令和７年度

滋賀県立大学
情報ネットワークシステム一式借入

要求仕様書

令和７年２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 概要構成
別紙 2　　次期 SPINS 概要構成案
別紙 3　　エッジスイッチ仕様
別紙 4-1　　(既存)アクセスポイント設置場所等
別紙 4-2　　(R6 年度)アクセスポイント設置場所等
別紙 4-3　　交流センター無線 LAN サイトサーベイ実施結果
別紙 4-4　　交流センター1階全体図面
別紙 5　　現行死活監視対象機器

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、Microsoft365、、TOEIC 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、学内無線 LAN 利用の利便性向上、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たっては、これまで SPINS で提供されてきたサービスを維持するとともに、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。本仕様書に記載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。

5. 提案条件に記載の内容について提案書を提出すること。提案内容について本学にて評価を実施し、より良い提案を優遇する。

1.3 現行SPINSの概要

1.3.1 全体の構成

現状の SPINS の概要構成は別紙1の通りである。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、本調達において廃止を行う回線負荷分散装置、本調達の対象となる、ファイアウォールが接続されている。

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。)

「SINET DMZ」および「商用 DMZ」には、それぞれ L2 スイッチ(以下、「DMZ スイッチ」)を導入し、外部向けサーバを接続している。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、「SINET DMZ」および「商用 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。

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。また、SINET の L2VPN サービスを利用して、学外で運用されている「BCP バックアップシステム(スマートストレージ)」、「学務事務管理システム」、「大学情報DB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 LAN 配線が使用されている。

講義棟・工学部・人間文化学部・人間看護学部・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、食堂には無線 LAN 設備が導入されている。無線 LAN 設備は導入年度によりメーカーが異なり、令和元年度に導入された設備はアクセスポイントおよび無線 LAN コントローラは Cisco 製、令和 6 年度に導入された設備はアクセスポイントおよび無線 LAN コントローラは Allied Telesis 製で構成されており、ともに無線 LAN を利用する際の認証方法は以下の通りとなっている。

無線 LAN を利用する際は、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構成となっている。一部の無線 LAN は PSK(事前共有鍵)認証を用いている箇所も存在する。

無線 LAN コントローラ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 を利用で切る構成となっている。

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、その後全学コアスイッチに接続される。全学コアスイッチから 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

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。

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
- 回線負荷分散装置

・ファイアウォール
・DMZ 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（令和元年導入分、令和 6 年度導入分）
・Radius サーバ
・DHCP サーバ
・ログ管理装置
・ネットワーク監視サーバ
・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。5. 提案条件に記載の内容について提案書を提出すること。提案内容について評価を実施し、より良い提案を優遇する。

2.1 全般

(1) リース期間は令和 7 年(2025 年)9 月 20 日から令和 13 年(2031 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、落札者が提示すること。

(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、本学担当者と協議し、適正な設定を行うこと。ただし、既設システムに設定されている有線および無線用 VLAN については、IP アドレスが不足していたり、建屋間・研究室間の通信制御を行う必要性が生じているため、一部 VLAN の構成および VLAN 間の通信制御方法を変更する可能性がある。本学担当者と協議し、適切な設定を行うこと。

(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、BCP バックアップシステム、財務会計システム、学務事務管理システム、大学情報データベースシステム、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・実現方法等を提案書に記載して説明すること。また、その費用も含むこと。落札者決定後、変更が必要な箇所等について、本学担当者の許可を得た上で実施すること。特に本調達では商用インターネット接続回線を廃止し、SINET が提供する「データセンタ接続冗長化サービス」を利用するが、現在、商用インターネット接続回線関連機器に接続されている機器等および設定されている内容を新システムに移行し、現行サービスが引き続き利用できるようにするとともに、廃止を行う機器、システムについて、本学担当者と協議の上で適切な対応を行うこと。また、本調達にて無線 LAN 利用時の認証方式を、これまでのWEB認証からIEEE802.1X PEAP 認証に変更を行うため、この新認証方式に必要となる既存教職員用 ActiveDirectory および既存学生用 ActiveDirectory 等の設定変更を本調達内で実施する必要がある。これら ActiveDirectory は別途、保守業者が保守を行っているため、当保守業者と連携して設定変更を実施することとし、これに必要となる費用を含むこと。保守業者との協議には本学担当者が同席する。なお、無線 MAC 認証は継続して利用できるよう設定を行うこと。

(7) 無線 LAN 設備については、既存設備の更新の他、新たに交流センターホールにおいて無線 LAN が利用できるよう、無線 LAN 設備の増設を行う。当該施設の無線 LAN サイトサーベイ実施結果(別紙 4-3)および図面(別紙 4-4)を参考に無線 LAN 増設を実施すること。

(8) 機器仕様は 1 台あたりに求める要件とする。
本調達で導入するサーバにはウイルス対策等セキュリティ対策ソフトウェアを導入すること。これに必要となる費用を含むこと。

2.2 配線

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

(2) 落札者決定後、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 接続用ルータを 2 台用意すること。
現在は SINET、商用インターネットのマルチホーミング接続であるが、本調達では商用インターネット接続回線を廃止し、SINET が提供する「データセンタ接続冗長化サービス」を利用する。

SINET メイン回線の速度は 10Gbps、バックアップ回線の速度は 10Gbps とし、BGP 接続が可能な 2 台の対外接続ルータを選定し、この 2 台をスタック接続した上で BGP 構成とすること。なお、SINET メイン回線およびバックアップ回線は本学が別途契約を行い用意する。

(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。

(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、253Gbps 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) 10/100/1000BASE-T のポートを 20 個以上有すること。
(7) 100/1000/2.5G/5GBASE-T のポートを 4 個以上有すること。
(8) SFP/SFP+スロットのポートを 4 個以上有すること。
(9) 筐体内部での電源冗長化に対応していること。
(10) 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) スタックケーブルで機器間(最大 8 台)を接続することにより、仮想的に 1 台の装置として扱うことができる、スタック機能(以下、スタック)を有すること。
(12) 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、PIM-SSMv4、PIM-SMv4、PIM-DMv4、PIM-SSMv6、PIM-SMv6、BGP 機能を有すること。（但しライセンス適用は可とする）
(13) SSH によるリモート接続が可能なこと。
(14) 2.3.4 項 ファイアウォールと 10Gbps×2 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。
(15) その他、現行の対外接続ルータに接続されている周辺システムを接続すること。
(16) L2VPN に対応したタグ VLAN による通信を可能とすること。

2.3.2 回線負荷分散装置（2 台）

SINET が提供する「データセンタ接続冗長化サービス」を利用するため、負荷分散装置は廃止とする。

2.3.3 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 10,000 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。

現行、負荷分散装置に実装している NAT 設定を移行することとし、商用インターネット接続回線廃止に伴う NAT 設定の調整をあわせて実施し、現行運用が引き続き行えるようにすること。

(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) ハードウェアとソフトウェアが一体となったアプライアンス機器であること。
(3) Active/Passive、Active/Active 両方の冗長構成に対応していること。
(4) 冗長構成の OS アップグレード作業時、セッションを維持しつつアップグレード作業が可能であること。
(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。

(6) 最大同時接続クライアント数が 10,000 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。

(7) Windows OS および Mac OS の端末にて IPSec によるリモートアクセス VPN に対応していること。。

(8) アプリケーションの制御が可能であること。

(9) 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。

(10) 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 6.8Gbps 以上であること。

(11) 各種機能（アプリケーション識別、IPS、アンチウィルス、アンチスパイウェア）を同時に使用した場合でも 3.2Gbps 以上の処理能力を有すること。

(12) 新規セッション数が秒間あたり、100,000 セッション以上を処理可能であること。

(13) 最大同時セッション数が、945,000 セッション以上を処理可能であること。

(14) セッション数が閾値を超えた場合に、自動的にセッションタイマーを短くすることでセッション数の増加を抑制し、セッションテーブルの消費を抑制する機能を有すること。

(15) 1G/2.5G/5G のマルチレートに対応した Ethernet インターフェースを有すること。

(16) 専用の HA 用インターフェースを 2 ポート以上有すること。

(17) 10/100/1000BASE-T のポートを 12 個以上有すること。

(18) SFP/SFP+スロット(1G/10Gbps)のポートを 4 個以上有すること。

(19) 筐体内で SSL に準拠した通信を復号し、アプリケーションの識別およびコンテンツ検査のポリシーが適用可能であること。

(20) SSL 復号通信のセッション数や暗号方式、SSL 復号失敗理由の情報を管理 GUI にて確認可能であること。

(21) 暗号化された PDF、Microsoft Office、ZIP、RAR ファイルと暗号化されていない前述ファイルの通信を区別してファイル名の可視化やフィルタリングが可能なこと。

(22) NAT 機能を有すること。

(23) 初期状態（デフォルト）で全てのトラフィックを対象にしたアプリケーションの識別のシグネチャが適用されていること。

(24) 1 つのセキュリティポリシーで IPv4 および IPv6 通信に対するアクセス制御やアプリケーション識別による制御が可能であること。

(25) 同一の TCP/UDP ポートを使用するアプリケーションに対し、異なるセキュリティポリシーを設定可能であること。

(26) ポリシー設定画面において、ポリシーが作成された日付と最後に更新された日付を確認できること。

(27) 有害な IP アドレスの最新のリストを保持し、それを基にアクセス制御が可能であること。

(28) ドメインフロンティング攻撃を検出して、防御できること。
(29) IEEE802.1Q VLAN トランク機能を有すること。
(30) IEEE802.3ad リンクアグリゲーション機能を有すること。
(31) SSH によるリモート接続が可能であること。
(32) 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。
(33) 2.4.1 項 全学コアスイッチと 10Gbps×2 本以上で接続すること。
(34) 2.3.5 項 DMZ スイッチと 1Gbps×2 本以上で接続すること。
(35) 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。
(36) 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。
(37) ISO/IEC15408(Common Criteria)の認定を取得していること。
(38) 設定操作に関しては、管理者毎に、その管理者が設定変更した分だけをコミットおよびロールバックできること。
(39) 設定情報を名前付きのスナップショットとして保存可能であり、またスナップショットから設定を復元できること。
(40) 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。

2.3.3.1 不正侵入防御機能

(1) 2.3.3 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、2.3.3 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。

2.3.3.2 アンチウィルス機能

(1) 2.3.3 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、2.3.3 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。

