線がダウンした場合、稼働している回線に通信を振り分ける機能を有すること。

(1) 19 インチラックに搭載および固定が可能であること。
(2) アプライアンス機器であること。
(3) 本学指定のサーバに対し、回線障害に備え、SINET 回線と商用インターネット回線の双方よりアクセスできること。
(4) NAT 機能を有すること。
(5) 2 台の冗長構成で導入し、1 台にハードウェア障害が発生した場合においても、ネットワークを停止させないような冗長構成とすること。
(6) 回線負荷分散方式として、セッション数に応じたロードバランスが可能なこと。
(7) 最大スループットが 7.5Gbps 以上であること。

(8) SFP スロットのポートを 4 個以上有すること。
(9) 現行の回線負荷分散装置に接続されている周辺システムを接続すること。
(10) SINET および商用インターネット回線障害を検知した際、トラップやメール等でシステム管理者に通知する機能を有すること。
(11) 本装置の更新前後で、負荷分散対象となる各学内システムの対外通信においてどのような変更および影響が生じるか提示すること。技術的根拠に基づき、詳細に検討されている場合は加点とする。

2.3.4 ファイアウォール(2 台)

ファイアウォールは2台にて冗長構成とし、外部(インターネット側)、内部(全学コア側)、DMZ セグメントを接続する。

最大同時接続クライアント数は 5000 程度を想定している。これらの負荷に耐えられるよう十分な性能を持った機器を選定すること。

(1) 19 インチラックに搭載および固定が可能であること。
(2) アプライアンス機器であること。
(3) Active-Standby の冗長構成が可能なこと。
(4) 1 台にハードウェア障害が発生した場合においても、ネットワークを停止させないような構成とすること。その際、片系に切替る為に別途機器が必要な場合は、併せて本調達内に含めること。
(5) 最大同時接続クライアント数が 5000 程度を想定している。これらの負荷に耐えられるよう十分な性能を持った機器を選定すること。
(6) IPsecVPN、SSLVPN 機能を有すること。
(7) アプリケーションの制御が可能であること。
(8) 各アプリケーションが占有する帯域利用率を出力するレポート機能を備えていること。
(9) アプリケーション制御機能を利用したファイアウォールの最大スループットが 5Gbps 以上であること。
(10) IPS 機能を利用した際の最大スループットが 2Gbps 以上であること。
(11) 10/100/1000BASE-T のポートを 12 個以上有すること。
(12) SFP スロットのポートを 4 個以上有すること。
(13) NAT 機能を有すること。
(14) IEEE802.1Q VLAN トランク機能を有すること。
(15) IEEE802.3ad リンクアグリゲーション機能を有すること。
(16) SSH によるリモート接続が可能であること。
(17) 2.8.3 項 ネットワーク監視サーバに対し、SNMP トラップの送信が可能なこと。
(18) 2.4.1 項 全学コアスイッチと 1Gbps×1 本以上で接続すること。

(19) 2.3.5 項 DMZ スイッチと 1Gbps×1 本以上で接続すること。
(20) その他、現行のファイアウォールに接続されている周辺システムを接続すること。
(21) ポリシールール毎に、ログの保存有無が設定可能であること。
(22) ISO/IEC15408(Common Criteria)の認定を取得していること。
(23) ファイアウォールの各種ログを蓄積し、そのログを元にレポートを作成する機能を有するサーバを導入する場合は加点とする。

2.3.4.1 不正侵入防御機能 (1.3.2 で説明する、更新対象外の「不正侵入防御装置」とは異なる)
(1) 2.3.4 項 ファイアウォールにて不正侵入防御機能を提供すること。
(2) 管理用 GUI にて本機能の設定が可能なこと。
(3) 管理用 GUI について、https にて接続が可能なこと。
(4) 不正侵入防御のシグネチャは時間、日毎に自動更新が可能なこと。
(5) P2P ソフトやインスタントメッセンジャーの遮断が可能なこと。
(6) 不正侵入と疑われるログをレポートする機能を有すること。
(7) 本機能の実現はファイアウォール以外の装置にて実現しても良いが、運用負荷および障害ポイントの軽減の観点から機器点数が増加することを回避するため、2.3.4 項 ファイアウォールにて同機能を提供する場合は加点とする。なお、本機能がファイアウォールのオプション機能となる場合は、そのライセンスを含んで提供すること。

2.3.4.2 アンチウィルス機能
(1) 2.3.4 項 ファイアウォールにてアンチウィルス機能を提供すること。
(2) WEB コンテンツにウィルスが含まれていた場合、アクセスしたユーザにその旨を通知し、その WEB コンテンツへのアクセスを遮断すること。
(3) 本機能の実現はファイアウォール以外の装置にて実現しても良いが、運用負荷および障害ポイントの軽減の観点から機器点数が増加することを回避するため、2.3.4 項 ファイアウォールにて同機能を提供する場合は加点とする。なお、本機能がファイアウォールのオプション機能となる場合は、そのライセンスを含んで提供すること。

2.3.4.3 WEB セキュリティ機能
(1) 2.3.4 項 ファイアウォールにて WEB セキュリティ機能を提供すること。
(2) フィルタリングのデータベースは定期的に自動でアップデートされること。
(3) ソース IP アドレスのセグメントごとに個別にコンテンツフィルタリングのポリシー設定が可能なこと。
(4) 任意の URL についてブラックリスト設定もしくはホワイトリスト設定が可能なこと。
(5) 管理用 GUI にてフィルタリングの設定が可能なこと。
(6) 禁止サイトへアクセスしたユーザに、カスタマイズしたメッセージを日本語で表示できること。

(7) 本機能の実現はファイアウォール以外の装置にて実現しても良いが、運用負荷および障害ポイントの軽減の観点から機器点数が増加することを回避するため、2.3.4 項 ファイアウォールにて同機能を提供する場合は加点とする。なお、本機能がファイアウォールのオプション機能となる場合は、そのライセンスを含んで提供すること。

2.3.5 DMZ スイッチ(2 台)

DMZ 用スイッチは、商用および SINET 用の DMZ セグメントに各 1 台ずつ設置すること。現行の DMZ スイッチ(2 台)に接続されている周辺システムを接続すること。

