学内情報ネットワーク等リース

仕様書

群馬県立県民健康科学大学

1. 目的

学内情報ネットワークとは、本学に所属する教職員及び学生がコンピュータネットワークにより接続されたPCなどの情報機器等を利用して、安全かつセキュリティを保持した状態で学内及び学外（インターネット等）と情報共有を行う設備及びサービスを示す。また、学内情報ネットワークの利用は、別紙８「群馬県立県民健康科学大学学内情報ネットワーク利用規程」によって規定される。また、本システムの導入は、既存の学術情報ネットワーク等リースのリース期間満了に対する機器更新等であり、既存の配線の張り替え、情報機器の置き換えを基本とするが、情報セキュリティ等、最新の技術に対応させるため、本仕様書に具体的な内容を示すものである。

2. 学内情報ネットワークの範囲と関連する情報システム

学内情報ネットワークの範囲は、図１に示す学内施設に敷設されたLAN配線設備及びコアスイッチ、フロアスイッチ、ファイアーウォール、認証機器、無線アクセスポイントなどの情報機器等と、学内の研究室、演習室、教室、事務室等に設置された情報コンセント（LANコンセント）等から構成される。また、機器認証、ユーザ認証等のサービスによって、情報機器の接続可否や利用者の通信制限、ファイアーウォール等の情報機器により、外部からの不正アクセスの制限、内部からの不正利用の禁止、利用制限を行い、また利用履歴の管理等を行えるようにすることとする。

学内情報ネットワークの接続する他の情報システムには、SINET接続サービス、インターネットサーバシステム（認証サーバ、メールサーバ、ファイルサーバ、ポータルサーバ等）、マルチメディア教室システム、外部向けwebサーバ（ホスティングサーバ）、学務システム（県立女子大共用システムにて、サーバ本体は女子大学内部に設置）、図書館情報システム（一部、外部サーバとの連携あり）、研究用外部サーバ等があり、それらの他の情報システム等との安全かつ適切な接続が求められるため、学内情報ネットワークの導入・設置に関して、それらの情報システムとの接続確認をあらかじめ考慮したシステム設計、動作確認が必要となる。特に接続速度低下やサービスの利用不可などが発生しないように十分に他のシステムとの接続状況を確認するとともに、セキュリティに留意し、安定かつ適正な利用が可能となるように注意する必要がある。

3.　導入機器及び設置場所

　システムの構成は、別紙１「システム構成図」のとおりで、構成する情報機器等は別紙２「システム構成機器」、別紙３「導入機器等仕様書」のとおりとします。

　設置場所は、基幹サーバシステムは、北棟３F サーバ室内とし、フロアスイッチ等は随時「システム構成図」に示す設置場所等とする。

　なお、既存の学術情報ネットワーク機器の更新となる為、既存の設置場所への置き換え配置を基本とするが、導入する機器の大きさ、仕様等の変更によっては、既存設置場所への敷設が困難となる場合が予想されるため、その場合は十分留意する必要がある。

　また、関連する情報機器との接続において、既存の情報システム側の設定変更、仕様変更等は原則行わないが、必要な設定変更は受注者の責任において実施することは可能とする。

4.　保守仕様

　別紙６「保守仕様」のとおり

5.　納入先

　群馬県立県民健康科学大学　北棟、西棟、南棟（別紙１「システム構成図」、別紙５　LAN コンセント設置場所及び無線 LAN-AP の利用可能範囲）参照）のとおりとする。

6.　導入方式

　長期リースによる賃貸借契約とする

7.　借入期間

　平成 31(2019)年 10 月 1 日から平成 36(2024)年 9 月 30 日まで　５年間

8.　支払方法

　契約代金の支払い請求を以下の各月の末日に請求することができる。

　なお、発注者は、特別の理由のない限り請求書を受理した日から３０日以内に口座振替により支払うものとする。

平成 31(2019)年度分については、平成 32(2020)年 3 月末日 （６月分)。
平成 32(2020)年度前期分については、平成 32(2020)年 9 月末日（６月分)。
平成 32(2020)年度後期分については、平成 33(2021)年 3 月末日（６月分)。
平成 33(2021)年度前期分については、平成 33(2021)年 9 月末日（６月分)。
平成 33(2021)年度後期分については、平成 34(2022)年 3 月末日（６月分)。
平成 34(2022)年度前期分については、平成 34(2022)年 9 月末日（６月分)。
平成 34(2022)年度後期分については、平成 35(2023)年 3 月末日（６月分)。
平成 35(2023)年度前期分については、平成 35(2023)年 9 月末日（６月分)。
平成 35(2023)年度後期分については、平成 36(2024)年 3 月末日（６月分)。
平成 36(2024)年度分については、平成 36(2024)年 9 月末日 （６月分)。

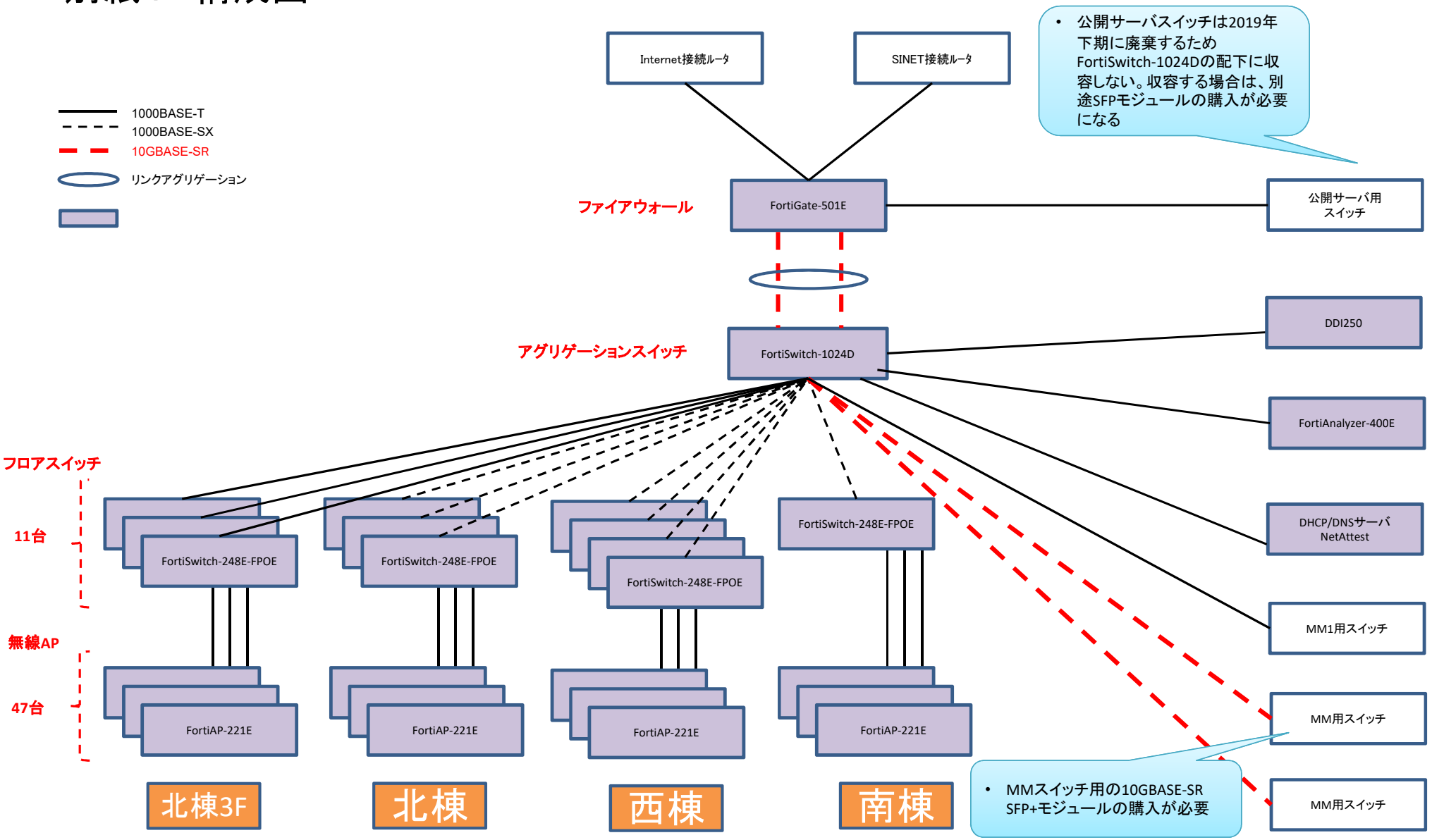
9. その他

受注者は、機器の据付、組立、設定及び保守にあたり、別紙７「個人情報取扱特記事項」を厳守すること。

付属資料

別紙１　システム構成図
別紙２　システム構成機器
別紙３　導入機器等仕様書
別紙４　VLAN リスト
別紙５　LAN コンセント設置場所及び無線 LAN-AP の利用可能範囲
別紙６　保守仕様書
別紙７　個人情報取扱特記事項
別紙８　群馬県立県民健康科学大学　学内情報ネットワーク利用規程
別紙９　仕様書質問事項

