高専統一ネットワークシステム整備一式

仕様書

令和８年６月

独立行政法人国立高等専門学校機構

目次

別紙資料

別紙 1. ネットワーク機器一覧
別紙 2. 更新作業スケジュール
別紙 3. 各拠点及び機構本部所在地一覧
別紙 4. 用語集

1. 本調達の概要

1.1.　調達件名

「高専統一ネットワークシステム整備一式」

1.2.　本調達の背景と概要

独立行政法人国立高等専門学校機構（以下「高専機構」という。）は、令和 5 年度に全国の国立高等専門学校 51 校（55 拠点）（以下「各拠点」という。）及び高専機構本部事務局（以下「機構本部」という。）において、ファイアウォールやスイッチ等ネットワーク機器、無線 LAN システムを構成するコントローラやアクセスポイント、ユーザ認証管理等を行う各種サーバからなる「統一ネットワークシステム」を再構築し、これら全ての機器調達及び運用・保守に係る役務の調達を行った。

なお、機構本部は東京都八王子市に所在する八王子オフィス、東京都千代田区に所在する竹橋オフィスの 2 か所あるが、1 つの統一ネットワークシステムを利用している。

各拠点及び機構本部でそれぞれ必要な機器数量は、別紙 1. ネットワーク機器一覧を参照すること。本調達において、前回調達と同様に各拠点及び機構本部のスケールメリットを活かした戦略的な調達を行い、令和 10 年 4 月から運用開始予定の次期高専統一ネットワークシステムの導入・移行・運用・保守等を調達する。

なお、次期高専統一ネットワークシステムでは後述する概要で示すとおり、SINET データセンタ又は SINET データセンタと相互接続する IaaS 又は SaaS 等データセンタ（以下「データセンタ」という。）に各種サーバを集約する。

実際の導入・移行作業は図 1 のとおり、令和 9 年度から約 1 年間かけて各拠点及び機構本部に対して段階的に行い、令和 10 年 4 月から 5 年間の運用・保守を開始する計画である。

現行の統一ネットワークシステムから次期統一ネットワークシステムへの移行については、
別紙 2. 更新作業スケジュールに従って行うことを原則とし、１拠点あたり３日で実施し、並行して行うのは最大２拠点とする。なお、詳細は高専機構と受注者との協議により決定する。

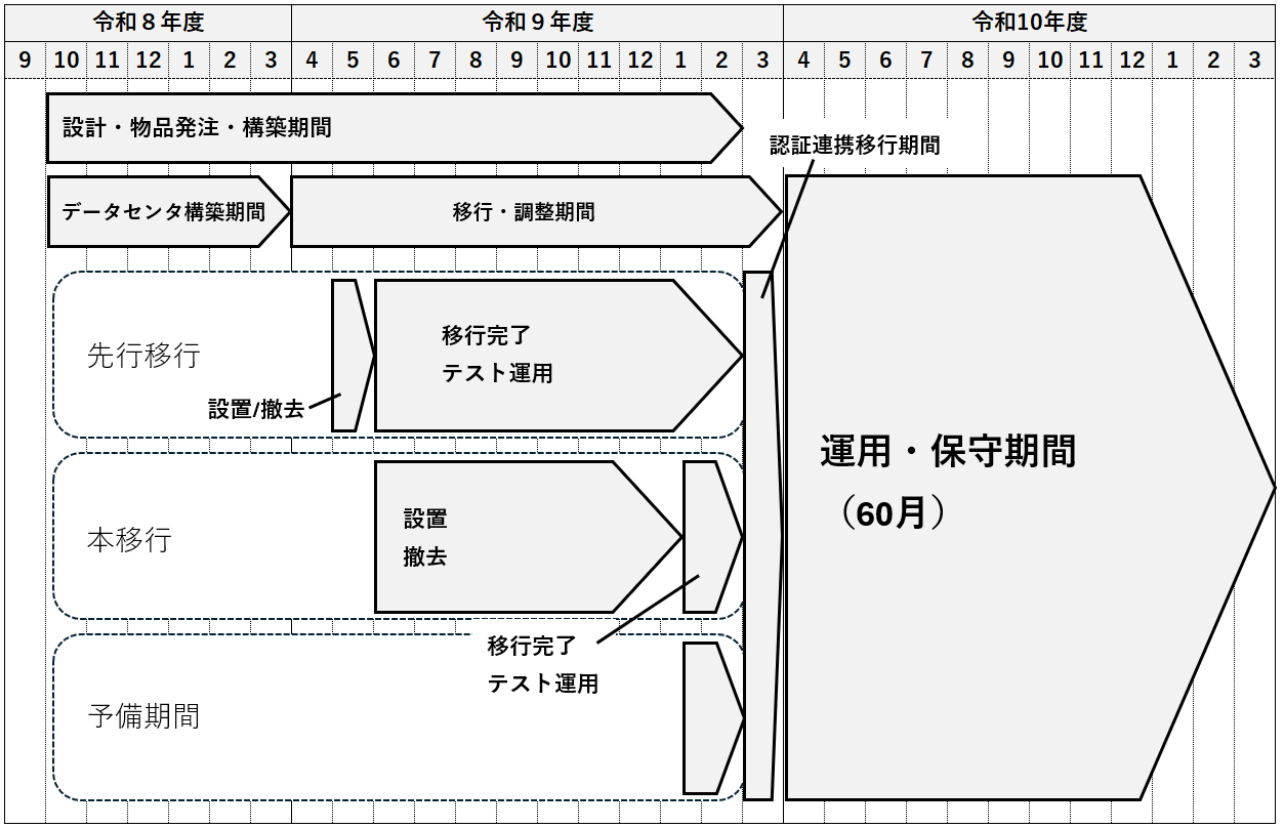

図 1. スケジュール概要

1.3. 契約期間

本調達の契約期間は、契約締結日から令和 15 年 3 月 31 日までとする。

ただし、各拠点及び機構本部に対する導入及び移行作業は契約締結日から令和 10 年 3 月 31 日までに完了し、令和 10 年 4 月 1 日より運用可能な状態とすること。

1.4. 所在地

各拠点及び機構本部の所在地については、別紙 3. 各拠点及び機構本部所在地一覧のとおり。

1.5. 用語

本調達特有の用語について、別紙 4. 用語集 に示す。

1.6.　高専統一ネットワークシステムの概要

1.6.1. 現行の高専統一ネットワークシステムの概要

現行の高専統一ネットワークシステムについては、各拠点及び機構本部を対象に令和 5 年 4 月 1 日より運用を行っている（概要は図 2 のとおり）。また、別調達にて SINET アクセス回線一式を整備することで、各拠点及び機構本部において共通のネットワーク機器、統一化されたネットワーク構成、外部接続回線を利用する環境を実現した。ただし、VLAN 構成やネットワーク認証等の利用形態等、一部統一されていない部分も残されており、この部分は各校の実情に合わせての運用となっている。

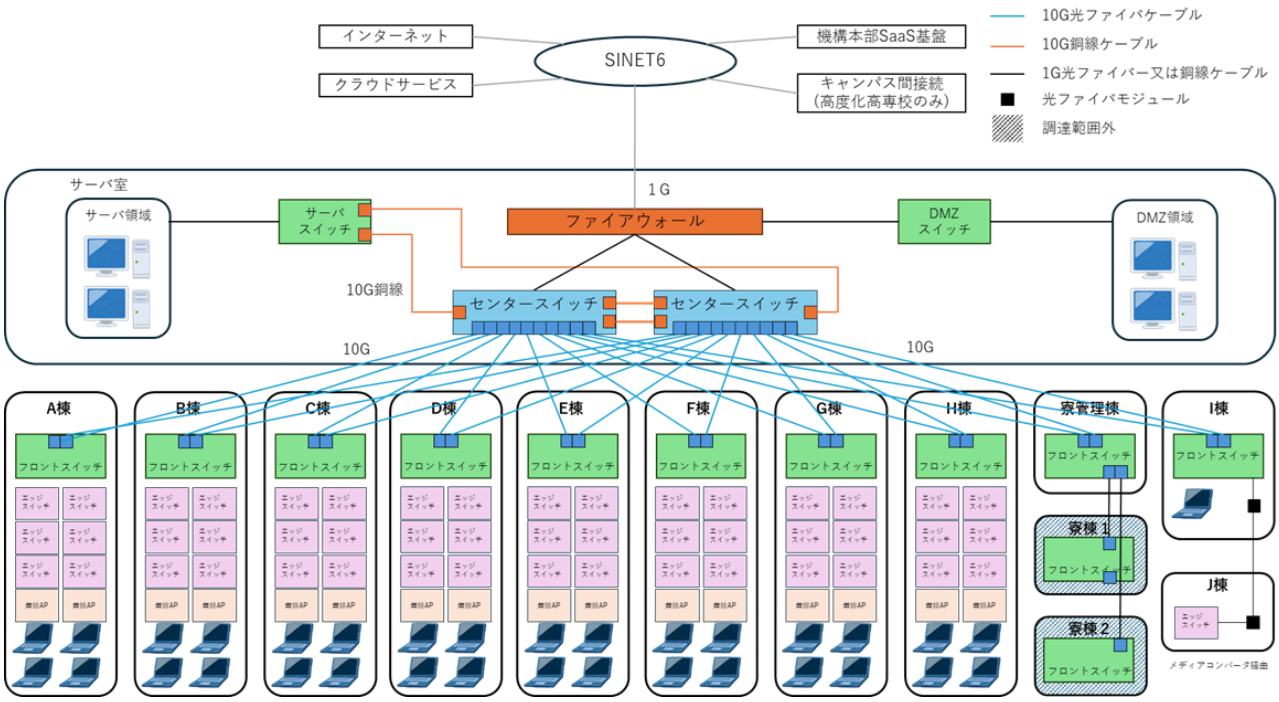

図 2. 現行の統一ネットワークシステム概図

1.6.2. 次期高専統一ネットワークシステムについて

1.6.2.1. 概要

本調達では、現行の高専統一ネットワークシステムを更新するとともに、現行システムにおいて未統一となっている部分について、論理設計・ネットワーク認証等を各拠点及び機構本部で揃えることにより、統一することを目指す。また、これ以外の現行システムにおける課題を整理した上で、ネットワーク及びサーバインフラに関する技術動向、国等が示す教育情報化に関する指針、第 2GSOC 等の独立行政法人に求められる情報セキュリティ対策を踏まえ、次期高専統一ネットワークシステムの整備方針を定めた。

下記に、次期高専統一ネットワークシステムで求める整備方針を示す。

・統一ネットワークシステムで稼働させるサーバをデータセンタにより集中管理すること。ただし、各拠点及び機構本部のインスタンスを分ける等の独立性を保つこと。
・高専統一ネットワークシステムの利用に必要な DNS、DHCP、SYSLOG 等サーバをデータセンタに集約配置すること。
・各拠点及び機構本部と、データセンタとの通信障害発生時でも以下の機能は利用できるよう可用性のある構成とすること。なお、障害発生時の詳細については各要件に示すほか、高専機構と協議すること。
  -RADIUS 機能(802.1X 認証及び MAC アドレス認証)
  -DHCP サーバ機能
  -内部 DNS 機能
・各拠点及び機構本部内に設置するファイアウォール⇔センタースイッチ、センタースイッチ⇔フロントスイッチ間を 10Gbps 以上とすること。ただし、各拠点及び機構本部内にサーバスイッチを設置する場合、センタースイッチ⇔サーバスイッチも同様に 10Gbps 以上とすること。
・各拠点及び機構本部内に設置する上記以外のスイッチ類及び無線アクセスポイント間の接続は 1Gbps 以上とすること。
・各拠点及び機構本部内に設置する無線アクセスポイントは Wi-Fi 7 又は後継規格に準拠した機器を導入すること。
・高専統一ネットワークシステムへ接続する際、802.1X 認証を原則とすること。また、ダイナミック VLAN に対応した認証規格で実装すること(802.1X 認証を原則とし、MAC アドレス認証も可能であること)。
・各拠点及び機構本部へ設置する機器について利用状況を可視化する管理ツールを導入すること。ただし、少なくとも下記の内容が可視化されること。
  -死活監視
  -トラフィック監視
  -ポートアップ・ポートダウン監視
  -CPU、メモリ、ファン等動作監視
・各拠点及び機構本部の通信、IDS/IPS ログをデータセンタで集約すること。
・機構本部が指定する TAXII サーバから TAXII プロトコルを用いた IoC 情報を取得し、各拠点及び機構本部に設置するファイアウォールへ配信すること。

・上記に定める各種機能の利用・管理に当たってライセンスが必要な場合は、受注者の負担にて用意すること。

1.6.2.2.　全体構成

本調達の全体構成を図 3-1、図 3-2 に示すいずれかの構成により提案すること。

ただし、図 3-2 の構成を採用する場合においても、各拠点及び機構本部に設置する「サーバ兼 DMZ スイッチ」については、別紙１「ネットワーク機器一覧」に記載の数量を必要とする。

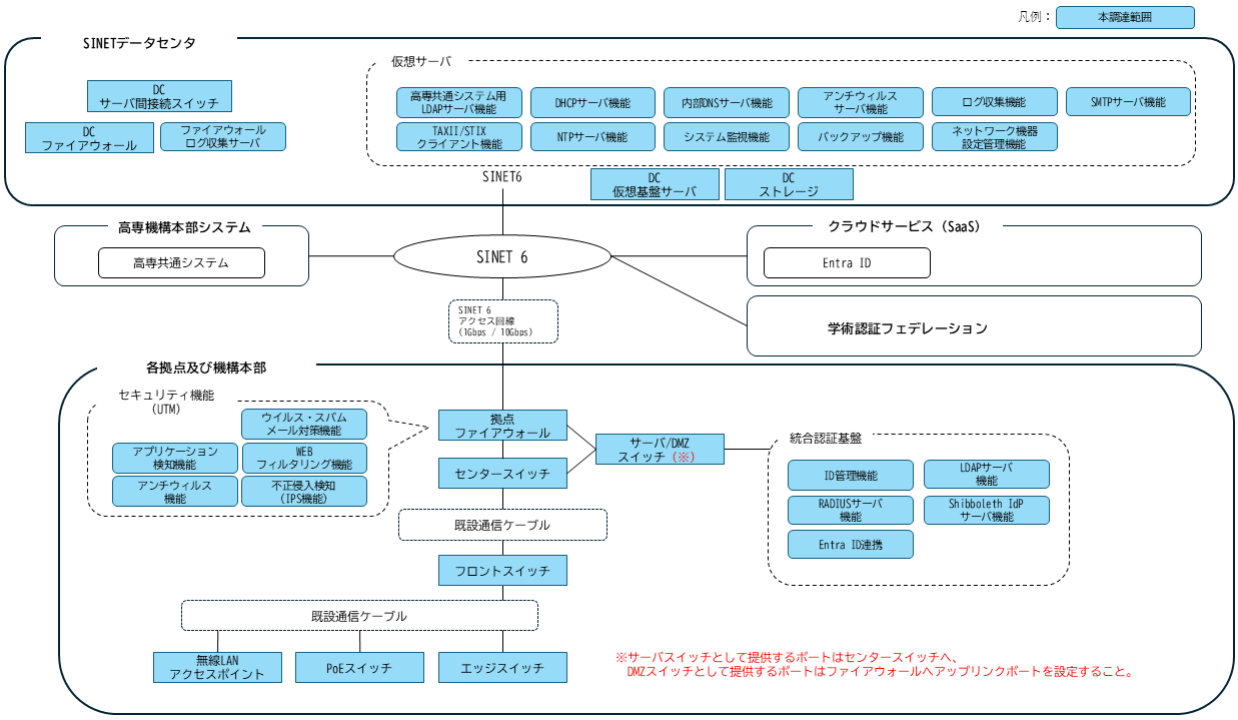

図 3-1. 全体構成（各拠点及び機構本部内に統合認証基盤を配置するパターン）

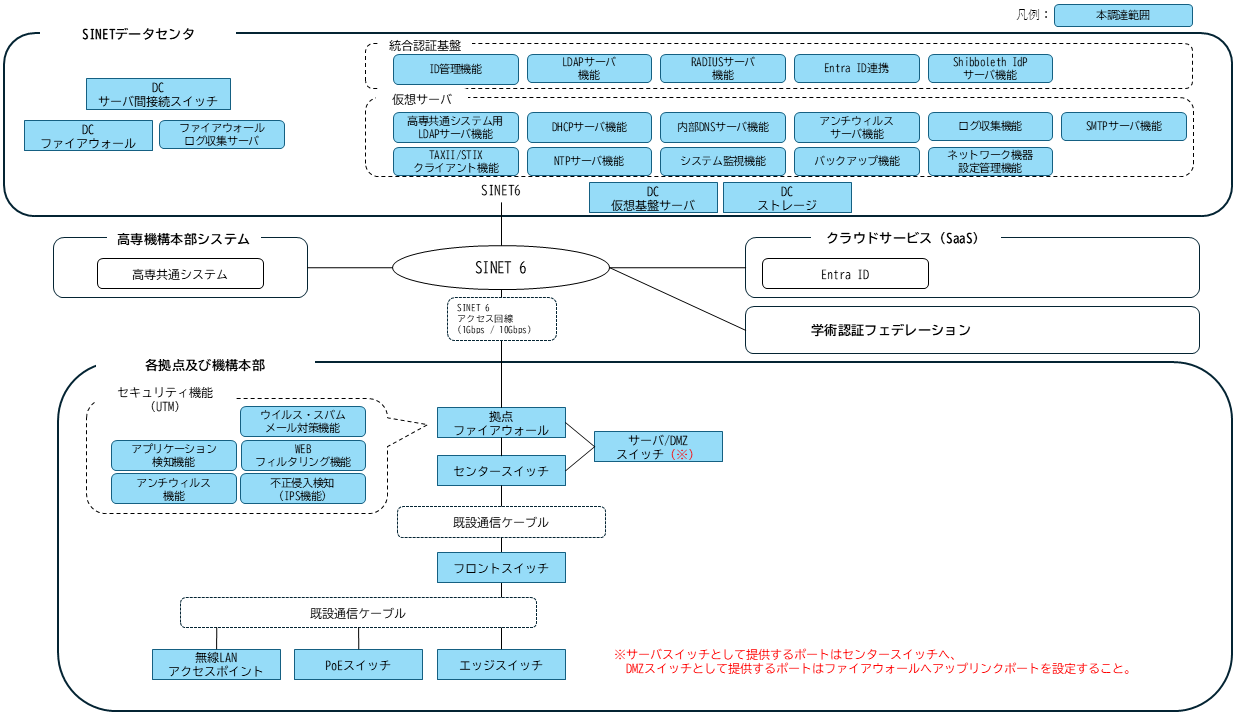

図 3-2. 全体構成(SINET データセンタに統合認証基盤を配置するパターン)

2. 導入・移行業務について

2.1. ネットワーク機器個別要件

(1) 本調達で導入する各ネットワーク機器の要件については、以下のとおりとする。

(2) 次期ネットワーク整備において、本調達の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.1.1. データセンタ内機器要件

2.1.1.1. DC ファイアウォール機器要件

(1) 19 インチラックに搭載可能であり、搭載に必要な金具等を用意すること。

(2) 入力電源は AC100V 又は AC200V(50Hz/60Hz)に対応していること。

(3) SYSLOG 排出機能を有し、SYSLOG 収集機能と連携可能なこと。ただし、SYSLOG はメッセージの Facility 及び Severity で分類されていること。

(4) SNMP 等の管理プロトコルに対応し、システム監視機能と連携可能なこと。

(5) NTP 又は SNTP に対応すること。

(6) 筐体は 2 台以上の冗長構成とし、耐障害性及び可用性を保つこと。なお、2 台以上の Active/Active 構成であり、かつ負荷分散が可能な場合は加点する。【加点】

(7) SINET ノード、項「2.1.1.2. DC サーバ接続機器要件」で示す機器等と接続可能な 100GbE QSFP28 インターフェースを 4 ポート以上有すること。ただし、SINET ノードと接続する際は 100GBASE-LR4（SINET が当機構に提供する回線の種別により、40GBASE-LR4 とする可能性がある）で接続すること。

その際、高専機構が指定する SINET ノードと当該 DC ファイアウォール機器を接続するケーブルを含めること。

(8) SINET ノードと DC ファイアウォール機器の間にスイッチやロードバランサー等の機器を設置する場合、SINET ノードと DC ファイアウォール間は(21)に示すスループットを保つよう構成すること。

(9) 管理用コンソールポートを 1 ポート以上有すること。

(10) SSH による管理が可能なこと。

(11) 設定は Web ブラウザ経由による GUI 又は管理用コンソール、SSH 経由による CLI のいずれにも対応していること。

(12) GUI 上で新旧ポリシーの差分が確認でき、任意の版(バージョン)にロールバックできること。

(13) FW と管理サーバは個別に構築し、管理コンソールによるポリシー及びログの集中管理をさせ、FW ローカル管理 Web UI へのアクセスを制御できること。

(14) 電源は 2 つ以上で冗長化すること。

(15) IPv4 のルーティング機能としてスタティック・ルーティング、ダイナミック・ルーティング（RIPv2、OSPFv2)に対応していること。

(16) IPv6 のルーティング機能としてスタティック・ルーティング、ダイナミック・ルーティング（RIPng、OSPFv3 のうちいずれか)に対応していること。

(17) IEEE802.1Q VLAN タギングに対応していること。

(18) IEEE802.3ad リンクアグリゲーションに対応していること。

(19) 同時セッション数は 1620 万セッション以上であること。
(20) 新規セッション数/秒は 190,000 セッション/秒以上であること。
(21) ファイアウォール性能が 100Gbps 以上であること。
(22) IPv4 において NAT 及び NAPT に対応していること。
(23) IPv6 によるファイアウォールのポリシーの設定が可能なこと。
(24) ポリシー数は 10,000 以上設定可能なこと。
(25) 高専機構が指定する TAXII/STIX Producer(脅威情報提供者)の脅威情報やブラックリスト IP アドレスをファイアウォールに自動取り込みを行うこと。TAXII/STIX Producer とファイアウォールとの間に機器や環境が必要な場合、用意すること。

2.1.1.2. DC サーバ接続機器要件

(1) 19 インチラックに搭載可能であり、搭載に必要な金具等を用意すること。
(2) 入力電源は AC100V 又は AC200V(50Hz/60Hz)に対応していること。
(3) SYSLOG 排出機能を有し、SYSLOG 収集機能と連携可能なこと。ただし、SYSLOG はメッセージの Facility 及び Severity で分類されていること。
(4) SNMP 等の管理プロトコルに対応し、システム監視機能と連携可能なこと。
(5) NTP 又は SNTP に対応すること。
(6) 筐体は 2 台以上の Active/Active 構成とし、耐障害性及び可用性を保つこと。
(7) 1 台の障害時には、自動的にもう 1 台の物理スイッチにて通信維持する機能を有すること。また交換時においても通信を維持すること。
(8) 電源ユニットおよび冷却ファンは冗長構成とすること。
(9) 稼働中に交換・追加が可能なホットスワップ対応であること。
(10) SINET ノード、項「2.1.1.1. DC ファイアウォール機器要件」に記載する機器等と接続可能な 100GbE QSFP28 インターフェースを 4 ポート以上有すること。ただし、SINET ノードと接続する際は 100GBASE-LR4 (SINET が当機構に提供する回線の種別により、40GBASE-LR4 とする可能性がある) で接続すること。
(11) 10GbE SFP+または 10GbE-T インターフェースを 24 ポート以上有すること。
(12) スイッチング容量が 1,000Gbps 以上であること。
(13) 最大パケット転送能力が 800Mpps 以上であること。
(14) IPv4/IPv6 通信が可能であること。
(15) IPv4 のルーティング機能としてスタティック・ルーティング、ダイナミック・ルーティング(RIPv2 又は OSPFv2)に対応が可能なこと。また、筐体仮想化と同時にルーティング機能を使用可能なこと。
(16) IPv6 のルーティング機能としてスタティック・ルーティング、ダイナミック・ルーティング(RIP ng、OSPFv3)に対応していること。
(17) ポート VLAN、タグ VLAN(IEEE802.1Q)機能を有すること。
(18) VLAN ID は 4,000 以上が設定可能であること。
(19) VLAN インターフェースとして 1,000 個以上の IP アドレスが設定可能なこと。
(20) IEEE802.3ad リンクアグリゲーションに対応していること。
(21) リンクアグリゲーション機能として、4 ポート以上/24 グループ以上を設定可能なこと。