(1) 19 インチラックに搭載および固定が可能であること。
(2) スイッチングファブリックは、176Gbps 以上であること。
(3) MAC アドレス登録テーブル数は 16,000 以上であること。
(4) 10/100/1000BASE-T のポートを 48 個以上有すること。
(5) SFP/SFP+スロットのポートを 4 個以上有すること。
(6) IEEE802.1Q に準拠した 4,092 以上の VLAN を設定可能なこと。
(7) ポートベース VLAN、IEEE 802.1Q タグベース VLAN に対応可能なこと。
(8) リンクアグリゲーション(IEEE802.3ad)をサポートし、8 ポート以上束ねて、静的、動的(LACP)に帯域を拡張する機能を有すること。
(9) 筐体内部での電源冗長化に対応していること。
(10) SSH によるリモート接続が可能なこと。
(11) 2.3.4 項 ファイアウォールと 1Gbps×1 本以上で接続すること。必要に応じて SFP モジュールを用意すること。
(12) その他、現行の DMZ スイッチに接続されている周辺システムを接続すること。接続に必要な SFP/SFP+モジュールを用意すること。
(13) 空きポートを最低 3 個以上確保すること。

2.3.6 L7 スイッチ

本システムはリプレースを必要とせず、既存機器を本学指定の場所に収集すること。

2.3.7 スパム対策装置

本システムはリプレースを必要とせず、既存機器を本学指定の場所に収集すること。

2.3.8 冗長化用スイッチ(必要数)

(1) 19 インチラックに搭載および固定が可能であること。
(2) 本システムの導入は必須ではないので、2.3 項 学外接続部の各システムの冗長化を行ううえで必要な場合に、必要な数を含んで導入すること。

(3) 導入する際は後述する 2.4.4.1 項 エッジスイッチ仕様 A と同等以上の製品を選定すること。

2.4 学内接続部

ここでは別紙 2 に示す学内接続部において必要とされる機能要件のみを述べる。この機能要件を満たすような学内接続部の詳細な構成および設計は請負者の責任において行うこと。なお、ここで述べる機能要件を実現するために、必ずしもそれぞれの機能に応じた機器を個別に準備する必要はなく、複数の機能を集約した機器を用いても問題はない。

2.4.1 全学コアスイッチ(1 筐体)

学内接続部の L3 機能は全学コアスイッチに集約する。

(1) 19 インチラックに搭載および固定が可能であること。
(2) 専用のスタックケーブルを用いて 2 台以上で 1 筐体の冗長構成とすること。但し、ハードウェア障害による停止を伴わないことを前提に、1 台で 1 筐体の構成でも良いものとする。なお、本項は 1 筐体における仕様とする。
(3) 冗長構成にて接続されている装置間では、コンフィグ、FDB、ARP テーブル、IP ルーティングテーブル等の各種情報を同期することが可能なこと。
(4) スイッチングファブリックは、1280Gbps 以上であること。
(5) MAC アドレス登録テーブル数は 16,000 以上であること。
(6) 筐体内部での電源冗長化に対応していること。
(7) リンクアグリゲーション(IEEE802.3ad)をサポートし、8 ポート以上束ねて、静的、動的(LACP)に帯域を拡張する機能を有すること。
(8) ゲートウェイ装置冗長プロトコルとして VRRP 機能を有すること。
(9) スタティックルーティング、ポリシーベースルーティング、RIPv1/v2、RIPng、OSPFv2、OSPFv3 機能を有すること。
(10) SSH によるリモート接続が可能なこと。
(11) 2.4.2 項 学部コアスイッチ(5台)と 10Gbps×2 本以上の LAG で接続すること。接続に必要な SFP+モジュールもしくはダイレクトアタッチケーブルを用意すること。
(12) 2.4.3 項 全学サーバスイッチ(2 台)と 10Gbps×2 本以上の LAG で接続すること。接続に必要な SFP+モジュールもしくはダイレクトアタッチケーブルを用意すること。
(13) 2.3.4 項 ファイアウォールと 1Gbps×1 本以上で接続すること。接続に必要な SFP モジュールを用意すること。
(14) その他、現行のコアスイッチに接続されている周辺システムの構成を確認し、接続に必要な SFP モジュールならびに SFP+モジュールを用意すること。

2.4.2　学部コアスイッチ(5 台)

学部コアスイッチは各学部棟および A5 棟に 1 台ずつ設置すること。

2.4.1 項 全学コアスイッチで述べたとおり学部コアスイッチは全学コアスイッチと接続する。

(1) 19 インチラックに搭載および固定が可能であること。
(2) スイッチングファブリックは、128Gbps 以上であること。
(3) SFP スロットのポートを 24 個以上有していること。
(4) SFP+スロットのポートを 4 個以上有していること。
(5) MAC アドレス登録テーブル数は 16,000 以上であること。
(6) 筐体内部での電源冗長化に対応していること。
(7) リンクアグリゲーション(IEEE802.3ad)をサポートし、8 ポート以上束ねて、静的、動的(LACP)に帯域を拡張する機能を有すること。
(8) IEEE802.1Q に準拠した 4090 以上の VLAN を設定可能なこと。
(9) ポートベース VLAN、IEEE 802.1Q タグベース VLAN に対応可能なこと。
(10) SSH によるリモート接続が可能なこと。
(11) 2.4.1 項 全学コアスイッチと 10Gbps×2 本以上の LAG で接続すること。接続に必要な SFP+モジュールもしくはダイレクトアタッチケーブルを用意すること。
(12) その他、現行の学部コアスイッチ(5台)に接続されている周辺システムを接続すること。接続に必要な SFP/SFP+モジュールを用意すること。

2.4.3　全学サーバスイッチ(2 台)

主に全学向けのサービスを行うサーバを収容するスイッチ。

(1) 19 インチラックに搭載および固定が可能であること。
(2) スタックケーブルなどを利用し、2 台の機器を仮想的に 1 台の装置として扱うスタック構成とすること。
(3) 筐体内部での電源冗長化に対応していること。
(4) スイッチングファブリックは、228Gbps 以上であること。
(5) MAC アドレス登録テーブル数は 12,000 以上であること。
(6) 10/100/1000BASE-T のポートを 48 個以上有すること。
(7) SFP/SFP+スロットのポートを 4 個以上有すること。
(8) IEEE802.1Q に準拠した 4,090 以上の VLAN を設定可能なこと。
(9) ポートベース VLAN、IEEE 802.1Q タグベース VLAN に対応可能なこと。
(10) リンクアグリゲーション(IEEE802.3ad)をサポートし、8 ポート以上束ねて、静的、動的(LACP)に帯域を拡張する機能を有すること。