2.3.3.3 WEB セキュリティ機能

(1) 2.3.3 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) SNS やドラッグ等、カテゴリ別に WEB フィルタリングが行えること。
(6) 管理用 GUI にてフィルタリングの設定が可能なこと。
(7) 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。
(8) 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、2.3.3 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 DMZ スイッチ（1台）

現行の、物理アプライアンスである 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。他の機器を活用して実装可能な場合は、物理アプライアンスでの設置は必須ではないが、現行と同様に DMZ ゾーンを提供するとともに、システム面・運用面の負荷、セキュリティに配慮した構成とし、実運用に支障が出ないことを提案書に記載して説明すること。

(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、506 Gbps 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) 2.3.3 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。

2.3.5　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 2.4.5 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。

2.3.6　SSL-VPN 接続システム

現状、SSL-VPN システムを DMZ ゾーンに設置し、Active-Stanby 構成で教職員が外部から学内システムを利用できる環境を提供しているが、システムライフサイクル等の問題が発生しているため、これに代わる新たな SSL-VPN 機能を提供すること。専用の物理アプライアンス等の設置は必須ではなく、他の導入機器を活用して実装可能な場合は、現行と同様に SSL-VPN 接続を提供するとともに、運用負荷、セキュリティに配慮した構成とし、実運用に支障が出ないことを提案書に記載して説明すること。

(1) 学外から以下のシステムにアクセス可能な環境を構築すること。
　(ア) グループウェア
　(イ) 大学情報データベースシステム
　(ウ) 学務事務管理システム
　(エ) 財務会計システム
　(オ) Web サーバシステムのコンテンツ
　(カ) その他、リモートデスクトップ端末を含む、本学が指定するシステム等
(2) SSL-VPN 経由で学外のウェブサイトやシステムにアクセスすることが可能であること。
(3) 利用者は最大 300 ユーザとし、同時に 50 ユーザが利用可能なこと。
(4) ユーザをグループで管理することが可能で、各グループ毎に専用の VLAN を割り当てることが可能であること。
(5) セキュリティ対策に十分に留意したシステムを構築すること。学外からの不正アクセス対策、脆弱性の対応、利用者認証方法等の詳細を提案書に記載して説明すること。
(6) パソコン（Windows、MacOS）に加え、スマートフォンおよびタブレット端末（iOS、Android）など多様な端末から利用可能なこと。
(7) ブックマーク機能を有し、複数の URL リンクを登録することが可能であること。
(8) 本学が指定するパスワードポリシーに対応可能な、文字数制限、大文字・小文字英字、数字、記号がパスワードに利用可能でき、パスワード無制限等の設定を行うことが可能であること。

(9) SSL-VPN 接続時の認証は本学が利用してる「統合認証基盤システム」の認証情報とは連携せず、独自の認証を提供可能であること。SSL-VPN 接続用ユーザ名・パスワードを盗用されても、学内システムを不正利用できないようにすること。
(10) 別途本学が用意する SSL サーバ証明書(NII 発行)を利用して、借入期間中は認証されたサイトとしてサービスを提供できること。
(11) 運用の拡張性を考慮し、SSL-VPN 接続する端末について MAC アドレスやウイルス対策の定義ファイル更新状況等をチェックし、条件を満たす端末のみ接続を許可する機能を有すること。
(12) 1 台の故障により影響を及ぼさないよう、複数台構成もしくは冗長構成をとること。
(13) アカウント毎のアクセス情報(アクセス日時、アクセス場所等)、認証結果(不一致、変更失敗、その他セキュリティに関する情報)等のログを一定期間保存可能であること。

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落札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(2 台)

学内接続部の L3 機能は全学コアスイッチに集約する。

接続される機器等の設定等を確認し、当該機器の ACL 等、必要となる設定を移行すること。

(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) 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。
(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、1.92Tbps 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、

PIM-SSMv4、PIM-SMv4、PIM-DMv4、PIM-SSMv6、PIM-SMv6、BGP、BGP+機能を有すること。（但しライセンス適用は可とする）

(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) 2.3.3 項 ファイアウォールと 10Gbps×2 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、253Gbps 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、506Gbps 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(81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。

以下、全エッジスイッチ仕様に記載の台数は現行の台数を記載している。本調達において交流センターホールにおいて無線 LAN を利用できるようにするとともに、上位エッジスイッチ、学部コアスイッチまでの通信経路を 10G に対応させること。室内への配線追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。

2.4.5、2.4.5.1、2.4.5.2、2.4.5.3、2.4.5.4、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。

2.4.5 エッジスイッチ 仕様 A(59 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 16,000 以上であること。
(4) 動作可能温度は 0℃～50℃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 PoE 出力ポートを 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。

2.4.5.1 エッジスイッチ 仕様 B(16 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) 筐体内部での電源冗長化に対応していること。
(3) スイッチングファブリックは、506Gbps 以上であること。
(4) MAC アドレス登録テーブル数は 16,000 以上であること。
(5) 10/100/1000BASE-T の PoE 出力ポートを 48 個以上有すること。
(6) ループ検知機能を有すること。
(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) 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。
(13) 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。

2.4.5.2 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、16Gbps 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) 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。

2.4.5.3 エッジスイッチ 仕様 D(3 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、40Gbps 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 PoE 出力ポートを 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) SSH によるリモート接続が可能なこと。
(7) 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。

2.4.5.4 エッジスイッチ 仕様 E(2 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、40Gbps 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 PoE 出力ポートを 16 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) SSH によるリモート接続が可能なこと。
(7) 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。

2.4.5.5 エッジスイッチ 仕様 F(1 台)(10G 対応スイッチの参考仕様)

(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、253Gbps 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 PoE 出力ポートを 24 ポート以上有すること。
(5) SFP/SFP+スロットを 4 ポート以上有すること。
(6) VLAN 登録数は 4,094 個以上であること。
(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。

2.4.6 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。

2.4.7 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、令和元年度に導入された設備(別紙 4-1)は、アクセスポイントおよび無線 LAN コントローラは Cisco 製であり、表中のアクセスポイントのうち No.1～60 までは本調達で更新を行うこと。また、本調達においてあらたに交流センターホールにアクセスポイントの増設を行うこと。

令和 6 年度に導入された設備(別紙 4-2)は、アクセスポイントおよび無線 LAN コントローラは Allied Telesis 製であり、更新は不要である。令和元年導入アクセスポイント更新分および交流センターホール増設分をこの Allied Telesis 製無線 LAN コントローラで管理できることが望ましいが、別メーカーのものでも構わない。ただし、別メーカーの機器等で管理する場合は、当該アクセスポイントを集中的に管理できる機能を提供するとともに、運用操作手順書を提出し本学においてアクセスポイントの設定変更を行えるようにすること。また、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。更新、増設を行うアクセスポイントおよびアクセスポイントを管理する無線 LAN コントローラのメーカー、アクセスポイントの管理方法等を提案書に記載すること。

また、無線 LAN に接続する端末の情報（アクセス日時、アクセス元 IP アドレス等）、認証結果（不一致、変更失敗、その他セキュリティに関する情報）等のログを 2.8.2 ログ管理システムに転送し、当該システム上で一元的に上述の情報を参照することが可能であること。

2.4.7.1 アクセスポイント（更新 60 台＋交流センターホール分増設台数）

記載の台数は現行の台数を記載している。このアクセスポイントを更新するとともに、交流センターホールで無線 LAN を利用できるようにするために必要なアクセスポイント台数、上位スイッチの機種・配線・想定無線電波拡散状況、貫通工事を行う場合はその方法・石綿対策等を提案書に記載すること。装置単体で 100/1000/2.5G/5GBASE-T のポートを 2 ポート以上搭載していること。

また、そのうち 1 ポート以上は IEEE 802.3at（Power over Ethernet +）に対応していること。

(1) Wi-Fi規格及びIEEE 802.11a/802.11b/802.11g/802.11n/802.11ac/802.11axに準拠していること。
(2) 2.4GHz/5GHz帯の同時使用に対応していること。
(3) 2.4GHz帯は4空間ストリーム、5GHz帯は8空間ストリームに対応していること。
(4) SSIDごとに利用するRADIUSサーバを自由に指定できること。セパレータ機能を有すること。
(5) IEEE 802.1X認証に対応し、EAP-TLS / EAP-TTLS / MSCHAPv2 / PEAPv0 /EAP-MSCHAPv2 / PEAPv1 / EAP-GTC /EAP-SIM / EAP-AKA / EAP-FAST / PSK方式が使用可能なこと。
(6) 認証方式としてオープンシステム認証、共有キー認証、WPA パーソナル、WPA エンタープライズが利用可能であること。
(7) キャプティブポータルによるWeb認証を有すること。
(8) 暗号化機能としてWEP（64/128bit）及びWPA/WPA2(TKIP/CCMP)、WPA3(CCMP/GCMP)が利用可能であること。
(9) MACアドレスフィルタリングが2,048以上設定可能なこと。また、CSVからのインポートに対応していること。

(10) 無線の利用状態を収集して、常に最適な電波出力とチャンネルを分析しアクセスポイントへ適用する機能を持つ自律型無線LANコントローラーにて管理ができること。
(11) 自律型無線LANコントローラー離脱時でも無線サービスの提供を継続できること。
(12) 日本語Web GUI（HTTP/HTTPS）に対応していること。
(13) 日本語マニュアルをインターネット上に公開していること。
(14) 同一メーカーのAC電源アダプターもしくはパワーインジェクターを必要台数導入すること。

2.4.7.2 無線 LAN コントローラ(1 台)

(1) 無線 LAN アクセスポイントを実際の環境に応じてフロアマップ上に配置させ、表示することで視覚的に管理できること。
(2) 無線チャンネルの表示(色によってチャンネル種別を表現)や無線電波出力の表示(大きさによって出力を表現)が可能であること。
(3) 無線 LAN アクセスポイントの一覧表示および検索が可能であること。
(4) 管理対象の無線 LAN アクセスポイント周囲の電波出力、チャンネルを常に認識し、最適化する機能を有すること。
(5) 電波出力・チャンネルの分析結果の適用は、スケジュール登録による任意のタイミングでの調整実施可能なこと。
(6) 無線 LAN アクセスポイントの設定情報の一部を共通化して管理できること。共通設定を無線 LAN アクセスポイントへ一括適用することで誤設定の防止や、設定工数の削減ができること。
(7) 無線 LAN コントローラ再起動の場合など、無線 LAN コントローラと無線 LAN アクセスポイント間で通信が一時的に不通になったとしても、無線サービスの提供を継続することが可能であること。
(8) 事前に定義した時間帯に、設定の変更やファームウェアのバージョンアップが行えるスケジューリング機能を有し、スケジュールされたタスクの自動実行ができること。
(9) 管理している無線 LAN アクセスポイントのログ表示が可能であること。また、ログは CSV 形式で出力可能なこと。
(10) 無線 LAN アクセスポイントは、最大 3000 台まで管理可能なこと。
(11) ソフトウェア製品であること。
(12) 日本語マニュアルを提出すること。
(13) 1 台の故障により影響を及ぼさないよう、複数台構成もしくは冗長構成をとること。