(22) リンクアグリゲーションされたポートのグループ内で負荷分散アルゴリズムを利用可能なこと。
(23) IEEE802.1d に準拠したスパニングツリー機能を有すること。
(24) IEEE802.1w に準拠した高速スパニングツリー機能を有すること。
(25) VLAN ごとにインスタンスを構成する場合は、IEEE802.1s に準拠した多重スパニングツリー機能を有すること。
(26) 送受信されるパケットを識別し、優先してパケット中継を行うことを可能とする優先制御機能を有すること。
(27) 接続確認を LED ランプ表示で確認できること。
(28) SSH による管理が可能なこと。
(29) 次期ネットワーク整備において、本調達の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.1.2. 各拠点及び機構本部機器要件

(1) 項「2.1.2.2. センタースイッチ」から項「2.1.2.8. 無線 LAN コントローラ」までの各スイッチ、無線アクセスポイント、無線 LAN コントローラについて、独自機能や詳細仕様の違いにより、期待通りの動作を妨げないことを保証すること。

2.1.2.1. UTM ファイアウォール

(1) 19 インチラックに搭載可能であり、搭載に必要な金具等を用意すること。
(2) 入力電源は AC100V(50Hz/60Hz)に対応していること。
(3) SYSLOG に対応し、SYSLOG 収集機能と連携可能なこと。ただし、SYSLOG はメッセージの Facility 及び Severity で分類されていること。
(4) SNMP 等の管理プロトコルに対応し、システム監視機能と連携可能なこと。
(5) NTP 又は SNTP に対応すること。
(6) 周囲温度が 0～40℃の環境で動作可能であること。
(7) 拡張スロットを含め、利用する通信ポートがスイッチ機器の背面パネルに存在する場合、別途ラックマウントレールキットなどを調達必須とし、運用面に支障が無いよう配慮すること。
(8) 10/100/1,000Mbps の Ethernet のインターフェースを８ポート以上有すること。
(9) 10GbE SFP+インターフェースを 4 ポート以上有すること。なお、必要なモジュールについては、別紙１「ネットワーク機器一覧」に示す。
(10) 管理用コンソールポートを 1 ポート以上有すること。
(11) SSH による管理が可能なこと。
(12) 設定は Web ブラウザ経由による GUI 又は管理用コンソール、SSH 経由による CLI のいずれにも対応していること。
(13) GUI 上で新旧ポリシーの差分が確認でき、任意の版(バージョン)にロールバックできること。
(14) FW と管理サーバは個別に構築し、管理コンソールによるポリシー及びログの集中管理をさせ、FW ローカル管理 Web UI へのアクセスを制御できること。
(15) データセンタに管理サーバを構築し、各拠点及び機構本部に設置する FW の管理が可能な構成とすること。

(16) 各拠点及び機構本部に配置するFWは各拠点及び機構本部が指定するユーザのみ当該拠点のFWへアクセスすることができること。
(17) 電源冗長化の上、少なくとも1系統は無停電電源装置に接続すること。無停電電源装置へ接続しない系統は各拠点及び機構本部の各商用電源(一次電源)へ接続すること。
(18) シリアルポートあるいはネットワーク経由により、無停電電源装置又は無停電電源装置と連携した他システムからのコマンドの投入により機器を自動的に停止できること。
(19) 3ラックユニットサイズ以下であること。ただし、無停電電源装置は含まない。
(20) IPv4のルーティング機能としてスタティック・ルーティング、ダイナミック・ルーティング（RIPv2、OSPFv2)に対応していること。
(21) IPv6のルーティング機能としてスタティック・ルーティング、ダイナミック・ルーティング（RIPng、OSPFv3のうちいずれか)に対応していること。
(22) IEEE802.1Q VLANタギングに対応していること。
(23) IEEE802.3adリンクアグリゲーションに対応していること。
(24) 論理的な仮想セキュリティ・ドメインを7個具備以上分割可能なこと。
(25) 同時セッション数は360万セッション以上であること。
(26) 新規セッション数/秒は140,000セッション/秒以上であること。
(27) ISO/IEC15408規格又はNIアクセスポイントーCCEVS CPP認定に適合しているファイアウォール機能を有すること。又は過去5年以内でCVE情報の総数が60件以下、かつCritical-Highが10件以下であること。
(28) ファイアウォール性能が39Gbps以上であること。
(29) IPv4においてNAT及びNAPTに対応していること。
(30) IPv6によるファイアウォールのポリシーの設定が可能なこと。
(31) ポリシー数は10,000以上設定可能なこと。
(32) 内部ネットワークをグループ化し、グループごとに異なるポリシー設定が可能なこと。
(33) IPSEC VPNに対応すること。
(34) IPSEC VPNトンネル数は2,000以上であること。
(35) IPSEC VPN性能は13Gbps以上であること。
(36) IPSEC VPN時接続ユーザ数は5以上であること。
(37) インターネットサービスのIPアドレスデータベースを有し、Microsoft Azure、Microsoft 365、Google、Zoom等を宛先に選択し、ルーティングできること。また、インターネットサービスのIPアドレスデータベース利用以外にも、アプリケーショントラフィック種別に基づくルーティング機能や、サーバ等の別コンポーネントによるアドレス取得自動化などで実現することも可能とすること。
(38) 高専機構が指定するTAXII/STIX Producer(脅威情報提供者)の脅威情報やブラックリストIPアドレスをファイアウォールに自動取り込みを行うこと。TAXII/STIX Producerとファイアウォールとの間に機器や環境が必要な場合、用意すること。
(39) 機器が属する同一シリーズ（同一ブランド・同一製品系統）について、過去5年以内でCVE情報の総数が15件以下、かつCritical-Highは5件以下である場合は加点する。 【加点】
(40) 論理的な仮想セキュリティ・ドメインは11個具備以上分割可能である場合は加点する 。【加点】

(41) 1 ラックユニットサイズ以下である場合は加点する。【加点】
(42) 本調達の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.1.2.2. センタースイッチ

(1) 19 インチラックに搭載可能であり、搭載に必要な金具等を用意すること。
(2) 入力電源は AC100V(50Hz/60Hz)に対応していること。
(3) 稼働中に交換・追加が可能なホットスワップ対応であること。
(4) SYSLOG に対応し、SYSLOG 収集機能と連携可能なこと。ただし、SYSLOG はメッセージの Facility 及び Severity で分類されていること。
(5) SNMP 等の管理プロトコルに対応し、システム監視機能と連携可能なこと。
(6) NTP 又は SNTP に対応すること。
(7) 周囲温度が 0～40℃の環境で動作可能であること。
(8) 拡張スロットを含め、利用する通信ポートがスイッチ機器の背面パネルに存在する場合、別途ラックマウントレールキットなどを調達必須とし、運用面に支障が無いよう配慮すること。
(9) 同一構成スイッチを 2 台で、仮想的に 1 台の論理スイッチとして稼働させる機能を有すること。または、2 台以上の Active/Active 構成とし、耐障害性及び可用性を保つこと。
(10) 各フロントスイッチとは 10Gbps インターフェースを介して接続されており、平常時、各フロントスイッチとの通信帯域は 20Gbps を確保すること。
(11) センタースイッチに接続されるネットワーク機器は原則冗長配線を行い、平常時はリンクアグリゲーションによる接続を行うこと。
(12) 1 台の障害時には、自動的にもう 1 台の物理スイッチにて通信維持する機能を有すること。また交換時においても通信を維持すること。
(13) 物理スイッチ 1 台あたり、10GbE SFP+インターフェースを有する 24 ポート以上有すること。
(14) スイッチング容量が 1,000Gbps 以上であること。
(15) 最大パケット転送能力が 800Mpps 以上であること。
(16) IPv4/IPv6 通信が可能であること。
(17) IPv4 のルーティング機能としてスタティック・ルーティング、ダイナミック・ルーティング(RIPv2 又は OSPFv2)に対応が可能なこと。また、筐体仮想化と同時にルーティング機能を使用可能なこと。
(18) IPv6 のルーティング機能としてスタティック・ルーティング、ダイナミック・ルーティング(RIP ng、OSPFv3)に対応していること。
(19) ポート VLAN、タグ VLAN(IEEE802.1Q)機能を有すること。
(20) VLAN ID は 4,000 以上が設定可能であること。
(21) VLAN インターフェースとして 1,000 個以上の IP アドレスが設定可能なこと。
(22) IEEE802.3ad リンクアグリゲーションに対応していること。
(23) リンクアグリゲーション機能として、4 ポート以上/24 グループ以上を設定可能なこと。
(24) リンクアグリゲーションされたポートのグループ内で負荷分散アルゴリズムを利用可能なこと。
(25) IEEE802.1d に準拠したスパニングツリー機能を有すること。
(26) IEEE802.1w に準拠した高速スパニングツリー機能を有すること。

(27) VLAN ごとにインスタンスを構成する場合は、IEEE802.1s に準拠した多重スパニングツリー機能を有すること。
(28) 送受信されるパケットを識別し、優先してパケット中継を行うことを可能とする優先制御機能を有すること。
(29) 接続確認を LED ランプ表示で確認できること。
(30) SSH による管理が可能なこと。
(31) 1 ラックユニットサイズ以下であること。
(32) DHCP relay 機能を有すること。
(33) 電源は冗長構成であること。
(34) 電源冗長化の上、少なくとも 1 系統は無停電電源装置に接続すること。無停電電源装置へ接続しない系統は各拠点及び機構本部の各商用電源(一次電源)へ接続すること。
(35) 管理用コンソールポートを 1 ポート以上有すること。
(36) ACL について Ingress で 9,216 以上、Egress で 1,024 以上定義できること。又は、2,000 件以上のエントリーが設定できること。
(37) 項「2.1.2.8. 無線 LAN コントローラ」と同じ基盤上で管理すること。
(38) SSH 及び筐体の Web 管理機能のいずれも利用できる場合は加点する。 【加点】
(39) 周囲温度が 0～50℃の環境で動作可能である場合は加点する。(ただし、結露しない状態に限る。)【加点】
(40) 本調達の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.1.2.3. フロントスイッチ

(1) 19 インチラックに搭載可能であり、搭載に必要な金具等を用意すること。
(2) 入力電源は AC100V(50Hz/60Hz)に対応していること。
(3) SYSLOG に対応し、SYSLOG 収集機能と連携可能なこと。ただし、SYSLOG はメッセージの Facility 及び Severity で分類されていること。
(4) SNMP 等の管理プロトコルに対応し、システム監視機能と連携可能なこと。
(5) NTP 又は SNTP に対応すること。
(6) 周囲温度が 0～40℃の環境で動作可能であること。
(7) 拡張スロットを含め、利用する通信ポートがスイッチ機器の背面パネルに存在する場合、別途ラックマウントレールキットなどを調達必須とし、運用面に支障が無いよう配慮すること。
(8) 10/100/1000BASE-TX Ethernet のインターフェースを 48 ポート以上有すること。
(9) 1GbE SFP のモジュールが挿入可能なポートを 2 以上有すること。
(10) 10GbE SFP+のモジュールが挿入可能なポートを 2 以上有すること。
(11) 10GbE SFP+ポートを 4 ポート以上有する場合は加点する。なお、このポートは(8)に示すポートとのコンボポートでも良い。【加点】
(12) スイッチング容量が 176Gbps 以上であること。
(13) 最大パケット転送能力が 131Mpps 以上であること。
(14) IPv4/IPv6 通信が可能であること。

(15) IPv4 のルーティング機能としてスタティック・ルーティングに対応が可能なこと。
(16) IPv6 のルーティング機能としてスタティック・ルーティングに対応していること。
(17) ポート VLAN、タグ VLAN(IEEE802.1Q)、ダイナミック VLAN 機能を有すること。
(18) VLAN ID は 4,000 以上が設定可能であること。
(19) 認証を利用するポートについてスタティック及びダイナミック VLAN に対応していること。
(20) IEEE802.1X 認証、MAC アドレス認証の機能を有し、1 ポートで IEEE802.1X 認証、MAC アドレス認証リクエストに対して、いずれにも対応可能なこと。
(21) RADIUS サーバと連携し、ユーザ/デバイス毎に認証の結果に応じたセキュリティポリシーを割り当てアクセス制御が行えること。
(22) 1 ポート配下に接続された複数機器それぞれに対して認証を適用可能なこと。
(23) RADIUS 通信の TLS による暗号化(RadSec:RFC6614)に対応していること。
(24) 802.1X 認証と MAC 認証の認証順、認証のプライオリティを設定可能なこと。
(25) DHCP Snooping 機能を有すること
(26) IEEE802.3ad リンクアグリゲーションに対応していること。
(27) リンクアグリゲーション機能として、4 ポート以上/24 グループ以上を設定可能なこと。
(28) リンクアグリゲーションされたポートのグループ内で負荷分散アルゴリズムを利用可能なこと。
(29) IEEE802.1d に準拠したスパニングツリー機能を有すること。
(30) IEEE802.1w に準拠した高速スパニングツリー機能を有すること。
(31) VLAN ごとにインスタンスを構成する場合は、IEEE802.1s に準拠した多重スパニングツリー機能を有すること。
(32) 送受信されるフレームを識別し、レートリミットによる制御機能を有すること。
(33) 接続確認を LED ランプ表示で確認できること。
(34) SSH による管理が可能なこと。
(35) 1 ラックユニットサイズ以下であること。
(36) DHCP relay 機能を有する場合は加点する。【加点】
(37) 管理用コンソールポートを 1 ポート以上有すること。
(38) 周囲温度が 0～50℃の環境で動作可能である場合は加点する。ただし、結露しない状態に限る。【加点】
(39) SSH 及び筐体の Web 管理機能のいずれも利用できる場合は加点する。 【加点】
(40) 本調達の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.1.2.4. エッジスイッチ(SFP 要)

(1) 19 インチラックに搭載可能であり、搭載に必要な金具等を用意すること。
(2) 入力電源は AC100V(50Hz/60Hz)に対応していること。
(3) SYSLOG に対応し、SYSLOG 収集機能と連携可能なこと。ただし、SYSLOG はメッセージの Facility 及び Severity で分類されていること。
(4) SNMP 等の管理プロトコルに対応し、システム監視機能と連携可能なこと。
(5) NTP 又は SNTP に対応すること。

(6) 周囲温度が 0～40℃の環境で動作可能であること。
(7) 拡張スロットを含め、利用する通信ポートがスイッチ機器の背面パネルに存在する場合、別途ラックマウントレールキットなどを調達必須とし、運用面に支障が無いよう配慮すること。
(8) 接続する端末数に応じて 10/100/1,000Base-T 8 ポートから 48 ポートの選択が可能なこと。各ポート数に応じた製品での提案が難しい場合は、必要ポート数を満たす製品を提案すること。なお、各拠点の物理的な制約についても配慮すること。
(9) 1GbE SFP のモジュールが挿入可能なポートを 2 以上有すること。
(10) 10GbE SFP+のモジュールが挿入可能なポートを 2 以上有する場合は加点する。【加点】
(11) スイッチング容量は、各々選定するポート数の最低数値を以下の通り示す。

8 ポートから 11 ポート：20Gbps
12 ポートから 15 ポート：28Gbps
16 ポートから 23 ポート：36Gbps
24 ポートから 47 ポート：52Gbps
48 ポート以上　　：100Gbps

なお、最低数値が下記数値以上である場合は加点する。【加点】

8 ポートから 11 ポート　：60Gbps
12 ポートから 15 ポート：68Gbps
16 ポートから 23 ポート：76Gbps
24 ポートから 47 ポート：92Gbps
48 ポート以上　　：140Gbps

(12) パケット転送能力は、各々選定するポート数の最低数値を以下の通り示す。

8 ポートから 11 ポート：13Mpps
12 ポートから 15 ポート：19Mpps
16 ポートから 23 ポート：24Mpps
24 ポートから 47 ポート：35Mpps
48 ポート以上　　：67Mpps

なお、最低数値が下記数値以上である場合は加点する。【加点】

8 ポートから 11 ポート：40Mpps
12 ポートから 15 ポート：46Mpps
16 ポートから 23 ポート：51Mpps
24 ポートから 47 ポート：62Mpps
48 ポート以上　　：94Mpps

(13) タグ VLAN(IEEE802.1Q)、ポート VLAN 機能を有すること。
(14) VLAN ID は 4,000 以上設定可能なこと。
(15) VLAN インターフェースとして 2 個以上の IP アドレスが設定可能なこと。
(16) 認証を利用するポートについてスタティック及びダイナミック VLAN に対応していること。
(17) IEEE802.1X 認証、MAC アドレス認証の機能を有し、1 ポートで IEEE802.1X 認証、MAC アドレス認証

リクエストに対して、いずれにも対応可能なこと。
(18) RADIUS サーバと連携し、ユーザ/デバイス毎に認証の結果に応じた VLAN attributes を割り当てアクセス制御が行えること。
(19) 1 ポート配下に接続された複数機器それぞれに対して認証を適用可能なこと。
(20) RADIUS 通信の TLS による暗号化(RadSec:RFC6614)に対応していること。
(21) DHCP Snooping 機能を有すること
(22) IEEE802.3ad リンクアグリゲーションに対応していること。
(23) リンクアグリゲーション機能として、4 ポート以上/8 グループ以上を設定可能なこと。
(24) IEEE802.1d に準拠したスパニングツリー機能を有すること。
(25) IEEE802.1w に準拠した高速スパニングツリー機能を有すること。
(26) VLAN ごとにインスタンスを構成する場合は、IEEE802.1s に準拠した多重スパニングツリー機能を有すること。
(27) 接続確認を LED ランプ表示で確認できること。
(28) SSH による管理が可能なこと。
(29) 1 ラックユニットサイズ以下であること。
(30) 管理用コンソールポートを 1 ポート以上有すること。
(31) 周囲温度が 0～50℃の環境で動作可能である場合は加点する。ただし、結露しない状態に限る。【加点】
(32) ファンレス又は、騒音レベルが 51dBA 以下もしくは 45dB 以下である場合は加点する。 【加点】
(33) SSH 及び筐体の Web 管理機能のいずれも利用できる場合は加点する。 【加点】
(34) 本調達の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.1.2.5. サーバ兼 DMZ スイッチ

(1) 項「2.1.2.3 フロントスイッチ」の各要件を満たすこと。なお、同項の各加点項目を満たす場合、同様に加点する。【加点】

2.1.2.6. PoE スイッチ

(1) 19 インチラックに搭載可能であり、搭載に必要な金具等を用意すること。
(2) 入力電源は AC100V(50Hz/60Hz)に対応していること。
(3) SYSLOG に対応し、SYSLOG 収集機能と連携可能なこと。ただし、SYSLOG はメッセージの Facility 及び Severity で分類されていること。
(4) SNMP 等の管理プロトコルに対応し、システム監視機能と連携可能なこと。
(5) NTP 又は SNTP に対応すること。
(6) 周囲温度が 0～40℃の環境で動作可能であること。
(7) 拡張スロットを含め、利用する通信ポートがスイッチ機器の背面パネルに存在する場合、別途ラックマウントレールキットなどを調達必須とし、運用面に支障が無いよう配慮すること。
(8) 提供するスイッチのすべてのポートで PoE/PoE+給電が可能であること。また、すべてのポートで同時に給電した際、項「2.1.2.7.無線アクセスポイント」で求める無線アクセスポイントが縮退・機

能制限無く利用可能なこと。

(9) 1GbE SFP のモジュールもしくは 10GbE SFP のモジュールが挿入可能なポートを 2 ポート以上有すること。

(10) インターフェースの速度及び全二重/半二重のオートネゴシエーションが可能であること。

(11) スイッチング容量は、各々選定するポート数の最低数値を以下の通り示す。

8 ポートから 11 ポート：20Gbps
12 ポートから 15 ポート：28Gbps
16 ポートから 23 ポート：36Gbps
24 ポートから 47 ポート：52Gbps
48 ポート以上　　：100Gbps

なお、最低数値が下記数値以上である場合は加点する。【加点】

8 ポートから 11 ポート　：60Gbps
12 ポートから 15 ポート：68Gbps
16 ポートから 23 ポート：76Gbps
24 ポートから 47 ポート：92Gbps
48 ポート以上　　：140Gbps

(12) パケット転送能力は、各々選定するポート数の最低数値を以下の通り示す。

8 ポートから 11 ポート：13Mpps
12 ポートから 15 ポート：19Mpps
16 ポートから 23 ポート：24Mpps
24 ポートから 47 ポート：35Mpps
48 ポート以上　　：67Mpps

なお、最低数値が下記数値以上である場合は加点する。【加点】

8 ポートから 11 ポート：40Mpps
12 ポートから 15 ポート：46Mpps
16 ポートから 23 ポート：51Mpps
24 ポートから 47 ポート：62Mpps
48 ポート以上　　：94Mpps

(13) タグ VLAN(IEEE802.1Q)、ポート VLAN 機能を有すること。

(14) VLAN ID は 4,000 以上設定可能なこと。

(15) VLAN インターフェースとして 2 個以上の IP アドレスが設定可能なこと。

(16) DHCP Snooping 機能を有すること

(17) IEEE802.3ad リンクアグリゲーションに対応していること。

(18) リンクアグリゲーション機能として、4 ポート以上/8 グループ以上を設定可能なこと。

(19) IEEE802.1d に準拠したスパニングツリー機能を有すること。

(20) IEEE802.1w に準拠した高速スパニングツリー機能を有すること。

(21) VLAN ごとにインスタンスを構成する場合は、IEEE802.1s に準拠した多重スパニングツリー機能を

有すること。
(22) 接続確認を LED ランプ表示で確認できること。
(23) 1 ラックユニットサイズ以下であること。
(24) 接続する無線アクセスポイントの数が少ない箇所は設計、利用、運用・保守に影響が無いことを前提に項「2.1.2.4.エッジスイッチ(SFP 要)」に PoE インジェクタを接続することも可能とする。ただし、PoE インジェクタは PoE/PoE+に対応すること。
(25) 管理用コンソールポートを 1 ポート以上有すること。
(26) PoE/PoE+はそれぞれ IEEE802.3af、IEEE802.3at であり、最大給電電力 100W の規格である IEEE802.3bt や同種のメーカー独自規格は認めない。
(27) 周囲温度が 0～50℃の環境で動作可能な場合は加点する。ただし、結露しない状態に限る。【加点】
(28) 提案機器がファンレス又は静音設計である場合は加点する。【加点】
(29) SSH 及び筐体の Web 管理機能のいずれも利用できる場合は加点する。 【加点】
(30) 本調達の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.1.2.7. 無線アクセスポイント

(1) 無線 LAN コントローラ又はクラウドによる集中管理が可能なこと。
(2) 無線 LAN コントローラ又はクラウドとの通信断においても無線アクセスポイントの動作が継続すること。ただし、設定変更機能についてはこの限りでない。
(3) IEEE802.11 に準拠し、IEEE802.11a/b/g/n/ac/ax/be のいずれにも対応すること。
(4) 同時接続する無線クライアント数は 200 台以上可能なこと。また、同時接続する無線クライアント数 50 台程度において安定運用可能であること。ただし、高負荷環境での利用時、利用開始時の一時的なアクセス集中による輻輳発生時、校内ネットワーク内の配線や他機器に帯域に起因するもの、故障又は障害時は例外とする。
(5) 屋内の見通しで 30m まで安定的に通信可能であること。
(6) WPA2/WPA3 Enterprise に対応していること。
(7) IEEE802.1X 認証機能を有すること。
(8) 項 2.1.2.6.で指定する PoE スイッチに接続し、機能制限・機能縮退なく稼働すること。
(9) 各拠点及び機構本部の物理構成により、PoE スイッチに接続できない場合、PoE インジェクタ等の給電装置を別途用意すること。その際、機能制限・機能縮退なく稼働すること。
(10) 天井部及び壁面部への設置を考慮し、ブラケット等により固着すること。
(11) 8 以上の SSID に対応したマルチ SSID 機能を有すること。また、うち 1 つを eduroam に対応させること。
(12) マルチ SSID の動作として、各 SSID でビーコン(BSSID)を識別して送信可能なこと。
(13) MLO に対応し、1 つの SSID で 6GHz、5GHz、2.4GHz が同時に利用できる機能を有すること。
(14) 1Gbps 以上の Ethernet ポートを有すること。
(15) 通信レートが異なる複数の端末が混在している場合に、無線通信時間を割り与えるエアタイムフェアネス機能又はそれに準ずる機能を有すること。
(16) 不正アクセスポイントを検出する機能を有すること。ただし、無線 LAN コントローラで実装するこ

