福島県立医科大学

附属学術情報センターファイアウォール機器仕様書

令和８年２月

公立大学法人　福島県立医科大学

目　次

Ⅰ　仕様書概要説明

１．調達の背景及び目的

本学では、学内の研究・教育の情報化を図ることを目的に、情報ネットワークシステム（学内 LAN）を導入しサービスを提供してきた。そのうちファイアウォール機器は、学内外からのトラフィックを監視・制御し、不正アクセス等の通信を遮断することで、サーバ等への不正侵入を防ぎ、データ漏洩・マルウェア感染といったリスクを低減することを目的とするものであり、本調達は、令和３年度に導入した機器の賃貸借期間終了に合わせ、年々巧妙化するサイバー攻撃にも対処させるものである。

２．調達物品名、構成内訳、調達の種類、賃貸借期間及び納入場所

（１）調達物品名

福島県立医科大学附属学術情報センターファイアウォール機器 １式

（２）構成内訳

・ファイアウォール装置 ２式
・DMZ スイッチ..... ２式
・無停電電源装置（UPS） ２式

（３）調達の種類

賃貸借

（４）賃貸借期間

令和８年８月１日～令和１３年７月３１日（６０か月）

（５）納入場所

福島県福島市光が丘１番地
福島県立医科大学　附属学術情報センターコンピュータ室

３．技術的要件の概要

（１）本調達物品に係る性能、機能、技術及びその他（以下「性能等」という。）の要求要件（以下「技術的要件」という。）は「Ⅱ　調達物品に備えるべき技術的要件」に示すとおりである。

（２）技術的要件はすべて必須の要求要件である。

（３）要求要件には最低限の要求要件を示しており、入札機器の性能等がこれを満たしていないとの判定がなされた場合には不合格となり、入札資格審査において資格がないとの判定を行う。

（４）入札機器の性能等が技術的要件を満たしているか否かの判定は、入札機器に係る技術仕様書その他の入札説明書で求める提出資料の内容を審査して行う。

（５）仕様書中で指定しているネットワークトポロジや装置の物理接続構成と比較し、より良いものと判断される構成を提案した場合には、それを有効とする。

４．その他

（１）技術仕様書の提出に際しては、提案システムが本仕様書の要求要件をどのように満たすか、あるいはどのように実現するかを要求要件ごとに具体的かつわかりやすく、資料等を添付する等して説明すること。

更に、技術仕様書には本学仕様書の要求要件を満たす場合には〇印を、代替措置等を行っている場合には△印を付して対応状況を表すこと。

審査するにあたって提案の根拠が不明確あるいは説明が不十分であり、客観的に判断できない場合には、要求要件を満たしていないものとみなす。

なお、提出された内容について、問い合わせやヒアリングを行うことがある。

（２）特に指定がない場合、入札機器は、技術仕様書の提出時点で原則として製品化されていること。

製品化されていない機器入札する場合は、技術的要件を満たすこと及び納期限までに製品化され納入されることを書面にて証明すること。

（３）導入スケジュールは、本学の担当者と十分に協議し、その指示に従うこと。なお、導入システムは令和８年８月１日から運用を開始する。

（４）システム導入の責任者は、導入設置の完了まで実質的なリーダーとして継続して担当できること。

（５）導入の過程で、本学から、技術的知識又は経験不足のため作業品質が低いと判断された担当者については、本学の要請に応じて代替担当者を新たに配置すること。

（６）導入作業にあたっては、情報セキュリティに十分配慮し、作業員全員に徹底すること。

（７）稼動開始時には、システムの不測の事態に備え、システム導入の責任者が立ち会うこと。

（８）システムが稼動するまでの間、その進捗状況及び作業内容の確認、問題点の協議・解決が円満に遂行できるよう、必要な事項を協議するための連絡会を開催すること。

（９）その他詳細は本学の指示によるものとする。

Ⅱ　調達物品に備えるべき技術的要件

（性能・機能に関する要件）

１．共通条件

システム全般について適用される共通条件について以下に示す。

（１）ネットワーク通信に使用するインターネットプロトコルのバージョンは、IPv4 とする。なお、各機器に割振る具体的な IP アドレスについては、契約後に本学と協議のうえ決定すること。

（２）通信装置に使用する光トランシーバを、１種類に付き１個以上、予備として用意すること。

（３）OS、ファームウェア等のセキュリティパッチ等については、出来る限り最新のものを適用すること。

（４）本調達により導入する機器のうち SNMP による管理機能を有するものは、原則として既存のネットワーク監視装置による監視を行うこととし、この設定等にかかる費用も見積もること。

（５）更新の対象となっていないネットワーク関連機器やサーバ等についても、再設定が必要になる場合はこれらの費用も見積もること。

（６）導入に際しては、既存のクライアント端末において設定変更が生じないように配慮すること。

（７）本調達により導入する機器で NTP クライアント機能を有するものについては、既存の NTP サーバに接続し時刻の調整を行うように設定を行うこと。

（８）スタック接続により複数台で構成されたスイッチに対し、リンクアグリゲーションにより別のスイッチを接続する場合には、リンクアグリゲーションを構成する各回線の接続先を複数のスイッチに分散させること。

（９）既存のファイアウォール機器のネットワーク構成については、別紙１「現行ファイアウォール機器ネットワーク構成図」を参照すること。また、既存機器の概要については、別紙２「既存機器概要」を参照すること。