(11) SSH によるリモート接続が可能なこと。
(12) 2.4.1 項 全学コアスイッチと 10Gbps×2 本以上の LAG で接続すること。接続に必要な SFP+モジュールもしくはダイレクトアタッチケーブルを用意すること。
(13) その他、現行の全学サーバスイッチ(2台)に接続されている周辺システムを接続すること。接続に必要な SFP/SFP+モジュールを用意すること。

2.4.4 エッジスイッチ(78 台)

建物内の各室内への LAN 配線を収容するためのスイッチ。学部エッジスイッチおよび支線スイッチの構成は現行の構成を基本して設計すること。なお、室内への配線増加がある場合にも対応すること。その上で、各スイッチには少なくとも 3 個以上の空きポートを確保すること。

2.4.4.1 項～2.4.4.4 項を満たすエッジスイッチを調達すること。各エッジスイッチの仕様は別紙 3 を参照すること。

2.4.4.1 エッジスイッチ 仕様 A(60 台)
(1) 機器設置に必要な金具を用意すること。
(2) スイッチングファブリックは、56Gbps 以上であること。
(3) MAC アドレス登録テーブル数は 8,000 以上であること。
(4) 動作可能温度は 0℃～40℃であること。
(5) ループ検知機能を有すること。
(6) VLAN 登録数は 4,092 以上であること。
(7) 10/100/1000BASE-T のポートを 24 ポート以上有すること。
(8) SFP スロットを 4 ポート以上備えていること。
(9) SSH によるリモート接続が可能なこと。
(10) 特殊フレームの送受信によりループを検出する機能に対応し、ループを検出した場合には、ポートをリンクダウンさせるなど設定した動作を自動実行可能なこと。
(11) その他、現行のエッジスイッチに接続されている周辺システムを接続すること。

2.4.4.2 エッジスイッチ 仕様 B(16 台)
(1) 機器設置に必要な金具を用意すること。
(2) スイッチングファブリックは、176Gbps 以上であること。
(3) MAC アドレス登録テーブル数は 16,000 以上であること。
(4) 動作可能温度は 0℃～40℃であること。
(5) ループ検知機能を有すること。
(6) VLAN 登録数は 4,092 以上であること。
(7) 10/100/1000BASE-T のポートを 48 ポート以上有すること。

(8) SFP スロットを 4 ポート以上備えていること。
(9) SSH によるリモート接続が可能なこと。
(10) 特殊フレームの送受信によりループを検出する機能に対応し、ループを検出した場合には、ポートをリンクダウンさせるなど設定した動作を自動実行可能なこと。
(11) その他、現行のエッジスイッチに接続されている周辺システムを接続すること。

2.4.4.3 エッジスイッチ 仕様 C(1 台)
(1) 機器設置に必要な金具を用意すること。
(2) スイッチングファブリックは、18Gbps 以上であること。
(3) MAC アドレス登録テーブル数は 4,000 以上であること。
(4) 10/100/1000BASE-T のポートを 8 ポート以上有すること。
(5) その他、現行のエッジスイッチに接続されている周辺システムを接続すること。

2.4.4.4 エッジスイッチ 仕様 D(1 台)
(1) 機器設置に必要な金具を用意すること。
(2) スイッチングファブリックは、18Gbps 以上であること。
(3) MAC アドレス登録テーブル数は 16,000 以上であること。
(4) 10/100/1000BASE-T のポートを 8 ポート以上有すること。
(5) VLAN 登録数は 2,048 個以上であること。
(6) PoE スイッチであること。
(7) SSH によるリモート接続が可能なこと。
(8) その他、現行のエッジスイッチに接続されている周辺システムを接続すること。

2.4.5 支線スイッチ
本システムの仕様は 2.4.4 項 エッジスイッチに含む。

2.4.6 無線 LAN
既に集中管理方式の無線 LAN 設備が導入されており、別紙 4 に示すアクセスポイントが学内に設置されている。表中のアクセスポイントのうち No.1～40 までは本調達で更新を行うこと。
No.41～48 は図書情報センターの管理下にないアクセスポイントであるが、現行は 2.4.6.3「無線 LAN コントローラ」に収容されている。これらアクセスポイントの更新は不要だが、当該コントローラ更新後も現行と同様にコントローラ配下に収容し、アクセスポイントの監視、設定変更等が集中的に行えるようにすること。当該無線コントローラを現行と異なるメーカーの機器に変更するなどして、当該コントローラから 2.4.6.3 に記載の管理操作が集中的に行えない場合は、個別にアクセスポイントの運用操作を行うことでも可とするが、この場合、アクセスポイント運用操作手順書を提出するとともに、アクセスポイントの設定変更の必要性が生じた場合、本学からの求めに応じて

請負者の責任においてこれら操作を行うこと。これら操作については契約期間中、対応を実施すること。なお、集中管理が行えない場合、2.4.6.3(14)により加点対象とならないので注意すること。

2.4.6.1 アクセスポイント(更新 40 台＋新規導入 11 台) ※新規導入は加点対象

(1) アクセスポイントは全48ヵ所の内、40ヵ所の現行機器を更新する。また、アクセスポイントの設置位置は別紙4を参照すること。
(2) 自動電波・出力調整機能を有すること。
(3) 無線LANの電波干渉が発生した際、最適なチャネルに遷移する機能を有すること。
(4) クライアント高密度の環境において、公平な通信帯域を確保できること。
(5) アクセスポイントと2.4.6.3項 無線LANコントローラとの間の通信を暗号化する機能を有すること。
(6) WEB認証、IEEE802.1X認証、PSK認証に対応できること。
(7) EAPに対応した認証が可能なこと。
(8) IEEE802.11a/b/g/n/ac に準拠およびWi-Fi認定を得ていること。
(9) 2.4GHzおよび5GHzのワイヤレスネットワークの同時運用が可能であること。
(10) 100/1000BASE-Tのポートを2ポート以上備えていること。
(11) 導入するアクセスポイントにて、eduroamが利用できるようにすること。
(12) 別紙5に示す【11台】を新規導入する場合は加点とする。その際、2.4.4項 エッジスイッチの空きポート数が足りない場合は機器を変更すること。また、2.4.4項 エッジスイッチ～2.4.6.2項 パワーインジェクタ間および2.4.6.2項 パワーインジェクタ～アクセスポイント間のLANケーブルの新設配線を行うこと。