とでも可能とする。

(17) 許可されたクライアントの MAC アドレス以外からの通信を行わせないことにより、不正アクセスを防止する仕組みを持つこと。

(18) SSID 毎に AP アイソレーション(無線 AP 折り返しによるクライアント端末間の通信を禁止する)機能が有効化可能なこと。

(19) 無線 AP はメッシュ機能をサポートし、ルート AP 及びメッシュ AP として動作可能であること。

(20) メッシュ無線 AP は、有線 LAN 接続なしで無線によりルート AP へ接続し、クライアント収容（アクセスポイント機能）と中継（バックホール）を同時に提供できること。

(21) 中継(バックホール)は 2.4GHz 又は 5GHz で通信を確立可能なこと。

(22) SYSLOG に対応し、SYSLOG 収集機能と連携可能なこと。

(23) PoE/PoE+はそれぞれ IEEE802.3af、IEEE802.3at であり、最大給電電力 100W の規格である IEEE802.3bt や同種のメーカー独自規格は認めない。

(24) 周囲温度が 0～50℃の環境で動作可能である場合は加点する。ただし、結露しない状態に限る。【加点】

(25) LED を消灯又は LED を減光させる方法がある場合は加点する。【加点】

(26) 無線アクセスポイント台数が追加される場合を想定し、無線アクセスポイントの管理インターフェイスは DHCP による IP アドレスを取得等、DHCP を前提とした ZTP(Zero Touch Provisioning)に対応していること。な手順での追加を行える場合は加点する。【加点】

(27) 本調達の理解のもとに提案者が無線 LAN システム(アクセスポイント、コントローラ含む)について重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

(28) 教室環境での利用を前提とした検証の実施や信頼に足る有効な実績・事例が提示されている場合は加点する。【加点】

(29) 教室での利用において、授業利用以外の無線接続等に対して接続制限等の管理が必要である。これらについてシンプルで無駄のない方策が、具体的に提案されている場合は加点する。【加点】

(30) 大講堂等の複数台アクセスポイント設置の際に必要となる、ハンドオーバー機能等の具体的提案がされている場合は加点する。【加点】

2.1.2.8. 無線 LAN コントローラ

(1) 項「2.1.2.7 無線アクセスポイント」を管理する無線 LAN コントローラであること。

(2) ハードウェアアプライアンス、仮想アプライアンス(VA)、クラウドにより提供すること。
ただし、ハードウェアアプライアンス又は仮想アプライアンスで提供する場合、「各拠点及び機構本部」又は「データセンタ」に設置すること。
なお、各拠点及び機構本部に設置する場合、1 ラックユニットサイズ以下であること。

(3) 各拠点及び機構本部ごとに無線アクセスポイントを一元的に管理できること。

(4) 各拠点及び機構本部ごとに無線クライアントの同時接続数が 5,000 台以上可能なこと。

(5) 無線アクセスポイントからの通信を無線 LAN コントローラ経由で通信する場合、無線 LAN コントローラと接続するネットワーク機器に対して 10GbE SFP+のインターフェース 2 ポート以上で接続すること。

(6) クラウド版で提供する場合、SLA が 99.95%以上であること。

(7) 管理者権限を拠点ごとに読み取り専用に設定できること。
(8) クラウドにて無線 LAN コントローラを提供する事業者は、クラウドサービス提供事業者ではなく、ISO/IEC 27001 及び ISO/IEC 27017 を取得していること。
(9) 配下の無線アクセスポイントについて、負荷分散、チャネル干渉回避、MAC アドレスフィルタリング機能を有すること。
(10) タグ VLAN(IEEE802.1Q)機能を有すること。
(11) SSID 毎に無線クライアントに割り当てる VLAN を設定する機能を有すること
(12) SSID 毎に認証・暗号化方式を設定する可能なこと。
(13) MAC アドレス認証機能を有すること。
(14) 802.1X 認証と組み合わせてダイナミック VLAN に対応していること
(15) SSID 毎に 802.1X 認証用の RADIUS サーバを指定可能なこと。
(16) MAC アドレス認証は、無線 LAN コントローラ内認証及び RADIUS サーバ認証のいずれにも対応すること。
(17) RADIUS サーバによる属性に基づいてダイナミック VLAN が提供可能なこと。
(18) 無線アクセスポイントの死活管理が可能なこと。
(19) 無線アクセスポイントをブリッジモードとして動かす場合でも、無線アクセスポイントと無線 LAN コントローラ間による管理パケットに基づき無線アクセスポイントを死活監視ができること。
(20) 5GHz と 2.4GHz 間のバンドステアリング機能を有すること
(21) 無線クライアントの MAC アドレス、IP アドレス、接続先アクセスポイントを管理する機能を有すること。
(22) 無線 LAN コントローラから、無線アクセスポイントの設定内容を一元管理できること。
(23) 無線 LAN コントローラから、無線アクセスポイントのファームウェアバージョンアップ・バージョンダウン機能を有すること。
(24) 30 日分のイベントログを保存する機能を有すること。
(25) 無線アクセスポイント交換時、無線 LAN コントローラ上の管理情報（例：シリアル番号、MAC アドレス、ライセンス情報など）を更新することで、ライセンスを継承可能であること。なお、変更項目はメーカー・製品仕様によって異なることを許容する。
(26) 無線 LAN コントローラに対する無線アクセスポイントの登録は、製品仕様に応じて必要な管理情報（例：シリアル番号、MAC アドレス、ネットワークプロファイル、ロケーション、AP グループ設定等）を登録することで利用可能となること。なお、登録項目はメーカー・製品仕様によって異なることを許容する。
(27) 無線アクセスポイントの再起動が必要な設定変更やファームウェアバージョンアップ・バージョンダウンを実施する際、無線アクセスポイントの再起動日時を任意で指定可能なこと。
(28) 無線 LAN コントローラは日本語及び英語に対応した GUI である場合は加点する。【加点】
(29) 無線 LAN コントローラにアクセスする PC に専用のソフトウェアを導入することなく管理可能である場合は加点する。【加点】
(30) 無線 LAN コントローラ及び無線アクセスポイントに対して遠隔によりトラブルシュートをサポートできる場合は加点する。なお、管理機器からの任意の宛先への Ping による疎通確認する機能を有する場合は加点する。また、管理機器からの任意の宛先への Traceroute する機能を有する場合

は加点する。【加点】

(31) 無線クライアントの接続不良などの問題を無線 LAN コントローラからトラブルシュートできる場合は加点する。なお、Wi-Fi 接続を失敗したクライアントに関する情報を分析する機能を有している場合は加点する。【加点】

(32) 無線電波状況(チャネル・パワー等)、クライアントの位置・トポロジー等を示すグラフィカルなヒートマップを表示する機能を有する場合は加点する。【加点】

(33) 無線 LAN コントローラで管理可能な無線アクセスポイントが 1,000 以上である場合は加点する。【加点】

(34) SSID 毎に無線を利用する時間帯を制御できる場合は加点する。【加点】

(35) 無線アクセスポイントのファームウェアを一括及び個別のいずれでもバージョンアップ・バージョンダウンできる場合は加点する。【加点】

(36) フロアマップ等の画像データを取り込み、地図データ上に、無線アクセスポイントの位置情報を重ねて表示できる場合は加点する。【加点】

(37) 無線ネットワーク上を通過した通信先情報やアプリケーションの利用状況を一覧やグラフで表示できる場合は加点する。【加点】

(38) ネットワークトポロジーの可視化のために、物理マップ及び論理マップを描画できる場合は加点する。 【加点】

(39) 管理画面で無線電波の出力情報をグラフィカルに表示でき、画面上で計画、変更ができる場合は加点する。【加点】

(40) 無線 LAN の使用状況を分析し、アクセスポイントの機能や出力を調整することで消費電力を自動的に削減できる場合は加点する。【加点】

(41) 管理者画面に対する管理ユーザ別のログイン履歴、設定変更時間、設定変更内容を表示できる場合は加点する。【加点】

(42) ダッシュボード機能で過去のネットワークやシステムのサマリー情報が参照できる場合は加点する。【加点】

(43) ダッシュボード機能でユーザのアクセスしたアプリケーションの統計情報が参照でき、アプリケーションの統計情報は、ネットワークポリシー毎、ロケーション等参照する範囲を限定する仕組みがある場合は加点する。【加点】

(44) レポートは日時を指定して自動的に生成・電子メール送信するスケジューリング機能を有する場合は加点する。【加点】

(45) レポートはアプリケーションの統計情報、無線クライアントの統計情報、管理している無線アクセスポイントの統計情報、その他の統計上から表示させる項目を選択可能な場合は加点する。【加点】

(46) 現在及び過去 30 日の接続情報(ユーザ名、クライアント MAC アドレス、周波数、SSID、接続元無線 AP、通信規格)が視認できること。

(47) 現在及び過去 90 日の接続情報(ユーザ名、クライアント MAC アドレス、周波数、SSID、接続元無線 AP、通信規格)が視認できる場合、加点する。【加点】

(48) 無線クライアントの表示では、アクティブなクライアントと非アクティブなクライアントの表示の切り替えが可能で、非アクティブなクライアントに関しては過去の情報を表示可能な場合は加点する。【加点】

(49) 無線クライアントのローミング履歴を確認可能で、各ローミング時のアソシエーション、認証、DHCP 応答、ゲートウェイ応答、DNS 応答なのでローミングに要した時間が確認できる場合は加点する。【加点】

(50) 管理している無線アクセスポイントを指定して、指定した無線アクセスポイントから提案する RADIUS サーバへの認証の成否をテストするツールが準備されている場合は加点する。【加点】

(51) 無線アクセスポイントに対するリモートパケットキャプチャ機能を有する場合は加点する。【加点】

(52) アクセスポイントの過去 30 日間の稼働履歴を、一覧で且つグラフィカルに確認することができる場合は加点する。【加点】

(53) アクセスポイントの過去 90 日間の稼働履歴を、一覧で且つグラフィカルに確認することができる場合は加点する。【加点】

(54) クラウドサービスとして提供される場合、ISMAP クラウドサービスリストもしくは ISMAP-LIU に登録されている場合は加点する。【加点】

(55) 各高専の担当者による無線 LAN システムの運用について具体的に提案されている場合は加点する。【加点】

(56) 学校での利用を考慮した無線 LAN コントローラについて、有効な実績・事例が提示されている場合は加点する。【加点】

(57) 無線 LAN コントローラの障害への対応について具体的に提案がされている場合は加点する。【加点】

2.1.3. セキュリティ(UTM)機能要件

(1) 本節で記載するセキュリティ(UTM)機能は項「2.1.2.1 UTM ファイアウォール」に記載するファイアウォールへ搭載されることを想定する。ただし、Web フィルタリング、不正侵入検知機能・アプリケーション制御機能は複数製品を組み合わせて実現してもよい。

(2) 各拠点及び機構本部ごとに独立して利用可能なこと。

(3) 適用可能なポリシー数は 10,000 件以上であること。

(4) DNS トラフィックを監視し、悪意あるドメインへのアクセスをブロックする機能を有すること。

(5) DNS 応答の改ざん・なりすましや、通信の盗聴・改ざんに起因する不正通信を検知・遮断する機能を有すること。

(6) セキュリティ機能において、本調達の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.1.4. Web フィルタリング機能

(1) 基本的なコンテンツフィルタリング機能を持っていること。

(2) 高等専門学校での運用に不要とされるサイトを制御するために、危険なサイトや不適切なサイト等のカテゴリーデータベースが用意されているとともに、無条件で通過する除外リスト、ブロックするリストを設定できること。

(3) 指定された URL やパターンに一致する Web ページを許可あるいはブロック可能なこと。

(4) 本調達で導入される認証システムによるユーザ認証を用い、ユーザグループに応じたポリシー設定が可能であること。

(5) ブロックされた場合、指定する内容を利用者の端末画面に表示できること。

(6) IPv6 に対応していること。
(7) URL に関わらずドメイン名をブロックする機能を有する場合は加点する。【加点】

2.1.5. 不正侵入検知(IPS)機能

(1) 不正侵入検知(IPS)機能を有すること。
(2) アノマリ型及びシグネチャ型による IPS 機能を有すること。
(3) IPS スループットが 17Gbps 以上であること。
(4) シグネチャにより攻撃を検知した時、攻撃パケットをブロックする機能を有すること。
(5) IPv6 に対応していること。

2.1.6. アプリケーション制御機能

(1) 基本的なアプリケーション制御機能を有すること。
(2) 10,000 種類以上のアプリケーションの識別を行い、ブロック実行、ログ取得が可能であること。
(3) 本調達で導入される認証システムによるユーザ認証を用い、ユーザグループに応じたポリシー設定が可能であること。
(4) IPv6 に対応していること。

2.1.7. アンチマルウェア機能

(1) 基本的なネットワーク通過型のアンチマルウェア機能を有すること。
(2) マルウェアパターンファイルによる検査を行い、マルウェアの検知、ブロックを行う機能を有すること。
(3) マルウェア検査は、HTTP/HTTPS/SMTP/POP3/IMAP の各プロトコルに対応していること。
(4) アンチマルウェア性能(HTTP)は、3Gbps 以上であること。
(5) アンチマルウェア性能(HTTPS)は、1.4Gbps 以上であること。
(6) マルウェアパターンファイルの自動更新が可能であること。
(7) IPv6 に対応していること。

2.2. サーバ機器個別要件

本調達で導入する各サーバ機器の要件については、以下のとおりとする。

2.2.1. 仮想基盤用物理サーバ/仮想化ソフトウェア

(1) 物理サーバ 2 台以上の構成で実現すること。
(2) サーバ類機器は SINET データセンタに設置すること。
(3) データセンタに設置するサーバ機器類はファイアウォールでセキュリティ対策を講じること。ただし、データセンタとファイアウォールは少なくとも 100Gbps x 2 以上（SINET が当機構に提供する回線の種別により、40Gbps x 2 以上とする可能性がある）のインターフェースで接続すること。
(4) データセンタに設置するサーバ機器類を接続するために必要なネットワーク機器、ネットワーク性能を備えること。
(5) 19 インチラックに搭載可能であり、搭載に必要な金具等を用意すること。ねじ止めが不可能である場合は別途耐震対策を施すこと。
(6) 周囲温度が 10～35℃の環境で動作可能であること。
(7) Web ブラウザ経由での管理が必要な場合は、以下のブラウザからの利用に対応していること。
    ① Microsoft Edge
    ② Google Chrome ブラウザ
    ③ Mozilla Firefox
(8) システムボード上やサーバの前面にモジュールやコンポーネントの異常・故障を通知する LED があり、OS 停止中でも通知ができること又はリモートから Web UI 等を利用してモジュールやコンポーネントの異常・故障を確認できること。
(9) ハードウェアの異常発生時にはメール通知が可能であること。
(10) 10GbE SFP+インターフェースを 4 ポート以上有すること。
(11) 内蔵ストレージは RAID1/RAID1+0/RAID6 のいずれかによる冗長化が可能であること。
(12) 内蔵ストレージは活線交換(ホットスワップ)が可能であること。
(13) 搭載する CPU は、仮想化支援機能をサポートしていること。また、導入時に有効にしていること。
(14) 仮想基盤は冗長構成とし、物理サーバの 1 台又はハイパーコンバージドインフラストラクチャー(HCI)の 1 ノードに障害が発生した場合でも運用の継続が可能なこと。
(15) 本調達で必要となる仮想マシンを搭載し、物理サーバの 1 台又はハイパーコンバージドインフラストラクチャー(HCI)の 1 ノードに障害が発生した場合の利用率が 90%を超えないリソース設計を行うこと。
(16) 仮想マシンに対してのメモリリソースを静的に割り当てることが可能であること。
(17) 仮想マシンに対しての CPU リソースを静的に割り当てることが可能であること。
(18) シックプロビジョニング及びシンプロビジョニングによる仮想ハードディスクが作成可能であること。
(19) 仮想ネットワークを作成し、物理 LAN ポートを複数の仮想マシンに対して割り当てることが可能なこと。また IEEE802.1Q VLAN タギングに対応していること。
(20) 外部ストレージに対して仮想マシンのバックアップが可能であること。
(21) 仮想サーバに対してアクセス可能なユーザ（事業者が使用するアカウントを除き 56 ユーザ以上）

のアクセス権設定が可能であること。
(22) Web ブラウザ又はクライアントツールで GUI 管理が可能であること。
(23) NTP 又は SNTP による時刻の同期を行うこと。
(24) 停電からの復電時に自動起動する設定が可能であること。仮想マシンについては指定した依存関係に従い自動起動できること。
(25) ファームウェアや OS、アプリケーション、証明書などに脆弱性が確認されるなど更新が必要になった場合に、速やかに更新可能なこと。
(26) 仮想基盤サーバ及び項 2.2.3「ネットワーク基盤サービス個別要件」記載の各仮想ホストに対して項 2.2.5.「アンチマルウェア機能」記載の各アンチマルウェア対策を行うこと。アンチマルウェア対策を行うこと。
(27) ハードウェア管理用 LAN ポートを 1 つ以上有する場合は加点する。【加点】
(28) OS 停止時でも電源投入などのリモート管理が可能である場合は加点する。【加点】
(29) CPU/メモリ/内蔵ストレージ/電源等のハードウェアの状態が確認可能である場合は加点する。【加点】
(30) 故障したコンポーネントの種類がサーバ前面のランプの LED もしくはリモート管理機能で確認可能である場合は加点する。【加点】
(31) IPv4 及び IPv6 に対応できる場合は加点する。【加点】
(32) リモート管理で通信の暗号化が可能である場合は加点する。【加点】
(33) リモート管理でユーザ制限が可能である場合は加点する。【加点】
(34) SYSLOG、SNMP 等に対応し、システム監視機能と連携可能な場合は加点する。【加点】
(35) 本調達の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.2.2. ストレージサーバ

(1) 項 2.2.3. ならびに 2.2.4. に示す各機能のストレージ領域およびバックアップ領域として、ストレージサーバを設置すること。
(2) ストレージサーバはバックアップ領域を除き筐体 2 台以上で冗長構成を取ること。また、仮想化ソフトウェアにより仮想マシンの格納先ストレージを別のストレージへ移行する機能を有すること。
(3) サーバ類機器はデータセンタに設置すること。
(4) データセンタに設置するサーバ機器類はファイアウォールでセキュリティ対策を講じること。
(5) データセンタに設置するサーバ機器類を接続するために必要なネットワーク機器、ネットワーク性能を備えること。
(6) 19 インチラックに搭載可能であり、搭載に必要な金具等を用意すること。ねじ止めが不可能である場合は別途耐震対策を施すこと。
(7) 周囲温度が 10～35℃の環境で動作可能であること。
(8) Web ブラウザ経由での管理が必要な場合は、以下のブラウザからの利用に対応していること。
①Microsoft Edge
②Google Chrome ブラウザ
③Mozilla Firefox

(9) 仮想マシンのバックアップ、各種ログ、及び物理サーバのストレージに置かない場合の仮想マシンの仮想ディスクの収容を想定すること。
(10) ストレージは RAID6/RAID1+0/RAID5+0/RAID-DP のいずれかにより冗長化し、少なくとも 2 個の物理ディスクに障害が発生した場合も無停止で動作すること。
(11) 10GbE SFP+インターフェースを 8 ポート以上有すること。
(12) iSCSI/CIFS/NFS/SMB の各プロトコルによる通信が可能であること。
(13) NTP 又は SNTP による時刻の同期を行うこと。
(14) 保持するデータの暗号化機能を有すること。
(15) Web ブラウザを通じた GUI 管理が可能であること。また、通信の暗号化が設定可能であること。
(16) 本調達で提供する各種サーバのバックアップに必要な容量を確保すること。また必要な容量とその根拠を示すこと。
(17) 本調達の機器類から収集するログの保管に必要な容量を確保すること。次のログについて 366 日以上の保管を行うこと。必要な容量とその根拠を示すこと。
①DHCP ログ
②認証システム操作/認証ログ
③本調達で導入するネットワーク機器及びサーバ類の SYSLOG
(18) 本調達で構築する各種サーバの仮想ディスクを収容する場合は、仮想ディスクに必要な容量を確保すること。必要な容量とその根拠を示すこと。
(19) ファームウェアや OS、アプリケーション、証明書などに脆弱性が確認されるなど更新が必要になった場合に、速やかに更新可能なこと。
(20) ストレージサーバに対して項 2.2.5.「アンチマルウェア機能」記載の各アンチマルウェア対策を行うこと。
(21) 本調達の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.2.3. ネットワーク基盤サービス個別要件

2.2.3.1. 内部 DNS 機能

(1) DNS プロトコルによる各拠点及び機構本部ごとのコンテンツサーバ機能を有すること。
(2) 各拠点及び機構本部ごとにプライマリとセカンダリを 1 サーバずつ動作させること。
(3) A レコード及び AAAA レコードに対応すること。
(4) DNS の冗長化機能を有すること。
(5) プライマリ DNS とセカンダリ DNS 間でゾーン情報の転送が可能であること。
(6) DNS プロトコルによる各高専用内のホストに対する、インターネット上のサーバ類を含むドメイン名と IP アドレスの名前解決機能を提供するキャッシュサーバ機能を有すること。
(7) 名前解決に当たっては、順引き及び逆引きに対応していること。
(8) ゾーン転送や問い合わせクエリー等の各種ログが取得・保管できること。
(9) ログを本調達で導入する SYSLOG サーバに送信可能であること。
(10) 1 拠点あたり同時に 2,000 から 8,000 端末での利用を想定しており、これに対応可能な性能を有すること。

(11) レコード数、ゾーン数等にライセンス等の制限がある場合は、本システムの利用要件を考慮した上で十分なライセンス数を導入すること。
(12) CLI 又は Web UI による管理が行えること。
(13) 拠点担当者の選択により CLI 又は Web UI で設定が行える場合は加点する。【加点】
(14) 本調達の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.2.3.2. DHCP 機能

(1) 各拠点及び機構本部ごとに動作させること。また、各拠点及び機構本部ごとに冗長化すること。
(2) IPv4 及び IPv6 に対応すること。
(3) IPv6 はステートフル・アドレスの付与が可能であること。
(4) 複数の VLAN に対する IP アドレスの割り当てが可能で、VLAN 毎に割り当てる IP アドレスの範囲が指定できること。
(5) MAC アドレスを使用した固定 IP アドレスの払い出しが可能なこと。
(6) 既存の固定 IP 端末の情報も管理できること。また任意に情報追加ができること。
(7) 重複した IP アドレスを管理する機能を有すること。
(8) 管理者を複数設定することが可能であること。
(9) ログを本調達で導入する SYSLOG サーバに送信可能であること。
(10) 1 拠点あたり同時に 2,000 から 8,000 端末での利用を想定しており、これに対応可能な性能を有すること。
(11) 割当アドレス数、スコープ数、割当制御数等にライセンス等の制限がある場合は、本システムの利用要件を考慮した上で十分なライセンス数を導入すること。
(12) CLI 又は Web UI による管理が行えること。
(13) 拠点担当者の選択により CLI 又は Web UI で設定が行える場合は加点する。 【加点】
(14) DHCP リース情報は IP アドレス管理（IPAM）と統合され、IP アドレスの割当・開放・予約状況が一元的に可視化できるとともに、過去 30 日以上のリース履歴を IP アドレス、MAC アドレス、ホスト名等で検索できること。
(15) 本調達の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.2.3.3. NTP 機能