2.4.7.3 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) Radius クライアントを少なくとも 7,000 以上エントリ登録が可能であること。
(4) 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。日時・ユーザ名・認証正否・接続元 IP アドレスが確認できること。
(5) 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。
(6) 文字コードは UTF-8、または Windows-31J をサポートしていること。
(7) ユーザ/端末/証明書アカウント情報を格納する内部アカウント管理データベースと認証を行う。
(8) RADIUS 機能をメインサーバ、レプリカサーバの構成で冗長化することが可能である。ただし、レプリカサーバにはアカウント機能や、設定情報を改廃する機能はないこと。
(9) MAC アドレス認証、IEEE802.1x 認証機能を有すること。
(10) 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(NII UPKI 電子証明書発行サービスより入手)することが可能だが、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。この場合、証明書のドメインは「usp.ac.jp」となる。
(11) 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。
(12) 外部の LDAP サーバや、ActiveDirectory に登録しているアカウントで認証を行うことが可能であること。LDAPサーバ、ActiveDirectory と連携する際は暗号化された通信で行うこと。
(13) 2.1 全般(6)に記載の既設 ActiveDirectory の設定変更を、保守業者と連携して実施すること。
(14) LDAPS に対応していること。
(15) 無線ゲストアカウントを作成することが可能であること。また、複数のアカウントの登録を一括で行えることとし、利用できる SSID をアカウント毎に指定できること。
(16) 最終認証日時管理機能により、未使用のアカウントを自動削除することが可能であること。
(17) eduroam に対応した機器を選定すること。
(18) 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 2.3.3 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。演習室からのインターネット接続については、NAT を用いて商用インターネット接続回線グローバル IP を利用しているが、商用回線の廃止に伴い、SINET 接続回線からインターネット接続する設定を行うこと。

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、2.4.7.3 項 RADIUS サーバ選定時に考慮すること。現行、証明サーバに保存されている証明書をインポートしているため、新システム移行時に、クライアント端末の証明書を切り替える必要がある。このサポートを行うこと。

2.7 内部サーバ

2.7.1 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。日時・ユーザ名・認証正否・接続元 IP アドレスが確認できること。
(5) 文字コードは UTF-8、または Windows-31J をサポートしていること。
(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 MAC アドレスの DHCP クライアントに指定した IP アドレスを払い出すことが可能であること。また、テキストファイルにより、一括登録/削除が可能であること。
(9) IP アドレスの払い出しを行うスコープの管理を行う機能を有し、スコープは最大 3000 まで登録可能であること。また、テキストファイルにより一括登録/変更が可能であること。
(10) それぞれのスコープに対し閾値(%)を設定することが可能で、閾値を超過した場合、管理者にメールで発報することが可能であること。
(11) 払い出した IP アドレスと MAC アドレスの状況を一覧で確認することが可能であること。
(12) DHCP 設定に登録した MAC アドレスの端末に対してのみ IP アドレスを払い出す制限を行うことが可能であること。また登録端末は、全スコープの合計で最大 20 万端末まで登録が可能であること。
(13) DHCP 最大払出アドレスが 50,000IP アドレスであること。
(14) ログをログ管理サーバに転送すること。

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5TB 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」「文書管理システム」「その他」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)

本調達で導入される各ネットワーク機器のログを収集、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。

(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 5 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落札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) 死活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、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)

BCP バックアップを SINET と直結の本学外のデータセンターに設置している。本システムに接続する設定を移行し、引き続き当該バックアップが行えるようにすること。

(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 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

2.4.7.2 項 無線 LAN コントローラ
2.4.7.3 項 RADIUS サーバ
2.7.1 項 DHCP サーバ
2.8.1 項 NAS
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

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 ログ管理システム、2.8.3 項 ネットワーク監視システム用の 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 ログ管理システム、2.8.3 項 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) バックアップジョブのスケジュール設定が可能で、あらかじめ定めたスケジュールでフルバックアップ・差分バックアップ等が自動取得でき、バックアップを世代管理することが可能であること。

3. 保守・支援体制

3.1 保守・支援内容

(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、2.3.3 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) Linux サーバを導入する場合は「RedHat Enterprise Linux」とし、メーカーサポートの提供が可能であること。期間内に OS のサポートが失効する場合は、サポートを受けることができる OS にシステム移行する、またはメーカーサポート期間を延長できる場合は延長を行うこと。いずれの場合も、その費用を含むこと。

(2) Windows サーバと同様に、ウイルス対策等セキュリティ対策ソフトウェアを導入すること。これに必要となる費用を含むこと。

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（ルータ含む、スイッチ、無線 AP）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) 距離や建物の構造上の問題等で無線 LAN アクセスポイントの設置が困難な場合や、無線 LAN アクセスポイントを設置するよりも安価で、且つ無線 LAN アクセスポイントと同等の無線 LAN 環境を提供できる場合は、無線の中継器を利用することも可とする。ただし、一般利用者の無線 LAN 利用に支障がでないことを事前に本学に説明し、承認を得ること。

(3) 本調達で導入する無線 LAN アクセスポイントで、eduroam を利用できるようネットワークを構築すること。現在は本学の利用者は学内の eduroam に接続できない仕様となっているが、これを本学利用者および eduroam 参加機関からの訪問者が接続できるように構築すること。

(4) 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。

(5) 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) 財務会計システム

(イ) 文書管理システム

(ウ) その他システム

(6) 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。

(7) 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。

(8) 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。

(9) 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。

(10) 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。

(11) 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。

(12) 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。

(13) 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。

(14) 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。

(15) 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。

(16) 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。

(17) 無線アクセスポイント設置に際し、施工者に義務付けられる施工前の石綿の事前調査・報告を適切に実施し、実施内容について本学担当者に報告を行うこと。

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任意の「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 システムの実績等

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 5 年間に実施した本システムと類似および同等以上規模の複数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. 契約相手方、教職員・学生数、契約名称、契約期間、契約金額を明記すること。

(2) 個人情報および情報セキュリティを管理するための認証・資格等

本調達では個人情報および情報セキュリティを取り扱うため、これらに関する認証や資格を証明する書類を提出すること。

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) SINET 提供「データセンタ接続冗長化サービス」を利用する運用

SINET が提供する「データセンタ接続冗長化サービス」を利用した運用に変更することについて、以下の項目について示すこと。

A. データセンタ接続冗長化サービスを適切に利用するために必要となる関連機器の物理的な接続方法、論理的な設定方法および達成できるメリットを示すこと。
B. 商用インターネット接続回線廃止に伴う関連機器および設定内容の移行方法を示すこと。
C. データセンタ接続冗長化サービスを提供する NII と調整が必要な内容を示すこと。

(5) 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。

(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. 2.3.3(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。
B. 2.3.3(9) 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. 2.3.3(40) 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。
D. 現行負荷分散装置に実装されている NAT 設定の移行方法を示すこと。

(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. 2.3.3.1(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. 2.3.3.1(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。

(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. 2.3.3.2(2) WEB コンテンツにウイ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. 2.3.3.2(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. 2.3.3.3(8) 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) DMZ スイッチの機能

DMZ スイッチの機能について、以下の項目を示すこと。

A. 商用インターネット接続回線廃止に伴う DMZ スイッチの統合方法を示すこと。

B. DMZ スイッチ機能を実現する箇所(機器名、システム名等)を示すとともに、システム・運用面の負荷、セキュリティ面で実運用に支障が出ないことを示すこと。

(11) 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。

(12) SSL-VPN 接続システムの機能

SSL-VPN の機能について、以下の項目を示すこと。

A. 2.3.6(5) セキュリティ対策に十分に留意したシステムであること、学外からの不正アクセス対策、脆弱性の対応、利用者認証方法について示すこと。

B. 2.3.6(12) 1 台の故障により影響を及ぼさない冗長構成について示すこと。

C. SSL-VPN 機能を実現する箇所(機器名、システム名等)を示すとともに、システム・運用面の負荷、セキュリティ面で実運用に支障が出ないことを示すこと。

(13) 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)(3) 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。

(14) 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。

(15) 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(13) 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。

(16) 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。

(17) 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. 交流センター1 階ホールへの無線 LAN 設備増設
設置するアクセスポイントの数、アクセスポイントとエッジスイッチを接続する有線 LAN の敷設経路、当エッジスイッチから学部コアスイッチ間の通信経路を 10G に対応させる方法、ホール内における、想定する 2.4GHz、5GHz 別の受信信号強度、アクセスポイント設置に際し、貫通工事を行う場合は工事手法および施工者に義務付けられる施工前の石綿の事前調査・報告の実施方法を示すこと。
B. 2.4.7.1、2.4.7.2 について、更新アクセスポイントおよび交流センター1 階ホールに増設するアクセスポイントの総数、給電方法および無線 LAN コントローラを含むメーカーを示すこと。
C. 令和 6 年度導入無線 LAN システムと同一のメーカーを導入する場合、当該無線 LAN コントローラの管理下に今回調達するアクセスポイントを置く方法を明示すること。同一メーカーを導入できない場合は、当該アクセスポイントを集中的に管理する操作等（設定

変更等含む)を示すこと。

D. 無線 LAN に接続する端末の情報(アクセス日時、アクセス元 IP アドレス等)、認証結果(不一致、変更失敗、その他セキュリティに関する情報)等のログを 2.8.2 ログ管理システムに転送する方法について明示すること。

E. 2.4.7.2(13) 1 台の故障により影響を及ぼさない冗長構成について示すこと。

F. IEEE802.1X PEAP 認証、PSK(事前共有鍵)認証、無線 MAC 認証の各認証方法について、実用例を含めて示すこと。

(18) 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. 2.4.7.3(18) 現状、学内 eduroam は、学外機関の利用者のみ利用できるが、これを学内関係者も利用できるよう変更を行う。これを実現するための認証の概要およびユーザの利用方法を示すこと。

(19) 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。

(20) 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 5 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。

(21) 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。

(22) 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。

(23) 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。

(24) 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. 3.2(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。