なお、詳細については、本学が所蔵する完成図書を参照すること。なお、完成図書の閲覧にあたっては、事前に本学の許可を得ること。

２．ネットワーク構成

２．１．ネットワーク構成

現在は、インターネット接続回線として次の２回線と接続している。メインの回線は国立情報学研究所（NII）の学術情報ネットワーク（SINET6）であるが、予備回線及びゲストアクセス用途としてトークネット社の TOCN を利用している。

サービス等名称	接続先	アクセス回線	接続速度
SINET6	SINET 福島データセンター	NTT 東日本 All-Photonics Connect	10Gbps
TOCN type R	TOCN	Tohknet	1Gbps

表１　インターネット接続回線

（1）ファイアウォール装置（２式）、DMZ スイッチ（２式）及び無停電電源装置（２式）を附属学術情報センターコンピュータ室のラック内（※それぞれの機器ごとに、原則として更新機器と同ラック）に設置すること。必要であれば、ラック内の既設機器の位置を調整して構わない。

　なお、ラックの配置については、別紙３「附属学術情報センターコンピュータ室平面図」を参照のこと。

（2）ファイアウォール装置（２式）と既設のインターネットアクセススイッチをそれぞれ 1 回線の 10GBASE-SR で接続すること。

（3）ファイアウォール装置（２式）と既設のコアスイッチをそれぞれ 2 回線の 10GBASE-SR で接続すること。

（4）２式の DMZ スイッチ同士を２本の 10Gbps 以上の回線で接続し、スタック構成とすること。なお、スタック構成は専用のスタック機構を使用してもかまわない。

（5）ファイアウォール装置（２式）を(4)の構成の DMZ スイッチとそれぞれ 2 回線の 10GBASE-SR で接続すること。（計 4 回線）

（6）ファイアウォール装置（２式）の HA ポート同士を 10Gbps 以上の帯域を持つ 2 回線以上の回線で接続すること。

（7）既設の DMZ スイッチに収容された各サーバや他のネットワーク装置からのネットワークケーブルを新設の DMZ スイッチに収容替えし、既存の接続を維持するよう必要な設定を行うこと。

（8）ファイアウォールのポリシー等の設定内容は原則として現在のものを引き継ぐものとするが、装置の特性を考慮した最適なポリシーを提案・設定すること。

（9）ファイアウォール装置（２式）は HA 構成（高可用性構成　Active/Passive または Active/Active）とし、一方に障害がある場合でも通信及び動作が継続できるようにすること。また、コンフィグや各種セキュリティ定義ファイル等が常に同期されること。

(10) アウトバウンドの通信について、通常の通信は SINET を、ゲストアクセス及び eduroam の通信は TOCN を経由して行われることとし、SINET の通信に障害があるときは、すべての通信が TOCN を経由するようにすること。また、この経路の切り替えについては自動的に行われること。

(11) インバウンドの通信は、通常時の通信は SINET を経由して行われることとし、SINET の通信に障害があるときに TOCN を経由すること。なお、現在経路の切り替えは外部の DNS サービス（IIJ DNS トラフィックマネージメントサービス）を利用した IP 切替にて行っているので、それを継承すること。

２．２．VPN サービス構成

（１）IPsec を利用した VPN 機能を提供すること。

（２）必要となるサーバ証明書については、本学が用意したものを利用すること。

（３）Windows、MacOS、iOS、Android の各 OS に対応した専用のクライアント接続アプリが利用できること。なお、アプリは学外から FW にアクセスして取得するか、App ストア、Play ストア等を通じて取得し、インストールが可能であること。

２．３．IP アドレスの構成

（１）DMZ 及び内部ネットワークの IP アドレスは、本学で使用しているクラス A のプライベート IP アドレス（10.0.0.0/8）を使用すること。

（２）SINET 接続部及び SINET 側に NAT 変換する IP アドレスは、本学が所有するグローバル IP アドレス（202.251.224.0/20）を使用すること。

（３）TOCN 接続部及び TOCN 側に NAT 変換する IP アドレスは、TOCN にて割り振られたグローバル IP アドレス（211.120.92.128/28）を使用すること。

（４）各種通信装置、管理装置には、予めネットワーク管理者によって定められた IP アドレス、サブネットマスク、デフォルトゲートウェイを設定すること。

（５）(1)～(4)以外の部分及び詳細については、本学担当者と打ち合わせて決定すること。

３．ネットワーク機器

ネットワークを構成する通信装置の仕様を以下に示す。

３．１．ファイアウォール装置（２式）

３．１．１．ハードウェア

（1）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型の UTM 機器であること。

（2）各単一の管理ポート（イーサネット、シリアルコンソール）で全てのモジュールを一元管理できること。

（3）専用の HA 用インターフェースを 3 ポート以上有すること。

（4）LAN のメディアとして、以下の通信用インターフェースを有すること。

・1G/2.5G/5G/10G 対応 RJ-45 port 12 ポート以上

・10G SFP+ port　10 ポート以上

・25G SFP28 port 4 ポート以上

（5）アプリケーション識別有効時のファイアウォールスループットは、19Gbps 以上であること。

（6）各脅威防止機能（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等）を同時に使用した場合でも、10Gbps 以上の通信処理能力を有すること。