別紙1　構成図


1000BASE-T
1000BASE-SX
10GBASE-SR
リンクアグリゲーション
Internet接続ルータ
SINET接続ルータ
• 公開サーバスイッチは2019年下期に廃棄するためFortiSwitch-1024Dの配下に収容しない。収容する場合は、別途SFPモジュールの購入が必要になる
ファイアウォール
FortiGate-501E
公開サーバ用スイッチ
アグリゲーションスイッチ
FortiSwitch-1024D
DDI250
FortiAnalyzer-400E
DHCP/DNSサーバ NetAttest
MM1用スイッチ
MM用スイッチ
MM用スイッチ
フロアスイッチ
11台
無線AP
47台
FortiSwitch-248E-FPOE
FortiSwitch-248E-FPOE
FortiSwitch-248E-FPOE
FortiSwitch-248E-FPOE
FortiAP-221E
FortiAP-221E
FortiAP-221E
FortiAP-221E
北棟3F
北棟
西棟
南棟
• MMスイッチ用の10GBASE-SR SFP+モジュールの購入が必要

別紙２「システム構成機器」

- ファイアーウォール
- ファイヤーウォール・ネットワーク解析装置
- ふるまい検知装置
- フロアスイッチ（Ｌ２）
- アグリケーションスイッチ
- DHCP サーバ/DNS サーバ
- ネットワーク管理用 PC
- 無線 AP
- 無停電電源装置
- ルータ

※サーバスイッチ及びハーフラックに関しては既存のモノを使用する

別紙３「導入機器等仕様書」

学内情報ネットワークの導入機器仕様について

本リース契約は、本学の学内において、学生が授業及び自己の学習において、また全教職員が大学の運営事務及び教育研究活動において、情報通信機器を用いて、Web 閲覧等による情報収集、公開 Web サーバによる情報発信、E-mail、SNS 等による情報交換等をスムーズに行うための学内情報通信基盤を整備し、学生と教職員が学内及び学外との情報通信を安全かつ適正に利用することを目的とする。

本学の学内情報システムは、2013 年 12 月から機器更新によりリース契約の運用を開始したが、本契約は、その継続リースとして従来の学術情報ネットワークの仕様、運用方法等を踏襲しつつ、技術革新による新たな技術の導入により、個人情報や学内施設の有する情報資産を安全かつ完全に、セキュリティを確保した状態で利用できる情報基盤を整備することとする。また、近年、流通する情報量の急増と学内利用者の増大に対応し、適正な接続帯域・速度を安定的に維持し、安全かつ簡便に情報機器を接続できる環境を目指す。

セキュリティ面については、特定多数の学生、教職員が同時に接続利用することに鑑み、学生が接続する LAN 回線（以下「学生 VLAN」とする）と教員が接続する LAN 回線（以下「教員 VLAN」とする）及びその他運営等で利用する LAN 回線（その他の VLAN 回線）を仮想ネットワーク（VLAN）によって、区画し、それぞれの VLAN 同士の接続を分離することによって、セキュリティ保持を行うものとする。また、教員 VLAN は、教員個々の VLAN として区画し、全教員数を上回る VLAN 設定を行うことが必要である。なお、区画設定する VLAN については、別紙４「VLAN リスト」に示す構成と、VLAN 数を設定可能な機能を有することを必須とする。

1　　システム構成

1.1　対象設備

学内情報ネットワークを構成する機器を規定するものである。

1.2　システム構成

本仕様書で規定する機能・性能を満足する装置にて構成するものとする。

1.3 基本要件

1.3.1 システム全体を見通したネットワーク設計を行い、機器の選定、設計を行うこと。

1.3.2 接続クライアント(ポート)間の通信プロトコル制限、経路制限、通信データ帯域制限等の機能により、ネットワーク全体の適正利用が可能な構成とすること。

1.3.3 セキュリティと接続速度を適正に管理、運用可能な構成とすること。

1.3.4 教員 VLAN に係る接続機器は、MAC アドレス認証にて、許可され登録された機器のみが、許可された範囲で、許可された通信プロトコルにて、許可されたデータ転送帯域にて、安全な通信が確保される機能を有すること。

1.3.5 学生 VLAN に係る接続機器は、パスワードによる認証方法とし、許可された範囲で、許可された通信プロトコルにて、許可されたデータ転送帯域にて、安全な通信が確保される機能を有すること。

1.3.6 接続機器の追加、変更等に対して、ネットワークシステムを長時間停止することなく、ハードウェア及びソフトウェアの追加・変更ができること。

1.3.7 接続機器の設定許可の追加、変更等は、情報部会ネットワーク管理者が容易に設定変更可能な機能を用意すること。

1.4 ネットワーク

1.4.1 導入については、事前に情報部会ネットワーク管理者に作業内容、作業計画を提出し、協議の上、日程等を調整・決定すること。

1.4.2 ネットワークシステムの設置にあたり、サーバラック等、無停電電源装置、機器設置に必要な機器を本調達に含むこと。

1.4.3 ネットワーク導入に際し、関連業者への影響、安全配慮を十分に行い、本学の情報部会ネットワーク管理者との日程協議を行うこと。また、学内の一般共用箇所にて作業を行う場合は、安全通路の確保を十分に行うこと。

1.4.4　システム移行後の旧機器の解体収集作業を実施すること

1.4.5　既存のネットワーク設定を本学情報部会ネットワーク管理者の指示に基づき、新ネットワークシステムに設定情報の登録、移行を実施すること。

1.4.6　稼働後のユーザ情報、接続機器等の変更が、本学情報部会ネットワーク管理者にて、web ベースにて、容易に設定変更可能であること。また、設定変更に関する操作マニュアルを用意すること。

1.4.7　ネットワークの遅延、通信障害が発生した場合等で、ネットワークの設定変更が必要な場合は、本学情報部会ネットワーク管理者と協議し、設定変更を提案すること。

1.5　ネットワーク構成

1.5.1　別紙１　システム構成図を構成する上で必要なネットワークトポロジ構成とすること。

1.5.2　1 つのインターフェースに複数の IP アドレスを設定し、論理的に複数セグメントとして動作することが可能なこと。

1.5.3　ギガビットイーサネットをバックボーンとする、基幹ネットワークを構築すること。

1.5.4　機器は、ファイアーウォール、アグリゲーションスイッチ、ネットワーク監視装置、、フロアスイッチ（Ｌ２）、サーバスイッチ、DHCP サーバ、DNS サーバ、ネットワーク管理用 PC、無線ＡＰ、サーバラック等で構成されること。