C. システム移行後の現行システムの取扱方針(機器、電源等の撤去)を示すこと。

(25) 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。

(26) 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

別紙3

エッジスイッチ仕様

NO	仕様	設置場所
1	エッジスイッチ　仕様A	A0棟1階 電話交換機室
2	エッジスイッチ　仕様A	A0棟2階 事務室（財務グループ）
3	エッジスイッチ　仕様A	A0棟2階 事務室（教務グループ）
4	エッジスイッチ　仕様A	A0棟2階 事務室（総務グループ）
5	エッジスイッチ　仕様A	A0棟2階 EPS
6	エッジスイッチ　仕様D	A0棟3階 教授会室
7	エッジスイッチ　仕様C	A0棟2階 コピー室
8	エッジスイッチ　仕様B	A1棟1階 EPS
9	エッジスイッチ　仕様A	A1棟2階 EPS
10	エッジスイッチ　仕様A	A1棟3階 A1-301中講義室
11	エッジスイッチ　仕様A	A1棟3階 A1-302中講義室
12	エッジスイッチ　仕様A	A2棟1階 EPS
13	エッジスイッチ　仕様A	A2棟2階 A2-201中講義室
14	エッジスイッチ　仕様A	A2棟2階 A2-202大講義室
15	エッジスイッチ　仕様A	A3棟1階 EPS
16	エッジスイッチ　仕様A	A3棟3階 A3-301大講義室
17	エッジスイッチ　仕様B	A4棟1階 EPS
18	エッジスイッチ　仕様A	A4棟2階 EPS
19	エッジスイッチ　仕様A	A4棟1階 A4-105講義室
20	エッジスイッチ　仕様A	A4棟2階 A4-205大講義室
21	エッジスイッチ　仕様A	A5棟1階 作業室
22	エッジスイッチ　仕様A	A5棟1階 EPS
23	エッジスイッチ　仕様A	A5棟2階 EPS
24	エッジスイッチ　仕様A	A5棟3階 EPS
25	エッジスイッチ　仕様B	A7棟1階 電気設備スペース
26	エッジスイッチ　仕様A	B0棟2階 情報機器室
27	エッジスイッチ　仕様B	B1棟1階 EPS
28	エッジスイッチ　仕様B	B1棟1階 EPS
29	エッジスイッチ　仕様A	B1棟1階 EPS
30	エッジスイッチ　仕様A	B1棟1階 EPS
31	エッジスイッチ　仕様A	B2棟1階 EPS
32	エッジスイッチ　仕様A	B2棟1階 EPS
33	エッジスイッチ　仕様B	B2棟2階 EPS
34	エッジスイッチ　仕様A	B2棟2階 EPS
35	エッジスイッチ　仕様A	B2棟2階 EPS
36	エッジスイッチ　仕様A	B2棟3階 301号室
37	エッジスイッチ　仕様A	B7棟1階 事務室（湖沼環境実験棟）
38	エッジスイッチ　仕様A	B8棟1階 管理室（環境管理センター）
39	エッジスイッチ　仕様A	B8棟1階 技師室（圃場実験施設）
40	エッジスイッチ　仕様A	B7棟2階 事務室（地域共生センター）

NO	仕様	設置場所
41	エッジスイッチ　仕様A	C2棟1階 事務室
42	エッジスイッチ　仕様B	C3棟1階 EPS
43	エッジスイッチ　仕様A	C3棟1階 EPS
44	エッジスイッチ　仕様B	C3棟1階 EPS
45	エッジスイッチ　仕様B	C3棟2階 電気室前ラック
46	エッジスイッチ　仕様B	C4棟1階 情報演習室
47	エッジスイッチ　仕様A	C4棟1階 情報演習室
48	エッジスイッチ　仕様A	C5棟1階 EPS
49	エッジスイッチ　仕様A	C5棟1階 EPS
50	エッジスイッチ　仕様B	C6棟1階 EPS
51	エッジスイッチ　仕様B	C7棟1階 情報機器室
52	エッジスイッチ　仕様B	C7棟1階 情報機器室
53	エッジスイッチ　仕様E	C7-305号室
54	エッジスイッチ　仕様E	C7-307号室
55	エッジスイッチ　仕様D	C7-310号室
56	エッジスイッチ　仕様A	C8棟2階 EPS
57	エッジスイッチ　仕様D	C8-204号室
58	エッジスイッチ　仕様A	C9棟1階 事務室
59	エッジスイッチ　仕様A	D0棟2階 大学院研究室
60	エッジスイッチ　仕様B	D2棟2階 EPS
61	エッジスイッチ　仕様A	D2棟2階 EPS
62	エッジスイッチ　仕様A	D2棟2階 EPS
63	エッジスイッチ　仕様B	D3棟2階 EPS
64	エッジスイッチ　仕様A	D5棟1階 EPS
65	エッジスイッチ　仕様A	D6棟1階 生活デザイン実習室Ⅰ
66	エッジスイッチ　仕様A	D7棟1階 大型映像機器室
67	エッジスイッチ　仕様A	D7棟1階 事務室（交流センター）
68	エッジスイッチ　仕様A	E0棟1階 電気室
69	エッジスイッチ　仕様A	E0棟2階 EPS
70	エッジスイッチ　仕様A	E1棟2階 EPS
71	エッジスイッチ　仕様A	E1棟2階 EPS
72	エッジスイッチ　仕様A	E2棟1階 更衣室
73	エッジスイッチ　仕様A	E2棟2階 EPS
74	エッジスイッチ　仕様A	E2棟2階 EPS
75	エッジスイッチ　仕様A	E3棟2階 EPS
76	エッジスイッチ　仕様A	E3棟2階 EPS
77	エッジスイッチ　仕様A	E4棟1階 EPS
78	エッジスイッチ　仕様A	E4棟2階 EPS
79	エッジスイッチ　仕様A	E4棟2階 EPS
80	エッジスイッチ　仕様B	E6棟1階 学部情報室
81	エッジスイッチ　仕様A	E7棟1階 EPS

別紙4-1

【既存】アクセスポイント設置場所等

NO	更改対象	アクセスポイント設置場所
1	○	A1棟3階 A1-301中講義室
2	○	A1棟3階 A1-302中講義室
3	○	A1棟1階自習室
4	○	A2棟2階 A2-201中講義室
5	○	A2棟2階 A2-202大講義室
6	○	A3棟3階 A3-301大講義室
7	○	A4棟1階 A4-105視聴覚室
8	○	A4棟2階 A4-205大講義室
9	○	A5棟2階 図書館 一般閲覧室(1)
10	○	A5棟2階 図書館 一般閲覧室(2)
11	○	A5棟3階 図書館 一般閲覧室(1)
12	○	A5棟3階 図書館 一般閲覧室(2)
13	○	A2棟1階 学生ホール
14	○	A2棟1階 食堂(1)
15	○	A2棟1階 食堂(2)
16	○	C4棟1階 学部情報室
17	○	C5棟3階 C5-304研究室
18	○	C6棟3階 C6-304研究室
19	○	C7棟3階 C7-305研究室
20	○	C7棟3階 C7-307研究室
21	○	C7棟3階 C7-310研究室
22	○	D7棟1階 ホワイエ（交流センター）
23	○	A7棟1階 A7-101中講義室
24	○	A7棟1階 A7-102中講義室
25	○	A7棟1階 自習室(1)
26	○	A7棟1階 自習室(2)
27	○	A7棟1階 特任教員室
28	○	A0棟2階 事務局（総務、経営戦略グループ）
29	○	A0棟2階 事務局（財務グループ）
30	○	A0棟2階 事務局（教務グループ）
31	○	A0棟2階 事務局（教務、学生・就職支援グループ）
32	○	A0棟2階 事務局（学生支援室）
33	○	A0棟3階 会議室（教授会室）
34	○	A0棟3階 会議室（評議会室）
35	○	A0棟3階 会議室（第1会議室）
36	○	A0棟3階 会議室（第2会議室）
37	○	D7棟1階 研修室（交流センター）
38	○	D7棟1階 事務室（交流センター）
39	○	D7棟2階 研修室6（交流センター）
40	○	D7棟2階 研修室7（交流センター）
41	○	C3棟1階　談話室
42	○	C3棟1階　談話室前ロビー
43	○	C1棟2階　C1-202材料科学実験室（学生実験室）
44	○	産学連携センター2階　　産学研究交流室1
45	○	C2棟実習工場2階　演習室
46	○	C1棟1階 C1-102機械システム工学実験室
47	○	C4棟2階 C4-210実習室
48	○	D0棟2階 D0-202会議室

NO	更改対象	アクセスポイント設置場所
49	○	E5棟1階 E5-101第一中講義室#1
50	○	E5棟1階 E5-101第一中講義室#2
51	○	E6棟1階 ナシェリア
52	○	産学連携センター2階 C8-204
53	○	C5棟2階 C5-201研究室
54	○	C5棟3階 C5-305研究室
55	○	C6棟1階 廊下
56	○	C6棟1階 廊下
57	○	C7棟3階 C7-311研究室
58	○	E1-101
59	○	E1-101の前廊下
60	○	E1-211

別紙4-2

【R6年度】アクセスポイント設置場所等

NO	アクセスポイント設置場所
1	A1棟1階 A1-112中講義室
2	A1棟3階 A1-113中講義室
3	A3棟1階 A3-101小講義室
4	A3棟1階 A3-102小講義室
5	A3棟1階 A3-104化学実験室
6	A3棟1階 A3-105小講義室
7	A3棟1階 A3-106小講義室
8	A4棟1階 A4-101小講義室
9	A4棟1階 A4-102小講義室
10	A4棟1階 A4-103小講義室
11	A4棟1階 A4-104小講義室
12	A4棟1階 A4-106小講義室
13	A4棟1階 A4-107中講義室
14	A4棟1階 A4-108中講義室
15	A1棟2階 A1-204中講義室
16	A1棟2階 A1-205中講義室
17	A1棟2階 A1-209講師控室
18	A3棟2階 A3-201小講義室
19	A3棟2階 A3-202小講義室
20	A3棟2階 A3-204生物実験室
21	A3棟2階 A3-205小講義室
22	A3棟2階 A3-206小講義室
23	A4棟2階 A4-201小講義室
24	A4棟2階 A4-202小講義室
25	A4棟2階 A4-203小講義室
26	A4棟2階 A4-204小講義室
27	A4棟2階 A4-206小講義室
28	A4棟2階 A4-207小講義室
29	A4棟2階 A4-209小講義室
30	A4棟2階 A4-210小講義室
31	A3棟3階 A3-303物理・地学実験室
32	A4棟3階 A4-301中講義室
33	A4棟3階 A4-302中講義室
34	A4棟3階 A4-303中講義室
35	A4棟3階 A4-304小講義室
36	A4棟3階 A4-305小講義室
37	A4棟3階 A4-306小講義室
38	A4棟3階 A4-307小講義室
39	E1棟1階 E1-101環境看護学実習室
40	E2棟1階 E2-102演習室7
41	E2棟1階 E2-103演習室8
42	E3棟1階 E3-101成熟看護実習室
43	E3棟1階 E3-102人体構造・機能実習室
44	E3棟1階 E3-104演習室9
45	E4棟1階 E4-101発達看護学実習室
46	E5棟1階 E5-102第2中講義室
47	E5棟1階 E5-103演習室1
48	E5棟1階 E5-104演習室2