（7）IPsec における VPN スループットは 9.5Gbps 以上であること

（8）新規セッション数が秒間あたり 200,000 セッション以上を処理可能であること。

（9）最大セッション数が 2,200,000 セッション以上を処理可能であること。

(10) 電源を内蔵し、冗長構成とすること。また、ホットスワップに対応していること。

(11) 最大消費電力が 450W 以下であること。

(12) 機器内部にログや設定等を保存するためのストレージとして、RAID1 により冗長化された 480GB 以上の SSD が搭載されていること。

(13) 19 インチ幅のラック搭載型とし，1RU 以内に収納可能であること。

(14) 管理通信処理用とデータ通信処理用でそれぞれ独立した処理プロセッサ・コアを使用していること。

３．１．２．ソフトウェア及び機能

（1）基本的な脅威対策として、脆弱性防御、アンチウィルス、アンチスパイウェア機能を有すること。

（2）本装置は TAP モード(ミラーポート接続)、L1 モード(MAC アドレスを保持しない)、L2(ブリッジ)モード、L3（ルータ）モードに対応し、仮想システム機能を利用せずに、一筐体内で複数のモードの混在設定が可能なこと。

（3）IEEE802.1Q VLAN トランク機能を有すること。

（4）IEEE802.1ax リンクアグリゲーション機能を有すること。（Static および LACP）

（5）ジャンボフレームをサポートすること。

（6）RIPv2, OSPFv3, BGP のダイナミックルーティングに対応していること。

（7）10 以上のバーチャルルータ機能を有すること。

（8）ファイアウォール機能および IPS などの脅威防御機能を利用可能な仮想システムを 10 個以上利用可能であること。

（9）Pingによるスタティックルートの死活監視を行い、監視先がダウンした際には当該ルートを動的に削除する機能を有すること。

(10) Static Route や Policy-Based Routing の Nexthop として、IP アドレス以外に FQDN を指定可能であること。

(11) マルチキャストルーティング(PIM-SM)に対応していること。

(12) NAT 機能を有すること。

(13) 宛先 NAT の変換先として、IP アドレス以外に FQDN を指定可能であること。

(14) ポリシー設定の送信元および宛先に FQDN が利用できること。なお、FQDN の IP アドレス情報は、DNS レスポンスの TTL に基づいて自動的に更新すること。

(15) DNS プロキシ機能を有すること。また、特定のドメイン毎に指定した DNS サーバーを利用する制御が可能であること。

(16) ポリシーベースの QoS に対応しており、アドレス、ポート番号、利用ユーザ、アプリケーションといった情報を基に帯域制御が可能であること。

(17) アドレス、ポート番号、利用ユーザ、アプリケーションの情報を基にセッション単位で指定したインターフェースに IP パケットを転送する機能を有すること。

(18) ファイアウォールを筐体内部で論理的に分割し、複数のファイアウォールを仮想的に動作させる機能を有し、仮想ファイアウォール単位で管理者を分割することが可能なこと。

(19) Active/Passive、Active/Active 両方の冗長構成に対応していること。なお、いずれの冗長構成でもアプリケーション識別や IPS 機能、アンチウィルス機能も制限なく利用可能なこと。

(20) 冗長構成時、セッションを維持しつつ OS のアップグレード作業が可能であること。

(21) 4000 種類以上のアプリケーションをポート番号に関わらず識別し可視化できること。

(22) 専用のアプリケーション識別エンジンを搭載しており、追加設定なく、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。

(23) ファイアウォールのポリシーは送信元/送信先とアプリケーション名を元に処理可能であること。

(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) 宛先/送信元の国別アドレスでポリシー制御が可能であること。

(27) ポリシー設定を簡素化するために、IP アドレスの任意のビットに対してワイルドカードマスクを使用した柔軟なアドレス指定が可能であること。

(28) 特定のイベントを検知した場合、そのイベントの送信元もしくは宛先の IP アドレスに関する通信に対して、一定時間異なるセキュリティポリシーを自動的に適用することが可能であること。

(29) ポリシー設定を CSV/PDF 形式で出力できること。

(30) ポリシー設定画面において、トラフィックに対する各ルールのヒット状況(ヒット数、最後のヒット日時、最初のヒット日時)を確認できること。

(31) 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。

(32) 任意の通信に対して、設定したポリシーが適切に機能するかどうかを GUI 上で確認するためのテスト機能を有すること。

(33) 設定ポリシー変更の際、すべてのセッションを再マッチングできること。

(34) アプリケーションに依存せず TCP/UDP ポート番号単位でセッションタイムアウト時間を設定可能であること。

(35) 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する機能を有すること。

(36) ポリシーの使用状況や通信内容を分析し、既存のポリシーに対するポリシー最適化機能を有すること。

(37) X-Forwarded-For(XFF)に付与された IP アドレスに基づいたセキュリティポリシーの制御が可能であること。

(38) HTTP/2 を利用するアプリケーションの可視化および制御が可能であること。

(39) ファイアウォールのポリシー毎にウィルス・スパイウェア、URL フィルタリング等のコンテンツ検査機能の有効/無効が設定可能であること。

(40) IPv4/IPv6 通信に対して、脆弱性防御、アンチウィルス、アンチスパイウェア、URL フィルタリング、ファイルフィルタ、データフィルタといったコンテンツスキャニング機能を、シングルエンジンで且つストリームベースで処理できること。