1.5.5　アグリゲーションスイッチに接続される各スイッチ間は、光ファイバーケーブル、又はＵＴＰ（Cat5E 以上）を用いたリンクで接続すること。

1.5.6　ファイアーウォール･アグリゲーションスイッチは、十分な機能と接続速度を有する場合は、同機能を有する一体型兼用機器も可とする。

1.5.7　ファイアーウォール･アグリゲーションスイッチは、サーバ室に設置し、各機器を収容すること。

1.5.8　ネットワーク監視装置はアグリゲーションスイッチまたはファイアーウォールと連携し、ネットワークの通信状況を効果的に

可視化可能とすること。またリモートにて、情報部会ネットワーク管理者が web 等で、遠隔監視が可能なこと。

1.5.9 サーバスイッチはファイアーウォールに接続し、サーバ室に設置された公開サーバ、内部用サーバ等のサーバ機器を収容すること。

1.5.10 フロアスイッチはコアスイッチに接続し、学内の各棟の各階に設置し、教室、演習室、研究室等の端末や無線ＡＰを収容すること。

1.5.11 無線ＡＰはフロアスイッチに接続し、無線端末を収容すること。

1.5.12 ＤＨＣＰサーバはＤＨＣＰクライアントに IP アドレス等、クライアントがネットワークに接続する際に必要な情報を配布すること。また、必要に応じて、情報部会ネットワーク管理者が web 等により設定変更が可能であること。

1.5.13 各棟や各階単位で簡便に拡張できる構成であること。接続エリアの追加等によってシステム停止を伴うネットワーク全体の構成設計変更が発生しないこと。

1.5.14 将来の拡張性や他システムとの相互接続のため、採用される技術は可能な限り IEEE などの標準技術を基準とすること。運用上不足する機能などは運用または標準技術を基礎とした拡張機能、及び標準規格化の動きのある技術等を検討するものとし、将来の変更に対して障害となる可能性を極力排除すること。

1.6 ネットワーク帯域

1.6.1 アグリゲーションスイッチに接続されるサーバスイッチ間で、設置場所が異なる主要な回線は、光ファイバーケーブル（1000Base-SX）以上の高速回線とすること。

1.6.2 アグリゲーションスイッチに接続されるサーバスイッチ間で、設置場所が同一回線は UTP (Cat6 以上) のリンクで接続し、1Gbps 以上の帯域を有すること。

1.6.3 サーバスイッチは 1000Base-T 以上のインターフェースをもつサーバを、必要数収容できること。

1.6.4 フロアスイッチは、1000Base-T または 1000Base-SX のインター

フェースをもちコアスイッチ、無線ＡＰと接続し、端末と100Base-TX/1000Base-T で接続できること。また無線ＡＰに給電する機能を持つこと。

1.6.5　VLAN 設定と連動して、特定の VLAN のネットワーク帯域を制限、調整可能な機能を有すること。

1.6.6　VLAN 設定と連動して、特定の VLAN のネットワークの通信可能なネットワークプロトコルを制限、調整可能な機能を有すること。

1.6.7　帯域を制限、プロトコルを制限等は、情報部会ネットワーク管理者が、容易に可能な機能を用意すること。

1.7　ドキュメント

1.7.1　本システムにおいて、システム構成・技術要件の確認、システムメンテナンスを容易に行うために、設計書、接続システム構成図、設定マニュアルなどのドキュメントを作成し、検索可能なデジタルファイルで添付すること。

1.7.2　ネットワークシステムにおける、各機器のハードウェアに関するマニュアルを、検索可能なデジタルファイルで提供すること。

1.7.3　ネットワークシステムの運用手順書、バックアップマニュアル及び障害切り分けマニュアルを、検索可能なデジタルファイルで提供すること。

1.7.4　上記のドキュメントは、日本語とする。

2　ネットワーク装置

2.1　ファイアーウォール　（1 式）

2.1.1　別紙１システム構成図を構成する上で、外部からのアタック、内部からの不正利用等のセキュリティに対して、十分機能を有するとともに、速度低下の生じない機能、構成であること。

2.1.2　1000Mbase-SX インターフェースを 8 ポート以上有すること。

2.1.3　10Gbase-SX インターフェースを 2 ポート以上有すること。

2.1.4　1GbE RJ-45 インターフェースを 8 ポート以上有すること。

2.1.5　秒間の最大新規セッション数が 300,000 以上であること

2.1.6　最大同時セッション数が 8,000,000 以上であること

2.1.7　ファイアーウォールは 22Gbps 以上の転送能力を有すること。（IPv4　64 バイト UDP、IPv6 64 バイト UDP）

2.1.8　レイテンシ(遅延)が 2μs 以下であること。

2.1.9　ポリシー数は 10,000 以上対応可能なこと。

2.1.10 脅威保護スループットは 4.7Gbps 以上であること。

2.1.11 暗号化通信の中身を検査する SSL インスペクション機能を有し、平均 5.7Gbps 程度のスループットを実現可能なこと。

2.1.12 IPsecVPN スループットは 20Gbps 以上であること。

2.1.13 IPS スループットは 5.2Gbps 以上であること。

2.1.14 ASIC を実装することにより高速処理を実現し、且つ、CPU の負荷を軽減する構造となっていること。

2.1.15 480GB 以上の容量の SSD を搭載していること。

2.1.16 電源が二重化されていること

2.1.17 管理専用ポートを 2 つ以上保有すること。

2.1.18 USB インターフェースを 2 つ以上保有し、USB メモリを利用して設定やファームウェアを起動時に読み込むことで容易にリカバリ可能なこと。

2.1.19 19 インチラックに搭載可能で、1RU 以内であること。

2.1.20 ファイルを再構成してスキャンする高度なウィルス検査方式(プロキシ型)およびパケットベースによるウィルス検知機能(フロー型)の双方を有すること。また、スキャン方式は選択が可能であること。

2.1.21 セキュリティ機能としてファイアーウォール機能、次世代ファイアーウォール機能(アプリケーション制御)、VPN 機能に加え、オプションとして不正侵入検知機能、アンチウイルス機能、Web フィルタリング機能、アンチスパム機能、DNS フィルタ機能の利用が可能であること。

2.1.22 各種シグネチャ・エンジンは自社開発であること。

2.1.23 セキュリティ機能はファイアーウォールポリシー毎に各機能の有効・無効の設定が可能なこと。

2.1.24 仮想システムごとに設定のバックアップ・リストアが可能なこと。

2.1.25 IPS 機能はユーザが個別でシグネチャを設定（カスタムシグネチャ）できる機能を有すること

2.1.26 80 カテゴリー以上のデータベースを持ち、カテゴリーごとに設定可能な Web フィルタリング機能を有すること。

2.1.27 仮想システムを利用することにより L3 型ファイアーウォールと L2 型ファイアーウォールが１台で混在可能なこと。

2.1.28 2,000 以上のアプリケーションを識別し遮断が可能なこと。

2.1.29 GUI 管理画面が日本語表示であること

2.1.30 ファイアーウォール、VPN、アンチウイルス、IPS 各部門において ICSA ラボなどの第三者機関による評価認定を取得していること。

2.1.31 10,000 以上の IPS のシグネチャを有すること。

2.1.32 HTTPS 通信の復号化ができ、アプリケーションの識別やコンテンツの検査が行えること

2.1.33 リモートアクセス用に SSL-VPN 機能を有し、スループットが 2.2Gbps 以上であること

2.1.34 Web プロキシサーバ機能を持つこと。

2.1.35 ネットワーク内の機器や OS を自動的に識別し、種別ごとのファイアーウォールポリシーを設定可能なこと。

2.1.36 無線 LAN コントローラ機能を有し、GUI で設定可能なこと。

2.1.37 スイッチのコントローラ機能を有し、GUI で設定可能なこと。
Active/Standby の冗長化構成が取れること。また、仮想システムごとにプライマリハードウェアを選択することで、
Active/Active 構成が取れること。

2.1.38 https 対応の Web インターフェースを有し、それ以外に SSH や Telnet による遠隔保守が可能であること。

2.1.39 WebUI は日本語対応していること。

2.1.40 WebUI 上でコマンドラインインターフェースを利用可能なこと。

2.1.41 ファイアーウォールのポリシー単位で、ユーザやグループ、アプリケーション、アンチウイルス、アンチスパム、IPS、Web フィルタリングのルールが設定できること。

2.1.42 仮想システムを複数設定可能なこと。仮想システム数は 10 以上標準対応可能なこと。

2.1.43 過去の設定を自動保存し、GUI 上で設定を比較する機能を持つこと。

2.1.44 複数の異なるバージョンの OS を保存できること。

2.1.45 複数台のファイアーウォールのファームウェア、シグネチャ、設定を一元管理できるアプライアンスと連携可能なこと。また、各ファイアーウォール装置がインターネットに接続しなくてもシグネチャを提供できること。