(1) 各拠点及び機構本部で共通の NTP サーバを 3 台以上備えること。ただし、利用者の端末に対する時刻配布は項「2.1.2.1 UTM ファイアウォール」で再頒布しても良い。
(2) 各拠点及び機構本部が有する各機器と時刻同期が可能であること。
(3) 本調達で導入する機器・ソフトウェアのうち、NTP による時刻同期機能を有するものについては、各機器・ソフトウェアに時刻同期の設定を行うこと。
(4) IPv4、IPv6 に対応できること。
(5) 外部 NTP サーバと時刻同期が可能であること。

2.2.3.4. メール配信システム(SMTP サーバ)機能

(1) 本件で導入する機器の異常等を通知するに当たって SMTP サーバが必要な場合は、各拠点及び機構本部ごとにメール配信システム(SMTP サーバ)機能を有すること。

(2) メール配信システムを用意する場合は、必要な権威 DNS サーバも併せて用意すること。なお、ドメインは機構本部が指定したものを使用すること。

(3) メール配信システムは送信元 IP アドレスが検証可能な SPF を権威 DNS サーバへレコード登録すること。

(4) メール配信システムは送信されるメールに対して電子署名（デジタル署名）を付与し、送信元の正当性と改ざん有無を検証可能となるよう DKIM を設定すること。

(5) メール配信システムは SPF 又は DKIM で検証失敗したメールの処理方法として reject を受信者側へポリシー通知可能となるよう DMARC を設定すること。

(6) 項「2.1.2. 各拠点及び機構本部機器要件」及び「2.2.4.1 各拠点及び機構本部用認証システム要件」を実装する機器について、

- 故障障害(死活監視)
- 発注者と合意した SNMP Trap

を高専機構が指定するドメインを用いてメール発報すること。

2.2.3.5. ログ収集機能

(1) 本調達で調達する各ネットワーク機器・サーバ機器から出力される syslog を収集する機能を有すること。保存するログの詳細については、機構と協議の上決定すること。

(2) ログの保存期間は、366 日以上とすること。なお、1 日あたりのデータ量はアーカイブ前段階で 30GB 程度を想定している。

(3) ログは直近 24 時間は生ログ(Raw Log)で保存し、日次あたりでアーカイブ化すること。

(4) ログファイルは機器及び日付が特定可能となるようファイル名を設定すること。

(5) SIEM(セキュリティ情報イベント管理)及び可視化の上、複数のログを用いて横断的に分析する機能がある場合は加点する。【加点】

2.2.4. ユーザ認証基盤サービス個別要件

2.2.4.1. 各拠点及び機構本部用認証システム要件(認証連携、LDAP 機能、RADIUS 機能、学認用 IdP 機能、Microsoft 365 連携)

(1) 単一又は複数の製品やサービスの組合せで、次のサービスを実現すること。なお、別途の契約を行うことが明示されている場合を除き、各サービス等の実装や利用に際し、ライセンス費用などの追加費用が発生しないこと。

(2) 各拠点及び機構本部ごとに独立して実装すること。

(3) り障時間が以下に記載する時間となるようバックアップ環境を構成すること。

平日(国民の祝日に関する法律第 3 条に規定する休日及び 12 月 29 日～1 月 3 日の年末年始を除く月曜日～金曜日。以下同じ。)の 9:00-17:00　…２時間以内

それ以外　…１４時間以内

なお、eduroam・学認 IdP については、バックアップの対象から除外するものとする。

(4) NTP 又は SNTP による時刻の同期を行うこと。
(5) LDAPv3 プロトコルに対応していること。
(6) LDAPoverSSL/TLS に対応し、NII の UPKI を含む任意の認証局の証明書を使用できること。
(7) POSIX 認証に対応していること。
(8) 任意の LDAP スキーマの拡張が可能であること。
(9) RADIUS の認証及びアカウンティングのプロトコルに対応していること。
(10) RADIUS 認証においてユーザ認証及び端末の MAC アドレスによる認証が可能であること。
(11) IEEE802.1X のユーザ名/パスワード及び EAP-TLS による認証に対応していること。
(12) RADIUS プロキシに対応し、NII の eduroam JP に参加するための設定がなされること。
(13) 本調達で導入するネットワーク機器と連携し、IEEE802.1X によるユーザの認証又は MAC アドレス認証を行うこと。
(14) Shibboleth IdP の機能を有し、NII の学認に参加するための設定がなされること。
(15) Shibboleth IdP の認証では、パスワード認証に加えて多要素/多段階の認証機能を有すること。
(16) 学外からの認証時のみ多要素/多段階の認証機能を要求する設定ができる機能がある場合は加点する。【加点】
(17) 多要素/多段階の認証機能を必須とするユーザと任意のユーザを設定できる機能がある場合は加点する。【加点】
(18) 高専機構で利用する Microsoft 365 の利用者認証を行う Entra ID(旧 Azure AD)と連携するために、各拠点及び機構本部用認証システムから Entra ID に、アカウント情報の同期が可能であること。同期に当たって単一障害点を排除する構成になっている場合は加点する。【加点】
(19) アカウント情報同期の自動化が可能であること。
(20) アカウント情報同期の通信は暗号化すること。
(21) Entra ID 連携用 AD を介した連携の場合、Microsoft 365 管理センターとのアカウント情報同期を即時に反映される場合は加点する。【加点】
(22) 各拠点及び機構本部用認証システムと Microsoft 365 管理センターが直接連携し、アカウントの情報同期を即時に反映される場合は加点する。【加点】
(23) 拠点ごとに 2,000 名以上のアカウント情報を管理できること。
(24) 拠点ごとに 10,000 台以上の端末の MAC アドレスを管理できること。
(25) 拠点ごとに 4,000 台以上の端末の同時利用が可能であること。
(26) 高度化再編校(4 高専 8 拠点)においては、4,000 名以上のアカウント情報を管理する機能を有すること。
(27) CSV ファイル及び LDIF ファイルによる一括登録/更新/削除などのアカウント情報の管理が可能であること。
(28) ユーザのグループ化が可能であること。
(29) 複数のアカウント管理者を設定し、指定した管理権限を委譲できること。
(30) 利用者自身がウェブブラウザからパスワードの変更が可能であること。
(31) 利用者自身が自身のパスワードをリセットできる機能を有する場合は加点する。【加点】
(32) 管理者によるアカウント管理・設定に関するすべての操作が Web ブラウザから可能なこと。
(33) 国家サイバー統括室(NCO)のインターネットの安全・安心ハンドブック VER5.10 で推奨される複雑

性などのパスワードの強度の設定が可能で、脆弱なパスワードを排除できること。

(34) 他の Active Directory 及び LDAP サーバとアカウント情報を連携する機能を有すること。ただし、本調達に含まれる認証システムから他の Active Directory や LDAP サーバへの一方向の連携で構わない。

(35) 各高専用の認証システムは、高専ごとに別途の契約を行うことより、Google Workspace にアカウント情報を同期できる場合は加点する。【加点】

(36) 拠点用認証システムでのアカウント操作は、他の認証システム(高専共通認証システム、高度化再編校の他方の拠点用認証システム、Entra ID、Google Workspace)へのアカウント操作は原則として即時に同期されること。もしネットワークの障害等により同期に失敗した場合は、自動で再同期する機能を有すること。

(37) サーバ証明書を使用する場合は、NII の UPKI 証明書を使用できること。なお、証明書の発行手続きは各拠点及び機構本部側で行うものとする。ただし、証明書は ACME(自動証明書管理環境)への対応又は同等の環境を整えること。

(38) 操作履歴・認証に関するログ及び eduroamJP サービス技術基準・運用基準で示すログを 1 拠点あたり 3TB を上限として取得できること。

(39) 既存の LDAP サーバ(AXIOLE-i)からパスワード情報を除くアカウント情報を引き継ぎ可能であること。

(40) 各高専用の認証システムから高専共通認証システムに、指定したユーザのアカウント情報の同期が可能であること。

(41) 各高専用の認証システムから高専共通認証システムへのアカウント情報のための通信は暗号化されること。

(42) 各高専用の認証システムから高専共通認証システムへ同期するスキーマはそれぞれの認証システムで管理できること。

(43) 高度化再編校では、いずれの拠点用認証システムからもアカウント情報の管理が可能であること。

(44) 高度化再編校内の拠点用認証システムでは、片方の拠点用認証システムからアカウント操作が他方の拠点用認証システムに反映されること。

(45) 高度化再編校内の拠点用認証システムでは、2 拠点分のアカウント数(4,000 名以上)を統合して利用できること。

(46) 高度化再編校内の各高専用の認証システム間の通信は暗号化されること。

(47) 本調達の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.2.4.2. 高専共通システム用認証機能

(1) 高専機構全体のアカウント情報を管理し、高専共通システムの認証サーバとして利用できるサーバを項「2.2.3.ネットワーク基盤サービス」の仮想基盤上に構成すること。また、当機構が指定する業務システム(給与システム、旅費システム等) と L2VPN 経由で認証プロトコル(LDAP 又は LDAPS 想定)で接続すること。なお、L2VPN は項 2.1.1.1. に示す DC ファイアウォール機器と当機構の指定するネットワーク機器と接続することを想定すること。

(2) 高専機構全体の教職員のアカウント情報を管理し、高専共通システムの認証システムとして利用可

能とすること。
(3) NTP 又は SNTP による時刻の同期を行うこと。
(4) LDAPv3 プロトコルに対応していること。
(5) LDAPoverSSL/TLS に対応し、NII の UPKI 証明書はじめ、任意の証明書を使用できること。
(6) POSIX 認証に対応していること。
(7) 任意の LDAP スキーマの拡張が可能であること。
(8) 既存の LDAP サーバからアカウント情報を引き継ぎ可能であること。
(9) 20,000 名以上のアカウント情報を管理する機能を有すること。
(10) 各高専の認証システムから高専共通認証システムに、指定したユーザのアカウント情報の同期が可能であること。
(11) 各高専用の認証システムから高専共通認証システムへ同期するスキーマはそれぞれの認証システムで管理できること。
(12) 各高専用の認証システムから高専共通認証システムへのアカウント情報のための通信は暗号化されること。
(13) 本要求の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.2.5. アンチマルウェア機能

(1) 本調達で導入する汎用 OS(Linux 又は Windows)が稼働するサーバには、物理サーバか仮想サーバかによらずマルウェア対策ソフトウェアを導入すること。なお、仮想基盤のハイパーバイザ及びアプライアンス機器は保護対象外とする。
(2) アンチマルウェア機能をインストールした各サーバが、メーカーの作成した、マルウェア定義ファイルをインターネット経由で取得できること。
(3) 定義ファイルの自動更新が可能であること。
(4) サーバ上の入力ファイル、出力ファイルを監視し、マルウェアファイルの侵入をリアルタイムで検出する機能を有すること。
(5) 手動検索及びスケジュール管理による定期的な検索機能を有すること。
(6) マルウェア検出時の動作として、手動処理・ファイル削除・隔離・マルウェア駆除の処理が可能であること。
(7) 重要と識別されるイベントが発生した場合に、拠点担当者へ電子メールによる通知を行えること。
(8) メール送信に用いるメールサーバは、拠点担当者と協議の上、以下の対応を行うこと。
① 各高専既設の業務用メールサーバの利用
② 上記が何らかの理由で利用できない場合、高専機構で利用する Microsoft 365 Exchange を利用
(9) マルウェア検知等のログを保存可能なこと。
(10) 管理ツール又は Web ブラウザを通じた GUI により各種監視の設定が実行可能である場合は加点する。【加点】
(11) 本要求の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.2.6. バックアップ・リストア機能

(1) 項「2.2.1 仮想基盤用物理サーバ／仮想化ソフトウェア」に定める仮想化ソフトウェア（ハイパーバイザ）については、仮想基盤用物理サーバごとにバックアップを取得できること。また、仮想化ソフトウェアを Windows、Linux 等の基本 OS 上で稼働させる構成とする場合は、当該基本 OS についても、仮想基盤用物理サーバごとにバックアップを取得できること。

(2) 項「2.2.3 ネットワーク基盤サービス個別要件」に定める項「2.2.3.1 内部DNS機能」から項「2.2.3.5 ログ収集機能」、項「2.2.4.ユーザ認証基盤サービス個別要件」及び項「2.2.5.アンチマルウェア機能」までの各機能について、当該機能を提供する仮想マシン単位でバックアップを取得すること。なお、複数の機能を 1 つの仮想マシンで提供する構成とする場合は、当該仮想マシン単位でバックアップを取得することで差し支えない。ただし、バックアップ・リストア機能を実現するためにバックアップ機能用の仮想マシンを構成する場合、当該仮想マシンにおけるバックアップデータ格納領域については、バックアップ対象外として差し支えない。

(3) 項「2.1 ネットワーク機器個別要件」及び項「2.2.7 ファイアウォールログ収集サーバ」に定める機器等について、Config、ACL、システム設定等の設定情報を、設定変更の都度又は少なくとも 3 か月に 1 回以上バックアップ可能な領域を用意すること。

(4) 本調達で導入するサーバ、ネットワーク機器等のバックアップを、ストレージにバックアップする機能を有すること。

(5) 障害が発生し交換した機器についても、データ及びコンフィグファイルを容易にリストア可能であること。

(6) 機構が指定した時間帯に自動的に実行動作をスケジューリングすることで、自動的にコンフィグファイル及びデータをバックアップ・リストア可能であること。

(7) バックアップ・リストア機能について、本要求の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.2.7. ファイアウォールログ収集サーバ

(1) 項「2.1.1.1 DC ファイアウォール機器要件」及び項「2.1.3 セキュリティ(UTM)機能要件」で排出する通信ログ及び IPS ログを収集すること。

(2) 各高専のログデータ(全拠点合計、無圧縮で平均 5,700GB/日、gzip 圧縮時平均 57GB/日)を収集すること。なお、クラウドサービスを利用する場合は、過去 1 年分以上のログを収集すること。

(3) ログ収集能力は各拠点および機構本部ごとに 10,000 ログ/秒以上であること。なお、全拠点合計で 200,000 ログ/秒以上であること。なお、クラウドサービスを利用する場合でも、この要件を満たすこと。

(4) 最新の脅威情報と連携して、取得済みログに対する再検査が可能である場合は加点する。【加点】

(5) タンパープロテクション(不正改ざん防止機能)を有し、外部、内部からの改ざん防止機能を有する場合は加点する。【加点】

(6) 本要求の理解のもとに提案者が重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.3. 信頼性要件

2.3.1. 可用性

(1) 耐障害性や可用性を重視して信頼性の高い機器構成とすること。

(2) すでに出荷・稼働実績を有する「標準的な既製品」かつ、未使用であること。なお、「標準的な既製品」とは、製造元が一般市場において販売するために、主要な製品系列の一環として製造する物品を指す。

(3) 冗長化する機器は切り替え、切り戻しのロジックを明確にし、片方の機器に障害が発生しても他の機器で通常通り業務が継続できること。

(4) 各種保存データや設定ファイル等は情報が正確に記録又は保存されること。

(5) 24 時間 365 日の稼働に耐えうる製品であること。

(6) SINET6 アクセス回線の断線や設備故障により、図 4 に示すデータセンタと各拠点及び機構本部間の通信障害発生時においても、既にネットワークへ接続済みの端末が IP アドレスを維持し、通信が継続できるよう構成すること。なお、SINET データセンタ内の SINET ノードと DC ファイアウォール等を接続する構内ケーブルも同様とする。そのため、DHCP サーバのリース時間は 8 時間以上に設定すること。また、上記障害について 24 時間～1 週間未満の期間が想定される場合は、48 時間以内に各拠点及び機構本部内の通信を復旧させること。なお、上記障害について 1 週間以上の期間が想定される場合は、対応について高専機構と別途協議すること。

(7) 本システムで機器障害影響について考慮・提案している場合は加点する。【加点】

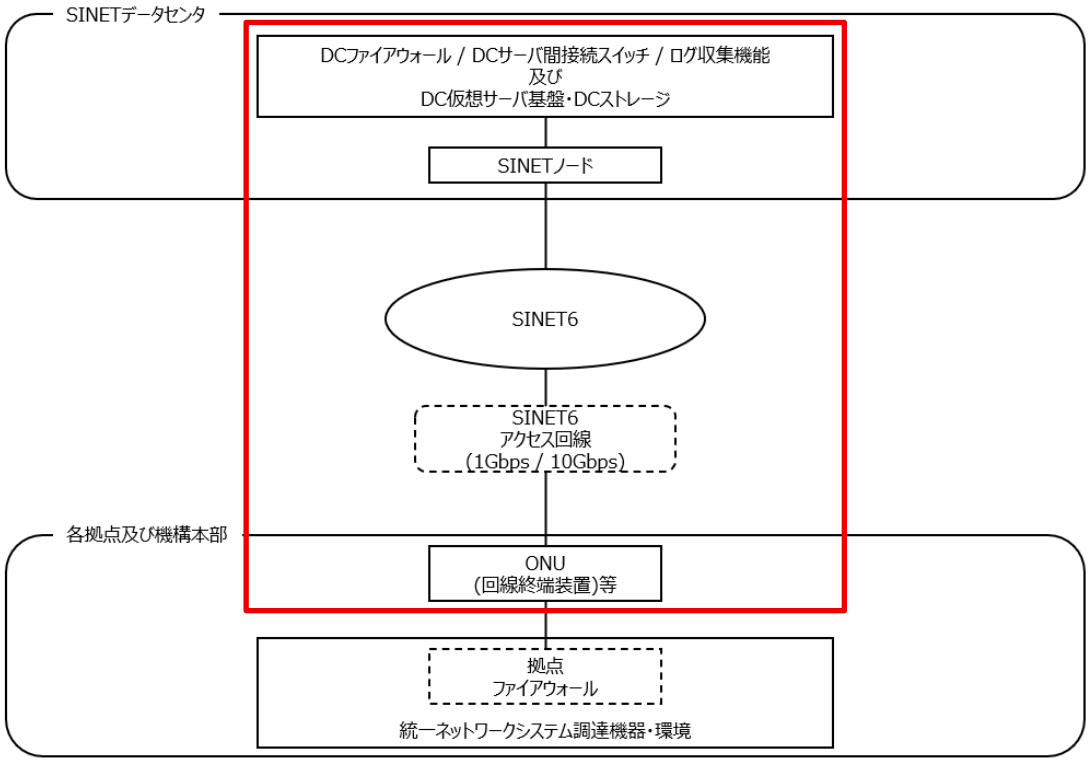

図 4. 想定する通信障害の範囲

2.3.2. 機密性

項「5.5. 情報セキュリティ要件」を参照のこと。

2.3.3. 拡張性

(1) 導入される無線 LAN コントローラについては、無線アクセスポイントの追加導入ができること。

(2) 応札時に、無線アクセスポイントの台数の許容値を示すこと。追加可能な無線アクセスポイントの数量や利用形態、必要なライセンス等について制約がある場合は応札時に明示すること。

(3) 広い範囲や長期間・長時間のサービス停止を要することなく、モジュール化など影響を局所化する方策を採用する場合は加点する。【加点】

(4) 以下の場合は加点する。【加点】

・無線 LAN アクセスポイントの追加方策について具体的な提案があること。

・提案する構成において追加可能なアクセスポイントの数量・利用形態等について制約が少ないこと。

・無線 LAN アクセスポイント追加時の役務についても考慮がされていること。

・有線 LAN 拡張性への対応方針が記載されていること。（高速化やスイッチ増への対応　等）

2.3.4. 上位互換性

OS を含む各種ソフトウェア・ファームウェアのアップデートに関しては、本調達の契約期間を通して、原則として構成や利用方法に大きな変更を行わずに実施可能であること。

2.3.5. システム中立性・事業継続性

特定の事業者・製品に依存することなく次期システムへの更改が可能であること。併せて各拠点及び機構本部で運用・保守を継続することが可能なシステム構成であること。

2.4.　各拠点及び機構本部用認証システムと外延システム連携について

図 5 に、本調達における認証連携の概要について示す。

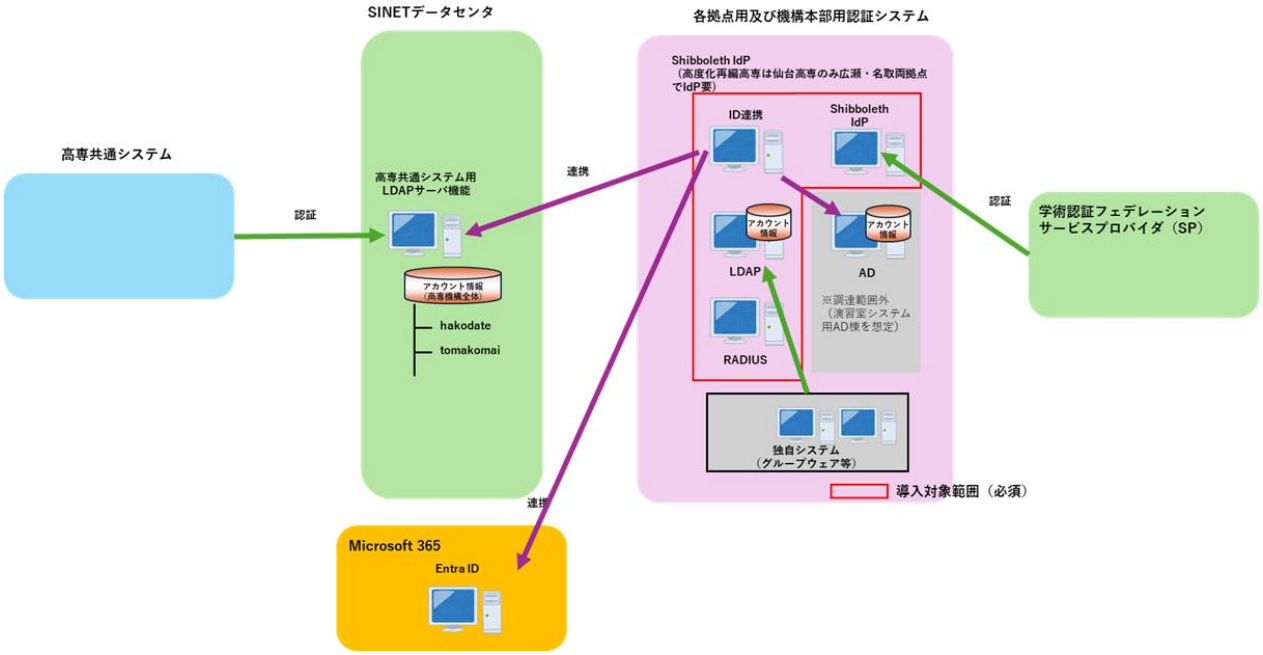

図 5. 認証連携の全体システムイメージ

2.4.1. 各拠点及び機構本部用認証システム要件

各拠点及び機構本部に設置するユーザ認証基盤システムに必要な要件を図 6 に記載する。なお、サーバ(LDAP サーバ・RADIUS サーバ・IdP サーバ等)の構成の設計方法は特に指定するものでないため、サーバ単位での要件記載ではなく必要な利用要件の記載とする。