2.4.6.2 パワーインジェクタ(更新 39 台＋新規導入 11 台)

2.4.6.1 項 アクセスポイントに給電を行うことができるパワーインジェクタを必要台数導入すること。ただし、アクセスポイントを接続する 2.4.4 項エッジスイッチが PoE 対応している場合は、当該スイッチからの給電で代用することでも可とするが、この場合、当該エッジスイッチに必要となる商用電力を確認し、電源工事が必要な場合は請負者の責任において実施することとし、必要な費用については本調達に含めること。

(1) 2.4.6.1 項 アクセスポイントに給電が行えること。
(2) 2.4.6.1 項 アクセスポイントと同一メーカーの製品であること。
(3) A0 棟 3 階 教授会室に設置するアクセスポイントは、2.4.4.4 項 エッジスイッチ 仕様 D より給電するため、この箇所のパワーインジェクタは不要とする。
(4) 2.4.6.1 項 アクセスポイントの項番(12)を含む場合、併せて本機器も必要数を含むこと。

2.4.6.3 無線 LAN コントローラ(2 台)

(1) 19 インチラックに搭載および固定が可能であること。
(2) アプライアンス機器であること。

(3) 不正なアクセスポイントを発見できる機能を有すること。
(4) 認証用のローカルデータベース、およびRADIUS、LDAPへの認証通信は、無線LANコントローラから纏めて行えること。
(5) WEB認証用のゲストユーザを作成できること。
(6) ゲストユーザは指定したSSID、アクセスポイント、期限にて管理できること。
(7) WEB認証で接続された場合、ユーザアカウント別、アクセスポイント別、時間別に利用状況に関する統計情報を取得できること。ただし、無線LANコントローラで利用状況等の統計レポート出力ができない場合は、当該情報をトラップ送信できること。
(8) ローカルゲストアカウントが作成できること。
(9) 本システムの管理者を複数作成できること。
(10) 1 台のコントローラで最大 150 アクセスポイント以上のサポートが可能であること。
(11) 50 アクセスポイント以上を管理できるライセンスを用意すること。
(12) 機器の冗長化構成がとれること。
(13) 別紙 4 に示すアクセスポイント（更新対象外も含む）を管理対象に含めること。
(14) 別紙 4 に示す No.41～48「2017 年度末 ICT センターで導入および 2018 年度末 ICT センターで導入」について、当該無線コントローラを現行と異なるメーカーの機器に変更するなどして、当該コントローラから 2.4.6.3 に記載の管理操作が集中的に行えない場合は、個別にアクセスポイントの運用操作を行うことでも可とするが、この場合、アクセスポイント運用操作手順書を提出するとともに、アクセスポイントの設定変更の必要性が生じた場合、本学からの求めに応じて請負者の責任においてこれら操作を行うこと。これら操作については契約期間中、対応を実施すること。なお、運用負荷および障害ポイントの軽減の観点から、1 つのシステムで別紙 4 に示す全てのアクセスポイントを管理できる場合は加点とする。また、(7)の統計情報取得が当該コントローラで実現できる場合は加点とする。
(15) 2.4.6.1 項 アクセスポイントの項番(12)を含む場合、併せて本機器の管理対象に含めること。

2. 4. 6. 4 無線 LAN 運用管理装置

本システムはリプレースしない。

2. 4. 6. 5 RADIUS サーバ（2 台）

(1) 19 インチラックに搭載および固定が可能であること。
(2) アプライアンス機器であること。
(3) 汎用の WEB ブラウザによるログの表示、検索が可能であること。
(4) 日本語のユーザインタフェースを有していることが望ましい。
(5) ユーザ単位に設定するユーザ情報に日本語「2バイト文字」が使用可能であることが望ましい。
(6) マスターからスレーブに対して、設定情報（コンフィグ）の同期が可能であること。
(7) 2 台の冗長構成で機能の提供が可能であること。

(8) MAC アドレス認証機能および IEEE802.1X 機能を有すること。
(9) RADIUS サーバの正当性をクライアントに対して証明するための証明書をインポート可能であること。なお、インポートする証明書は本学より提供するが、クライアントの証明書更新に関する手順書は請負者にて作成し、本学に提供すること。
(10) クライアント証明書の一括発行、失効、ダウンロードが可能であること。
(11) 外部の Active Directory/LDAP サーバにあるアカウント情報を参照し、認証情報として利用することができること。
(12) LDAPS に対応していること。
(13) 有効期限が切れたアカウントに対して、自動削除する機能を有すること。
(14) eduroam に対応した機器を選定すること。
(15) eduroam に接続するための手順書を提出すること。

2.5 演習室接続部

演習室ネットワークから 2.3.4 項 ファイアウォールおよび 2.4.3 項 全学サーバスイッチへ接続すること。

2.6 事務ネットワーク

事務ネットワークは IEEE802.1X 認証を利用しているため、2.4.6.5 項 RADIUS サーバ選定時に考慮すること。

2.7 内部サーバ

2.7.1 プロキシサーバ

本システムはリプレースを必要とせず、既存機器を本学指定の場所に収集すること。

現行では、演習室クライアントがプロキシ設定を行っているため、システム切替え時にその点を考慮した移行を行うとともに、2.3.4.2 項 アンチウイルス機能、2.3.4.3 項 WEB セキュリティ機能も当サーバで実施しているため、これら機能の移行を行うこと。

2.7.2 DHCP サーバ(2 台)

(1) 19 インチラックに搭載および固定が可能であること。
(2) アプライアンス機器であること。
(3) RFC2131 に準拠すること。
(4) GUI によるログの表示、検索が可能であること。
(5) ユーザ単位に設定するユーザ情報に、日本語「2 バイト文字」が使用可能であること。
(6) マスターからスレーブに対して DHCP 情報の同期が可能であること。
(7) 2 台の冗長構成でリース情報を共有可能であること。
(8) 特定の MAC アドレスに対して、固定の IP アドレスを払い出すことが可能であること。

(9) リース範囲を VLAN ごとに設定可能であること。
(10) リース状況一覧を管理画面で確認でき、MAC アドレスをキーにした検索が可能であること。
(11) 不正な DHCP 要求があった際 IP アドレスの払い出しをしないこと。
(12) 10,000IP アドレス以上の払い出しが可能なこと。
(13) MAC アドレスの一括データ登録が可能であること。