2.1.46 複数台のファイアーウォールのログを集中管理し、レポート生成可能なアプライアンスと連携可能なこと。

※参考機器　フォーティネット社 FortiGate-501E

2.2 ファイアーウォール・ログ解析装置　(1 式)

2.2.1 ファイアーウォール装置のファイアーウォール機能の情報・ログを収集・解析する機能を有すること。

2.2.2 1GbE RJ-45 インターフェースを 4 ポート以上有すること。

2.2.3 DB-9　シリアル管理コンソールを保有すること。

2.2.4 3TB x4 本、合計 12TB のストレージを搭載していること。

2.2.5 RAID 構成時は最大 6TB 利用可能であること。

2.2.6 HDD は交換可能なこと。

2.2.7 RAID 0/1/5/10(デフォルト 10)に対応していること。

2.2.8 消費電力は最大 93W 以内、平均 133W 以内であること。

2.2.9 放熱 456 BTU/h 以下であること。

2.2.10 19 インチラックに搭載可能で 1RU 以下であること。

2.2.11 1 日当たりのログ処理量は最大 200GB 以上であること。

2.2.12 分析時のログ処理持続レートは 1 秒あたり最大 6,000 であること。

2.2.13 連携可能なネットワークデバイス数が最大 200 以上であること。

2.2.14 次世代ファイアウォール(UTM)と管理・レポーティング装置間は、SSL 暗号化されたログ通信が保たれること。

2.2.15 次世代ファイアウォール(UTM)のログを収集・アーカイブする機能を有し、ネットワークの使用状況をグラフィカルに可視化できること。

2.2.16 シンプルで直感的な検索機能を使って、ネットワークのアクティビティやトレンドを検索し、レポートを作成可能なこと。

2.2.17 カスタマイズ可能 PD テンプレートでレポート表示可能なこと。IOC（Indicators of Compromise：侵害指標）を自動的に提供可能なこと。

2.2.18 アプリケーション、送信元、送信先、Web サイト、セキュリティの脅威、管理情報の変更、システムイベントのサマリを表示可能なこと。

2.2.19 事前定義済みのセキュリティイベントを容易にカス タマイズし、自動アラートを設定可能なこと。

2.2.20 カスタマイズ可能な NOC-SOC　ダッシュボードを有していること。

2.2.21 syslog サーバとして利用可能でサードバーティのログも受信できること。

2.2.22 https 対応の Web インターフェースを有し、それ以外に SSH や Telnet による遠隔保守が可能であること。

2.2.23 GUI は一般的な Web ブラウザを利用したものであること。

2.2.24 WebUI は日本語対応していること。

※参考機器:　FortiAnalyzer-400E

2.3　ふるまい検知装置　（1 式）

2.3.1　検出したイベントを、メール、SMTP/Syslog で通知可能なこと。

2.3.2　日次/週次/月次でログからレポートを作成できること。

2.3.3　既知の不正プログラムの通信を検知し、ログへの記録および管理者への通知ができること。
2.3.4　未知の不正プログラムの通信を検知し、ログへの記録および管理者への通知ができること。
2.3.5　標的型攻撃の通信を検知し、ログへの記録および管理者への通知ができること。
2.3.6　Web ベースの管理コンソールを利用して、ブラウザで設定および操作が行えること。
2.3.7　C&C サーバへのアクセスを検知できること。
2.3.8　不正な URL へのアクセスが検知できること。
2.3.9　既知の不正プログラムのダウンロードやアップロードが検知できること。
2.3.10 脆弱性攻撃の通信を検知可能なこと。
2.3.11 検知対象の除外設定が可能なこと。
2.3.12 通信監視用のポートとして 10/100/1000 BASE-T イーサネットポートを 3 以上有すること。
2.3.13 解析処理可能な総スループットが 250Mbps 以上であること。
2.3.14 DVD-RAM ドライブを内蔵できること。
2.3.15 外部接続可能な USB3.0 対応のインターフェスを標準で 2 ポート以上搭載していること。

※参考機種　Deep Discoery Inspector250

2.4　フロアスイッチ　(11 式)
2.4.1　本装置はサーバ室に設置のサーバスイッチを構成し、サーバや、サーバ室内の他のネットワーク機器を収容する機能を有すること。
2.4.2　1GbE SFP インターフェースを 4 ポート以上有すること。
2.4.3　1GbE RJ-45 インターフェースを 48 ポート以上有すること。
2.4.4　PoE 給電(802.3af/802.3at)ポートが 48 個以上かつ総給電量は 740W 以上であること。
2.4.5　シリアルコンソールポートを持つこと。

2.4.6　19 インチラックに搭載可能で、1RU 以内であること。
2.4.7　スイッチング容量は双方向で 104Gbps 以上であること。
2.4.8　消費電力は最大 120W(非給電時)以下であること。
2.4.9　レイテンシ(遅延)が 1μs 以下であること。
2.4.10 ジャンボフレームに対応していること。
2.4.11 ポートスピードおよび伝送形態のオートネゴシエーションが可能なこと。
2.4.12 IEEE 802.1D MAC ブリッジ / STP に対応していること
2.4.13 IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) に対応していること。
2.4.14 IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) に対応していること。
2.4.15 STP ルートガード機能をサポートしていること。
2.4.16 STP BPDU ガード機能をサポートしていること。
2.4.17 エッジポート / Port Fast 機能を持つこと。
2.4.18 IEEE 802.1Q VLAN タギング機能をサポートしていること。
2.4.19 プライベート VLAN 機能をサポートしていること。
2.4.20 IEEE 802.3ad LACP によるリンクアグリゲーション機能をサポートしていること。
2.4.21 https 対応の Web インターフェースを有し、それ以外に SSH や Telnet による遠隔保守が可能であること。
2.4.22 次世代型ファイアウォール(UTM)の GUI から集中管理可能なこと。

※参考機器　FortiSwitch 248E-FPOE

2.5 アグリゲーションスイッチ　(1 式)

2.5.1　本装置はサーバ室に設置のサーバスイッチを構成し、サーバや、サーバ室内の他のネットワーク機器を収容する機能を有すること。
2.5.2　10GbE SFP+ インターフェースを 24 ポート以上有すること。
2.5.3　シリアルコンソールポートを持つこと。
2.5.4　19 インチラックに搭載可能で、1RU 以内であること。

2.5.5　スイッチング容量は双方向で 480Gbps 以上であること。
2.5.6　消費電力は最大 140W 以下であること。
2.5.7　レイテンシ(遅延)が 800 ns 以下であること。
2.5.8　ジャンボフレームに対応していること。
2.5.9　ポートスピードおよび伝送形態のオートネゴシエーションが可能なこと。
2.5.10 IEEE 802.1D MAC ブリッジ / STP に対応していること
2.5.11 IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) に対応していること。
2.5.12 IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) に対応していること。
2.5.13 STP ルートガード機能をサポートしていること。
2.5.14 STP BPDU ガード機能をサポートしていること。
2.5.15 エッジポート / Port Fast 機能を持つこと。
2.5.16 IEEE 802.1Q VLAN タギング機能をサポートしていること。
2.5.17 プライベート VLAN 機能をサポートしていること。
2.5.18 IEEE 802.3ad LACP によるリンクアグリゲーション機能をサポートしていること。
2.5.19 https 対応の Web インターフェースを有し、それ以外に SSH や Telnet による遠隔保守が可能であること。
2.5.20 次世代型ファイアウォール(UTM)の GUI から集中管理可能なこと。
※参考機器　FortiSwitch 1024D

2.6　ＤＨＣＰ／ＤＮＳサーバ　(1 式)
2.6.1　本装置はネットワークに接続される端末機器等に IP アドレスを配布する役割を実現する機能を有すること。
2.6.2　内部ＤＮＳサーバ機能を端末機器等、ＤＮＳ情報を配布する役割を実現する機能を有すること。
2.6.3　ネットワークは、10/100/1000BASE-T(X)以上有すること。