NO	アクセスポイント設置場所
49	E5棟1階 E5-105演習室3
50	E7棟1階 E7-101第3中講義室
51	E7棟1階 E7-102第4中講義室
52	E7棟1階 E7-103演習室4
53	E7棟1階 E7-104演習室5
54	E7棟1階 E7-105演習室6
55	E0棟2階 E0-201会議室
56	E2棟2階 E2-212談話室
57	E3棟2階 E3-201特別研究室
58	E4棟2階 E4-201研究費室2
59	A5棟1階 個人閲覧室5

【別紙 4-3】

滋賀県立大学

交流センター無線LANサイトサーベイ

実施結果

2024 年 3 月

1　はじめに

1.1　調査目的

本調査及び情報分析は、滋賀県立大学交流センターにおける無線 LAN 環境の新設に伴い、導入予定のアクセスポイントによる無線 LAN 利用エリア内の電波伝搬状況及び周辺に存在するアクセスポイントの外来波の影響有無について確認を行った。電波環境分析の基礎データは AirMagnet Surveyの収集機能を使用、当該ソフトウェアの解析機能を基にし、本報告書を作成している。

本報告は調査日に取得したデータを基に作成している。クライアントの動作状況及び電波状況は曜日、時間、周辺の外来電波等により若干の変化が発生することに注意すること。

資料画像は AirMagnet Survey のレポート作成機能で抽出した画像を切り抜き、使用している。変更加工は行っていない。

1.2　調査日時

2024 年 2 月 6 日（水） 13 時 30 分～14 時 20 分
2024 年 2 月 7 日（木） 11 時 30 分～12 時 30 分

1.3　調査場所

滋賀県立大学　交流センター 対象エリア

1.4　調査

1.5　調査方法

無線 LAN 利用検討エリア内にて、AirMagnet Survey を使用し、仮設置したアクセスポイントの受信信号強度及び周辺アクセスポイントの外来波情報を収集。

1.6　図中の表記

表 1. 図中に記載している記号

記号	内容
	アクセスポイントを仮設置した場所
	無線 LAN 利用エリア

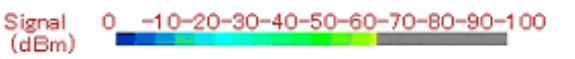


図 1. 図中に記載している受信信号強度

受信信号強度の良否を色で表します。青色に近いほど品質が良いことを表す。

1.7　調査に利用した機器・ソフトウェア

1.7.1 使用した無線 LAN 機器

アクセスポイント　：CISCO 9115 axi-q

1.7.2 情報収集に使用した機器

使用機器　：HP ELITEBOOK 830-G8
OS　：Microsoft　Windows 11 Professional
プロセッサ　：11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz　2.80 GHz
実装メモリ　：8.00GB
無線 LAN アダプタ　：Edimax AC-1750

1.7.3 情報収集に使用したソフトウェア

ソフトウェア　：NetAlly AirMagnet Survey Pro Ver.10.3

1.8　判定基準

表 2. 判定基準としきい値

説明	しきい値
電波伝搬範囲の合否	受信信号強度の値が-67dBm 以上は合格
外来波の影響有無	受信信号強度の値が-75dBm 以上は特に影響あり
	受信信号強度の値が-85dBm 以上は影響あり
	受信信号強度の値が-86dBm 以下は影響なし