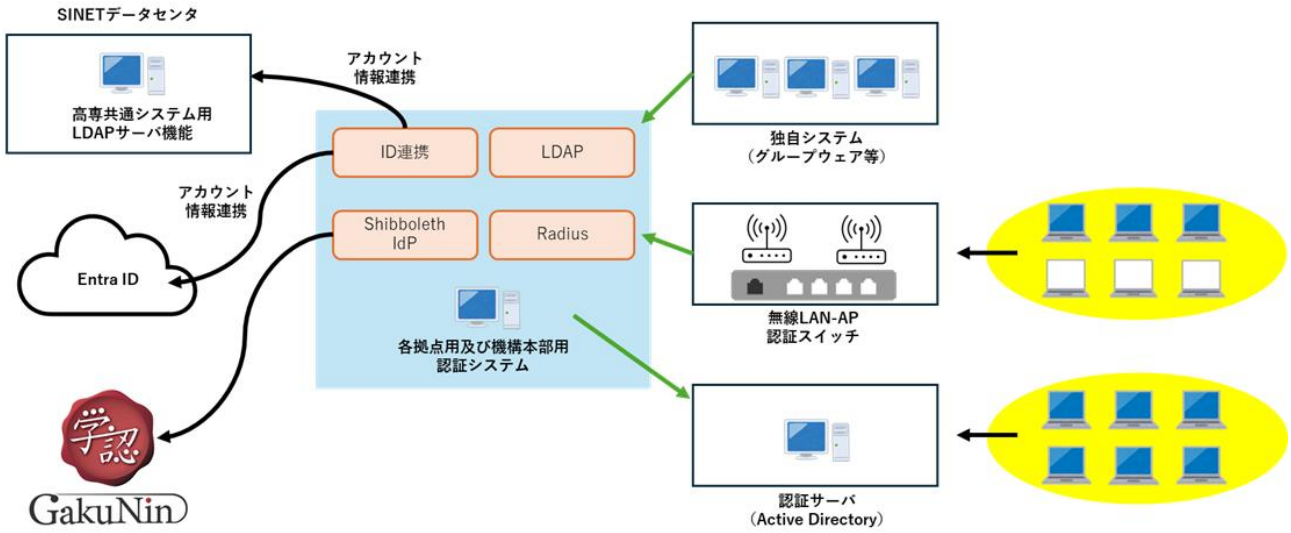

図 6. 認証サーバ構成(各拠点及び機構本部用)共通要件

2.4.1.1. Microsoft 365 連携要件

Microsoft 365 連携の例を図 7 に示す。

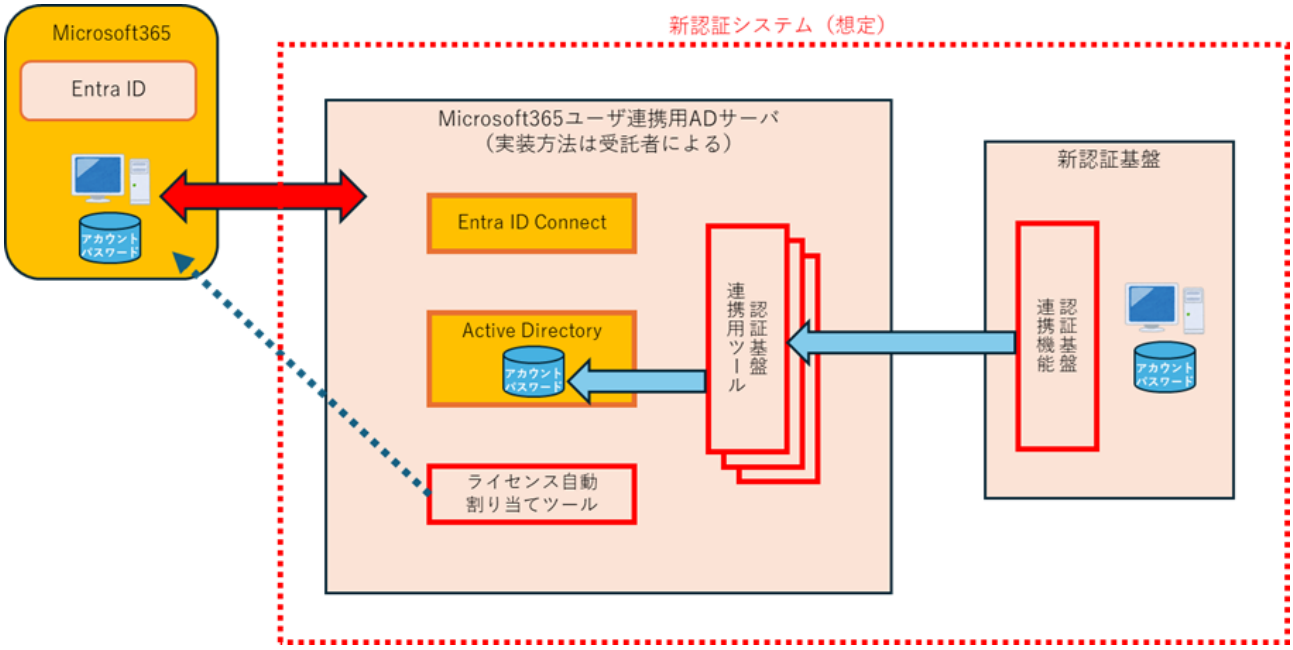

図 7 Microsoft 365 連携

Microsoft 365 のアカウント名については、各拠点及び機構本部のアカウント名と同一だが、ドメイン名は基本違う。

（例）：各拠点及び機構本部のアカウントと Microsoft 365 アカウントの UPN が異なるパターン

高専側アカウント	hoge@aaa-nct.ac.jp
Microsoft 365 アカウント	hoge@aaa.kosen-ac.jp

また、各拠点及び機構本部のアカウントと Microsoft 365 アカウントが同一の拠点も複数ある。

（例）：各拠点及び機構本部のアカウントと Microsoft 365 アカウントの UPN が同一のパターン

高専側アカウント	hoge@bbb-nct.ac.jp
Microsoft 365 アカウント	hoge@bbb-nct.ac.jp

なお、Microsoft 365 アカウントは各拠点及び機構本部のアカウントと同一か否かによらず、多要素認証を実施している。

2.4.1.2.　認証サーバ間の同期要件

高専共通システム用認証サーバとの同期を図 8 に示す。

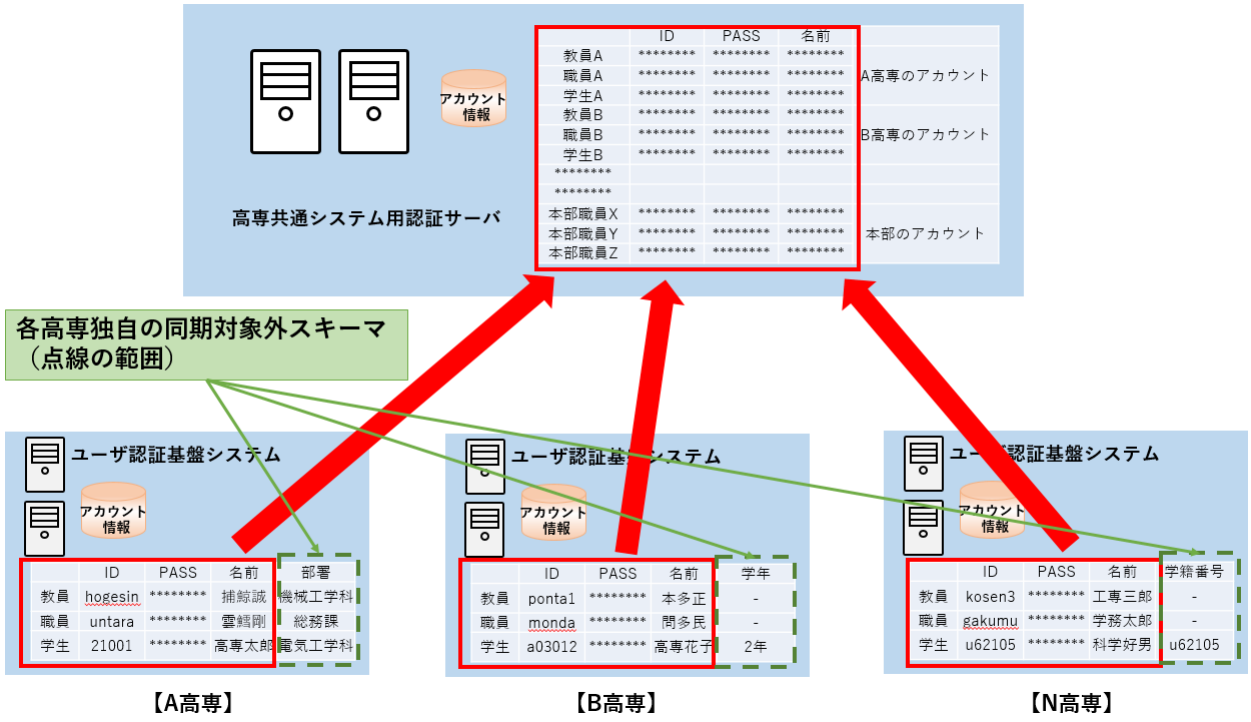

図 8. 認証サーバ間の同期

また併せて、高度化再編校の同期についての補足図を図 9 に示す。

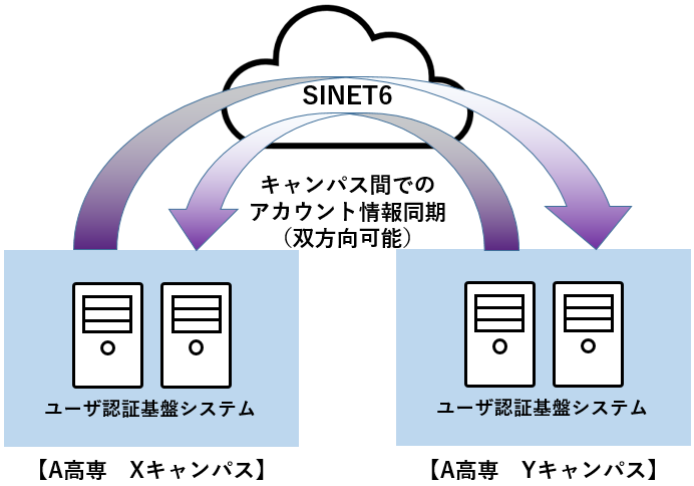

図 9. 高度化再編校における複数キャンパス間の同期

2.4.2. eduroam 構築要件

各拠点及び機構本部は eduroam JP に参加している。他の高専・大学の教職員や学生がネットワーク

を利用できるように、各拠点及び機構本部に設置するユーザ認証基盤システム、ファイアウォール、スイッチ、無線アクセスポイントについて eduroam 設定を行うこと。

ただし、eduroam JP の参加申請は各拠点及び機構本部の担当者が行うものとし、eduroam 事務局との調整を含むその他の要件については、高専機構と別途協議を行うこととする。

2.4.3. IPsec VPN 構築要件

各拠点及び機構本部のリモートメンテナンス用に、項「2.1.2.1. UTM ファイアウォール」について IPsec VPN による接続が可能となるよう設定を行うこと。また、各拠点及び機構本部の管理者によりトンネル・インターフェースの有効・無効を切り替えられることとし、無効とされた場合は IPsec VPN のリクエストに対して応答しないよう設定を行うこと。

2.4.4. 外延システム要件

各拠点及び機構本部ごとに現行ネットワークシステムと連携・接続して運用されているシステム（以下「外延システム」という。）について、高専統一ネットワークシステムへの移行を行うこと。

2.5. 設計作業について

2.5.1. 全般

(1) 受注者は高専統一ネットワークシステム整備にあたり、現状調査、基本設計、詳細設計を行うこと。設計方針並びに内容の説明は図表等を用いてわかりやすく行い、高専機構の承認を得ること。

(2) 本調達の特性を考慮したうえで、設計の要点と対応について機構が有用と認める提案がある場合は加点する。【加点】

2.5.2. 現状調査

(1) 高専統一ネットワークシステムの設計に先立ち、各拠点及び機構本部における現行ネットワークシステムの設計書、運用に係るドキュメント等を確認し、現状について精査すること。

(2) 受注者は現地調査のスケジュールを作成し、各拠点及び機構本部との調整を受注者が行うこと。その際各拠点及び機構本部の日程都合を尊重すること。

(3) 現地調査の前に必要な情報の収集のために、受注者の責で調査票を作成し高専機構の許可を得ること。各拠点及び機構本部への調査票配布・回収は高専機構を通して行う。

(4) 現地調査は、各拠点及び機構本部のうち、全拠点の調査を基本とする。調査不要とする拠点がある場合は、理由や対応を明示のうえ、高専機構の許可を得ること。

(5) 現地調査において、現行ネットワークシステムを構成するネットワーク機器、サーバ機器等の設定値についてドキュメントとの差分がある可能性があるため、最新状況を把握すること。

(6) 現状調査以降も状況の変化が想定されるため、適宜、最新状況の確認を行うこと。確認に当たって機構が有用と認める手法があれば提案を行い、高専機構と協議のうえ対応すること。

(7) 各拠点及び機構本部への現状調査の結果、別紙 1「ネットワーク機器一覧」に記載される各拠点及び機構本部ごとの必要数と実際の必要数が異なる場合は、本調達での全調達数量を超えない範囲で、導入数の調整を行うこと。

(8) 調整の際は、受注者の責で別紙 1「ネットワーク機器一覧」を更新し本部の承認を得ること。作業完了確認の際は更新後の別紙 1「ネットワーク機器一覧」を使用する。

(9) 本調達の特性を考慮した機構が有用と認める現状調査の手法について提案がある場合は加点する。【加点】

2.5.3. 基本設計

(1) 受注者は、本仕様書に示す要件及び現状調査の結果を基に基本設計書を作成すること。

(2) 基本設計書には物理設計、論理設計、実現方式等、図表を用いてわかりやすく記載することとし、目次内容については高専機構の承認を得ること。

(3) ネットワークに関しては、必要に応じて各拠点及び機構本部担当者と設計内容に関して協議を行い設計すること。記載内容は受注者の提案を元に高専機構と協議の上決定するものとするが、少なくとも以下について記載があること。

- 全体方式設計
- 全体物理構成
- 全体論理構成
- ネットワーク論理構成図

・サーバ論理構成図
・命名規則
・各システム方式設計
・可用性設計・冗長化設計
・インフラ運用設計
・セキュリティ設計
・ファシリティポリシー設計(電源配線ポリシー、ケーブル配線ポリシー、ラック搭載ポリシー等)

(4) 本調達の特性を考慮したうえで、基本設計の要点と対応について機構が有用と認める提案がある場合は加点する。【加点】

2.5.4. 詳細設計

(1) 受注者は本仕様書に示す要件及び基本設計書で定義した内容を詳細化し、具体的なパラメータ等を定義した詳細設計書を作成すること。詳細設計書には、作業を実施するために必要となる環境情報等を記載することを想定しており、下記に示す項目を含むこと。なお、詳細については高専機構と協議の上決定するものとする。

・IP アドレス
・VLAN
・アクセスコントロール設定
・ネットワーク接続認証方法(認証先は本調達で導入する認証システムとなる)
・UTM のセキュリティ設定
・DNS サーバ、DHCP サーバについては、現行から移行する既存システムの設定
・監視サーバについては、基本的な監視として本調達で導入する機器の IP アドレスの設定
・インフラ詳細設計(IP アドレス一覧、機器諸元、ポートアサイン表等)
・ネットワーク機器パラメータ設計
・サーバ機器パラメータ設計(仮想サーバ設計含む)
・サーバ機能設計(DHCP スコープ設計、NTP 設計、DNS 設計、監視設計、機器設定管理設計、ログ設計等の設定内容)
・ユーザ認証機能設計
・ファシリティ設計(ラック構成図、電源接続図、結線図等)
・その他拠点配置に依存する項目
・その他必要と考えられる項目

(2) 詳細設計書の作成に当たっては、高専機構が提供する、ネットワークにおける環境設定に係る基本的な情報を記載したシートである「パラメータシート」の内容を踏まえること。「パラメータシート」は各拠点及び機構本部ごとに作成しており、その内容については、契約後開示する。

(3) 詳細設計書については、該当する各拠点及び機構本部における作業日の 75 日前には、高専機構担当者ならびに各拠点及び機構本部担当者の承認を受けること。なお、当該承認に係る（案）のやり取りについては、電子ファイルベースでのやり取りを基本とするが、その内容に応じ、適宜必要なメンバーでの打ち合わせを実施すること。

(4) 本調達の特性を考慮したうえで、詳細設計の要点と対応について機構が有用と認める提案がある場合は加点する。【加点】

2.6. 構築作業について

2.6.1. 事前構築

(1) 事前構築では、単体テスト・結合テストを実施し、機能の正常性を担保すること。単体テスト・結合テストの内容については、あらかじめ高専機構担当者によるレビューを受けること。
(2) 本調達で納入する機器の設定やソフトウェアのインストール等については、詳細設計書に基づいて実施すること。
(3) 受注者は外部の人及び部外者が入れないセキュリティが確保された作業場所で事前構築を行い、本番環境搬入後に実施する設定作業等は最小限のものとすること。
(4) 事前構築で必要となる検証機器や作業場所等は、受注者側の責任で準備することとし、運搬経費、役務作業の場所に係る経費等については、全て受注者の負担とすること。
(5) 本調達の特性を考慮したうえで、事前構築の要点と対応について機構が有用と認める提案がある場合は加点する。【加点】

2.6.2. 本番環境構築

(1) 本調達の特性を考慮したうえで、本番環境構築の要点と対応について機構が有用と認める提案がある場合は加点する。【加点】
(2) 各拠点への展開の方針や進め方が有用で妥当と考えられる場合は加点する。【加点】

2.6.2.1. 全般

(1) 事前構築において正常稼働が確認された機器は、各拠点及び機構本部担当者と調整の上、搬入し構築を行うこと。
(2) 本番環境構築作業においては、作業中の拠点以外の現行ネットワークシステムの運用に影響を与えないこと。
(3) 本番環境へ導入するすべての機器に対して、各種設計書に従い設定作業を行うこと。
(4) 本調達範囲内において、設定作業後は、連携して機能するシステム単位においてテストを行い、正常性稼働を担保すること。また正常性稼働が担保できる根拠を各拠点及び機構本部担当者に提出し承認を得ること。
(5) 本調達の本番環境構築は、拠点が全国に及び状況も様々である。日程調整の簡易さや効率性、現地作業の期間短縮など、受注者の考える要点とその対応について提案すること。

2.6.2.2. 搬入設置

(1) 搬入については、トラックの搬入等、各拠点及び機構本部に申請・許可が必要なことについては、あらかじめ各拠点及び機構本部に申請し許可を得ること。
(2) 各拠点及び機構本部担当者の指示する場所に搬入・設置を行い、養生品、梱包材等は撤去すること。
(3) 受注者が個別に各拠点及び機構本部担当者に連絡し、搬出入のルート、養生は、各拠点及び機構本部担当者の指示に従うこと。また、搬入に当たって必要な手続及び打合せについては、受注者が遅

滞なく行うこと。手続き及び打ち合わせはリモートにて行うこと。

(4) 施設内で作業を行う際は、社員証ならびに各拠点及び機構本部担当者が指定する名札等を常に目に見えるよう携行すること。

(5) 他業者に影響が出ないように、作業日程について事前に各拠点及び機構本部担当者と協議すること。

(6) 作業に関連して起きた一切の事故・障害及び諸設備等の破損等に関しては、受注者の負担と責任において修理、修復又は交換を行い現状復旧すること。

(7) 移行作業において他システム等への影響が想定される場合は、作業内容、影響範囲、影響時間等明確にし、事前に各拠点及び機構本部担当者に対して承認を得ること。

2.6.2.3. 本番切替

(1) ネットワークは導入時、受入テスト期間に入る時点で切り戻しが不可能となる。そのため受入テストを開始することを以て本番切替と定義する。なお、DNS・DHCP などのネットワーク基盤サービスについても同様とする。

(2) 移行の詳細については項「2.8 移行作業について」を参照のこと。

(3) 受注者は、本番切替判定基準を作成すること。本番切替判定基準として、少なくとも以下(1)～(3)を含むこと。

① 障害対策が実施されていること。また想定される障害について、それぞれの影響範囲が明確になっていること。

② システムの運用や操作の手順が明確になっていること。

③ トラブル発生時の体制、方針、手続が明確にされていること。

(4) 本番切替判定会議を開催すること。参加者は受注者と拠点担当者とする。

(5) 拠点担当者が切替可否を判断する為の判断材料を提供すること。

(6) 事前のテストが完了し、すべて合格していること。

2.6.2.4. 認証切替

認証の本番切替は認証主体により下記 4 種が想定される。

・ネットワーク導入時のネットワーク接続認証の切替
※ネットワーク切替と同様に受入テスト開始を本番切替と考える。

・各拠点及び機構本部担当者が行う学認の認証切替
※受注者の範囲外のため本節の対象外とする。

・高専機構が行う想定の高専共通システム認証切替
※高専機構が主体となり実施を行うため本節の対象外とする。

・受注者及び各拠点及び機構本部が行う想定の Microsoft 365 認証連携切替(受注者の採用する実現方式により本作業が不要の可能性もある。)
※当連携切替作業を本番切替とする。

2.6.2.5. 導入支援

(1) 本調達機器以外のシステム等との接続において不具合が発生した場合は、原因の切り分けを行い、本調達の機器に起因する問題については速やかに対処すること。また、本調達機器以外のシステム

等に起因する場合は、その各拠点及び機構本部担当者に積極的な技術支援及びアドバイスを行うこと。

(2) 本調達機器以外のシステム等における設定作業等は、各拠点及び機構本部の担当者又はシステム等納入業者・保守業者が行うが、受注者は適宜連携・情報共有を行うこと。

(3) 各拠点及び機構本部の既存システム等との接続を円滑に行うため、各拠点及び機構本部担当者及び既存機器提供事業者と連携し、支障なく稼働できるよう導入構築を行うこと。

(4) 以下の作業内容については、各拠点及び機構本部担当者及び既存機器提供事業者が行うが、不具合等が発生した場合は、各拠点及び機構本部担当者に積極的な技術支援及びアドバイスを行うこと。

2.7. 接続作業について

本調達においては既設の配線を利用することを前提とする。以下に、本調達の範囲について記載する。

2.7.1. 設置場所

(1) ラック・設置場所については、各拠点及び機構本部が、納入される製品に適合するよう用意・準備する。

(2) サーバ室の空調は各拠点及び機構本部のサーバ室へ設置済のものを用いる。

(3) 受注者の現地調査の結果、不足や問題が懸念される場合は、各拠点及び機構本部担当者へ報告を行い、各拠点及び機構本部の責任において対応を行うものとする。

(4) 下記の記載がある場合は加点する。【加点】

・本調達の特性を考慮した、接続作業の要点と対策について記載があること。

・事前に行われている、ケーブル配線工事への対応についての記載があること。

2.7.2. 現地調査・打合せ

(1) 各拠点及び機構本部によって、機器の設置場所・設置形態は様々である。接続作業の実施に当たっては事前に現地調査を実施すること。現地調査実施時には拠点担当者立会いのもと、十分な打合せ・確認を実施し、設置場所・配線経路・電源等について齟齬のないように留意すること。

(2) 現地調査の結果に基づき拠点別の作業計画書を策定し、事前に拠点担当者の承認を得ること。なお、構築期間中における各拠点及び機構本部の個別の事情(建物改修工事・サーバ室移転工事等)を伴うことが想定される場合は、該当拠点と打合せを行い、その事情を考慮した内容とすること。

(3) 本調達の特性を考慮した、現地調査の要点と対策について記載がある場合は加点する。【加点】

2.7.3. ケーブルの流用

(1) 導入機器間を接続するために必要な各パッチケーブルについては、本調達に含むものとし、受注者が準備すること。

(2) 各拠点及び機構本部に敷設済みの光配線、UTP ケーブル及び無線アクセスポイント用 UTP ケーブル（以下「既設ケーブル」という。）については、拠点ごとに既設のものを利用すること。受注者による現地調査の結果、既設ケーブルの配線に不足や問題があることが判明した場合は、各拠点及び機構本部担当者への報告を行うこと。本不足・問題については、各拠点及び機構本部において、本調達の導入に合わせた対応を行うこととする。

2.7.4. 接続作業

(1) 導入した各種機器間の接続作業及び整線を行うこと。接続に必要となるケーブルならびに部材（端子等）は受注者が準備することとし、各拠点及び機構本部の設計内容に合わせて適切な製品・数量を、受注者の負担により設置すること。なお、本調達に必要なパッチケーブルを図 10 に示す。

(2) 光パッチケーブルはシングルモード(OS1 又は OS2)又はマルチモード(OM3 又は OM4)のいずれかを選定し準備すること。UTP パッチケーブルはカテゴリ 6A を準備すること。なお、一部拠点では OM2 の既設ケーブルが使用されている場合がある。