2.6.4　ポートは６ポート以上有すること。
2.6.5　形状は、EIA 19 インチ、ラックマウントタイプであること。
2.6.6　電源は、90～264Vac、47～63Hz 内に収まること。
2.6.7　最大消費電力は、67VA 以下であること。
2.6.8　発熱量は、228.6BTU/h、57.6kcal、67W 以下であること。
2.6.9　適合規格は、VCCI Class A、FCC Class A、CE、UL、RoHS　PSE（電源ケーブル）であること。
※参考機種 NetAttest D3　(D3-ST52-A)

2.7　ネットワーク管理用 PC　(1 式)
2.7.1　本装置はネットワーク機器を管理するノート PC 又はタブレット装置であること。
2.7.2　OS は、Windows10Pro(64bit)であること。
2.7.3　セキュリティチップ（TPM2.0）を有すること
2.7.4　CPUCorei5－8350Ｕ－1.70GHz 以上または、同等レベルであること
2.7.5　メモリは、8GB 以上であること。
2.7.6　キーボードは、86 キー、JIS 配列準拠であること
2.7.7　液晶は、14.0 型ＨＤ以上であること。
2.7.8　ストレージは、暗号化機能付フラッシュメモリディスク 256GB 以上であること
2.7.9　通信は、802.11ac 無線 LAN(インテル(R) vPro(TM) テクノロジー対応)&Bluetooth であること
2.7.10 リカバリデータディスク+ドライバーズディスク追加(Win10pro)を有すること
2.7.11 Office は、Office Professional 2016 以上であること
2.7.12 バックアップ用 USB 媒体を用意すること
※参考機種　LIFEBOOK U748/S

2.8　無線ＡＰ（アクセスポイント）(47 式)

2.8.1　本装置は各フロアで無線 LAN 端末を接続するためのアクセスポイントであり、主に学生が利用可能な、講義室、演習室、実習室、調理室、大学院演習室、大学院院生室、図書館等に設置し、十分なセキュリティを確保し、安全な接続を可能とする機能を有すること。

2.8.2　本ネットワークにて、利用可能な範囲を別紙５「LAN コンセント設置場所及び無線 LAN-AP の利用可能範囲」に示す。なお、設置箇所及び設置機器の数量については、事前に十分な無線 LAN サーベイを実施し、利用範囲を十分に網羅するものとする。

2.8.3　ラジオ数が 2 つ以上であること。

2.8.4　内蔵アンテナを 4 つ以上有すること。

2.8.5　Radio 1 は 2.4Ghz b/g/n(2x2:2 ストリーム)に対応し、最大テータレートは 400Mbps 以上であること。

2.8.6　Radio 2 は 5Ghz a/n/ac(2x2:2 ストリーム)に対応し、最大テータレートは 867Mbps 以上であること。

2.8.7　10/100/1000Base-T RJ45 ポートを 1 ポート以上有すること。

2.8.8　Type A USB ポートを 1 ポート以上有すること

2.8.9　サイズは高さ 47mm、幅 160mm、奥行き 160mm 以内であること。

2.8.10 重量 0.5kg 以下であること。

2.8.11 消費電力は最大 13W 以下であること。

2.8.12 PoE(IEEE 802.3af)による給電が可能なこと。

2.8.13 同時 SSID が 16 以上であること

2.8.14 ローカルブリッジ、トンネル、メッシュ各タイプの SSID をサポートすること。

2.8.15 ラジオあたりの最大クライアント数は 512 以上であること。

2.8.16 LED オフモードをサポートすること。

2.8.17 802.11ac Wave 2 MUMIMO をサポートすること。

2.8.18 送信ビームフォーミング （TxBF）をサポートすること。

2.8.19 次世代型ファイアウォール(UTM)の GUI から集中管理可能なこと。

※参考機器　FortiAP-221E

2.9　無停電電源装置　（1 式）

2.9.1　学内情報ネットワークシステムを構成する機器に対応する無停電電源装置を必要台数設置すること。

2.9.2　インターフェース：USB / COM を有すること。

2.9.3　定格容量：1500VA / 1200W 以上の性能を有すること。

2.9.4　出力コンセント：NEMA 5-15R×6 個を有すること。

2.9.5　電源部：AC100V、NEMA 5-15P 以上の性能を有すること。

2.9.6　19 インチ標準ラックに収容可能な 2U サイズであること。

※参考機種　高機能無停電電源装置(Smart-UPS SMT 1500RMJ)