2.8 運用支援設備

2.8.1 NAS(1 式)

(1) 19 インチラックに搭載および固定が可能であること。
(2) アプライアンス機器であること。
(3) ディスク容量は 12TB 以上であること。
(4) OS はサーバ用 OS を搭載していること。
(5) 10/100/1000BASE-T のポートを 2 ポート以上有すること。
(6) 全学サーバスイッチと 1Gbps×1 本以上で接続すること。
(7) 2.8.2 項 ログ管理システム、2.8.3 項 ネットワーク監視システムの OS バックアップデータを格納すること。
(8) 2.8.4 項 BCP バックアップシステムに対して、1 日 1 回、自動でバックアップする仕組みを構築すること。
(9) 2.8.4 項 BCP バックアップシステムの対象である「財務会計システム」「学務事務管理システム」「文書管理システム」「図書システム」のデータは、本学にてバックアップを実施する。これらバックアップファイルの保存先を提供すること。

2.8.2 ログ管理システム(1 式)

別紙６に示すスイッチおよびサーバからのログを収集、整理し、管理者に適切に表示するために必要なサーバである。なお、別紙６に示すスイッチ等は現行のスイッチ等の名称で記入しているので、本件で導入されるスイッチ等の名称とは必ずしも一致しない。また、導入数量についても必ずしも一致しない。

(1) 19 インチラックに搭載および固定が可能であること。
(2) 各システムから送信される syslog メッセージを受信し、ログデータの管理が行えること。
(3) ログデータは 6 ケ月間の保存が可能であること。なお、現行システムのログ容量は 1 カ月あたり約 5GB である。
(4) 1 日 1 回、ログデータをアーカイブし、2.8.1 項 NAS にバックアップすること。
(5) 以下に示す機能を有するソフトウェアを導入する場合は加点とする。
(ア) 検索条件を指定して、検索条件に一致するログを抽出することができること。
(イ) 検索したログ結果を一括ダウンロード可能であること。

(ウ) ログデータの統計レポート出力が可能であること。

2.8.3　ネットワーク監視システム(1 式)

本調達で導入された各ネットワーク機器の死活監視以外に、別紙7に示す既存の各種オペレーティングシステムが動作するサーバ、クライアントの死活監視、および既存の WEB、DNS、Mail サーバなどのサービス監視を行うサーバである。これを実現する際に、サーバ側あるいはクライアント側で設定が不要なエージェントレス方式であることが望ましいが、エージェントのインストールが必要な場合は請負業者にて実施すること。

(1) 19 インチラックに搭載および固定が可能であること。
(2) 最大 500 ノードの監視が可能なこと。
(3) 本調達にて導入するシステム以外に、既に監視しているノードを監視対象とすること。
(4) GUI にて管理できること。
(5) ICMP による死活監視を実施すること。
(6) メールサービスや WEB サービス等を提供しているサーバについて、ポート監視を実施すること。
(7) SNMP トラップによる通知を受信すること。
(8) 必要な MIB ファイルをインストールすること。
(9) 各監視にて異常を検知した際には、ネットワーク監視システムに通知すると共に、あわせて本学の運用管理者に対してメールにて通知を行うこと。
(10) 重要な障害については、本学保有の警報灯(警子ちゃん)に通知する機能を有すること。または、警報灯を新たに納入し、そちらに通知する機能を有すること。
(11) 各サービスのアラート履歴やアラートの統計情報が参照できること。
(12) ネットワークの状態(正常・異常)を視覚的に把握できるようマップを作成すること。
(13) マップは各棟(A 棟～E 棟)、演習室ネットワーク全体、全学ネットワーク全体、サーバ機器全体の各マップを作成すること。
(14) リソース監視(CPU 情報、メモリ情報、ディスク使用率)を行う場合は加点とする。

2.8.4　BCP バックアップシステム(1 式)

(1) 本学外に BCP バックアップシステムを構築すること。
(2) BCP バックアップシステムはインターネットを経由せず、SINET と直結の本学外のデータセンター等に接続すること。
(3) BCP バックアップ対象ファイルの総容量は現在 300GB であるが、将来的な拡張を見越して最大 400GB の容量を想定している。バックアップ対象ファイルを 2 世代以上保存できるように、保存領域を 800GB 以上用意すること。なお、データセンター等の利用料金は本学が別途負担するものとする。

(4) 2.8.1 項 NAS 上のデータを 1 日 1 回、自動でバックアップする仕組みを構築すること。
(5) 自然災害等に起因し、本学のネットワークが利用できない状況下におかれた場合でも、SINET を介して BCP バックアップシステムにアクセスし、当該データの取り出しが行えること。
(6) BCP バックアップの成否通知を、本学管理者のメールアドレスに送付する機能を有することが望ましい。

2.9 無停電電源装置(必要数)
(1) 19 インチラックに搭載および固定が可能であること。
(2) 常時インバータ方式の無停電電源を併設し、瞬時停電対策を行うこと。
(3) リース期間中に無停電電源装置のバッテリ交換が必要となる場合は、請負者の責任において交換することとし、必要な費用については本調達に含めること。
(4) 商用電源が 5 分以上停電した場合にはすべてのサーバ機器が自動的に停止できるようにすること。
(5) 以下のシステムを無停電電源装置に接続すること。
2.3.1 項 対外接続ルータ
2.3.3 項 回線負荷分散装置
2.3.4 項 ファイアウォール
2.4.1 項 全学コアスイッチ
2.4.2 項 学部コアスイッチ
2.4.3 項 全学サーバスイッチ
2.4.6.3 項 無線 LAN コントローラ
2.4.6.5 項 RADIUS サーバ
2.7.2 項 DHCP サーバ
2.8.1 項 NAS
2.8.2 項 ログサーバ
2.8.3 項 ネットワーク監視サーバ

2.10 KVM 装置
(1) 19 インチラックに搭載および固定が可能であること。
(2) 2.8.1 項 NAS、2.8.2 項 ログサーバ、2.8.3 項 ネットワーク監視サーバ用の KVM を用意すること。

2.11 バックアップソフトウェア
(1) 2.8.2 項 ログサーバ、2.8.3 項 ネットワーク監視サーバについて、構築時に OS のバックアップを実施し、ハードウェア故障時などに復旧できるようにするソフトウェアを導入すること。
(2) 構築時だけでなく、運用中に設定変更が生じた場合は本学にてバックアップを実施するため、