(41) カスタムでアプリケーションおよび脆弱性防御のシグネチャを作成できること。

(42) 外部から IP アドレス/Domain/URL 情報を自動的に取り込み、ポリシー制御に反映する機能を有すること。また、取り込んだリストによるアクセス制御が行われた場合、ログに記録されること。

(43) 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。

(44) 内部クライアントから外部の危険なサイトや C&C サーバに対する通信開始時に行われる悪意のあるサイトに対する DNS 正引き(名前解決)が行われた場合に、ファイアウォール上で予め定義した偽りの IP アドレスを返答させることにより、不正通信を行った内部クライアントの IP アドレスの特定が可能な機能を有すること。

(45) カテゴリベースの URL フィルタリング機能が利用可能であること。また、機能を利用する際に、単一のカテゴリではなく複数のカテゴリによって制御することが可能であること。

(46) URL フィルタリングのカテゴリとして、マルウェア、フィッシング、C&C、リスクベースおよび新規に登録された DNS ドメインのカテゴリが提供されていること。

(47) ファイアウォールのセキュリティポリシー上で URL カテゴリを直接指定し、URL カテゴリ毎のアクセス制御が可能であること。

(48) URL フィルタリングの機能において、User-Agent、Referer、X-Forwarded-For の情報が記録できること。

(49) URL カテゴリ毎に、クレデンシャル情報の漏洩を防止する機能を有すること。

(50) Web サイトのコンテンツ内容を機械学習によって装置上で検査し、未知の有害サイトへのアクセスをリアルタイムに遮断することが可能であること。

(51) Google や Dropbox 等の SaaS アプリケーションに対して、HTTP リクエストヘッダに企業用のドメインを挿入することにより、個人アカウントの使用を制限できること。

(52) 悪意のある DNS サイトに対して、クラウドベースの脅威情報データベースとリアルタイムに連携することにより、新たな脅威を迅速に遮断することが可能であること。

(53) DNS で検出した脅威情報のカテゴリに応じて、ポリシーのアクションを設定することが可能なこと。

(54) PDF、Excel、WORD、PPT、ZIP など 200 種類以上のファイルタイプによる通信の可視化やフィルタリングが可能なこと。

(55) 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。

(56) クレジットカード番号、またはカスタマイズした文字列パターンでのデータフィルタが可能であること。

(57) 「防弾ホスティング」プロバイダに関する IP アドレス情報を取得し、ログ出力またはブロックする機能を有すること。

(58) IoT デバイスに対する可視化とリスク分析、ポリシーの適用による脅威の防御が可能であること。

(59) VxLAN トンネル内の通信データの検査が可能であること。

(60) DoS 攻撃に対し、ハードウェア処理による防御機能を有すること。

(61) Active Directory 等と連携し、IP アドレスとユーザ情報を紐付け、可視化と制御が可能であること。

(62) Captive Portal によるユーザの認証が可能であり、かつ、多要素認証に対応すること。

(63) Syslog による外部認証システムと連携可能であり、Syslog メッセージより取得したユーザ情報を基にトラフィックの可視化と制御が可能であること。

(64) Web プロキシ装置が付与した X-Forwarded-For の情報を元にユーザ識別機能が使用できること。

(65) SAML 2.0 に対応した認証機能を有し、SP として動作すること。

(66) 脅威ログが確認された場合に、対象となるユーザを自動で隔離、または、通信を制限する機能を有すること。

(67) 未知のファイルを仮想 OS 環境で実行して解析するサンドボックス機能を提供すること。

(68) サンドボックス機能をクラウドで提供する場合は、少なくとも 30,000 社以上の利用実績があり、日本国内にも解析システムが存在すること。

(69) サンドボックス機能は、Windows OS の実行形式のファイルに加え、PDF ファイル、Microsoft Office ドキュメントや Java アプレット(JAR, Class)、Android OS の実行形式のファイルである APK など、未知のマルウェア感染が疑われるファイルを自動的に仮想 OS 環境上で 200 以上の検査項目によって検査し、未知のマルウェアの早期発見と対策が可能なクラウドシステムと連携する機能を有すること。

(70) サンドボックスで危険と判定された場合、その解析結果を管理 GUI にて参照可能なこと。また、解析を行った検体ファイルをダウンロードすることが可能であること。

(71) メール本文に含まれる URL リンク情報を検査し、危険と判定された場合、その URL リンクへのアクセスを自動的に遮断する機能を有すること。

(72) macOS で使用される Mach-O、DMG、PKG、Application bundle のファイルタイプ及び Linux でで使用される ELF ファイルタイプが解析可能なこと。

(73) ZIP, 7-Zip や RAR の圧縮形式のファイルが解析可能なこと。

(74) HTTP/HTTPS, SMTP, POP3, IMAP, FTP および SMB で転送されるファイルが解析可能なこと。

(75) 実行ファイルや Script ファイルを機械学習によって装置上で検査し、未知の有害ファイルをリアルタイムに遮断することが可能であること。

(76) 未知の脅威が確認された場合に、感染の疑いのある端末を自動で隔離する機能を有すること。

(77) 筐体内にサーバ証明書と鍵をインポートし、その証明書と鍵をもとに該当するサーバ宛ての SSL 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。
(78) 筐体内で SSH 通信を復号し、ポートフォワード通信を検知可能であること。
(79) 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。
(80) クライアント証明書要求など、特定の理由で SSL 復号ができないと判断された URL は、自動的に一定時間 SSL 復号除外する機能を有すること。
(81) IPSec 及び SSL VPN によるリモートアクセス VPN に対応していること。
(82) SSL VPN による最大接続数は、1800 接続以上であること。
(83) VPN 接続において Windows、macOS、AndroidOS 及び iOS に対応したクライアント（エージェント）ソフトウェア（アプリ）が賃貸借期間中、使用可能であること。
(84) VPN 接続時は、既設の RADIUS サーバにおいて認証されるよう設定を行うこと。