2.9 ルータ　（2 式）

2.9.1　10/100/1000BASE-T を 10 ポート以上で有すること。

2.9.2　ルーティングプロトコルは、IPv4 であり、static・RIP・RIPv2・VLSM 対応・OSPFv2・BGP4 に対応していること。

2.9.3　WAN プロトコルは、PPPoE・ IPoE 無線 WAN データコネクトに対応していること。

2.9.4　VLAN は、タグ VLAN,ポート VLAN に対応していること。

2.9.5　保守・管理機能は、telnet・FTP ・SSH サーバ・SFTP サーバ・SNMP・SNTP・Syslog・sFlow に対応していること。

※参考機種　Si-R G200B

別紙4　VLANリスト

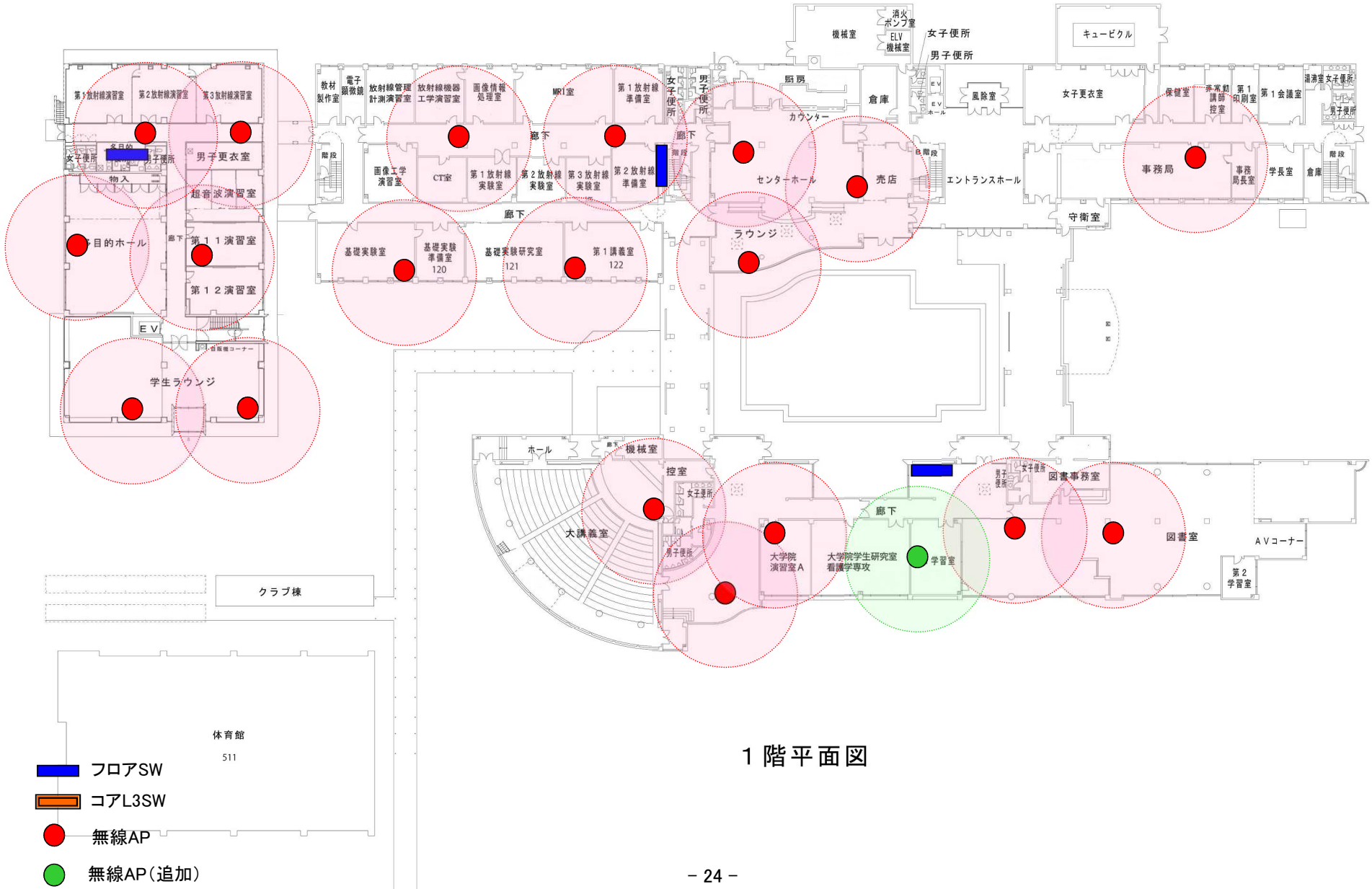
	VLAN名称	旧VLAN名	内容	対象・場所	プロトコル等制限	固定IP可能	固定接続先	接続予定数
1	KANRI	KANRI	管理用VLAN	サーバ関連	なし	○	サーバ室内サーバ	複数台
2	TG	TG	図書館業務用	図書館情報システム管理用 ブレインテック管理対象サーバ	なし	○ ○	図書館内執務室内PC 図書館内執務室内サーバ	5 1
3	TP	TP	図書館パブリック	図書館 学生ラウンジ（有線） キャリア情報室	あり（http,httpsのみ） あり（http,httpsのみ） あり（http,httpsのみ）	○ ○ ○	図書館学生利用PC 学習用PC・プリンター 就職情報等閲覧用PC	6 11 2
4	PR	PR	教職員用共有プリンター用	第一共同研究室PR 第二共同研究室PR 第三共同研究室PR 第二印刷室プリンター、複合機 第三印刷室プリンター、複合機 第四印刷室プリンター、複合機 西棟廊下1（西） 西棟廊下2（東）	あり あり あり あり、印刷のみ あり、印刷のみ あり、印刷のみ あり、印刷のみ あり、印刷のみ	○ ○ ○ ○ ○ ○ ○ ○	第一共同研究室PR 第二共同研究室PR 第三共同研究室PR 第二印刷室 第三印刷室 第四印刷室 西棟廊下1（西） 西棟廊下2（東）	2 2 2 5 5 5 3 2
5	P	P	学生（大学院学生ののぞく）	講義室、教室、演習室、無線LAN-AP	あり（http,httpsのみ）			600
6	M	M	看護学研究科院生 放射学研究科院生	看護学研究科所有PC・プリンター 大学院生持ち込みPC 診療放射線学研究科所有PC・プリンター 大学院生持ち込みPC	なし なし なし なし		看護学研究科院生室 診療放射線学研究科院生室	60
7	MM	MM	【マルチメディア教室1、2】	マルチメディア教室1、2PC サーバ室MMサーバ、スイッチ	なし	○	マルチメディア教室1、2	130
8	**E1**	**E1**	**実験演習VLAN1**	**第一放射線準備室**	なし	○	**第一放射線準備室**	2
9	E2	E2	**実験演習VLAN2**	**画像情報処理室（治療）**	なし	○	**画像情報処理室（治療）**	30
10	E3	E3	実験演習VLAN3	画像処理演習室（CR室）	なし	○	画像処理演習室（CR室）	30
11	E4	E4	実験演習VLAN4	放射線学研究科演習室D	なし	○	**放射線学研究科演習室D**	30
12	E5	E5	実験演習VLAN5	放射線学研究科演習室C	なし	○	放射線学研究科演習室C	30
13	E6	E6	実験演習VLAN6	第1放射線演習室	なし	○	第1放射線演習室	30
14	E7	E7	**実験演習VLAN7**	**第2放射線演習室**	なし	○	**第2放射線演習室**	30
15	E8	E8	**実験演習VLAN8**	**第3放射線演習室**	なし	○	**第3放射線演習室**	30
16	E9	E9	**実験演習VLAN9**		なし			
17	E10	E10	**実験演習VLAN10**		なし			
18	JIMU	**JIMU**	**事務局職員PC（県庁ネットワークは含まず）**	事務局学内用PC、非常勤室PC、	なし			30
19	T0	**T0**	**非常勤講師**		なし		**ダイナミック**	30
20	T1	T1	学長		なし	○＊	学長室、ダイナミック	30
21	**T2**	**T2**	教員1		なし	○＊	教員研究室1、ダイナミック	30
22	T3	**T3**	教員2		なし	○＊	教員研究室2、ダイナミック	30
23	**T4**	**T4**	教員3		なし	○＊	教員研究室3、ダイナミック	30
24	T5	**T5**	教員4		なし	○＊	教員研究室4、ダイナミック	30
25	**T6**	**T6**	教員5		なし	○＊	教員研究室5、ダイナミック	30
26	T7	**T7**	教員6		なし	○＊	教員研究室6、ダイナミック	30
27	**T8**	**T8**	教員7		なし	○＊	教員研究室7、ダイナミック	30
28	T9	**T9**	教員8		なし	○＊	教員研究室8、ダイナミック	30
29	**T10**	**T10**	教員9		なし	○＊	教員研究室9、ダイナミック	30
（略）	（略）	**（略）**	（略）				（略）	
100	**T70**	**T70**	教員70		なし	○＊	教員研究室70、ダイナミック	30
101	**T71**	**T71**	教員71		なし	○＊	教員研究室71、ダイナミック	30
102	**T72**	**T72**	教員72		なし	○＊	教員研究室72、ダイナミック	30
103	**T73**	**T73**	教員73		なし	○＊	教員研究室73、ダイナミック	30
104	**T74**	**T74**	教員74		なし	○＊	教員研究室74、ダイナミック	30
105	**T75**	**T75**	教員75		なし	○＊	教員研究室75、ダイナミック	30
106	**T76**	**T76**	教員76		なし	○＊	教員研究室76、ダイナミック	30
107	**T77**	**T77**	教員77		なし	○＊	教員研究室77、ダイナミック	30
108	**T78**	**T78**	教員78		なし	○＊	教員研究室78、ダイナミック	30
109	**T79**	**T79**	教員79		なし	○＊	教員研究室79、ダイナミック	30
110	**T80**	**T80**	教員80		なし	○＊	教員研究室80、ダイナミック	30
111	**T81**	**T81**	教員81		なし	○＊	教員研究室81、ダイナミック	30
112	**T82**	**T82**	教員82		なし	○＊	教員研究室82、ダイナミック	30
（略）	（略）		（略）				（略）	

別紙5　LANコンセント設置場所及び無線LAN-APの利用可能範囲

区分	用途	無線LAN-AP
学長室		×
事務局・執務室		○
第一会議室		×
非常勤講師室		×
印刷室	第二印刷室　プリンター用	×
	第三印刷室　プリンター用	×
	第四印刷室　プリンター用	×
大会議室		○
応接室		×
学部長室		×
共同研究室	第一共同研究室　プリンター用	×
	第二共同研究室　プリンター用	×
	第三共同研究室　プリンター用	×
	第一共同研究室　教員用	×
	第二共同研究室　教員用	×
	第三共同研究室　教員用	×
	第一共同研究室　パブリック用	×
	第二共同研究室　パブリック用	×
	第三共同研究室　パブリック用	×
教員個人研究室	教員個人研究室	×
講義室	各　講義室	○
演習室	各　演習室	○
実習室	各　実習室	○
調理室		○
大学院演習室		○
大学院院生室	看護A，B、放射	○
第一放射線準備室	北棟1F実験エリア	○
画像情報処理室（治療）	北棟1F実験エリア	○
画像処理演習室（CR室）	北棟1F実験エリア	○
第1放射線演習室	西棟1F	○
第2放射線演習室	西棟1F	○
第3放射線演習室	西棟1F	○
放射線学研究科演習室D	北棟3Fエリア	○
放射線学研究科演習室C	北棟3Fエリア	○
図書館執務室		
図書館閲覧室		○
ホワイエ	図書館前	○
ラウンジ	大講義室前	○