必要な手順書を作成すること。

3. 保守・支援体制

3.1 保守内容

(1) 本調達で導入されたネットワークおよびそれらに付随するシステムが健全に動作し、かつ障害が発生した場合にすみやかに対応できるよう遠隔監視の体制を確立すること。

(2) 遠隔監視に必要となるリモート接続は、2.3.4 項 ファイアウォールの VPN 機能を用い、本学のインターネット接続回線経由で行っても構わない。この他に必要となるネットワーク機器、監視用の PC 端末等は、請負者の負担とし、本調達の費用に含めること。

(3) リモート接続時は 2.8.2 項 ログ管理システム、2.8.3 項 ネットワーク監視システムに接続できる環境を構築すること。

(4) 運用開始後の本学からの導入システムに関する質問・問い合わせに対応するための窓口を準備すること。

(5) 本システムを構成する機器の稼動および運用に関する問題点について、本学担当者の要求に応じて随時援助、協力すること。

(6) 本学で実施するシステムの日常的運営業務については、作業負担が軽減されるよう、必要、且つ十分な作業内容・手順を明示した手順書を作成し提供すること。

(7) 月 1 回、発生した障害内容および対応状況について、報告書を提出し、報告すること。

3.2 ハードウェア保守

(1) 導入する全ての機器はハードウェア保守を提供すること。

(2) ハードウェア保守はオンサイト対応を行うこと。

(3) 2.4.4 項 エッジスイッチについて、IP アドレスを付与するなどの設定行為が一切不要で、予備機と故障機を交換することで、復旧できるシステムを構築する場合は、先出しセンドバック保守の契約でも良いものとする。この場合、各機器の最新の設定内容（Config ファイル）の管理は自動で行われる仕組みであること。交換時に復旧できない場合はオンサイト対応を実施すること。

3.3 ソフトウェア保守

(1) 導入する Linux サーバは「Red Hat Enterprise Linux」とし、メーカーサポートの提供が可能であること。

3.4 保守対応日および時間

(1) E-mail による保守受付は 24 時間 365 日とすること。

(2) 電話による保守受付およびオンサイト保守は、平日（年末年始、土日祝日は除く）の 9 時～17 時とすること。

(3) 月曜日から金曜日の平日 9 時～15 時までに連絡を受理した障害は、4 時間以内に 1 次対応を実施すること。なお、1 次対応とは停止したサービスを仮復旧させることを指す。

(4) 平日 15 時～17 時までに連絡を受理した障害は、翌営業日午前中までに 1 次対応を実施すること。
(5) 1 次対応完了後は完全復旧を速やかに実施すること。

3.5 物品管理

(1) 備品、配線、モジュール等を除くすべての機器について、リース物品であることを示す管理タグを添付すること。管理タグには導入年、導入システム名、リース期間、リース会社名を明記すること。
(2) リース物品の管理簿(トレーサビリティ管理表)を作成すること。
(3) リース期間中機器の変更があった場合は、その結果を管理簿に反映し、本学に報告すること。

3.6 予備機

(1) 冗長化していないネットワーク機器(ルータ、スイッチ)は予備機を 1 台以上、予備機として用意すること。ただし、2.4.1 項 全学コアスイッチはその限りではない。
(2) ネットワーク機器(ルータ、スイッチ)の SFP モジュール、SFP+モジュール、ダイレクトアタッチケーブル、スタックケーブルは 1 個以上、予備機として用意すること。

4. 施行

4.1 構築作業

(1) 2 項 構成の要件について導入する各システムの設計・構築作業を実施すること。

(2) 本調達で導入する無線 LAN アクセスポイントで、新たに eduroam を利用できるようネットワークを構築すること。

(3) 3.2 項 ハードウェア保守(3)で、IP アドレスを付与するなどの設定行為が一切不要で、予備機と故障機を交換することで、復旧できるシステムを構築する場合は、対象機器の交換作業が容易に行えるよう、設置方法について手順書を作成するとともに、本学担当者と協議の上で設置すること。

(4) 以下のバックアップデータを 2.8.1 項 NAS に保存できる領域を作成すること。また、そのデータを 1 日 1 回、2.8.4 項 BCP バックアップシステムに自動で転送すること。

(ア) 財務システム

(イ) 学務事務管理システム

(ウ) 文書管理システム

(エ) 図書システム

(5) 本調達で設置する機器の電源容量を算出し、必要な電源が確保できない場合は電源工事（必要な配線作業、電気工事を含む）を実施すること。電源工事を行う際は関係部署との調整に協力を行い、他システム等に影響を及ぼさないよう本調達に関する必要な情報提供を行なうこと。

(6) 移行作業において新旧機器の二重設置を実施する場合は必要な電源容量を算出し、必要な電源が確保できない場合は電源工事を実施すること。

(7) 電源工事を実施する場合、既存の受電設備の使用並びに配線経路等については施工前に担当職員と十分協議し、工事計画書を提出すること。

(8) 本調達のシステムと既設システムとの間で問題が生じた場合、本学と協議の上、責任を持って原因の切り分けを行い、問題を解決すること。なお、既設システム構築業者と協議が必要な場合は本学担当者が同席する。

(9) 調達機器の搬入に際しては本学施設に損傷を与えないよう十分な注意をするとともに、施設に損傷を与えた場合は受注者の責任においてこれを修復すること。また、搬入時には受注者が必ず立ち会うこと。

(10) 更新する機器や新設機器、および流用する機器の設置は現行の什器の利用を前提とすること。

(11) 更新対象の各システムにおいて必要なデータについては移行すること。

(12) 移行に伴うアクセス権については本学と協議のうえ、適切に付与すること。

(13) 最終的に導入される機器、導入手段、配線の変更、更新など、すべての作業について、あらかじめ本学担当者と十分協議し、要件定義書および基本設計書を提出すること。

(14) 本調達において保守対象外となる消耗品が含まれている場合は、あらかじめこれを明記すること。

(15) 本調達では更新しない以下の現行機器についても本学指定の場所(学内)に収集すること。

2.3.2 帯域制御装置

2.3.6 L7 スイッチ

2.3.7 スパム対策装置

2.4.6.4 無線 LAN 運用管理装置

2.7.1 プロキシサーバ

4.2 完成図書

(1) 本件完了の際に、以下に示す「完成図書」を 1 部、印刷物を提出するとともに、それらを編集可能な電子媒体(CD や DVD など)で 1 部、提供すること。