３．１．３．管理インターフェース

（1）Web ブラウザ及び CLI で管理可能であり、操作端末側に別途ソフトウェアをインストールする必要がないこと。
（2）設定操作は、装置単体で候補コンフィグを作成し、コミット操作にて設定を有効にするアーキテクチャであること。また、候補コンフィグを実行中の状態に戻すことが可能であること。
（3）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。
（4）WebUI 上で候補コンフィグと実行中コンフィグの差分が確認できること。
（5）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。
（6）設定ファイルについては XML 形式でインポート/エクスポート可能であること。
（7）セキュリティ機能毎（ファイアウォール、アンチウイルス、IPS など）で管理 WebUI が統一されていること。
（8）Web ユーザインターフェースは日本語及び英語に対応しており、設定変更を伴わずに言語切替ができること。
（9）1 つの管理インターフェースを用いて Syslog の送出、シグネチャの自動アップデートおよびサンドボックスとの連携が可能であること。
(10) トラフィックログ、脅威ログ、URL フィルタリングログ、認証ログについて複数のログを串刺しで検索する機能を持っていること。
(11) SNMP プロトコルによる管理処理部のメモリ利用率、スワップ利用率、仮想システム毎のセッション利用率、およびデータ転送処理部のパケットバッファ利用率のモニタリングが可能なこと。
(12) 外部 syslog サーバにログ出力可能であること。また、各 Syslog サーバー毎に送出するログフォーマットの設定が可能であること。
(13) 送信元/宛先 IP アドレス、送信元/宛先国名、アクション、通信量、Malware カテゴリ等のログ属性でログをフィルターし、特定のログのみをメール通知、Syslog、SNMP で通知することが可能であること。

(14) インターネット経由でファームウェアならびにシグネチャファイルを製品に直接ダウンロードおよびインストール可能であること。また Proxy 経由でもこれが可能であること。

(15) レポートデータを PDF 形式でエクスポートし、スケジュール機能により定期的に電子メールに添付し送付することが可能であること。

(16) 通信量の統計情報を元に、宛先/送信元の国別で通信量を世界地図上に視覚的に表示する機能を有すること。

(17) Web ユーザインターフェース上で動的に表示を切り替えることができるリアルタイムレポート機能を搭載し、利用頻度の高いアプリケーション、URL カテゴリ、脅威をランキング形式で表示できること。

(18) 50 以上の事前に定義されたレポートテンプレートおよびカスタムレポート機能を有し、それらを PDF 形式にして設定されたスケジュールで自動メール送信可能なこと。

(19) 特定時間内で発生した脅威や通信（アプリケーション）を視覚的に表示し、マウスクリックのみで情報をフィルタして抽出できる機能を有すること。

(20) 過去と現在の通信内容を比較し、その差分を表示するレポート機能を有すること。

(21) トラフィックをモニタして相関的に分析し、ボットネット感染が疑われる端末をレベル順にリストアップするレポート機能を有すること。

(22) SaaS アプリケーションに特化したレポート機能を有し、それを PDF 形式で出力可能なこと。

３．１．４．付帯事項

（1）形状は 1U サイズのボックス型であること。

（2）冗長化のため、同モデル同型の 2 台の装置による HA 構成とすること。

（3）AC100V、50Hz で動作すること。

（4）信頼性の関係から冗長化電源を搭載すること。

（5）3.3 の無停電源装置（UPS）に電源を接続すること。なお、1 台の装置から 2 式の UPS にそれぞれ接続することで UPS の冗長化を図ること。

（6）既存の 19 インチラックにマウントすること。

３．２．DMZ スイッチ（２式）

対外的に公開するサーバ等を収容するネットワークスイッチである。既存の DMZ スイッチを置き換え、現在収容しているサーバ等の収容替えも併せて行う。

３．２．１．LAN スイッチ機能

（１）2 式を 3.2.4(2)の構成としたとき、LAN のメディアとして次表に示すポート数（合計数）を提供できること。なお、次表の数量にはスタック接続に使用するポートは含まれていない。

ポートの種類	ポート数
10GBASE-SR	4
10GBASE-T	4
1000BASE-T	48

表２　エッジスイッチ　必要ポート数

（２）1000BASE-T ポートについては、100BASE-TX 及び 10BASE-T にも対応し、速度とデュプレックスモード（Full/Half）について、オートネゴシエーション対応であり、ポートの接続（MDI、MDI-X）について自動設定可能であること。