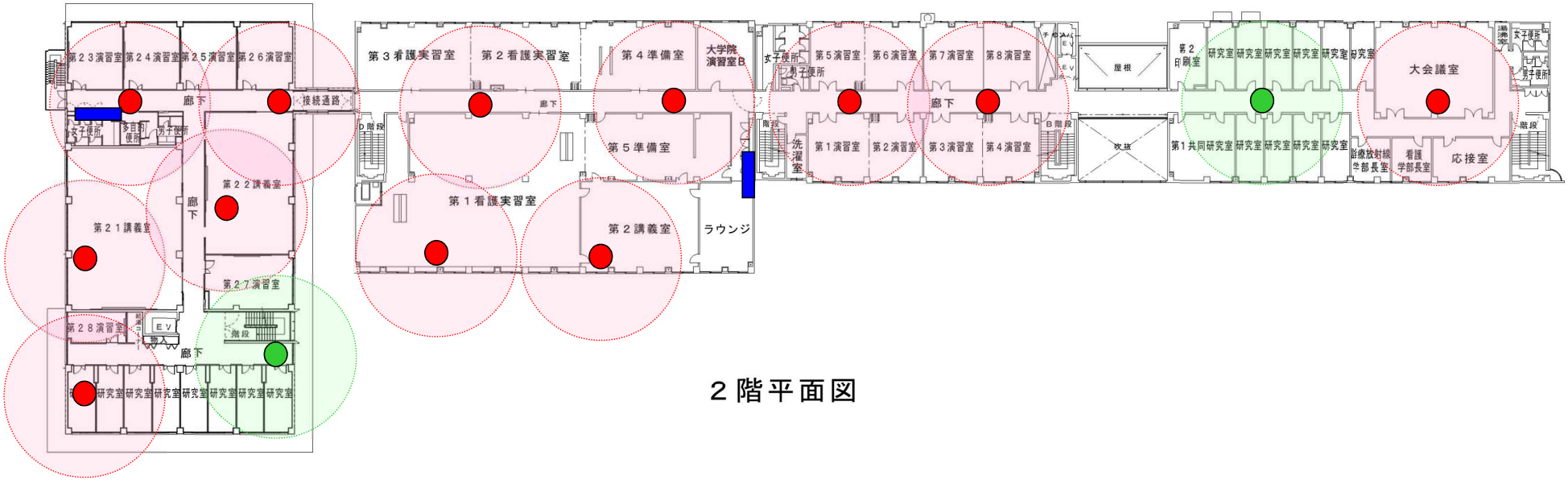
別紙５　LANコンセント設置場所及び無線LAN-APの利用可能範囲

１階　平面図



１階平面図

2階　平面図



２階平面図

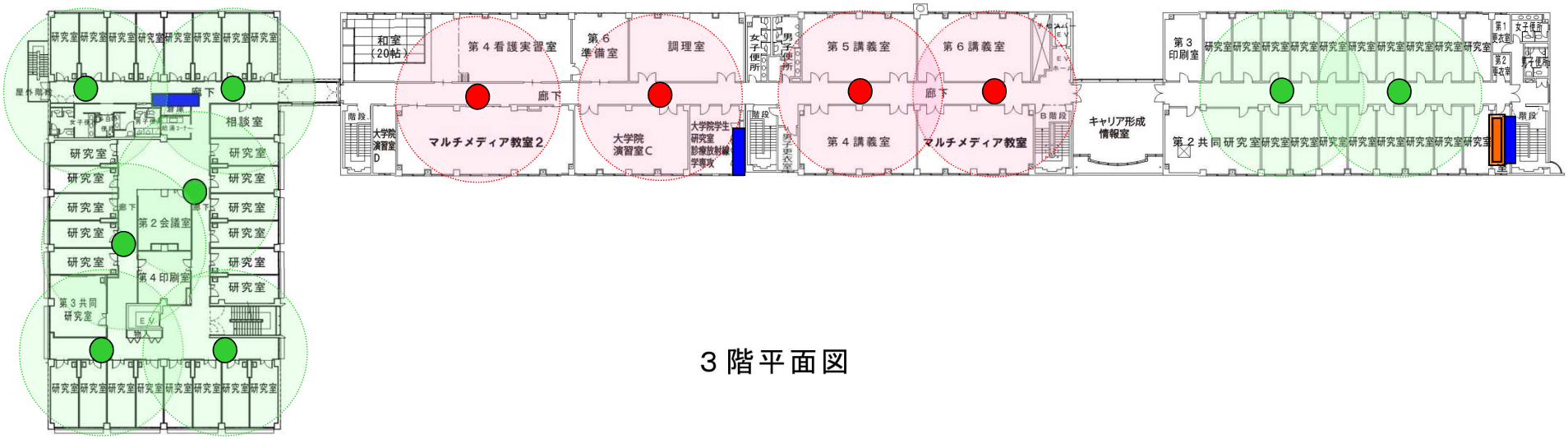
フロアSW

コアL3SW

無線AP

無線AP（追加）

3階　平面図



３階平面図

フロアSW

コアL3SW

無線AP

無線AP（追加）

別紙６

保守仕様書

常に良好な状態でリース期間中、学内情報ネットワークを使用できるよう、納入機器、システム及びサービスについて以下の保守を行うこととする。

1.　システム保守

1.1. システムの運用保守に必要な情報を提供し、質問や問合せ等を受け付けるため、電話、電子メールによる窓口を用意すること。

1.2. 平日の執務時間中（9:00～17:00）においては、本学からの連絡等によって障害発生の事実を知った時点から起算して、２時間以内を目安に初期対応を行うこと。

1.3. ハードウェア及びソフトウェアに不備が協議のうえ認められた場合には、受注者の責任において処置を行うこと。

1.4. 本仕様を構成するすべての機器、製品の復旧、保守等は受注者が責任を持って行うこと。

2.　セキュリティ対策

2.1. サーバへのアクセス状況を監視するために、毎日のアクセスログを取得する機能を備え、その状況の閲覧及び印刷ができること。

2.2. サーバ機器等には、ウィルス感染防止の機能を有し、感染防止に万全を期すること。また、ウィルス定義ファイルを最新の状態に維持するための機能を有すること。

2.3. 導入する機器については、本学と協議しセキュリティ対策を施すこと。

2.4. 群馬県公立大学法人情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）に基づき接続設定を施し、報告書を提示すること。検査項目は以下の点を含むこと。

- インターネット接続前に疑似アタックを行い、オンサイト検査を実施すること。

2.5. 納入する際にインターネットのセキュリティアタック検査を施し、検査結果報告を提出すること。

2.6. 情報セキュリティポリシーに基づいて、具体的な対策の手順を定めた「実施手順案」について本学と協議のうえ作成すること。

3. ユーザ支援

3.1. システム導入時に、学内情報ネットワーク等の構成するシステムの操作手順マニュアルを作成し、受注者の負担により提供すること。

3.2. 受注者は、システムの操作手順に関して、システム導入時に管理者向け教育を実施すること。

3.3. 受注者は、本システムへの設定データの移行、システム調整、運用状況の確認及び報告書の作成、コンサルテーション等のため、本学の依頼に応じて支援を行うこと。

3.4. 受注者は、本システムへ設定変更等が生じた際に、本学からの要求に応じて、操作支援を行うこと。

4. 保守の範囲

次の項目については、受注者の経費に含むものとする。

4.1. 機器及びシステム等の障害への対応

4.2. 障害時及び技術サポート時の担当者（技術員、SE 等）の派遣経費

4.3. 修理及び部品交換等の技術料

4.4. 代替機器の提供及び運搬費（発送・受注に要する経費など）

4.5. 障害機器の発送・受取などに要する経費

4.6. ウィルス駆除ソフトウェア等の最新修正プログラム及びデータファイルの提供

4.7. 運営管理等における技術サポート

4.8. ソフトウェアアップデート等、セキュリティ対策における技術サポート

4.9. 設定変更等における技術サポート

5. 保証期間

納入後５年間は、通常の使用により故障した場合の修理は無償とする。

6. 特別保守料について

次の事由について保守業務を行う場合は、受注者はその都度個別見積りを行い、発注者と協議のうえ、特別保守料を決定したうえで、当該保守業務を行うものとする。ただし、緊急を要する場合は、受注者は事後に特別保守料を見