A. 納入機器一覧

(ア) トレーサビリティ管理表

B. 完成図面

(ア) ネットワーク構成図

(イ) フロア配置図

(ウ) 配線系統図

(エ) ラック図

(オ) 電気系統配線図

C. 機器環境設定表

(ア) 機器コンフィグ

(イ) パラメータシート

D. 運用マニュアル

(ア) 各機器のログイン方法

(イ) 各機器の設定変更方法

(ウ) 各機器の起動方法および停止方法

(エ) 各機器のログ確認方法

(オ) システム運用管向け運用マニュアル

(カ) システム利用者向け運用マニュアル

E. 試験結果

F. 付属品・予備リスト

G. 完成写真

(ア) 施工前写真

(イ) 施工後写真

H. 故障復旧体制図

(2) 英語版・日本語版の資料・マニュアルがある場合は日本語版を提供すること。

4.3 情報保護等

(1) 請負者は、業務を通じて知り得た秘密を他人に漏らしてはならない。また、他の目的に利用してはならない。

(2) 本学の許可なくシステムから個人情報を所得してはならない。また、個人情報の漏洩を防ぐために必要な措置をとること。

4.4 リース満了後の取扱い

(1) 本調達で導入されたすべての物品は、リース満了後、本学に移譲すること。ただし、サービスはその限りでは無い。

4.5 機器の撤去について

(1) 既存機器は撤去し、別途、指示する本学指定の場所(学内)に収集すること。

5. 提案条件

本仕様書に基づく提案内容であることを示すために、提案書には少なくとも以下で述べる事項が含まれていなければならない。各事項の提案書への記載方法、記載順については任意とするが、各項目の提案書記載箇所を様式「提案条件対応表」に記載すること。なお、提案条件として記載を求めた項目について、提案書に記載がない場合は失格となるので注意すること。

5.1 システムの実績

本システムの納入に係る入札参加者の履行能力、ネットワークシステムの導入実績を評価するため、下記の項目について示すこと。

(1) 情報ネットワークシステムの構築実績

入札参加者が過去に実施した本システムと類似および同等以上規模の構築実績について、以下の項目を示すこと。本システムと類似の実績とは、大学における別紙2に示すようなネットワークシステムとそれらを管理するためのサーバ等の構築が既に完了し、正常稼働しているものとし、ネットワーク機器のみの納品や個別のサーバまたは本システムに含まれないシステムの納入はこれに含まれないものとする。

A. 契約者、契約名称、契約期間、契約金額を明記すること。

5.2 提案システム

提案するシステムの考え方、全体構成について以下の項目について示すこと。

(1) 提案するシステムの基本方針

提案の検討において設定した基本方針を以下の項目について準拠して示すこと。

A. 提案における基本方針を明確に示すとともに、方針を反映した提案内容の概略並びに関係個所を明記すること。

B. 提案するシステムの全体構成を示し、構成における提案システムの特徴を明記すること。

(2) 提案構成品一覧

提案システムを構成する機器およびソフトウェアについて、下記の項目を一覧化して示すこと。なお、一覧の作成にあたっては、各名称を本仕様書に記載の設備名称、機能名称等に準拠するものとするが、同一設備を複数で構成する場合や本仕様書に記載はないが、提案のシステムに必要となるものについては、名称の記載方法や注釈等により、分かりやすい表記に留意すること。