（３）装置のスイッチング容量は 240Gbps 以上であること。

（４）パケット転送能力（スループット）は、180Mpps 以上であること。

（５）ジャンボフレームをサポートしていること。

（６）32,000 個以上の MAC アドレスをサポートしていること。

（７）IEEE802.3ad に準拠するリンクアグリゲーションをサポートしていること。

（８）IEEE802.1D スパニングツリー及び IEEE802.1w ファストスパニングツリー（Rapid STP）に対応していること。

（９）L2 ループ検出機能を有すること。なお、ループ検出時のポートの自動切断及びループ解消後のポート自動回復機能を併せて有すること。

(10) DHCP スヌーピング機能を有すること。

３．２．２．VLAN 機能

（１）メディアの区別なくスイッチポートベース VLAN の設定が可能であること。

（２）VLAN ID は 4,000 個以上設定可能なこと。

（３）スイッチポートベース VLAN に対して、IEEE802.1Q に準拠する VLAN Tagging の設定が可能であること。

３．２．３．スイッチ管理機能

（１）SNMP v1 v2 v3 エージェントをサポートしていること。

（２）RMON プローブをサポートしていること。

（３）ポートのミラーリングが可能であること。

（４）RJ-45 又は USB によるシリアルコンソールポートを装備していること。

（５）telnet,SSHv2 サーバをサポートしており、CLI によるリモート管理が可能であること。

（６）Web GUI によるリモート管理が可能であること。

（7）ICMP Ping をサポートすること。
（8）設定内容を容易にバックアップ／リストアすることが可能であること。

３．２．４．付帯事項
（1）形状は 1U サイズのボックス型であること。
（2）冗長化のため、２式のスイッチによるスタック接続構成とすること。
なお、10Gbps 以上の高速なインターフェースでスタック接続するものとし、複数接続することでスタック接続を冗長化すること。
（3）ファイアウォール装置（２式）との接続に使用するインターフェースは、１台に集中させずに２台に分散させること。
（4）AC100V、50Hz で動作すること。
（5）信頼性の関係から冗長化電源を搭載すること。
（6）現行の DMZ スイッチを収容している既存の無停電電源装置（UPS）に電源を収容すること。
（7）既存の 19 インチラックにマウントすること。

３．３．無停電電源装置（２式）
（1）常時インバータ給電方式またはラインインタラクティブ方式の UPS であること。
（2）定格入力電圧は AC100V で動作すること。
（3）最大入力電流は 15A 以内であること。
（4）出力波形は、通常時及びバックアップ運転時とも正弦波であること。
（5）入力プラグ形状は、NEMA5-15P であること。
（6）出力コンセントは、NEMA5-15R に準拠したものを６つ以上装備していること。
（7）出力容量は、上記プラグ形状の場合 1240VA 以上であること。
（8）１台当たりのバックアップ時間は 500W 負荷時で 20 分以上であること。
（9）ユーザによるバッテリーのホットスワップが可能であること。.
(10) 指定した時間停電が続く場合には、自動的に停止する機構を有すること。
(11) 19 インチラックに搭載可能であり、必要な搭載金具を有していること。
(12) 19 インチラック搭載時のユニット数は 2U 以下であること。
(13) イーサネットインターフェースを有していること。
(14) SNMP v1 v2 v3 エージェントをサポートしていること。
(15) telnet 及び SSH v2 をサポートしていること。

（性能・機能以外の要件）

１．搬入、据付、配線、調整、設定等

（１）導入システムの設置場所への搬入、据付、配線、調整及びソフトウェアの設定は受注者が行い、各機器の動作確認及び既設システムを含むネットワーク全体の動作確認を行うこと。

（２）接続に必要なケーブル類、変換コネクタを用意し、機器及びネットワークを接続すること。

（３）導入時の作業スケジュール及び体制を明示すること。また、作業内容については本学担当者と随時打合せること。

（４）導入については、業務に支障がないように十分配慮し、計画的に行うこと。また、搬入・据付などの際には施設及び設備に損傷を与えないよう注意するとともに、受注者が必ず立ち会うこと。

（５）本調達は、既存のシステムの更新であるが、更新におけるシステムの停止は極力短期間とし、計画的に行うこと。また、実施にあたっては、本学担当者と十分に協議すること。

（６）電源設備については、既存の単相 100V 50Hz で正常に稼動すること。

（７）LAN については、基本的に既存の LAN 配線及び設備を使用すること。ただし、LAN 配線の追加や変更が必要な場合は、この費用も見積もること。

（８）LAN 配線を行ううえで、部屋・天井等に入る場合には、事前に許可を得ることとし、作業においては著しい騒音を発しないように努めること。

（９）機器の学内 LAN 接続に際し、既存のネットワークスイッチ、サーバ等の設定変更が必要な場合は、既存機器の納入業者と協議のうえ、設定を行うこととし、この費用も併せて見積もること。

(10) 賃貸借期間の満了時または解約時の機器等の返還に要する全ての費用は本調達に含むこと。
なお、機器等に含まれる本学用設定の消去行うこと。

(11) 作業は原則として、平日の 9 時から 17 時までとする。ただし、システムの切り替え時や作業の進捗状況等によりやむを得ずこの時間以外に作業が必要な場合は事前に本学と協議のうえ行うこと。
また、システムの切り替えは、学内外のユーザへの影響を考え、深夜～早朝帯（0 時～6 時）にスケジューリングすること。

(12) 19 インチラックへの機器の取り付けにあたって、奥行きのある機器については、マウントアングルの位置を調整するなど工夫し取り付けること。なお、既設のマウントアングルで対応できない場合は、新たにマウントアングルを用意し機器を取り付けること。