1.9　アクセスポイント仮設置位置

1.9.1 交流センター1 階 アクセスポイント仮設置位置

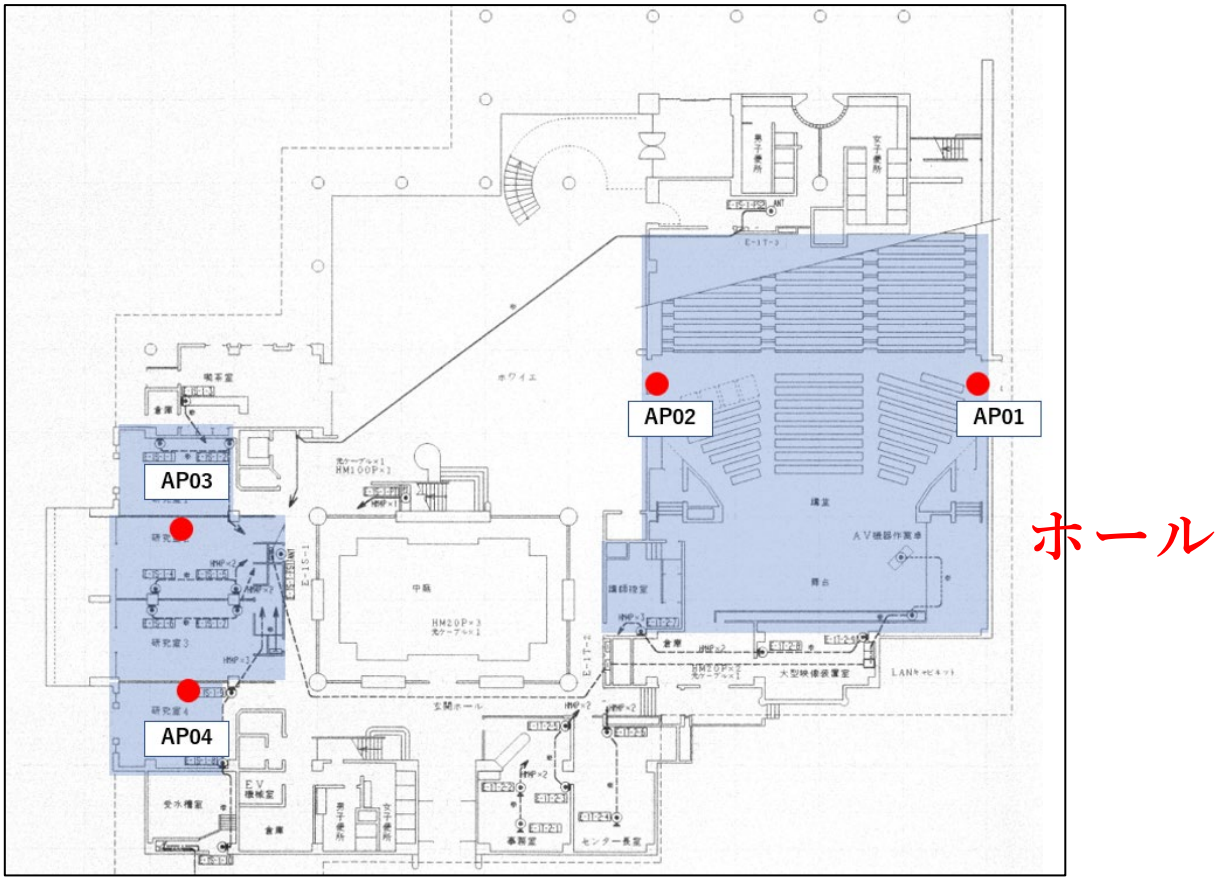


図 2. 交流センター1 階 アクセスポイント仮設置位置

1.10　電波調査経路

1.10.1　交流センター1 階 電波調査経路

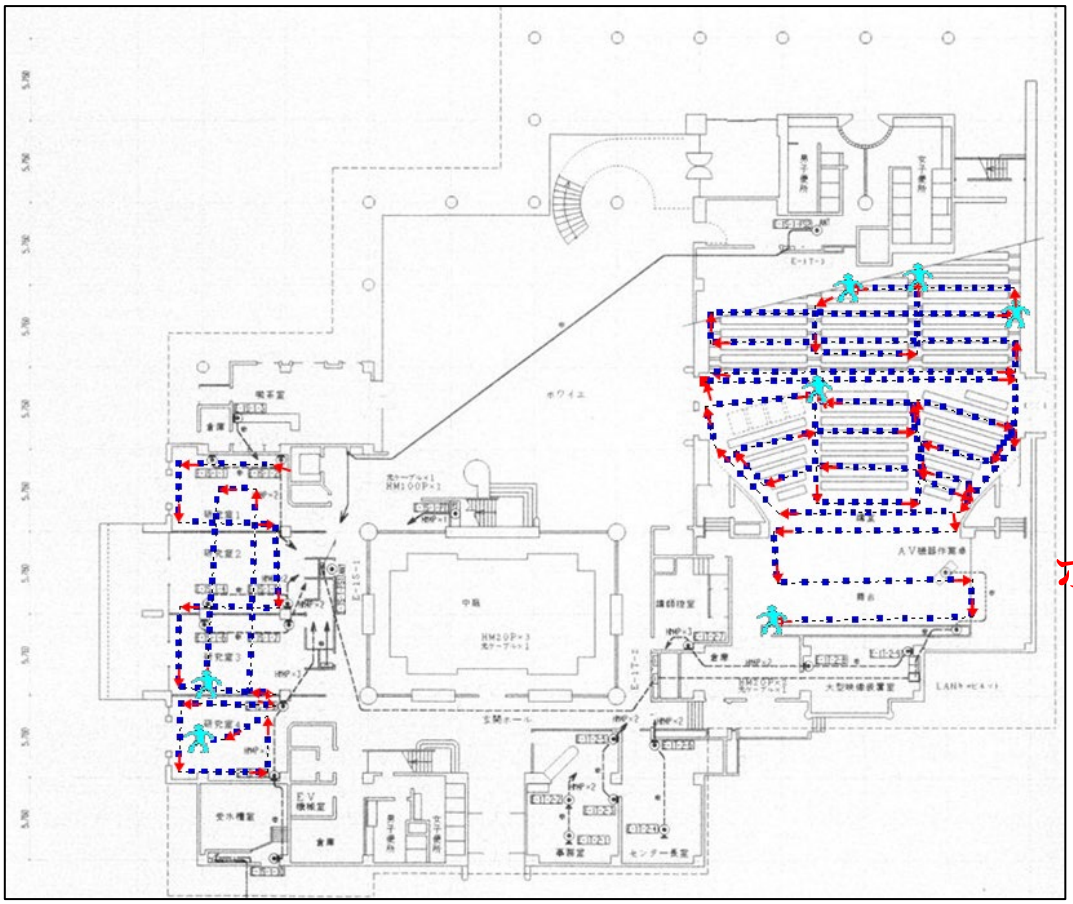


図 4. 交流センター1 階 電波調査経路

2　受信信号強度

アクセスポイントから受信した受信信号強度及び電波伝搬範囲を図示で表す。

2.1　交流センター1 階 2.4GHz 帯の受信信号強度

2.1.1 2.4GHz 帯全体の受信信号強度

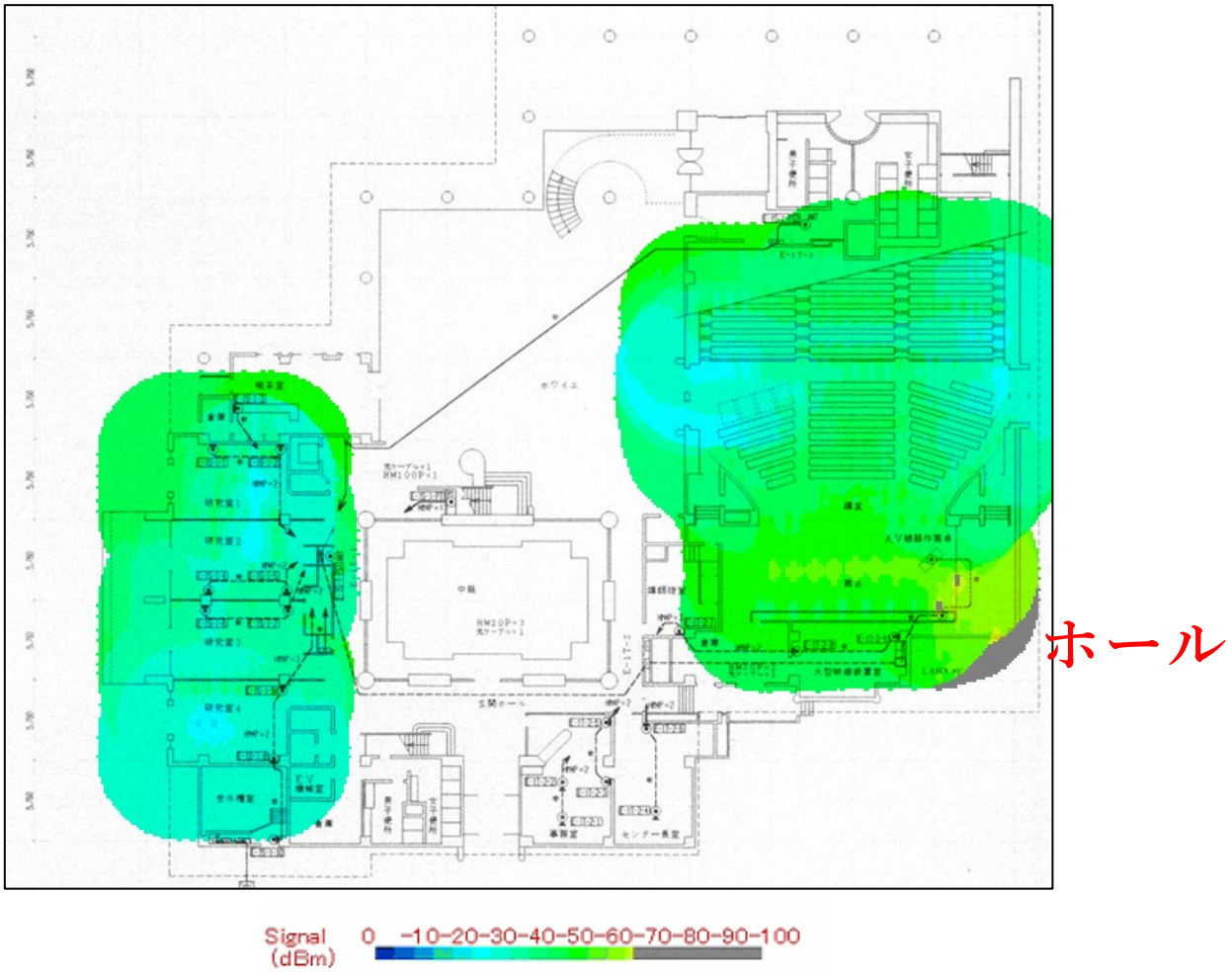


図 6. 2.4GHz 帯全体の受信信号強度

2.1.2 5GHz 帯全体の受信信号強度

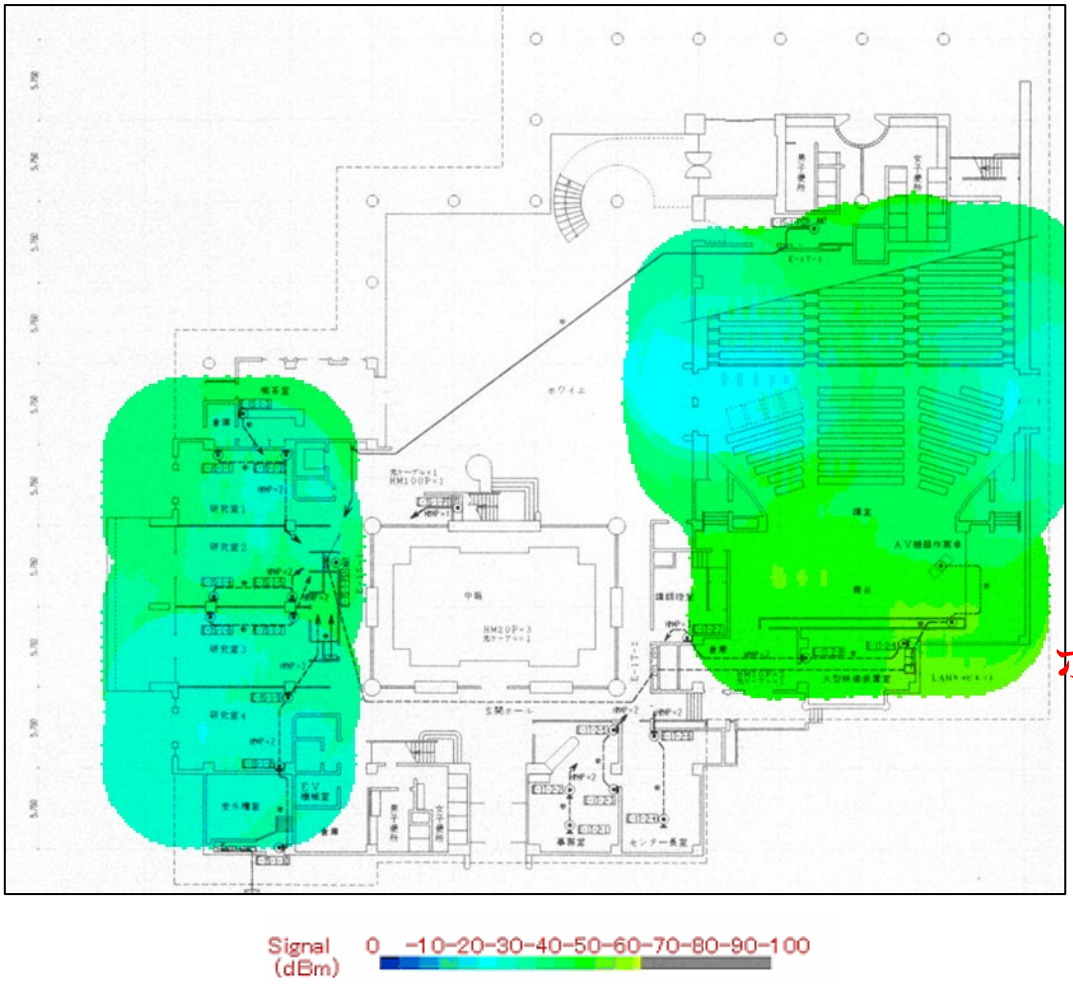


図 7. 5GHz 帯全体の受信信号強度

4　結果

調査結果をフロア毎に報告する。

4.1　交流センター1 階

仮設置したアクセスポイントの電波伝搬範囲を調査した結果、受信電波強度のしきい値を-67dB で判定した場合、無線 LAN 利用検討エリア全域で値を超えていることを確認。

アクセスポイント設置目安台数は、5 台。講堂は 2 台で測定しておりますが 3 台設置を推奨する。

周辺に存在するアクセスポイントについては、受信信号強度のしきい値を-85dBm で判定した場合、新規設置のアクセスポイントへ影響のある恐れがあるアクセスポイントを多数検出した。

5　参考

5.1　用語について

① 受信信号強度

無線 LAN 機器はデータレートごとに必要となる信号強度が決まっており、感度の値に基づいている。受信信号強度が強いほど、データレートは高くなる。

② 受信感度

受信感度とは、通信に必要な受信品質を確保できる最小受信入力電力のこと。

③ 外来波

無線 LAN 機器を導入しようとしている場所・範囲へ、他から同一周波数帯域で飛んできた電波のこと。無線 LAN 機器は受信感度以上の信号を受信すると通信に影響がある。

④ 雑音

受信に影響を与える電波のこと。無線 LAN 機器は受信感度以上の信号を受信すると雑音として検出する。

⑤ 信号対雑音比

信号対雑音比とは、信号電力と雑音比のこと。信号強度から雑音をひいたもので、電波の品質はこの値で判断する。信号対雑音比の値が 10dB 未満の場合は無線 LAN 機器の利用には適しない。