(3) 現地調査の結果、既設ケーブル以外の既設部材について、可能な場合は流用を行ってよいものとする。なお、光スプライスボックスについては、現地調査時にコネクタ形状を十分に確認すること。ただし、光スプライスボックスとスイッチの接続に用いる光パッチケーブルは流用を認めないため、受注者が新規で調達すること。

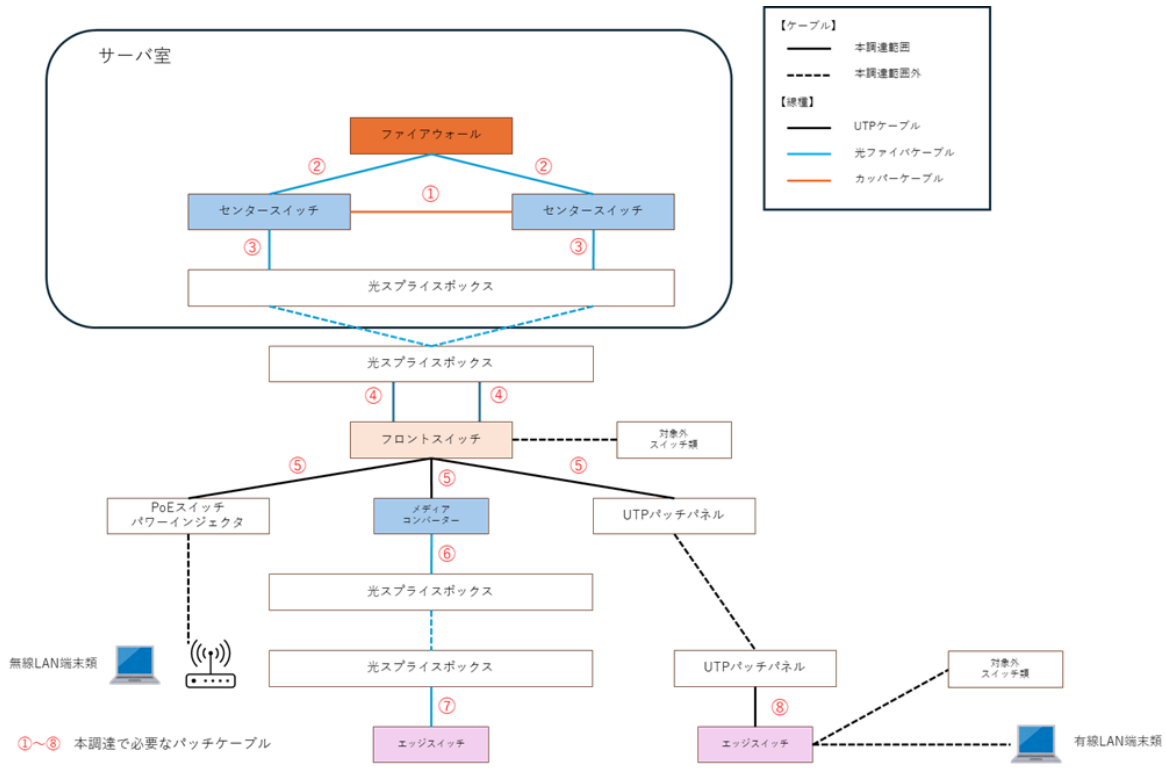

図 10. 本調達で必要なパッチケーブル

① センタースイッチ～センタースイッチ間のスタック用等を準備すること。

② ファイアウォール～センタースイッチ間の光ファイバーケーブルを準備すること。ただし、ケーブル長は最大 7m を見込むこと。

③ センタースイッチ～光スプライスボックス間の光ファイバーケーブルを準備すること。ただし、ケーブル長は最大 7m を見込むこと。

④ 光スプライスボックス～フロントスイッチ間の光ファイバーケーブルを準備すること。ただし、ケー

ブル長は最大 7m を見込むこと。

⑤ フロントスイッチ～PoE スイッチ(PoE インジェクタ)/メディアコンバータ/UTP パッチパネル間の UTP ケーブルを準備すること。ただし、ケーブル長は最大 7m を見込むこと。

⑥ メディアコンバータ～光スプライスボックス間の光ファイバーケーブルを準備すること。ただし、ケーブル長は最大 7m を見込むこと。

⑦ 光スプライスボックス～エッジスイッチ間の光ファイバーケーブルを準備すること。ただし、ケーブル長は最大 7m を見込むこと。

⑧ UTP パッチパネル～エッジスイッチ間の UTP ケーブルを準備すること。ただし、ケーブル長は最大 7m を見込むこと。

2.7.5. 電源工事

(1) 電源は既設の電源を用いること。

(2) 現地調査を行い、回路数・容量等の確認を行うこと。

(3) 現地調査の結果、回路数・容量等に不足があると判断する場合は、拠点担当者への報告を行うこと。

(4) 各拠点及び機構本部の責任において電源配線工事を実施する。

2.7.6. ラックへの設置

(1) サーバ室に設置する必要がある機器は各拠点及び機構本部指定のラックに搭載すること。

(2) 現地調査を行い、ラック・設置場所の確認を行うこと。

(3) 現地調査の結果既存のラック搭載場所や設置場所が不足する場合は、拠点担当者に報告を行うこと。

(4) 各拠点及び機構本部の責任において、受注者の機器設置までにラックのスペース確保や新規ラック設置を実施する。

(5) 標準的な 19 インチラックへの設置を想定している。現地調査の結果標準的なラックではなく設置に問題がある場合は、拠点ごとの担当者に報告を行うこと。問題への対応については、各拠点及び機構本部が、受注者の機器設置までに対応を行う。

(6) ラックマウントが不可能な機器については、受注者の負担によって耐震ベルト等の転倒防止対策を行うこと。

(7) 本調達の特性を考慮した、ラック設置の要点と対策について記載がある場合は加点する。【加点】

2.7.7. 無線アクセスポイントの設置

(1) 無線 LAN アクセスポイントを、各拠点及び機構本部の指示に基づいて設置すること。

(2) 既設ケーブルへの接続を行うこと。ケーブルの末端を確認し、パッチケーブルが必要になる場合は準備すること。

(3) 本調達の特性を考慮した、無線 LAN アクセスポイント設置の要点と対策について記載がある場合は加点する。【加点】

2.7.8. 既設機器の対応

(1) 本調達で導入する機器を設置する箇所に、置換対象の機器が設置されている場合は、各拠点及び機構本部担当者の指示に従い取り外しすること。

(2) 取り外した既設機器については各拠点及び機構本部担当者の指示に従い、同一拠点内の指定する場所に移動させること。
(3) 既設の認証基盤については、受入テスト期間中に本調達で導入する認証基盤と並行稼働を行う想定である。継続してネットワークへの接続が必要とされるため、それに伴う障害等の異状について考慮すること。
(4) 各拠点及び機構本部への現地調査の結果、既設認証システムと連携している個別システムがある場合は、今回導入する認証システムと連携を引き継ぐ必要があるため、該当する拠点や業者と連携の上、移行・連携作業を支援すること。
(5) 本調達の特性を考慮した、ラック設置の要点と対策について記載がある場合は加点する。【加点】

2.7.9. その他

(1) 敷設した各種ケーブルには敷設元及び敷設先が判断可能となるラベルを貼付すること。ラベルに明記する内容やルールについては、高専機構と協議の上決定することとする。
(2) 受注者側の管理上必要な管理ラベルについては、受注者にて貼付すること。
(3) 本調達で導入する各機器について、機器ごとに管理情報を記載したラベルを目視できる場所に張付すること。

2.8.　移行作業について

2.8.1. 全般

(1) 受注者は、以下の作業を実施すること。

・移行計画書の作成
・移行設計
・移行手順の作成
・移行リハーサルの実施
・移行判定
・移行作業の実施

移行の流れを以下に示す。

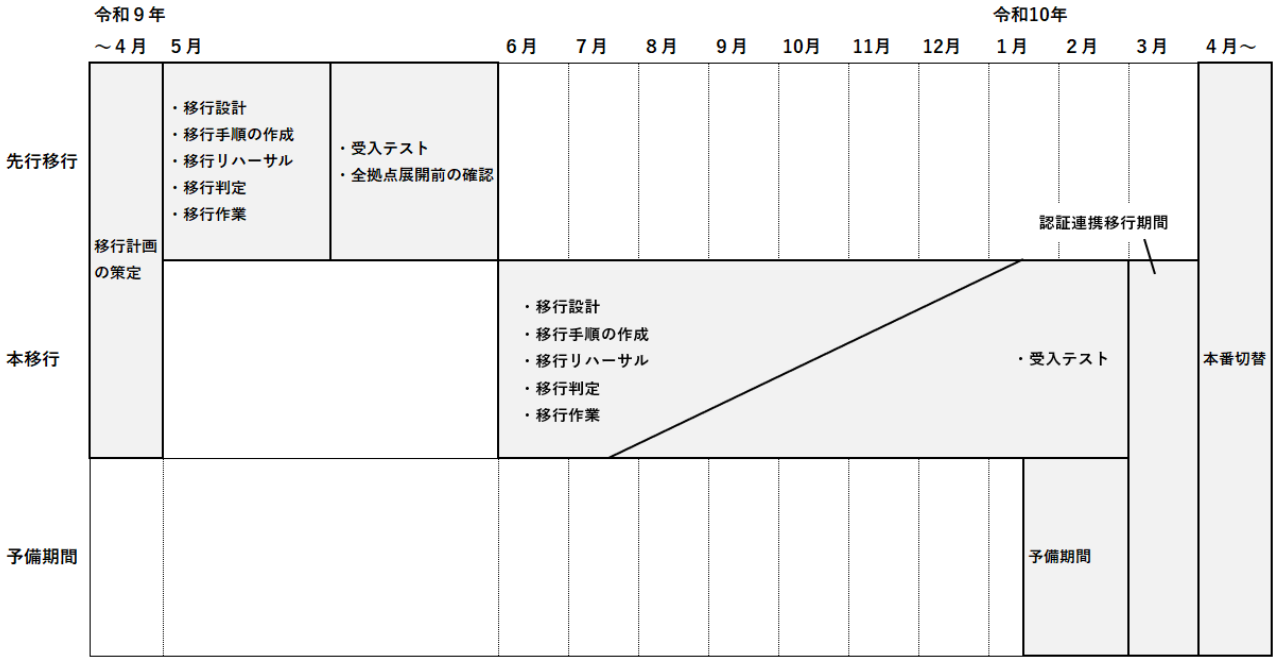

図 11. 移行の流れイメージ

(2) 本調達の理解のもとに提案者が移行について重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

2.8.2. 移行計画の策定

(1) 受注者は、各拠点及び機構本部の移行計画書を作成し高専機構の承認を得ること。

(2) 移行計画書には、少なくとも以下を記載すること。

・体制及び役割
・移行範囲・対象
・移行スケジュール

移行スケジュールについては、別紙 2. 更新作業スケジュールに基づき策定すること。なお、各拠点及び機構本部の作業はそれぞれ３日以内に完了するよう調整することとする。

・移行方式
・移行判定基準
・受入テストの内容、実施手順

(3) 現行ネットワークシステム及び業務の継続に影響がないよう考慮して移行計画を策定すること。移行計画については、移行作業の進捗に応じ適宜、各拠点及び機構本部担当者と協議のうえ調整を行うこと。なお、移行作業後 1 週間は、迅速な支援を可能とする特別な体制をとることとし、その体制についても移行計画書に含めること。
(4) 移行計画書の内容に以下のことが認められる場合は、加点する。【加点】
・仕様書をより具体化した、提案者の想定する移行計画が記載されていること。
・上記計画が本調達の特性を考慮したものとなっていること。
・現行ネットワーク・業務への影響の最小化が考慮されていること。

2.8.3. 移行設計

(1) 高専機構の承認を受けた移行計画書に基づいて、移行設計を行うこと。
(2) 本調達の特性を考慮した、移行設計実施の要点と対応方針が記載されている場合は加点する。【加点】

2.8.4. 移行手順の作成

(1) 高専機構の承認を受けた移行計画書に基づいて、移行手順書を作成すること。移行手順書には、少なくとも以下を記載すること。
・体制及び役割
・連絡先
・移行作業、操作手順
・移行タイムチャート、想定時間
・切り戻し手順
・作業状況報告の内容とタイミング
・各拠点及び機構本部担当者が必要とする作業
(2) 本調達の特性を考慮した、移行手順作成の要点と対応方針が記載されている場合は加点する。【加点】
(3) 移行手順書の内容が具体的と機構が認めた場合は加点する。【加点】

2.8.5. 移行リハーサル

(1) 受注者は移行リハーサル計画を策定し、各拠点及び機構本部担当者の承認を得ること。なお、移行リハーサルとは、 移行の本番を想定して、移行作業、操作手順、移行タイムチャート、想定時間、切り戻し手順を確認することを指す。
(2) 受注者は計画に基づき、移行リハーサルを実施すること。
(3) 移行リハーサル完了時には移行リハーサル結果報告書を作成し、各拠点及び機構本部の承認を得ること。

2.8.6. 移行判定

(1) 移行リハーサルの結果を移行判定基準と照らし合わせ、移行作業の実施可否判定を行う。
(2) 受注者は、移行判定を行うために必要な判断材料を整理した上で、移行判定会議を開催すること。参加者については拠点担当者を含む高専機構の担当者ならびに受注者とする。
(3) 移行判定会議は拠点別に、全ての拠点で実施するものとし、移行の判定は当該会議での決定を以て行うものとする。
(4) 本調達の特性を考慮した、想定する移行判定の流れの記載がある場合は加点する。【加点】

2.8.7. 移行作業

(1) 移行手順書に基づいて、移行作業を行うこと。
(2) 移行作業の実施状況を、移行手順書に従って各拠点及び機構本部担当者に報告すること。
(3) 本調達で要求する機能は移行作業完了後より利用できること。なお、受注者の責により一部機能が利用できない等の場合は、代替機能を受注者の負担で提供すること。
(4) 移行作業の実施中に不測の事態により移行作業を完遂できないと受注者が判断した場合には、各拠点及び機構本部担当者の承認を以て、現行ネットワークシステムへの切り戻しを行うこと。切り戻し作業は受注者の責任と費用負担により実施すること。また、切り戻し後のリカバリ計画を速やかに立案し、各拠点及び機構本部担当者ならびに高専機構に報告し承認を得ること。
(5) 移行作業後、問合せやトラブルに対応すること。なお、高専機構が指示した場合、稼働立ち合いを行うこと。
(6) 本調達の特性を考慮した、移行作業中及び作業後の特別体制について具体的な提案があり、有用と考えられる場合は加点する。【加点】

2.8.8. 移行・切替のスケジュール

(1) 図 11 に基づき、受注者にて応札時にスケジュールを提示すること。
(2) 以下の場合は加点する。【加点】
・仕様書をより具体化した、提案者の想定する移行スケジュールの記載がされていること。
・想定スケジュールの狙い、根拠が示されていること。

2.8.9. 移行単位

(1) 本システムの移行は大きく表 1 の移行単位に分類される。

表 1. 移行の概要

移行単位	概要	対象拠点
先行移行	令和 9 年 5 月前半に移行設計～移行作業を行う。5 月後半に、受入テスト並びに各拠点への展開前の確認を行う。	・東京高専 ・機構本部

移行単位	概要	対象拠点
本移行	令和 9 年 6 月～令和 10 年 1 月前半に移行設計から移行作業を行い、1 月後半から 3 月末までに受入テストを行う。	・東京高専を除く各拠点
予備期間	本移行期間で実施できなかった拠点の作業を行うことを想定している。作業内容については、受注者と高専機構が協議のうえ決定する。	

(2) 以下に該当する場合は加点する。【加点】
・各移行単位に対して、要点と対応が記載されている。
・よりよいと思われる方式の提案がある。
(3) Microsoft365 連携の移行について、提案者の方式が効率性や実現性の観点で有用であると考えられる場合は加点する。【加点】

2.8.9.1. ネットワーク及びネットワーク基盤サービス等の移行

(1) 本調達の主目的の一つであるネットワーク整備に関わる領域であり、以下を含むこと。
① ネットワーク
・各種スイッチ
・ファイアウォール
・無線アクセスポイント
② ネットワーク基盤サービス
・内部向け DNS
・DHCP
・NTP
③ 本調達導入機器向けの基本サービス
・ログ管理
・死活監視
・ネットワーク機器設定管理
・ウイルス対策
・バックアップ

(2) 本領域では既存機器の置き換えが発生するためネットワークの停止が伴うものと考えられ、各拠点及び機構本部の非営業日中の切替を想定している。拠点ごとの作業時間等の詳細については、各拠点及び機構本部担当者と協議のうえ決定すること。
(3) 切替後、受入テスト期間中はユーザによる実際の利用が行われるため、本番運用に耐える品質を担保すること。
(4) 演習室など本調達範囲外のネットワークについては、本ネットワークシステムの切替後も既存のネットワークを継続して利用するものとする。本調達範囲外のネットワークにおける設定変更等が

必要となる場合は、各拠点及び機構本部担当者が実施することを前提とする。受注者は、当該設定変更に関し、各拠点及び機構本部担当者からの要請に応じて、可能な範囲で技術的支援（設定方法の提示、助言等）を行うこと。

2.8.9.2. 認証基盤の移行

認証基盤のリプレースに関わる領域である。

関わる機器の設置に関しては移行作業より先行又は同時に完了している必要がある。

(1) 既存の高専共通システム用認証機能は、完全にシステムの切替が完了する令和9年度末日まで並行して利用する。受注者はこれについて考慮すること。

(2) 各拠点及び機構本部用認証システムについては、現行システムにおける同システム（AXIOLE）と同様、一つの製品で求められる全ての機能を網羅することを想定しているが、複数の製品を組み合わせて機能を実現する場合は、応札時にその方式について明示すること。

(3) アカウントデータ及びRADIUS認証用のMACアドレスについて、各拠点及び機構本部担当者が提供するデータに基づいて登録を行うこと。なお、提供するデータの形式はCSVもしくはLDIFとし、ユーザ・パスワードを含めた登録を行う場合は加点する。【加点】

(4) 以下に各領域の想定を記載する。

①ネットワーク接続の認証

ユーザが本調達で導入するスイッチや無線アクセスポイントに接続する際の認証は、本調達で導入する各拠点及び機構本部用認証システムを用いることとする。

②学認連携の移行

学認の認証は、各拠点及び機構本部用認証システムの機能を用いて行うこととするが、切替を行うまでは、既存の各拠点及び機構本部用認証システムを用いる。切替作業は、各拠点及び機構本部担当者が拠点ごとのスケジュールで行うこととする。

受注者は、本切替に対して技術支援を行うこと。

③Microsoft 365連携の構築

高専機構テナントのMicrosoft 365（Entra ID）への認証連携は、各拠点及び機構本部用認証システムの機能を用いて、APIで行うこととする。受注者は、連携切替前のMicrosoft 365のライセンス・利用状況・グループ設定が切替後も適切に引き継がれる方法を提案し、高専機構と協議のうえ実施すること。

(5) 各拠点及び機構本部用認証システムへのアカウントデータの投入ならびにアカウントごとの連携操作は、各拠点及び機構本部担当者が行うことを想定している（受注者の採用する実現方式により本作業が不要の可能性もある）。

(6) 本調達の特性を考慮した認証基盤の移行方法等について具体的な提案があり、有用と考えられる場合は加点する。【加点】

2.8.9.3. 高専共通システム等の認証の移行支援

高専共通システム等、項2.8.9.1、2.8.9.2に記載したもの以外の連携切替は、各拠点及び機構本部が新認証システムにアカウントデータ移行が完了したことを確認したうえで、高専機構担当者が行う。受注者は情報提供と技術支援を行うこと。

2.9. 担当者への教育について

2.9.1. 教育の種別

(1) 受注者は、表 2 の教育について実施すること。

表 2. 教育訓練の種別

種別	対象者	対象人数	想定時間
拠点担当者用教育	各拠点及び機構本部担当者	１拠点につき 5 名～10 名程度	1～2 時間
機構担当者用教育	高専機構担当者	5 名程度	2 時間
運用教育	各拠点及び機構本部担当者ならびに高専機構担当者	１拠点につき 5 名～10 名程度	1～2 時間

(2) 本調達の特性に応じた教育訓練が提案されており、有用と考えられる場合は加点する。【加点】

2.9.2. 内容

(1) 教育の内容には以下を含むこと。なお、下記に限らず、製品の特性に応じた教育が必要な場合は内容に含めること。
- ・システムの基本操作方法
- ・各機器の設定・稼働状況の確認方法
- ・障害発生時の一次対応方法（連絡手順等）

(2) 「拠点担当者用教育」については物理的な事項と運用に関する手順を中心に、実際の機器を用いた訓練とすること。

(3) 「機構担当者用教育」についてはシステム管理者向けの内容とすること。

(4) 「運用教育」については、システムの変更及び人事異動による担当者変更を想定した内容とすること。

(5) 受注者は、教育に用いる教材・資料の提供を行うこと。教材・資料は、高専機構経由で各拠点及び機構本部担当者に配布する。

(6) 各教育の形式については、集合形式あるいは録画教材又はオンライン教材を用いたオンデマンド形式による実施でも可とする。

(7) 教育内容について、本調達の特性を考慮した機構が有用と認める提案がある場合は加点する。【加点】

2.9.3. マニュアル作成

(1) 受注者は、下記に示す本調達で導入したシステム・機器・ソフトウェアについて日本語によるマニュアルを作成すること。
- ・スイッチ各種
- ・無線アクセスポイント、

・無線 LAN コントローラ
・ファイアウォール
・認証基盤（RADIUS クライアント追加手順を含む）
・その他各種サーバ

(2) マニュアルの内容として、設定変更を含め、想定される運用について記載すること。具体的には以下の内容を想定するが、詳細は高専機構と協議の上決定すること。
・システム操作方法
・各機器の設定方法
・障害時の対応方法
・システム運用方法(システム停止時及び起動時の操作方法等)

(3) 教育は本マニュアルを以って行うこと。
(4) マニュアルについて、本調達の特性を考慮した機構が有用と認める提案がある場合は加点する。【加点】

2.9.4. 時期

教育時期については以下を想定している。高専機構と協議の上決定すること。
・拠点担当者用教育：移行作業時
・機構担当者用教育：全拠点の移行作業完了後
・運用教育：年１回以上の実施に加え、システム運用に変更があったとき
（なお、オンデマンド教材の提供による場合は、年１回の教材提供に加え、システム運用変更時の教材の更新とする）

2.9.5. 教育場所

(1) 各拠点及び機構本部での教育に当たっては本調達で設置済みの機器を用いてもよい。他に各拠点及び機構本部で用意する必要がある設備・部材については各拠点及び機構本部担当者と事前に調整を行うこと。
(2) 教育場所、利用機材・部材について、本調達の特性を考慮した機構が有用と認める提案がある場合は加点する。【加点】

2.10. 報告について

以下のタイミング・手法で機構本部に報告を行うこと。
・キックオフミーティング（業務開始時・テレビ会議）
・各拠点及び機構本部における日次作業報告（日次・高専機構が指定したチャットツール）
・各拠点及び機構本部における作業完了報告（日次・高専機構が指定したチャットツール）
・問題発生時の打ち合わせ（不定期・テレビ会議）
・作業完了報告会（作業完了後・テレビ会議）

2.11. 作業完了確認について

(1) 受注者は、各拠点及び機構本部への構築・移行については作業完了後、各拠点及び機構本部担当者に納品物一覧表の提示ならびに作業内容の説明を行うこと。

(2) 各拠点及び機構本部担当者は、移行計画書に記載された方法に従って受入テストを実施する。

(3) 受注者は期日までに全拠点の受入テストの結果に基づき、高専機構担当者の作業完了確認を受けること。

(4) 確認の結果、成果物等に仕様内容に適合しない不備又は誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行い、変更点について各拠点及び機構本部担当者に報告を行った上で、指定された日時までに再度納品すること。