A. 設備名称、機能名称、機器名称(型番)、メーカー名、数量を明記すること。また、各製

品の仕様を示すこと。

B. 本調達の対象外となる既存機器の接続方法を明記すること。設定変更を行う場合は、その理由、設定内容を明記すること。

(3) 既存環境の引き継ぎ

既存環境の引継ぎについて、以下の項目を示すこと。

A. 既存システム・機器に設定されている項目を引き継げない場合は、該当箇所、理由、対応方法を示すこと。

(4) 対外接続ルータの機能

対外接続ルータの機能について、以下の項目を示すこと。

A. BCP バックアップシステムに関し、通信の振り分け方法、重要データを学外に送信することに対するセキュリティを確保するための方法を示すこと。

(5) 回線負荷分散装置の機能

回線負荷分散装置の機能について、以下の項目を示すこと。

A. 2.3.3 本学の SINET 回線と商用インターネット回線をマルチホーム化し、効率的な回線使用や回線障害によるネットワーク停止リスク低減の方法を示すこと。

B. 2.3.3(5) 1台にハードウェア障害が発生した場合においても、ネットワークを停止させない冗長構成について示すこと。

C. 2.3.3(10) SINET および商用インターネット回線障害を検知した際、トラップやメール等で管理者に通知する機能について示すこと。

D. 2.3.3(11) 装置の更新前後で、負荷分散対象となる各学内システムの対外通信において、どのような変更および影響が生じるかを示すこと。

(6) ファイアウォールの機能

ファイアウォールの機能について、以下の項目を示すこと。

A. 2.3.4(4) 1台にハードウェア障害が発生した場合においても、ネットワークを停止させない冗長構成について示すこと。

B. 2.3.4(8) 各アプリケーションが占有する帯域利用率のレポート機能について示すこと。

C. 2.3.4(23) ファイアウォールの各種ログを蓄積し、当該ログをもとにレポートを作成する機能を有するサーバを導入する場合はその詳細を示すこと。

(7) 不正侵入防御機能

不正侵入防御機能について、以下の項目を示すこと。

A. 2.3.4.1(6) 不正侵入と疑われるログをレポートする機能の詳細を示すこと。

B. 2.3.4.1(7) 不正侵入防御機能を実現する箇所(機器名、システム名等)を示すこと。

C. 不正侵入を検知した際の管理者への通知方法を示すこと。

(8) アンチウイルス機能

アンチウイルス機能について、以下の項目を示すこと。

A. 2.3.4.2(2) WEB コンテンツにウィルスが含まれていた場合、アクセスしたユーザにその旨を通知し、その WEB コンテンツへのアクセスを遮断する機能について示すこと。

B. 2.3.4.2(3) アンチウイルス機能を実現する箇所(機器名、システム名等)を示すこと。

(9) WEB セキュリティ機能

WEB セキュリティ機能について、以下の項目を示すこと。

A. 2.3.4.3(6) 禁止サイトへアクセスしたユーザに、カスタマイズしたメッセージを日本語で表示できる機能について示すこと。

B. 2.3.4.3(7) WEB セキュリティ機能を実現する箇所(機器名、システム名等)を示すこと。

(10) 冗長化用スイッチの機能

冗長化用スイッチの機能について、以下の項目を示すこと。

A. 冗長化用スイッチの設置個所および役割を示すこと。

B. ハードウェア保守形態、障害発生時の対応方法について示すこと。

(11) 全学コアスイッチの機能

全学コアスイッチの機能について、以下の項目を示すこと。

A. 2.4.1(2) 機器構成、冗長構成を示すこと。

B. 2.4.1(11) 学部コアスイッチ、2.4.1(12) 全学サーバスイッチ、2.4.1(13) ファイアウォールとの接続形態を示すこと。

C. ハードウェア保守形態、障害発生時の対応方法について示すこと。

(12) 学部コアスイッチの機能

学部コアスイッチの機能について、以下の項目を示すこと。

A. エッジスイッチとの接続形態を示すこと。

B. ハードウェア保守形態、障害発生時の対応方法について示すこと。

(13) 全学サーバスイッチの機能

全学サーバスイッチの機能について、以下の項目を示すこと。

A. 2.4.3(14) 現行の全学サーバスイッチに接続されている周辺システムの接続方法および必要となる機器等を示すこと。

B. ハードウェア保守形態、障害発生時の対応方法について示すこと。

(14) エッジスイッチ・支線スイッチの機能

エッジスイッチ、支線スイッチの機能について、以下の項目を示すこと。

A. 2.4.4) エッジスイッチ、2.4.5) 支線スイッチの機器構成、必要台数を示すこと。
室内への配線増加がある場合はその配線図を示すこと。

B. ハードウェア保守形態、障害発生時の対応方法について示すこと。

(15) 無線 LAN の機能

無線 LAN の機能について、以下の項目を示すこと。

A. 2.4.6.1(12)、2.4.6.2) について、新規導入分アクセスポイント11台の導入の可否、導入可能な場合、配線および本システムで導入するアクセスポイントの電源供給方法等の情報を、接続するエッジ・支線スイッチを用いて示すこと。

B. 2.4.6.3(7) WEB 認証で接続された場合、ユーザアカウント別、アクセスポイント別、時間別利用状況に関する統計情報を取得できる機能について詳細および方法を示すこと。

C. 2.4.6.3(12) 機器構成、冗長構成を示すこと。

D. 2.4.6.3(14) 無線 LAN コントローラを用いた、更新対象アクセスポイント40台、ICT センター導入アクセスポイント8台、新規導入アクセスポイント11台（導入可能な場合）の管理方法を示すこと。ICT センター導入アクセスポイント8台を無線 LAN コントロ―ラで一元管理できない場合はその旨を記載した上で、当該アクセスポイントの本学の運用管理方法および契約期間中に設定変更が生じた場合の対応方法を示すこと。

E. 現状の無線 LAN に係る認証、SSID の運用方法等を踏まえ、本システムで導入する関連機器での認証、SSID の運用方法について示すこと。

(16) Radius サーバの機能

Radius サーバの機能について、以下の項目を示すこと。

A. 2.4.6.5(15) Eduroam 認証の概要およびユーザの利用方法を示すこと。

(17) ログ管理システムの機能

ログ管理システムの機能について、以下の項目を示すこと。

A. 2.8.2(5) 各システムから収集したログ等について、検索条件に一致するログの抽出、検索結果の一括ダウンロード、統計レポート出力機能がある場合は詳細を示すこと。

B. ログ管理システムを動作させるサーバ構成を示すこと。

C. ログ管理システムの OS、ソフトウェア名を示すこと。

(18) ネットワーク監視システムの機能

ネットワーク監視システムの機能について、以下の項目を示すこと。

A. 本システムで導入する機器、システムのほか、別紙7に示す既存のサーバ・クライアントの死活監視およびサービス監視の方法を示すこと。

B. 2.8.3(9) 各監視にて異常を検知した際にネットワーク監視システムに通知するとともに本学の管理者にメールで通知する方法を示すこと。

C. 2.8.3(11) 各サービスのアラート履歴やアラートの統計情報参照の詳細を示すこと。

D. 2.8.3(12)(13)) 各棟、演習室ネットワーク、全学ネットワーク、サーバ機器全体のマップおよびネットワークの状態を視覚的に把握できるマップの概要および利用方法を示すこと。

E. 2.8.3(14) リソース監視（CPU 情報、メモリ情報、ディスク使用率）を行うことが出来る場合は、その方法を示すこと。

F. 監視を行う機器等にエージェントが必要となる場合はその導入方法を示すこと。

G. ネットワーク監視システムを動作させるサーバ構成を示すこと。

H. ネットワーク監視システムの OS、ソフトウェア名を示すこと。

(19) BCP バックアップシステムの機能

BCP バックアップシステム機能について、以下の項目を示すこと。

A. BCP バックアップシステムを提供する、外部のサービス名、事業者名、SINET との接続構成、月額利用料金、保存領域等サービス概要を示すこと。

B. BCP バックアップの具体的な手法および考慮したセキュリティ対策を示すこと。
なお、バックアップ対象ファイルは本調達で導入される保存領域に本学側で保存する。

(20) 無停電電源装置

無停電電源装置を設置する機器・システムを示すこと。

(21) バックアップソフトウェアの機能

バックアップソフトウェアの機能について、以下の項目を示すこと。

A. 2.8.2) ログ管理システム、2.8.3) ネットワーク監視システムについて、構築時に OS のバックアップを実施し、ハードウェア故障時などに復旧できるようにすることとしている件について、その手法を示すこと。

(22) 環境構築

環境構築機能について、以下の項目を示すこと。

A. 本調達に必要な電源容量について、工事が伴う場合はそれらを明らかにすること。

B. 4.1(3) エッジ・支線スイッチの故障時の対応について、IP アドレスを付与するなどの

設定が一切不要で、予備機と故障機を交換し、復旧できるシステムを構築する場合は、対象機器の交換作業を容易に行えるようにする必要がある。これについて対処方法を示すこと。

(23) 設置・移行作業

設置・移行作業について、以下の項目を示すこと。

A. 導入作業の日程およびプロジェクト体制を示すこと。

B. 利用するサーバ室内の既存ラックについて、その内部での機器配置を示すこと。

C. 既存システムとの接続について、対象、手法を示すこと。

(24) 保守・サポート

保守・サポートについて、以下の項目を示すこと。

A. 保守・サポートの実施体制を明らかにし、要求仕様を満たすことを示すこと。

以上。