⑥ データレート

単位時間あたりにどれくらいのデータが処理あるいは送受信されるかを表す。 ⑦ BSSID（Basic Service Set Identifier）

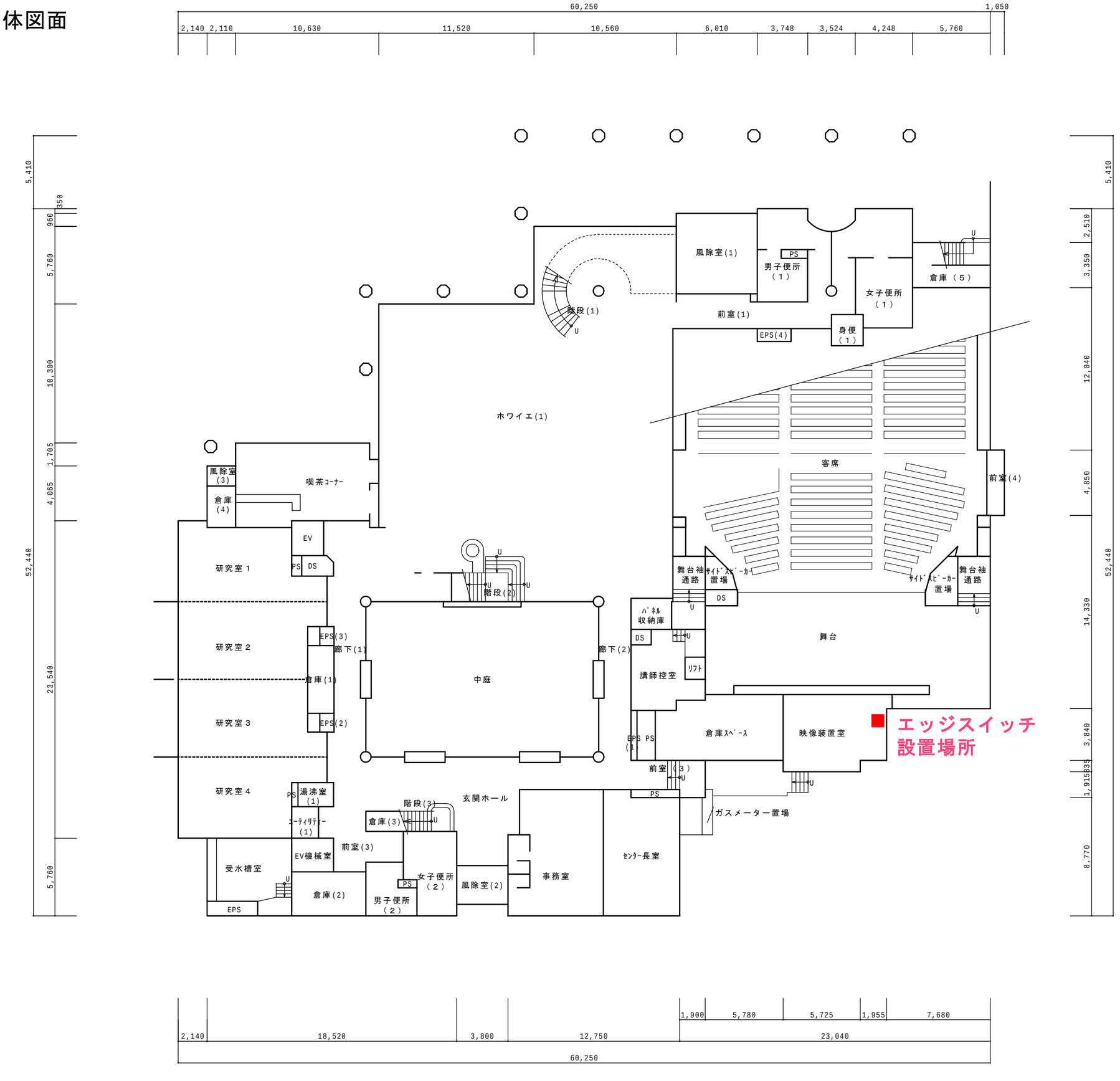
無線 LAN における識別子のこと。通常は無線 LAN の MAC アドレスと同じものを使用する。

⑧ ESSID（Extended Service Set Identifier）

無線 LAN における識別子のこと。無線 LAN 通信において、 ネットワーク同士の混信を避けるために設定される ID のこと。無線 LAN 接続時に特定のネットワークを指定する識別名で「SSID」「ネットワークネーム」とも呼ばれる。無線 LAN では、同じ ESSID を設定したアクセスポイントや端末同士で通信する。ESSID が異なるアクセスポイント・端末とは通信できない。

【別紙4-4】

交流センター1階全体図面



別紙5

現行死活監視対象機器

※茶色部は、今回の調達で削減されると想定する機器
※青色部は、今回の調達対象機器ではないが死活監視に含める機器

NO	監視対象機器(ホスト名)	機種	タイプ	監視項目
1	A5-F1	AT-SBx8112	Allied Telesis Switch	SNMP,PING
2	A5-AF0	AT-x510-52GTX	Allied Telesis Switch	SNMP,PING
3	A5-DMZ1	AT-x510-52GTX	Allied Telesis Switch	SNMP,PING
4	EC-DMZ1	AT-x510-52GTX(商用回線)	Allied Telesis Switch	SNMP,PING
5	A5-SINET1	x530L-28GTX	Allied Telesis router	SNMP,PING
6	A5-SHOYO1	C1111-8P(商用回線)	Cisco 1100 Series Router	SNMP,PING
7	A5-LC1	F5-BIG-LC-I2600(負荷分散)	BIG-IP i2600 LinkController	SNMP,PING
8	A5-LC2	F5-BIG-LC-I2600(負荷分散)	BIG-IP i2600 LinkController	SNMP,PING
9	A5-FW1	PAN-PA-3220	PA-3220 with redun	SNMP,PING
10	A5-FW2	PAN-PA-3220	PA-3220 with redun	SNMP,PING
11	A5-FWR1	PAN-M-200	Palo Alto firewall	SNMP,PING
12	A5-DHCP1	Account@Adapter	ACP-APDHCP	PING
13	A5-DHCP2	Account@Adapter	ACP-APDHCP	PING
14	A5-WLC1	AIR-CT3504-K9	Cisco 3504 Wireless Controller	PING
15	A5-AF1	AT-x510-28GSX	Allied Telesis Switch	SNMP,PING
16	A0-AF1-S1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
17	A1-AF1-S2	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
18	A2-AF1-S3	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
19	A3-AF1-S4	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
20	A4-AF1-S5	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
21	B7-AF1-S9	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
22	A7-AF1-S10	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
23	B7-AF1-S11	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
24	A0-AF1-S1-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
25	A0-AF1-S1-T3-P1	AT-SH230-10GP	Allied Telesis Switch	SNMP,PING
26	A0-AF1-S1-T2	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
27	A0-AF1-S1-T4	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
28	A4-AF1-S5-L105	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
29	A4-AF1-S5-L205	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
30	A0-AF1-S1-T3	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
31	A1-AF1-S2-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
32	A4-AF1-S5-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
33	A1-AF1-S2-L301	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
34	A1-AF1-S2-L302	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
35	A2-AF1-S3-L201	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
36	A2-AF1-S3-L202	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
37	A3-AF1-S4-L301	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
38	A5-AF1-S13	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
39	A5-AF1-S13-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
40	A5-AF1-S13-T2	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
41	A5-AF1-S13-T3	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
42	B0-BF1	AT-x510-28GSX	Allied Telesis Switch	SNMP,PING
43	B0-BF1-S1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
44	B1-BF1-S2	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
45	B1-BF1-S3	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
46	B2-BF1-S4	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
47	B8-BF1-S5	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
48	B8-BF1-S6	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
49	B1-BF1-S2-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
50	B1-BF1-S3-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
51	B2-BF1-S4-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
52	B2-BF1-S4-T2	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
53	B2-BF1-S4-T3	AT-x230-28GT	Allied Telesis Switch	SNMP,PING

54	B2-BF1-S4-T4	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
55	B2-BF1-S4-T5	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
56	C3-CF1	AT-x510-28GSX	Allied Telesis Switch	SNMP,PING
57	C3-CF1-S1	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
58	C3-CF1-S2	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
59	C4-CF1-S3	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
60	C6-CF1-S4	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
61	C9-CF1-S5	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
62	C8-CF1-S6	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
63	C7-CF1-S7	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
64	C7-CF1-S8	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
65	C3-CF1-S2-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
66	C3-CF1-S2-T2	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
67	C2-CF1-S1-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
68	C5-CF1-S2-T4	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
69	C4-CF1-S3-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
70	C5-CF1-S2-T5	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
71	D3-DF1	AT-x510-28GSX	Allied Telesis Switch	SNMP,PING
72	D0-DF1-S1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
73	D2-DF1-S2	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
74	D3-DF1-S3	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
75	D5-DF1-S4	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
76	D6-DF1-S5	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
77	D7-DF1-S6	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
78	D2-DF1-S2-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
79	D2-DF1-S2-T2	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
80	D7-DF1-S6-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
81	E0-EF1	AT-x510-28GSX	Allied Telesis Switch	SNMP,PING
82	E0-EF1-S1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
83	E2-EF1-S2	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
84	E4-EF1-S3	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
85	E6-EF1-S4	AT-x510L-52GT	Allied Telesis Switch	SNMP,PING
86	E0-EF1-S1-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
87	E1-EF1-S2-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
88	E1-EF1-S2-T2	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
89	E2-EF1-S2-T3	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
90	E2-EF1-S2-T4	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
91	E3-EF1-S3-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
92	E3-EF1-S3-T2	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
93	E4-EF1-S3-T3	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
94	E4-EF1-S3-T4	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
95	E7-EF1-S4-T1	AT-x230-28GT	Allied Telesis Switch	SNMP,PING
96	EC-F1-S1	AT-x530L-28GTX	Allied Telesis Switch	SNMP,PING
97	EC-F1-S2	AT-x530L-28GTX	Allied Telesis Switch	SNMP,PING
98	EC-F1-S201F	AT-x530L-52GTX	Allied Telesis Switch	SNMP,PING
99	EC-F2-S201F	AT-x530L-28GTX	Allied Telesis Switch	SNMP,PING
100	EC-F1-S202F	AT-x530L-52GTX	Allied Telesis Switch	SNMP,PING
101	EC-F2-S202F	AT-x530L-28GTX	Allied Telesis Switch	SNMP,PING
102	EC-F1-S203F	AT-x530L-52GTX	Allied Telesis Switch	SNMP,PING
103	EC-F2-S203F	AT-x530L-28GTX	Allied Telesis Switch	SNMP,PING
104	EC-F1-S301F	AT-x530L-52GTX	Allied Telesis Switch	SNMP,PING
105	EC-F2-S301F	AT-x530L-28GTX	Allied Telesis Switch	SNMP,PING
106	EC-F1-S302F	AT-x530L-52GTX	Allied Telesis Switch	SNMP,PING
107	EC-F2-S302F	AT-x530L-28GTX	Allied Telesis Switch	SNMP,PING
108	EC-F1-S303F	AT-x530L-52GTX	Allied Telesis Switch	SNMP,PING
109	EC-F2-S303F	AT-x530L-52GTX	Allied Telesis Switch	SNMP,PING
110	slogadm	Dell PowerEdge R340 Server	ログ収集サーバ	PING
111	netadm	Dell PowerEdge R340 Server	死活監視サーバ	PING
112	UPS005	BU75RWQ6	無停電電源装置	PING
113	UPS006	BU75RWQ6	無停電電源装置	PING
114	A5-RADIUS1	SNS-3615-K9	Cisco radius server	SNMP,PING
115	A5-RADIUS2	SNS-3615-K9	Cisco radius server	SNMP,PING