(13) UTP ケーブルの接続にあたっては、既設のケーブルホルダー等を使用するとともに整線し、機器のインジケーターランプ等が隠れないように配線すること。

(14) 光パッチケーブルの接続にあたっては、ケーブルを保護するよう配線方法を工夫すること。

２．保守及び支援体制

（１）契約期間中の機器の故障等に伴う修繕にかかる費用（修理、交換、再設定作業）及びファイアウォール装置のソフトウェアのライセンス使用に係る費用は本調達に含むこと。

なお、各装置の保守の基準は次のとおりとする。

機器名称	保守の基準
ファイアウォール装置	オンサイト　24 時間 365 日対応
DMZ スイッチ	オンサイト　24 時間 365 日対応
無停電電源装置	センドバック　平日　9:00～17:00 対応

表３　保守の基準

（２）保守・支援にかかる費用は本調達に含むこと。

（３）保守・支援の範囲は本調達で導入した全ての機器（※導入オプション含む）及びソフトウェア（ファームウェア含む）とする。

（４）機種によって(1)の保守が困難である場合は、技術仕様書に代替措置を記述すること。

（５）本システムを受注した場合の保守部門の組織体制（組織図及び人員）に関する書類（様式は任意）を技術仕様書と共に提出すること。

（６）故障等の受け付けや緊急対応時の問い合わせについては、機器の種類に関わらず一元的な窓口であること。

（７）マルチベンダーの機器に対応が可能であること。

（８）機器の修理後は、設定含め原則として故障前の状態に復旧すること。

（９）保守作業を行った場合は、作業報告書を提出し、本学担当者の確認を受けること。

(10) 機器の修理または保守について、本学担当者と協議の結果、緊急対応が必要であると判断された場合は、利用者への影響が少なくなるように作業日時を調整し、現地調査及び関連業者への問い合わせ等の作業を含め実施すること。

(11) 仕様書中に特に記述がない場合は、次の記述に基づき、導入機器情報、設定及び操作マニュアル等に関するドキュメントを提出すること。

（ア）導入機器の機種、型番、シリアル番号等の一覧

（イ）各機器の日本語操作マニュアルを１機種につき１部ずつ提供すること。

（ウ）各ハードウェア及びソフトウェアの設定にあたっては、作業記録を残すとともに、行った設定についてドキュメントとして提供すること。

（エ）各マニュアル及びドキュメントについては、印刷物だけではなく、電子形体のものを併せて提供すること。

（オ）受注者が作成したマニュアル、ドキュメント及び図表等については、本学において加筆、修正、印刷、配付及びホームページ等で公開することを認めること。

(12) すべてのシステムについて、本学管理担当者に対する説明会または講習会を行うこと。

(13) システムの運用、設定その他に関する問い合わせに対してヘルプデスクを行うこと。必要であれば、現地対応を行うものとする。なお、受け付け・対応時間は、平日 9 時から 17 時とし、一元的な窓口とすること。

３．情報セキュリティ

（１）本調達に係る業務に遂行にあたり、予め情報セキュリティを確保するための実施体制を整備し、書類（様式は任意）にて報告すること。

（２）本調達に係る業務に関して本学から提供された情報、その他知り得た情報を、本学が承諾した場合を除き、実施体制に定めた者以外の者には秘密とすることとし、また、当該業務の遂行以外の目的には使用しないこと。なお、当該業務の終了後においても他者に漏洩しないこと。

（３）本調達に係る業務の遂行において情報セキュリティが侵害され又はそのおそれがある場合には、速やかに報告すること。

（４）セキュリティホールの発覚などにより緊急を要する重大なセキュリティ上の問題が発生し、ファームウェアのアップデートやパッチの適用等の対策が必要になった場合は、本学に情報提供すること。

（５）本調達に係る業務の一部を他の事業者に再請負により行わせる場合には、本学が求める情報セキュリティ対策と同水準の情報セキュリティを確保するための対策を再請負先に求めること。