積りすることができる。

なお、特別保守料の支払いの条件については、両者別途協議のうえ決定し、発注者は受注者に支払うものとする。

6.1. 受注者の故意、過失に起因して生じた障害

6.2. 発注者側の保守対象機器の使用操作上の誤りまたは発注者側が保守対象機器の納入場所の環境を所定の条件に設定・維持することを怠ったことにより生じた障害

6.3. 火災、水害、地震、落雷等天災地変、その他両者いずれの責にも帰することのできない事由から生じた障害

6.4. 保守時間帯以外の時間帯における訪問修理

7. 保守業者からの協力について

7.1. 発注者は保守対応状況報告書の提出を求められた場合には、遅滞なくこれに応じること。

7.2. リース期間満了における調達機器のデータ消去及び撤収に要する経費は、受注者が全額を負担する。

7.3. リース期間満了後の機器撤収作業及び日程については、リース期間満了の１か月後までに両者協議のうえ作業を円滑に実施すること。

8. その他

8.1. リース物件中、システムフロント統合装置及び認証サーバ装置一式について、ソフトウェアのインストール、設定及び運用管理方法等の変更を発注者が行う場合は、受注者と協議するものとする。なお、接続機器設定及び接続機器の変更設定にしては、これによらず発注者が必要に応じて変更できるものとする。

8.2. リース物件中、ネットワークサーバ一式についてソフトウェアのインストール、設定及び運用管理方法等の変更等について、受注者は発注者と協議の上行うものとし、変更等を行った場合は、ソフトウェアリスト、システム仕様書、システム設定ポリシー等に関するドキュメントを整理の上、その都度、提出すること。

別　記

個人情報取扱特記事項

（基本的事項）

第１　乙は、個人情報の保護の重要性を認識し、本契約による業務の実施に当たっては、個人の権利利益を侵害することのないよう、個人情報を適正に取り扱わなければならない。

（秘密の保持）

第２　乙は、本契約による業務に関して知ることができた個人情報をみだりに他に知らせてはならない。本契約が終了し、又は解除された後においても、同様とする。

（収集の制限）

第３　乙は、本契約による業務を処理するために個人情報を収集するときは、その目的を明確にするとともに、本契約の目的を達成するために必要な範囲内で、適法かつ公正な手段により行わなければならない。

２　乙は、本契約による業務を処理するために個人情報を収集するときは、あらかじめ目的を明示した上で、本人から収集し、又は本人以外から収集するときは本人の同意を得た上で収集しなければならない。

（利用及び提供の制限）

第４　乙は、甲の指示があるときを除き、本契約による業務に関して知ることができた個人情報を本契約の目的以外の目的のために利用し、又は甲の承諾なしに第三者に提供してはならない。

（適正管理）

第５　乙は、本契約による業務に関して知ることができた個人情報の漏えい、滅失及びき損の防止その他の個人情報の適正な管理のために必要な措置を講じなければならない。

（廃棄）

第６　乙は、本契約による業務に関して知ることができた個人情報について、保有する必要がなくなったときは、確実かつ速やかに破棄し、又は消去しなければならない。

（複写又は複製の禁止）

第７　乙は、本契約による業務を処理するために甲から引き渡された個人情報が記録された資料等を、甲の承諾なしに複写し又は複製してはならない。

（再委託の禁止）

第８　乙は、本契約による業務については、第三者にその取扱を委託してはならない。ただし、本契約第２７条に該当する場合は、この限りではない。

（資料等の返還等）

第９　乙は、本契約による業務を処理するため、甲から提供を受け、又は乙自らが収集し、若しくは作成した個人情報が記録された資料等は、本契約完了後、直ちに甲に返還し、又は引

き渡すものとする。

ただし、甲が別に指示したときは、その指示に従うものとする。

（業務従事者への周知及び監督）

第１０　乙は、本契約による業務に従事している者に対して、在職中及び退職後において、本業務に関して知ることができた個人情報をみだりに他に知らせ、又は不当な目的に使用してはならないこと、これに違反した場合は、参加団体の個人情報保護条例により罰則が適用される場合があることなど、個人情報の保護のために必要な事項を周知するとともに、本契約による業務を処理するために取り扱う個人情報の適切な管理が図られるよう、必要かつ適切な監督を行わなくてはならない。

（立入調査）

第１１　甲は、必要があると認めるときは、乙が本契約による業務を処理するに当たり、取り扱っている個人情報の状況について、随時調査することができる。

（事故報告）

第１２　乙は、本契約書に違反する事態が生じ、又は生じるおそれのあることを知ったときは、速やかに甲に報告し、甲の指示に従うものとする。

群馬県立県民健康科学大学学内情報ネットワーク利用規程

（趣旨）

第１条　この規程は、群馬県立県民健康科学大学（以下「本学」という。）内に設置した学内情報ネットワーク（以下「学内ネット」という。）の利用に関し、必要な事項を定めるものとする。

（管理）

第２条　学内ネットの管理は、学術国際委員会（以下「委員会」という。）が行い、学術国際委員会委員長を学内ネット管理責任者（以下「管理責任者」という。）とする。

２　学内ネットの運用は、情報部会が行い、学内ネット運用管理責任者（以下「ネット運用管理者」）は、情報部会員の中から選出し、管理責任者が指名する。

（利用者）

第３条　学内ネット利用者は、本学学生、教職員及び管理責任者が特に認める者とする。

２　管理責任者が特に認める者については別に定めるものとする。

（利用方法）

第４条　利用希望者は、学内ネット利用申請書（別記様式第１号～第３号）を運用管理責任者に提出して、承認を得るものとする。

（接続機器利用）

第５条　利用者が、情報機器を学内ネットに接続する場合は、学内ネット機器接続利用申請書（別記様式第４号～第７号）を運用管理責任者に提出して、承認を得るものとする。

２　情報機器を学内ネットに接続した者は、次の各号の責任を負う。

（１）接続した機器の管理責任

（２）接続した機器の利用者の監督責任

（利用に関する規律）

第６条　学内ネットは、教育、研究、管理運営及びその他管理責任者が認める目的に利用するものとする。

２　利用者は、次の各号に定める不適切な利用をしてはならない。

（１）学内ネット接続機器の破壊

（２）法令あるいは公序良俗に反する行為

（３）学内・学外のネットワークに対する不正アクセス行為

（４）個人を誹謗・中傷する行為

（５）著作権、知的財産権、肖像権、プライバシーなどを侵害する行為

（６）自己のＩＤ、パスワードの使用を他者に認め、ネットワークを利用させる行為

（７）コンピュータウィルス対策を怠る行為

（８）営利を目的としてネットワークを利用する行為

（９）その他、委員会が不適当と認めた行為

（報告）

第７条　学内ネット接続機器の故障、前条第２項の規定に該当する事項を発見した場合は、速やかに委員会に報告するものとする。

（利用制限又は停止）
第８条　委員会は、第６条第２項の規定に違反した利用者に対して学内ネットの利用制限又は停止をすることができる。
（その他）
第９条　この規程に定めのない事項については、その都度、委員会で協議して定める。

附　則
この規程は、平成30年4月1日から施行する。

別紙9

（Ａ４縦）仕様書質問事項

（送付先） 群馬県立県民健康科学大学 総務会計係　黒崎　あて ＦＡＸ　０２７－２３５－２５０１	（質問者） 名　　称 代表者職氏名　　印
送信日　令和　　年　　月　　日	

仕様書質問事項

1　質問者

名　　称	
所　属　名	
担当者職氏名	
連　絡　先	ＴＥＬ　　－　　－　　ＦＡＸ　　－　　－

2　質問事項

質　問　項　目	
質　問　内　容	
備　　考	※備考欄は大学側使用欄のため記入不要 受領日： 連絡日： その他：

3　その他

（1）　ＦＡＸによる送信を原則とし、送信後電話にて送信完了の旨を連絡すること。

（2）　質疑内容の確認のため、質問担当者へ連絡をすることがあります。

（3）　質問事項が複数の場合、同一様式を添付のこと。