116	bkadm01	WS5420RN12W6	TeraStation WSS Windows Storag	PING
117	fsw01		Windows	PING,CIFS/SMB
118	fs01		Linux	PING
119	info-lib01		Windows	PING
120	info-lib02		Windows	PING
121	dl01		Linux	PING,LDAP,DNS
122	dl02		Linux	PING,LDAP,DNS
123	off-dc02		Windows	PING
124	man-ld01		Windows	PING
125	met-ld01		Linux	PING,LDAP
126	web-ld02		Linux	PING,HTTP
127	web-ld01		Linux	PING,HTTP
128	HUS用UPS		無停電電源装置	PING
129	off-ad01		Windows	PING
130	off-ad02		Windows	PING
131	dsk-gw01		Windows	PING,HTTP
132	off-dm01		Linux	PING,DNS
133	ses1-mx01		Linux	PING,DNS
134	shc1-mx01		Linux	PING,DNS
135	nurse1-mx01		Linux	PING,DNS
136	off-dm02		Linux	PING,DNS
137	mech1-mx01		Linux	PING,DNS
138	mat1-mx01		Linux	PING,DNS
139	e1-mx01		Linux	PING,DNS
140	off1-mx01		Linux	PING,DNS
141	kanri1-mx01		Linux	PING,DNS
142	kanri2-mx01		Linux	PING,DNS
143	line4	DNS(商用回線)	Linux	PING,DNS
144	spins2		Linux	PING,DNS
145	off-we01		Linux	PING,HTTP
146	off-we11		Linux	PING,HTTP
147	ssl-01	PSA-300(現行SSL-VPN)	PulseSecure(Ivanti)	PING
148	ssl-02	PSA-300(現行SSL-VPN)	PulseSecure(Ivanti)	PING
149	ssl-0102	SSL-VPN用VIP		
150	vboot VIP			PING,HTTP
151	smtp		Linux	PING , 25
152	vc-01		Linux	PING,HTTP
153	vboot01		Windows	PING
154	vboot02		Windows	PING
155	vboot03		Windows	PING,HTTP
156	glexa		Linux	PING,HTTP
157	vm-03		仮想ホストサーバ	PING
158	vm-02		仮想ホストサーバ	PING
159	vm-01		仮想ホストサーバ	PING
160	kanri2020		Windows	PING
161	C7-311		Allied Telesis Switch	PING
162	C5-305			PING
163	C5-201		Allied Telesis Switch	PING
164	C6-304			PING
165	C3-CF1-S2-WA305	AIR-AP2802I-Q-K9	Cisco Access Point	PING
166	C5-CF1-S2-WA201	AIR-AP2802I-Q-K9	Cisco Access Point	PING
167	C6-CF1-WA01	AIR-AP2802I-Q-K9	Cisco Access Point	PING
168	C6-CF1-WA02	AIR-AP2802I-Q-K9	Cisco Access Point	PING
169	C7-CF1-WA311	AIR-AP2802I-Q-K9	Cisco Access Point	PING
170	C3-CF1-S2-WA304	AIR-AP2802I-Q-K9	Cisco Access Point	PING
171	C6-CF1-S4-WA304	AIR-AP2802I-Q-K9	Cisco Access Point	PING
172	E2-EF1-S2-WA01			PING
173	E2-EF1-S2-WA101			PING
174	E2-EF1-S2-WA211			PING
175	C8-2F-AP02			PING
176	C7-CF1-WA305	AIR-AP2802I-Q-K9	Cisco Access Point	PING
177	C7-CF1-WA307	AIR-AP2802I-Q-K9	Cisco Access Point	PING

178	C7-CF1-WA310	AIR-AP2802I-Q-K9	Cisco Access Point	PING
179	liy-vmc	RX2530 M2	Windows	PING
180	BAC01	RX2530 M2	Windows	PING
181	spins35		Linux	PING,HTTP
182	spins1		Linux	SSH,PING,DNS
183	keihoadm	ISA - DN1000-1R	警告灯	PING
184	A0-2F-AP01	AIR-AP2802I-Q-K9	Cisco Access Point	PING
185	A0-2F-AP02	AIR-AP2802I-Q-K9	Cisco Access Point	PING
186	A0-2F-AP03	AIR-AP2802I-Q-K9	Cisco Access Point	PING
187	A0-2F-AP04	AIR-AP2802I-Q-K9	Cisco Access Point	PING
188	A0-2F-AP05	AIR-AP2802I-Q-K9	Cisco Access Point	PING
189	A0-3F-AP01	AIR-AP2802I-Q-K9	Cisco Access Point	PING
190	A0-3F-AP02	AIR-AP2802I-Q-K9	Cisco Access Point	PING
191	A0-3F-AP03	AIR-AP2802I-Q-K9	Cisco Access Point	PING
192	A0-3F-AP04	AIR-AP2802I-Q-K9	Cisco Access Point	PING
193	A1-1F-AP01	AIR-AP2802I-Q-K9	Cisco Access Point	PING
194	A1-301-AP01	AIR-AP1852I-Q-K9	Cisco Access Point	PING
195	A1-302-AP01	AIR-AP1852I-Q-K9	Cisco Access Point	PING
196	A2-1F-AP01	AIR-AP1852I-Q-K9	Cisco Access Point	PING
197	A2-1F-AP02	AIR-AP1852I-Q-K9	Cisco Access Point	PING
198	A2-1F-AP03	AIR-AP1852I-Q-K9	Cisco Access Point	PING
199	A2-201-AP01	AIR-AP1852I-Q-K9	Cisco Access Point	PING
200	A2-202-AP01	AIR-AP1852I-Q-K9	Cisco Access Point	PING
201	A3-301-AP01	AIR-AP1852I-Q-K9	Cisco Access Point	PING
202	A4-105-AP01	AIR-AP1852I-Q-K9	Cisco Access Point	PING
203	A4-205-AP01	AIR-AP1852I-Q-K9	Cisco Access Point	PING
204	A7-1F-AP01	AIR-AP2802I-Q-K9	Cisco Access Point	PING
205	A7-1F-AP02	AIR-AP2802I-Q-K9	Cisco Access Point	PING
206	A7-1F-AP03	AIR-AP2802I-Q-K9	Cisco Access Point	PING
207	A7-1F-AP04	AIR-AP2802I-Q-K9	Cisco Access Point	PING
208	A7-1F-AP05	AIR-AP2802I-Q-K9	Cisco Access Point	PING
209	C1-102-AP01	AIR-AP2802I-Q-K9	Cisco Access Point	PING
210	C1-2F-AP01	AIR-AP2802I-Q-K9	Cisco Access Point	PING
211	C2-2F-AP01	AIR-AP2802I-Q-K9	Cisco Access Point	PING
212	C3-1F-AP01	AIR-AP2802I-Q-K9	Cisco Access Point	PING
213	C3-1F-AP02	AIR-AP2802I-Q-K9	Cisco Access Point	PING
214	C4-210-AP01	AIR-AP2802I-Q-K9	Cisco Access Point	PING
215	C4-CF1-S3-WA151	AIR-AP2802I-Q-K9	Cisco Access Point	PING
216	C8-2F-AP01	AIR-AP2802I-Q-K9	Cisco Access Point	PING
217	D0-202-AP01	AIR-AP2802I-Q-K9	Cisco Access Point	PING
218	D7-1F-AP01	AIR-AP1852I-Q-K9	Cisco Access Point	PING
219	D7-1F-AP02	AIR-AP2802I-Q-K9	Cisco Access Point	PING
220	D7-1F-AP03	AIR-AP2802I-Q-K9	Cisco Access Point	PING
221	D7-2F-AP01	AIR-AP2802I-Q-K9	Cisco Access Point	PING
222	D7-2F-AP02	AIR-AP2802I-Q-K9	Cisco Access Point	PING
223	E5-101-AP01	AIR-AP2802I-Q-K9	Cisco Access Point	PING
224	E5-101-AP02	AIR-AP2802I-Q-K9	Cisco Access Point	PING
225	E6-1F-AP01	AIR-AP2802I-Q-K9	Cisco Access Point	PING
226	LIB-2F-AP01	AIR-AP1852I-Q-K9	Cisco Access Point	PING
227	LIB-2F-AP02	AIR-AP1852I-Q-K9	Cisco Access Point	PING
228	LIB-3F-AP01	AIR-AP1852I-Q-K9	Cisco Access Point	PING
229	LIB-3F-AP02	AIR-AP1852I-Q-K9	Cisco Access Point	PING
230	A1-112-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
231	A1-113-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
232	A1-204-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
233	A1-205-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
234	A1-209-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
235	A3-101-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
236	A3-102-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
237	A3-104-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
238	A3-105-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
239	A3-106-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING

240	A3-201-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
241	A3-202-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
242	A3-204-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
243	A3-205-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
244	A3-206-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
245	A3-303-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
246	A4-101-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
247	A4-102-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
248	A4-103-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
249	A4-104-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
250	A4-106-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
251	A4-107-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
252	A4-108-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
253	A4-201-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
254	A4-202-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
255	A4-203-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
256	A4-204-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
257	A4-206-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
258	A4-207-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
259	A4-209-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
260	A4-210-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
261	A4-301-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
262	A4-302-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
263	A4-303-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
264	A4-304-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
265	A4-305-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
266	A4-306-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
267	A4-307-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
268	A5-LIB-1F-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
269	E0-201-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
270	E1-101-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
271	E2-102-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
272	E2-103-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
273	E2-212-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
274	E3-101-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
275	E3-102-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
276	E3-104-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
277	E3-201-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
278	E4-101-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
279	E4-201-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
280	E5-102-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
281	E5-103-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
282	E5-104-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
283	E5-105-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
284	E7-101-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
285	E7-102-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
286	E7-103-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
287	E7-104-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
288	E7-105-AP-R6	AT-TQ6702 GEN2	Allied Telesis Access Point	PING
289	a5-wlc-r6		Windows	PING
290	captive-p		Linux	PING