（６）本番運用データは原則として、テストデータとして使用しないこと。やむを得ず使用する際は機密情報を消去した上で使用すること。

（７）下表に示す各システムについて、次のセキュリティ要件を満たすこと。

（ア）次のセキュリティ機能を持つこと。

・主体認証機能

・アクセス制御機能

・権限管理機能

・証跡管理機能

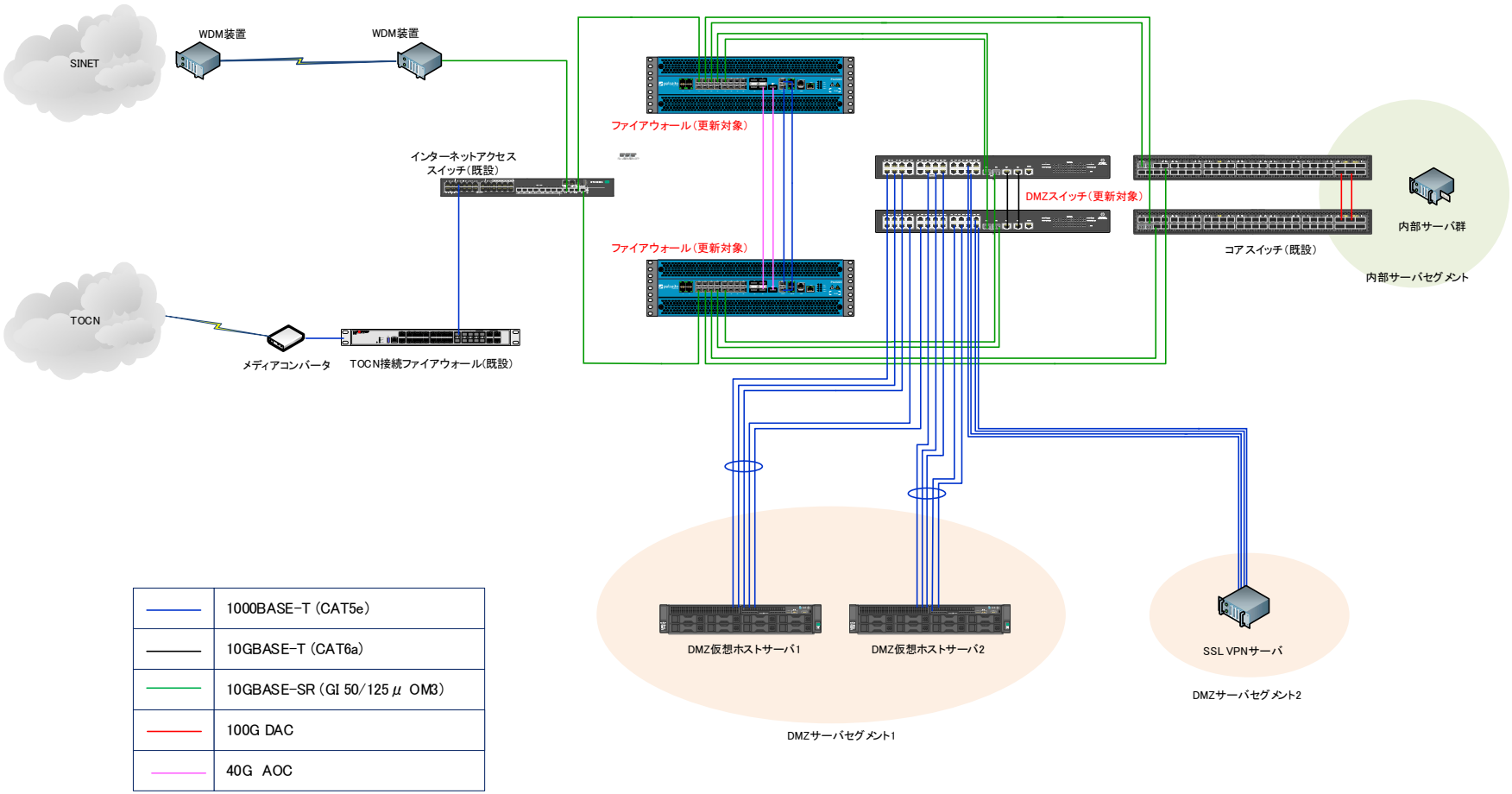
（イ）セキュリティ修正（ファームウェア、ドライバの修正等を含む）が提供されること。

項番	対象システム等	対　　象	
		（ア）セキュリティ機能	（イ）セキュリティ修正
3.1	ファイアウォール	システム管理機能	ファームウェア
3.2	DMZ スイッチ	システム管理機能	ファームウェア
3.3	無停電電源装置	システム管理機能	ファームウェア

表４　セキュリティ機能と修正の提供

＜資料＞

別紙１　現行ファイアウォール機器ネットワーク構成図



別紙２　既存機器概要

１．主な更新対象機器一覧

項番	機器等名称	メーカー、機種名	設置場所	備考
(1)	ファイアウォール装置（２式）	パロアルト PA-5220	附属学術情報センターコンピュータ室	２式で HA 構成
(2)	DMZ スイッチ（２式）	HPE OfficeConnect 1950 24G 2SFP+2XGT	附属学術情報センターコンピュータ室	２式でスタック構成
(3)	無停電電源装置（２式）	OMRON OMRON BN150R	附属学術情報センターコンピュータ室	ファイアウォール装置用

２．主な非更新関連機器一覧

項番	機器等名称	メーカー、機種名	設置場所	備考
(1)	コアスイッチ（２式）	HPE 5710 48SFP+ 6QSFP+/2QSFP28 Switch	附属学術情報センターコンピュータ室	２式でスタック構成
(2)	インターネットアクセススイッチ	HPE FlexNetwork 5140 24G 4SFP+ HI Switch	附属学術情報センターコンピュータ室	
(3)	ゲスト用ファイアウォール	Fortinet ForitiGate 101F	附属学術情報センターコンピュータ室	
(4)	SSL-VPN サーバ	F5 BIG-IP i2600 APM	附属学術情報センターコンピュータ室	
(5)	無停電電源装置	OMRON BN150RA	附属学術情報センターコンピュータ室	DMZ スイッチ、SSL-VPN サーバ用
(6)	DMZ 仮想ホストサーバ（２式）	HPE DL380 Gen10	附属学術情報センターコンピュータ室	
(7)	内部 Web サーバ	仮想マシン	附属学術情報センターコンピュータ室	
(8)	Radius サーバ	仮想マシン	附属学術情報センターコンピュータ室	
(9)	ネットワーク監視装置	Zabbix Enterprise　アプライアンス ZS 7700	附属学術情報センターコンピュータ室	

別紙３　附属学術情報センターコンピュータ室　ラック配置図