3. 運用・保守業務について

3.1. 運用保守実施計画の策定

(1) 本業務については運用保守実施計画を策定したうえで行うこと。運用保守実施計画については、以下の事項を満たすこと。

(2) 受注者は運用保守業務の開始前までに運用保守計画を示した運用保守業務実施計画書を策定し、高専機構の承認を得ること。

(3) 運用保守業務実施計画書には、少なくとも以下の内容を含めること。なお、運用保守業務実施計画書の記載内容の詳細については、落札後に高専機構と協議のうえ決定するものとする。

・運用保守業務対象範囲、運用保守体制/役割、コミュニケーションルール
・情報セキュリティ対応、データ/文書の取扱い対応
・報告/会議体
・運用保守業務項目一覧
・運用保守業務成果物
・定期報告書フォーマット

(4) 提案書に、想定する運用保守計画書について具体的な記載がある場合は加点する。【加点】

3.2. 運用業務について

受注者は、以下の範囲について運用業務を行うこと。ただし、運用開始までにその内容について高専機構の承認を得ること。

3.2.1. 問合せ対応業務

(1) 受注者は各拠点及び機構本部担当者からの運用に関する依頼に対し、これらを一元的に受付ける問合せ窓口を設置すること。電話による受付時間については、平日の 9：00～17：30 とすること。

(2) (1)の対応時間を上回る受付時間の提案があった場合は加点する。【加点】

(3) 電子メールによる受付けについては休日・夜間帯を含め常時行うこととし、翌営業日より迅速な対応を開始できるよう体制を構築すること。

(4) 本調達の理解のもとに提案者が問合せ対応業務について重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

3.2.2. ドキュメント維持

(1) 受注者は、本調達の運用に必要となる各種ドキュメントについて作成し、常に最新の状態を維持すること。対象とするドキュメントには、運用手順書、設定情報一覧、連絡体制図、障害対応手順、問合せ対応に関する記録その他本調達の遂行に必要な資料を想定するが、詳細は機構と協議の上、決定するものとする。

(2) 受注者は、運用作業の実施、問い合わせ対応、設定変更、障害対応その他の業務によりドキュメントの内容に変更が生じた場合には、その内容を速やかに反映し、関係者が適切に参照できる状態を保持すること。また、ドキュメントの更新に当たっては、記載内容の正確性及び整合性を確保するとともに、必要に応じて高専機構担当者へ報告し、承認を得ること。

3.2.3. 技術支援

(1) 受注者は、各拠点及び機構本部担当者からの軽微な設定変更依頼に対し、内容を確認の上、必要な設定変更を実施すること。対象とする作業は、各拠点及び機構本部と協議の上、決定する。

(2) 受注者は、依頼内容の受付に当たって、実施の可否、影響範囲、作業内容及び必要な確認事項を整理し、対象拠点管理者と調整の上で対応すること。なお、変更内容がシステム全体に影響を及ぼす恐れがある場合又は本調達の範囲を超える余地がある場合は、速やかに高専機構担当者へ報告し、別途協議すること。

(3) 受注者は、設定変更作業の実施に当たっては、業務影響を最小限とするよう十分配慮するとともに、必要に応じて作業手順、確認結果及び変更内容を記録し、関係者が参照できる状態を保持すること。

(4) また、作業完了後は、実施内容及び結果を対象拠点担当者へ報告するとともに、当該対応に伴いドキュメントの更新が必要となる場合には、速やかにその内容を反映すること。

(5) 技術支援の内容に、各拠点及び機構本部担当者からの、新規外延システムの接続にあたっての技術的な助言を含む場合は加点する。【加点】

3.2.4. リモート接続環境

(1) 受注者は、項 3.2.3 に定める技術支援を実施するため、必要に応じて利用するリモート接続環境として、IPsec VPN による接続手段を整備すること。

(2) 当該 IPsec VPN については、常時接続を行う運用とはせず、平時は無効化された状態で管理することを前提とし、必要な場合に限り有効化の上で利用すること。ただし、有効化及び無効化の操作は各拠点及び機構本部担当者にて実施するものとする。

(3) 受注者は、IPsec VPN の有効化、接続、作業実施、切断及び無効化に至る一連の手順を明確にした手順書を作成し、各拠点及び機構本部担当者が参照可能な状態で配備すること。

(4) 当該手順書には、接続開始及び終了の条件、実施責任者、確認事項、作業実施時の注意事項、切断後の状態確認その他安全な運用に必要な事項を記載すること。

(5) 受注者は、IPsec VPN を利用した作業の実施に当たっては、作業目的、接続日時、作業者、実施内容その他必要な事項を適切に記録し、高専機構担当者から求めがあった場合には速やかに提示できるようにすること。

(6) なお、IPsec VPN での接続の際は、多要素認証を必須とし、アクセス元を国内に制限するものとする。

3.3. 保守業務について

3.3.1. 問合せ対応業務

(1) 受注者は各拠点及び機構本部担当者からの問合せ及び保守対応等の依頼に対し、これらを一元的に受付ける問合せ窓口を設置すること。受注者は受け付けた問合せの内容に応じ、調査及び製品ベンダ問合せ等を実施したうえで回答を行うこと。ただし、学生・各拠点及び機構本部担当者以外の教職員からの問合せについては、各拠点及び機構本部が対応を行うこととし、受注者による対応は不要とする。

(2) 問合せ対応範囲は本調達で納入するハードウェア製品、ソフトウェア製品及び提供されるクラウド

サービス等とするが、これらに関連する事項の問合せについても、対応内容について高専機構と協議の上、本運用保守業務に支障を来さない範囲で支援を行うこと。

(3) 問合せは電話及び電子メール等の日本語による受付けを行い、日本語で回答を行うこと。

(4) 電話による受付時間については、平日の 9：00～17：30 とすること。

(5) (4)の対応時間を上回る受付時間の提案があった場合は加点する。【加点】

(6) 電子メールによる受付けについては休日・夜間帯を含め常時行うこととし、翌営業日より迅速な対応を開始できるよう体制を構築すること。

(7) 問合せ対応にあたり各拠点及び機構本部担当者ならびに高専機構担当者と受注者の間でログ・コンフィグ・パッチ等の電子ファイルを授受する仕組みとして、機構が保有する Microsoft 365 の利用を想定している。受注者が提供できるもので、より適切と思われる仕組み・サービスがあれば提案すること。

(8) 受注者は、依頼内容、対応進捗及び対応結果等、受付け対応の履歴管理を行い、項「3.4. 報告について」に記載されている会議にて報告すること。

3.3.2. アナウンス業務

受注者は提供されるサービスのメンテナンス、計画停止及び障害等について、各拠点及び機構本部担当者向けにメール等で情報共有を行うこと。

3.3.3. 製品保守

本運用保守業務における製品保守要件について以下に記載する。

3.3.3.1. 製品保守共通要件

(1) 本調達では、拠点ごとに異なる令和 9 年度の機器導入時から令和 10 年度の本稼働開始までを受入テスト期間としている。本受入テスト期間を含め、令和 15 年度末(令和 16 年 3 月末)までを採用する製品の保守対象期間とすること。

(2) 本調達での導入製品において、期間中に必要なライセンス費用・利用料などはすべて本契約に含めること。

(3) 本調達で採用する製品については、すべて保守の対象とすること。

(4) 製造元や代理店の保守が受けられない場合は、対象及び対応を提案書に明示すること。

(5) 本調達の運用期間終了後も保守サービスが継続できる場合は加点する。【加点】

(6) 機器交換等で設置されていた機器を撤去する場合は、データの消去を行った上でデータ消去証明書を提出すること。なお、データ消去の詳細な要件については、項「4.2. データ消去」に記載された通りとする。

(7) 本調達の理解のもとに提案者が製品保守について重要と考える観点において機構が有用と認める提案がある場合は加点する。【加点】

3.3.3.2. ハードウェア保守要件

(1) 受注者はサービスデスクにて受付けたハードウェアに係る仕様、設定方法及び不具合等の問合せに対し、平日の 9：00～17：30 の間、ハードウェア問合せ対応支援を行うこと。

(2) 受注者は必要に応じて製品ベンダへのエスカレーション等を実施し、原因追究及び対応策の策定等を行うこと。
(3) 受注者はハードウェア保守依頼を受付け、ハードウェア保守要員アサイン等の対応を行うこと。

3.3.3.3. ハードウェア保守業務

(1) ハードウェア保守の範囲は本調達で納入されるハードウェア製品に係る内容とし、既設ハードウェア製品については範囲外とする。
(2) 本調達で納入されるハードウェア製品については、以下の内容でハードウェア保守対応を行うこと。なお、以下の内容を上回る保守サービスの提案があった場合は加点する。【加点】
(3) オンサイト対応を行う場合、対応時間は 9:00～17:30 の間を含むものとし、平日の対応とする。なお、休日も対応を行う提案があった場合は加点する。【加点】

①オンサイト対応が必要な機器
・センタースイッチ
・ファイアウォール
②先出センドバック対応が必要な機器
・上記以外の納入されるハードウェア製品

(4) 設定の復旧については各拠点及び機構本部担当者が実施可能なこと。復旧手順については、項「2.9. 担当者への教育について」の記載に従いマニュアルを作成し各拠点及び機構本部担当者ならびに高専機構担当者に共有すること。
(5) 本調達で採用される製品については無期限保証やライフタイム保証といった、製品ライフサイクルの延長に寄与する保守施策がある場合は加点する。【加点】
(6) ハードウェア保守の要点と対応について、地域や人的要員等本調達の特性を考慮した機構が有用と認める提案がある場合は加点する。【加点】
(7) 全拠点について、仕様書記載レベルを上回る保守サービスが提案されている場合は加点する。その際過剰なコスト負担や制約がないこと。【加点】

3.3.3.4. オンサイト保守

(1) オンサイトハードウェア保守は、採用する機器の標準的な保守条件において受付け後翌営業日以内にオンサイトでの作業が行われること。なお、冗長化されているハードウェア製品については、高専機構担当者の許可により、冗長化されていないハードウェア製品と比して対応までの日数が長くなることを許容する場合がある。
(2) 業務開始時に、各拠点及び機構本部に対するオンサイト保守についての問い合わせ窓口を提示すること。
(3) 冗長化されていないハードウェア製品で、オンサイト保守対応の機器に関しては、受付後 2 時間以内に、対応スケジュールを該当機器が運用されている拠点担当者及び高専機構担当者に連絡すること。
(4) 受注者は保守作業の一環として、設定の復旧を行うこと。

3.3.3.5.　先出センドバック保守

(1) 先出センドバック保守とは、各拠点及び機構本部担当者から故障の連絡があった際、置き換え対象機器を受注者・製造元又は代理店から送付し、拠点ごとの担当者が接続変更を行った後に故障機器を送り返す保守形態のことをいう。なお、拠点ごとの担当者による接続変更に、各機器の設定の復旧は含まれないものとする。
(2) 受注者は、置き換え対象機器の設定の復旧を行うこと。
(3) 先出センドバック保守対応を行うにあたり、各拠点及び機構本部からの保守対応依頼日を起点として、原則翌営業日までに置き換え対象機器の各拠点及び機構本部への発送作業に着手すること。なお、ライセンス変更受付け等の作業時間制約がある場合は応札時に明示すること。また、機器送付のリードタイムの低減措置として予備機を各拠点及び機構本部に配備する場合は、本仕様書の導入機器一覧に加えて配備する機器・数量及び対象拠点を応札時に示すこと。
(4) 先出センドバック保守の対象には、無停電電源装置の定期バッテリ交換を含むものとする。
(5) (3)の各拠点及び機構本部への発送について、原則翌営業日までに可能な場合は加点する。【加点】

3.3.3.6.　ソフトウェア保守要件

(1) 受注者はサービスデスクにて受付けたソフトウェアに係る仕様、設定方法及び不具合等の問合せに対し、平日の 9：00～17：30 の間、対応・支援を行うこと。
(2) 対応・支援の範囲は本調達で納入されるファームウェア、OS 及び導入ソフトウェアに係る内容とし、各拠点及び機構本部に既存のソフトウェアについては対象外とする。
(3) 受注者は必要に応じて製品ベンダへのエスカレーション等を実施し、原因追究及び対応策の策定等を行うこと。
(4) 本調達の特性を考慮したうえで、ソフトウェア保守の要点と対応について機構が有用と認める提案がある場合は加点する。【加点】
(5) 各拠点担当者の実施する修正プログラム適用について、十分に簡易と考えられる方法が提案されている場合は加点する。【加点】

3.3.3.7.　修正プログラム提供業務

(1) 受注者は本調達で導入された機器のファームウェア、OS 及び導入ソフトウェアに対する修正パッチ、メンテナンスリリース及びマイナーリリース等の修正プログラムについて、契約期間中は無償での提供を行うこと。メジャーリリース及び開発停止等修正プログラムが手に入らなくなる場合は、別途協議を行うこととする。
(2) 項 2.2.3.　～項 2.2.6.の各機能を提供するサーバ及び項 2.2.7.のサーバを構成するファームウェア、OS(カーネル、ドライバ、シェル等)、ミドルウェア、アプリケーション、証明書について、脆弱性等が確認された場合は、確認された時点から 2 週間以内に更新すること。
(3) 修正プログラムについては、本調達で導入する標準構成において問題が発生しないことを検証したうえで提供すること。
(4) 修正プログラムの適用により作成したマニュアルの内容に変更が生じる場合は、マニュアルを更新すること。
(5) 修正プログラムの適用作業に係るスケジュールについては、各拠点及び機構本部担当者と協議の上、

作業を行うこと。

3.4. 報告について

(1) 受注者は受付け対応及び対応作業履歴を元に定期報告書を作成のうえ、高専機構へ下記頻度で対面又はオンラインの会議を開催し報告を行うこと。なお、これによらず緊急性の高い事象が生じた場合は、別途会議を開催し報告を行うこと。

・令和 10 年度までは 2 週ごとに 1 回以上

・令和 11 年度以降は 1 月ごとに 1 回以上

(2) 定期報告書の詳細については落札後に高専機構と協議のうえ決定とするが、少なくとも以下の内容を含めること。

・問合せ及び保守対応履歴、対応ステータス

・メンテナンス情報

・修正プログラムリリース情報

・各拠点及び機構本部の状況概要

(3) ファイアウォールログ収集サーバで収集したログについて分析の上、月 1 回以上、高専機構へ報告すること。分析観点は原則として受注者で検討すること。ただし、高専機構より提示した場合は、それに従うこと。

3.5. 作業完了確認について

(1) 受注者は、本調達の履行状況について、高専機構が月次で作業完了の確認を実施できるよう、業務実績を取りまとめた月次報告書及びこれに付随する証跡資料を提出すること。

(2) 高専機構は、提出された月次報告書、保守定例会議の内容その他必要な資料に基づき、当該月に実施された運用保守業務が本業務の要件を満たしていることを確認し、これをもって月次の確認を行うものとする。

(3) 受注者は、月次の確認に当たり、少なくとも以下の事項を確認可能な資料を提出すること。

①問合せ対応業務の実績

問合せ受付件数、対応内容、対応状況、未完了案件の有無及び継続対応案件の進捗状況が確認できること。

②アナウンス業務の実績

各拠点及び機構本部担当者向けに実施したメンテナンス、計画停止、障害等に関する情報共有の実施状況が確認できること。

③報告の実績

当月に実施した定期報告の日時、実施方法、報告内容及び報告資料が確認できること。

④製品保守業務の実績

ハードウェア保守、ソフトウェア保守、製品ベンダへのエスカレーション、オンサイト保守、先出センドバック保守その他保守対応の実施状況が確認できること。

⑤修正プログラム提供業務の実績

修正プログラム、メンテナンスリリース、マイナーリリース等に関する提供状況、検証状況、適用要否の判断及び必要に応じた調整状況が確認できること。

⑥ドキュメント更新状況

本調達に関連して更新又は新規作成した手順書、マニュアル、設定情報、運用資料等の有無及びその内容が確認できること。

⑦未解決事項及び課題

当月末時点で未完了の案件、翌月以降に継続する課題、機構側との協議が必要な事項等が整理されていること。

(4) 受注者は、月次報告書を原則として翌月 5 営業日以内に提出すること。提出期限の詳細は、契約締結後に高専機構と協議の上、定めるものとする。

(5) 高専機構は、提出された月次報告書等に不備又は記載内容の不足があると認める場合には、受注者に対して補正又は追加資料の提出を求めることができる。受注者は、当該指摘を受けた場合、速やかに必要な補正又は追加提出を行うこと。

4. 引取

4.1. 本契約満了時の引取

(1) 本契約満了後、次々期システムが正常に稼働することが確認できた後に、各拠点及び機構本部担当者の指示に従い、受注者の責において受注者が納入した機器の引取を行うこと。ただし、次々期システムの移行作業から引取までの期間、機器の保管場所の確保は各拠点及び機構本部で行う。

(2) 受注者は、引取対象の機器一覧を作成し、各拠点及び機構本部担当者に確認を行い、その承認を得ること。なお、一覧作成にあたり、現地調査を行っても構わない。

(3) 引取のために必要な全ての経費(養生品、機材、及び車両等を含む。)は、全て受注者の負担とする。

4.2. データ消去

(1) 保守業務に伴う機器の入替や、契約満了時・解除時のデータ消去については受注者の責任において行い、設置されている各拠点及び機構本部担当者の承認を得た上で撤去すること。なお、データ消去は、米国国防総省規格又は NATO 規格に準ずる消去方法にて完全に消去するか、物理破壊を行いデータが読み出せない状態にすること。

(2) データ消去や物理破壊できないスイッチ類、無線アクセスポイント等については、メーカーにて規定されている設定の消去手順での対応を行い、データ消去証明書の提出を行うこと。なお、故障により起動できない等、上記の方法ではデータ消去が困難な場合は、消去方法を機構に提案し、協議の上決定された方法で実施すること。

(3) データ消去作業に必要な場所及び消去に必要な機器については、受注者の負担で用意すること。

(4) データ消去作業終了後、受注者は、データの消去完了を明記した証明書を高専機構に提出すること。

4.3. 廃棄

(1) 適切なデータ処理等により、情報漏洩等のリスクがないと確認された撤去対象機器については、「資源の有効な利用の促進に関する法律「(平成 3 年 4 月 26 日法律第 48 号)」等のリサイクル関連法に基づき、事前に担当職員の承認を得た上で、原則、受注者の負担において再利用・再資源化すること。

(2) ただし、再利用・再資源化が不可能である機器並びに情報漏洩の危険性がある機器及び媒体については、以下の方針に基づき、廃棄すること。

① 受注者は、「廃棄物の処理及び清掃に関する法律(昭和 45 年 12 月 25 日法律第 137 号)」、その他の関連法令を遵守し、データ消去が完了した不要機器を適法、かつ安全、確実に廃棄すること。

② 廃棄作業完了後、受注者は、廃棄作業が適法に完了したことを示す廃棄完了証明書又は廃棄作業報告書を各拠点及び機構本部担当者に提出すること。

③ サーバ、ストレージ等、情報漏洩の危険性がある機器及び媒体については、物理的な破壊を行った上で、廃棄すること。

5. その他の要件

5.1. 作業場所

(1) 本調達において各拠点及び機構本部における作業以外での、作業場所及び必要となる設備、備品及び消耗品等については、受注者の責任において用意すること。また、必要に応じて高専機構担当者が現地確認を実施することができるものとする。
(2) 各拠点及び機構本部において作業場所が必要と受注者が判断する場合は、要件を明示すること。各拠点及び機構本部により状況が異なるため、受託後に現地調査や調査依頼通知等の手順をとること。
(3) 各拠点及び機構本部において作業を行う場合には、各拠点及び機構本部担当者の指示に従うこと。

5.2. 作業実施体制について

本調達の実施体制として重要と考慮される点が明らかにされ、体制として提案されている場合は加点する。【加点】

5.2.1. 体制図について

(1) プロジェクトの推進体制及び受注者に求める作業実施体制は図 12 及び表 3 のとおりである。受注者のチーム編成については想定であり、受注者決定後に高専機構との協議に基づき見直しを行うこと。なお、移行期間と運用期間の体制は別に作成すること。また、受注者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成すること。
(2) 応札者は応札時にプロジェクト実施体制及び役割を明示すること。
(3) 本調達の実施体制として重要と考慮される点を明らかにし、体制として提案すること。
(4) 作業工程やタスク毎に必要となるスキルを正確に定義し、適切な知識及び経験を有する要員を配置すること。

本調達の関連事業者と受注者の範囲を図 12 に示す。

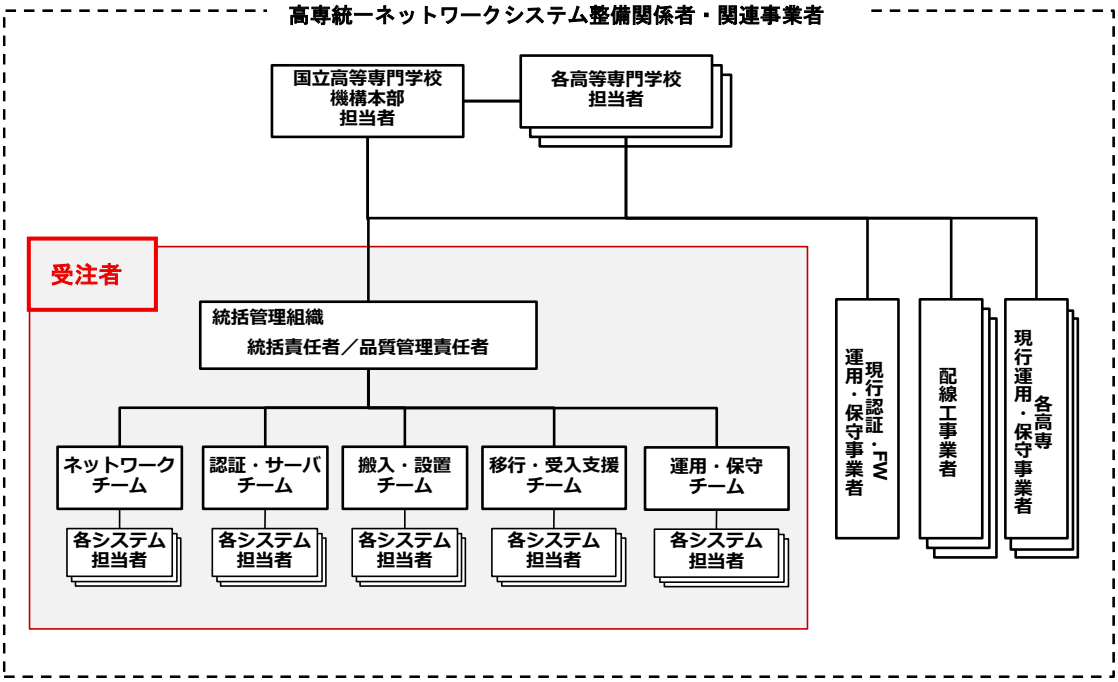

図 12. 体制図

5.2.2. 体制内の役割

受注者の体制について、想定する役割と内容について表 3 に示す。

表 3. 体制

No.	役割	要件
1	統括管理組織	作業全般を統括する組織を設置し、統括責任者を窓口とする。 統括管理組織は、高専機構に対して決定事項等の報告を行い、承認を得る。
2	統括責任者	本調達の契約期間中において統括管理組織の責任者として統括責任者を配置し、高専機構の承認に基づき、各チームの作業を統括管理する。なお、受入テストのサポートを除き、設計・構築・導入・移行時においては、本調達に係る作業に専任する。
3	チーム体制	統括管理組織の下に、チームリーダと各システム担当者で構成されるチームを設置する。 ネットワークチーム、認証・サーバチーム、搬入・設置チーム、移行・受入支援チーム、運用・保守チーム等の設置を想定している。 なお、同一チーム内のリーダとシステム担当者との兼務は前提としていない。

No.	役割	要件
4	品質管理責任者	本作業における成果物等の品質管理に関する責任者を、統括管理組織に 1 名以上配置する。品質管理責任者が他の役職を兼務することは前提としていない。

5.2.3. 作業要員に求める資格等の要件

体制には、以下の資格等を有する者を、最低１名ずつ含めること。

5.2.3.1. 統括責任者相当

(1) 複数拠点から成るネットワークの更新プロジェクトのマネジメントについて、10 年以上の経験を有すること。
(2) 過去 5 年以内において、教育研究機関(大学等)における拠点全体のネットワーク更新プロジェクトのマネジメント経験を有すること。
(3) 以下のいずれかの資格又は同等の資格を有すること。
・Project Management Institute (PMI) が認定する PMP(Project Management Professional)
・独立行政法人情報処理推進機構 (IPA) による情報処理技術者(プロジェクトマネージャ)
(4) 仕様書記載以外に本調達に機構が有用と認める資格・スキル・実績をもった人員を配置している場合は加点する。【加点】

5.2.3.2. チームリーダ相当

(1) 複数拠点から成るネットワークの更新プロジェクトのマネジメントについて、5 年以上の経験を有すること。
(2) 過去 5 年以内において、教育研究機関(大学等)における拠点全体のシステムの設計、構築、運用等のプロジェクトを実施した経験を有していること。
(3) 以下の資格又は同等の資格を有すること。
・独立行政法人情報処理推進機構 (IPA) による情報処理技術者(ネットワークスペシャリスト)
(4) 仕様書記載以外に本調達に機構が有用と認める資格・スキル・実績をもった人員を配置している場合は加点する。【加点】

5.3. プロジェクト管理

5.3.1. 全般

(1) 受注者は、契約締結後 2 週間以内にプロジェクト計画書を提出し、高専機構の承認を得ること。
(2) プロジェクト計画書には、少なくとも以下を記載すること。
・スケジュール
・実施体制
・実施内容
・会議体・コミュニケーション方法
(3) 受注者は、プロジェクト進捗管理を行うとともに、項「2.10. 報告について」および項「3.4. 報

告について」に定める方法において状況を高専機構に報告し、問題が発生した場合には速やかに高専機構に報告し、協議の上問題解決に努めること。

(4) 管理手法や使用ツールについては、高専機構との協議の上決定するものとする。

(5) 本調達の特性を考慮したうえで、プロジェクト管理の要点と対応について機構が有用と認める提案がある場合は加点する。【加点】

(6) 本調達の特性を考慮した機構が有用と認める管理手法やツールが提案されている場合は加点する。【加点】

5.3.2. 進捗管理

(1) 受注者は、プロジェクト進捗管理を行うとともに項「5.3.7.会議体」に記載する会議において状況を報告し、問題が発生した場合には速やかに高専機構に報告し、協議の上問題解決に努めること。

(2) 本調達の特性を考慮した機構が有用と認める提案がなされている場合は加点する。【加点】

5.3.3. 課題管理

(1) 課題管理に当たり、以下の内容を一元管理することとし、その他必要と考えられる項目についても管理する仕組みとすること。また、一連のワークフローを意識した管理プロセスを整備すること。

- 課題内容
- 影響範囲
- 優先度
- 発生日
- 担当者
- 対応策
- 対応状況
- 対応結果
- 解決日
- 起票・検討・対応・承認

(2) 本調達の特性を考慮した機構が有用と認める提案がなされている場合は加点する。【加点】

5.3.4. QA 管理

(1) 各拠点及び機構本部との質疑については QA として課題とは別に管理すること。

(2) 本調達の特性を考慮した機構が有用と認める提案がなされている場合は加点する。【加点】

5.3.5. 品質管理

(1) 作業工程毎に品質評価基準を定めたうえで作業を行うこと。

(2) 次の作業工程に推移する際は、品質管理における責任者および担当者による評価を実施し、高専機構に報告を行うこと。

(3) 本調達の特性を考慮した機構が有用と認める提案がなされている場合は加点する。【加点】

5.3.6. リスク管理

(1) 技術的観点、進捗的観点、人員・地域的観点、また本調達と類似するシステム構築案件実施の知見から、本プロジェクトの遂行に影響を与えるリスクを識別し、その発生確率・要因・影響等を整理すること。また発生確率と影響度からリスクの優先度を決定し、それに応じた対策を行うこと。
(2) リスクについて、定期的に監視・評価し、その結果を反映・報告すること。
(3) リスクを顕在化させないための対応策(体制や手順等)を策定すること。
(4) 想定されるリスクと対応が具体的に記載されている場合は加点する。【加点】

5.3.7. 会議体

(1) 受注者は、項「2.10. 報告について」および項「3.4. 報告について」で規定する会議等を開催した際、全体の進捗状況、課題解決状況、作業の進行に影響を及ぼす課題や問題等を報告すること。なお、課題解決状況が十分でない等、高専機構が必要と判断した場合は、各会議の開催頻度は、作業の進捗状況により、受注者と高専機構の協議の上、変更できるものとする。
(2) 開催する会議で協議又は報告する事項については、すべて資料を作成し論理的かつ効率的に行うこと。
(3) 別途必要な会議については、高専機構と協議を行い、これを設置すること。
(4) 本調達の特性を考慮した機構が有用と認める会議体やコミュニケーション方法について提案がある場合は加点する。【加点】

5.3.8. 構築計画の策定

(1) 受注者は、構築計画書を作成し、高専機構の承認を得ること。
(2) 構築計画書には少なくとも以下を記載すること。
  ・ネットワーク構築方法
  ・サーバ構築方法
  ・スケジュール
  ・体制及び役割
  ・制約条件及び前提条件
(3) 高専統一ネットワークシステムの構築は、構築計画書に基づいて行うこと。
(4) 構築完了後、構築結果報告書を作成し、高専機構に報告すること。
(5) 構築結果報告書は先行移行、本移行、予備期間（作業を実施した場合）のそれぞれに係るものに加え、全以降フェーズを総括したものを作成すること。
(6) 本調達の特性を考慮し、構築計画策定での要点と対応について記載がある場合は加点する。【加点】

5.4. 仕様書不適合責任

(1) 受注者は、本調達について作業完了確認を行った日を起算日として1年間、成果物に対する仕様書不適合責任を負うものとする。その期間内において不適合があることが判明した場合には、その不適合が高専機構の指示によって生じた場合を除き(ただし、受注者がその指示が不適当であることを知りながら、又は過失により知らずに告げなかったときはこの限りでない。) 受注者の責任及び負担において速やかに修正等を行い、指定された日時までに再度納品するものとする。なお、修正方法等については事前に高専機構の承認を得てから着手するとともに、修正結果等についても高専機構の承認を受けること。また、前述の期間経過後であっても、成果物等の不適合が受注者の故意又は重大な過失に基づく場合は、その責任を負うものとする。

(2) 高専機構は、前項の場合において、不適合の修正等に代えて、当該不適合により通常生ずべき損害に対する賠償の請求を行うことができるものとする。また、不適合を修正してもなお生じる損害に対しても同様とする。

5.5. 情報セキュリティ要件

5.5.1. 共通方針

情報セキュリティ対策の共通方針として、以下の方針に従い高専統一ネットワークシステム全体の情報セキュリティ対策を実施すること。

(1) 受注者は、情報セキュリティ管理責任者を設け、情報セキュリティ対策実施のための体制を整備すること。

(2) 受注者は、業務開始時に、情報セキュリティインシデントに関する連絡方法・対応手順等を明示して高専機構の承認を得ること。情報セキュリティインシデントが発生した場合には速やかに高専機構に報告し、必要な対策を講じること。

(3) 情報セキュリティ対策の実施に当たっては、政府機関等のサイバーセキュリティ対策のための統一基準群ならびに、高専機構で策定している情報セキュリティ関係規則（契約後開示する）に準拠すること。

(4) 以下の場合は加点する。【加点】

・プロジェクト実行時のセキュリティ対策実施体制について具体的に提案がある。

・セキュリティ対策の手続きについて具体的な提案がある。

5.5.2. システムの情報セキュリティ対策

本調達で導入するネットワークシステムに関するセキュリティ対策については、項5.5.3.～5.5.9.の点に留意すること。なお、導入するそれぞれの機器におけるセキュリティ対策については、項「2. 導入・移行業務について」の要件に従って実施すること。

5.5.3. 脆弱性対策

(1) 高専統一ネットワークシステムで利用しないプロセス、サービス等は原則停止又はアンインストールすること。

(2) 本調達で導入する各機器に対して製造元から脆弱性に関する情報が公開された場合、当該脆弱性がもたらすリスクを確認した上で高専機構へ報告すること。

(3) 脆弱性対策を行う場合は、製造元より入手したセキュリティパッチやファームウェア等のリリース情報を基に十分に検証した上で本番環境へ適用すること。
(4) 本調達で導入する機器は、定義ファイルやバージョンアップ等の継続的な更新を行うための仕組みを備えること。
(5) 本調達で導入するサーバには、アンチマルウエアソフトウェア等により不正プログラム対策を実施すること。
(6) 以下の場合は加点する。【加点】
・本システムで想定するリスク及び対応方針について具体的な記載がある。
・提案者の適切な事例・実績による対応案や手段・手法の記載がある。

5.5.4. データ保護

(1) 悪意のある第三者によるデータの改ざんを防ぐため、通信経路上での通信データの盗聴、サーバ内の情報への不正アクセス、各種ログファイルの改ざん等への対策を講じること。
(2) 機密性のあるデータを公衆回線や外部記録媒体によって伝送する場合には暗号化を行うこと。
(3) 想定するリスク及び対応方針について具体的な記載がある場合は加点する。【加点】

5.5.5. アクセスログ管理

(1) 本調達で導入する機器(ファイアウォール及び認証サーバ)について、アクセスログの取得を行い、不正アクセスの疑いがあった場合に追跡できるようにすること。
(2) 担当者が簡易な操作でアクセスログの確認を行える仕組みを提供すること。
(3) 過去１年分以上のアクセスログを、本調達で導入する項「2.2.2. ストレージサーバ」のストレージ上に保管すること。
(4) ファイアウォールのアクセスログ・IDS/IPS 機能の検知及び防御されたログについては、データセンタ内に設置する集約ログサーバにも転送すること。
(5) アクセスログ確認を行える仕組みについて、具体的な運用イメージで示されており、その仕組みが過剰なものでなく、簡易ではあるが機能上足りている場合は、加点する。【加点】

5.5.6. 情報セキュリティ侵害が発生した場合の対処

(1) 本調達業務の遂行において、各拠点及び機構本部の情報資産(サーバ、ネットワーク機器、回線などの高専統一ネットワークのシステム及びそれらに附帯するソフトウェア及びデータ、高専統一ネットワークシステムが提供する情報処理としてのサービス、電子、紙媒体に関わらず各拠点及び機構本部が保有するドキュメント類及びそれらに記載された情報、その他各拠点及び機構本部の所有に帰属するもの)にセキュリティ侵害が発生した、又は発生する恐れがある場合には、速やかに高専機構へ報告すること。
(2) 以下の場合は加点する。【加点】
・想定する作業・手続きについて具体的な提案がある。
・提案者の適切な実績・事例に基づいた提案がある。

5.5.7. 機密保護

高専機構ならびに各拠点及び機構本部から受注者に提供するすべての情報及び資料等は、本契約期間中の如何を問わず、第三者に開示、漏えい又は他の目的に使用しないこと。ただし第三者に開示の必要性がある場合は、開示方針や漏えいの防止策を明示し高専機構の承認を得ること。

5.5.8. データ管理

(1) 本調達業務で利用及び作成するデータ等は、一元的に管理を行うこと。また、作業従事者の権限に応じたアクセス権を設定しデータの漏えい等がないよう対応すること。
(2) 受注者の作業端末は定期的にセキュリティチェックを行い、セキュリティ上の問題がないことを確認し、結果を項 2.10.ならびに項 3.4.に示す報告業務の中で高専機構に報告すること。
(3) 暗号化においてサーバ証明書を使用する場合、NII の UPKI 電子証明書発行サービスを利用する想定であり、証明書発行手続きは、可能な限り受注者が ACME(自動証明書管理環境)への対応又は同等の環境を整えることとし、手動で行う場合は各拠点及び機構本部側で行うものとする。
(4) 以下の場合は加点する。【加点】
・想定する作業・手続きについて具体的な提案がある。
・提案者の適切な実績・事例に基づいた提案がある。

5.5.9. その他のセキュリティ対策

(1) 受注者は下請負も含む本調達に関わる者すべてに対して情報の漏えい、消去、不正アクセス、不正利用等の防止を目的としたセキュリティ教育を実施すること。
(2) 本調達業務に係る情報を知り得る内部関係者による、故意又はオペレーションミスに起因する情報漏えい、改ざんを防止、抑止するための対策を講じること。
(3) 業務の一部を外部業者に下請負する場合は、下請負先に対しても同様の情報セキュリティ対策を義務付けること。
(4) 移行作業に際して現行設定に情報セキュリティの脆弱性があることを受注者が認識した場合は、脆弱性を抱えたままの設定を新システムに引き継ぐのではなく、各拠点及び機構本部担当者にその旨を報告し対応を協議すること。
(5) パスワードを設定する場合は高専機構パスワードポリシーに準拠したパスワードを設定すること。なお、高専機構パスワードポリシーの内容については、契約後開示する。
(6) 導入する機器等について ISMAP クラウドサービスリストならびに ISMAP-LIU に登録されている場合は加点する。【加点】
(7) 移行に伴う現行脆弱性発見時の対応について、想定する作業・手続きについて具体的な提案がある場合は加点する。【加点】

5.6. 入札参加要件

5.6.1. 公的な資格や認証等の取得

(1) 総合的な情報セキュリティを確保するために、本調達の実施部門(事業所)は、ISMS(適合性評価制度)認証基準に基づく一般財団法人日本情報経済社会推進協会による JISQ27001 又は海外の認定機関により認定された審査登録機関による ISO/IEC27001 又はこれと同等以上の認証を受けているこ

と。
(2) プライバシーマークや JAPiCO マークの認証を受けている、又はこれらと同等以上の個人情報保護に関する施策を実行していること。
(3) 建設業法に基づく電気通信工事業の許可を受けていること。

5.6.2. 受注者の実績

(1) ネットワーク、ハードウェア、OS、ミドルウェアの選定・構築方法を標準化した、システム・インフラの選定・構築方法論を受注者自身が有し、属人性を排除した設計・構築が可能であること。
(2) 過去 5 年以内において、官公庁若しくは独立行政法人における、全国 40 拠点以上のネットワークに関する設計、構築、保守、運用等のプロジェクトを請け負った経験がある場合は加点する。【加点】
(3) 全国いずれかの高専又は大学のネットワークに関する設計、構築、保守、運用等のプロジェクトを請け負った経験がある場合は加点する。【加点】
(4) 本作業遂行において、各拠点及び機構本部担当者と日本語により円滑かつ適切なコミュニケーションが図れること。
(5) 本作業の円滑な遂行に必要な経営基盤及び資金、設備等の十分な管理能力を有し、本作業の目標達成、計画遂行、継続的実施に必要な組織、要員、設備及び施設を有していること。
(6) 本調達の特性を考慮した観点からこれまでの受注実績があげられており、また本調達への事例適用の考え方が記載されている場合は加点する。【加点】

5.6.3. 複数事業者による共同提案

(1) 複数の事業者が共同提案する場合、その中から全体の意思決定、運営管理等に責任を持つ共同提案の代表者を定めるとともに、本代表者が本調達に対する入札を行うこと。
(2) 共同提案を構成する事業者間においては、その結成、運営等について協定を締結し、業務の遂行に当たっては、代表者を中心に、各事業者が協力して行うこと。事業者間の調整事項、トラブル等の発生に際しては、その当事者となる当該事業者間で解決すること。また、解散後の瑕疵担保責任に関しても協定の内容に含めること。
(3) 共同提案を構成する全ての事業者は、本入札への単独提案又は他の共同提案への参加を行っていないこと。
(4) 共同提案を構成する全ての事業者は、全ての入札参加要件を満たすこと。

5.7. 知的財産権の帰属

(1) 受注者は、受託業務の実施の過程において、高専機構が開示した情報(公知の情報等を除く。)及び契約履行過程で知り得た情報並びに成果物に関する一切の情報を、本受託業務の目的以外に使用又は第三者に開示又は漏洩してはならないものとし、そのために必要な措置を講ずること。
(2) 本ネットワークシステムの設計・構築工程で生じた納入成果物(パッケージソフトウェアを除く。)に関して、著作権法第 21 条から第 28 条までに定める全ての権利は高専機構に帰属するものとする。
(3) 受注者は、いかなる場合も著作者人格権を行使しないこととし、また、第三者をして行使させない

ものとする。

(4) 受注者が本受託業務の実施の過程で生じた納入成果物に係る著作権を自ら使用し又は第三者をして使用させる場合は、高専機構と別途協議するものとする。

(5) 納入成果物に第三者が権利を有する著作物が含まれている場合は、高専機構が特に使用を指示した場合を除き、受注者は当該著作物の使用に必要な費用の負担を含む一切の手続を行うものとする。この場合、受注者は当該著作物の使用許諾条件につき、高専機構の了承を得るものとする。

(6) 本受託業務の実施に関し、第三者との間で著作権に係る権利侵害の紛争等が生じた場合は、当該紛争の原因が専ら高専機構の責めに帰す場合を除き、受注者は自らの責任と負担において一切を処理するものとする。なお、高専機構は紛争等の事実を知ったときは、速やかに受注者に通知することとする。

5.8. 遵守事項

5.8.1. 契約条件

(1) 契約は、落札後すみやかに行うこと。

(2) 提案書に記載された事項は、業務を実施する上で最低限遵守すべき事項とするため、受注者には履行義務・成果物作成義務が発生する。

(3) 受注者は、本要求仕様及び提案書の記載事項の実現に係る費用一切を含むものを賃貸料として契約すること。

(4) 高専機構の要求による借入期間の延長には応じることとし、借入期間の延長の場合、サービス内容等について、高専機構担当者との協議に応じること。

5.8.2. 作業管理上の遵守事項

(1) 受注者は、担当者の指示に従い、作業の進捗状況及び予定を文書によって説明することとし、その都度担当者の承認を得て作業を進めること。

(2) 本調達仕様書に具体的な記述がない事項であっても、本調達の遂行、本システムの安定稼働、及び関係するシステムとの接続に必要と認められる本システム側の対応が発生した場合は、高専機構担当者と協議・検討の上実施すること。

(3) 本調達の契約履行期間の満了、全部又は一部の解除、又はその他契約の終了事由の如何を問わず、本調達が終了となる場合には、受注者は高専機構が継続して本事業を遂行できるよう必要な措置を講じ、他社に移管する作業の支援や引継ぎを行うこと。

5.8.3. 環境への配慮

グリーンコンピューティング(グリーン IT)への対応

システムを構成する機器等については「グリーン購入法」に基づいた製品を可能な限り導入すること。

5.8.4. 下請負の制限及び下請負を認める場合の条件

(1) 受注者は、業務の全部を第三者に下請負することはできない。

(2) 受注者における統括責任者を下請負先事業者の社員や契約社員とすることはできない。

(3) 受注者は下請負の行為について一切の責任を負うものとする。また、下請負先に対しては、受注者

と同等の義務を負わせるものとする。
(4) 下請負先における情報セキュリティの確保については受注者の責任とする。
(5) 高専機構の求めに応じて、下請負先の資本関係・役員等の情報、業務の実施場所、作業要員の所属、保有資格、実績等に関する情報を提供すること。
(6) 高専機構の求めに応じて、受注者が下請負先事業者の業務(情報セキュリティ対策も含む。) の履行状況を確認・報告すること。
(7) 下請負による情報セキュリティ上の脅威に対して情報セキュリティが十分確保されるよう、具体的な対応方法の提案すること。
(8) 本調達の特性を考慮したうえで、下請負の管理に関して機構が有用と認める提案がある場合は加点する。【加点】

5.8.5. 承認手続

(1) 本調達の実施の一部を合理的な理由及び必要性により下請負する場合には、あらかじめ下請負の相手方の商号又は名称及び住所並びに下請負を行う業務の範囲、下請負に対する管理方法、下請負の必要性等について記載した申請書を高専機構に提出し、あらかじめ承認を受けること。
(2) 前項による下請負の相手方の変更等を行う必要が生じた場合も、前項と同様に下請負に関する書面を高専機構に提出し、承認を受けること。

5.8.6. その他特記事項

5.8.6.1. サプライチェーンリスクマネジメントについて

(1) 受注者は、サプライチェーン・リスクの要因となる脆弱性を発生させない又は増大させないための管理体制を構築すること。また、応札時に管理体制図を機構に提示すること。
(2) 受注者は、機構がサプライチェーン・リスクに係る情報セキュリティインシデントを認知した場合又はその疑いが生じた場合に、必要に応じて業務内容、作業プロセス又は成果物を立ち入り検査等で機構が確認することを了承すること。
(3) 本調達において使用する機器等については予め機構に機器等リストを提出し、機構がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、代替品選定やリスク低減対策等、機構と迅速かつ密接に連携し提案の見直しを図ること。
(4) その他、サプライチェーン・リスクに関し、以下の資料を提出し、対策を講じていることを証明した場合は加点する。【加点】
- ・当該システムに関して、想定されるサプライチェーン・リスク及びそれに対する軽減策についての説明資料
- ・想定されるサプライチェーン・リスクに鑑み、当該システムで使用される機器を選定した理由に関する説明資料
- ・調達機関の意図しない変更や機密情報の窃取等が行われないことを保証するための具体的な管理手順や品質保証体制を証明する書類
- ・当該システムに調達機関の意図しない変更が行われるなどの不正が見つかったときに、追跡調査等を実施する手順及び体制を示す資料
- ・各種認証取得に関する資料

・我が国政府機関における類似のシステム構築・運用実績

5.8.6.2.　ワーク・ライフ・バランス等の推進に関する評価

女性の職業生活における活躍の推進に関する法律に基づく認定企業(えるぼし認定企業)、次世代育成支援対策推進法に基づく認定企業(くるみん認定企業等)及び、青少年の雇用の促進等に関する法律に基づく認定企業(ユースエール認定企業)については加点するので、認定されていることが確認できる書面の写しを提出すること。なお、複数の認定が該当する場合は、最も配点が高い区分により加点することとする。【加点】

5.8.6.3.　各種法令等の遵守及び費用の計上

(1) 受注者は、本調達の遂行にあたり、関連する関係諸法令及び条例等を遵守すること。
(2) 受注者は、業務責任者を配置すること。あわせて、関連する関係諸法令及び条例等により選任・配置が求められる責任者、主任者、技術者、その他有資格者を必要に応じて定め、本調達の実施期間中、所定の業務に従事させること。
(3) 石綿（アスベスト）事前調査、高所作業等、本調達の実施に必要となる各種法令対応に係る費用は、本調達の受託費用に含めること。

5.8.6.4.　次期 SINET への移行について

現行の SINET6 については 2027 年度に終息し、次期 SINET の本格運用が 2028 年度から開始される予定と、NII から発表されている。SINET6 から次期 SINET への移行をサポートすること。

以上

別紙１－１　ネットワーク機器一覧（本調達）

No.	高専名	ファイアウォール						センタースイッチ										フロントスイッチ										エッジスイッチ										サーバ兼DMZスイッチ					メディアコンバータ		光リピータ		アクセスポイント		PoEスイッチ								
		FW本体	1000BASE-SX	SFP_10G - SR	SFP_10G - LR	10GBASE-T	DAC	CSW_24ポート	スタックケーブル	サーバ兼DMZスイッチ専用（SFP_10G-SR）	CSW_SFP_1G-RJ45	CSW_SFP_1G-SX	CSW_SFP_1G-LX	CSW_SFP_10G-SR	CSW_SFP_10G-LR	CSW_SFP_10GBASE-T	CSW_SFP_DAC	FSW_48ポート	FSW_SFP_1G-SX	FSW_SFP_1G-LX	FSW_SFP_10G-SR	FSW_SFP_10G-LR	FSW_SFP_10GBASE-T	FSW_SFP_DAC	ESW_12ポート	ESW_24ポート	ESW_48ポート	ESW_SFP_1G-SX	ESW_SFP_1G-LX	ESW_SFP_10G-SR	ESW_SFP_10G-LR	ESW_SFP_10GBASE-T	ESW_SFP_DAC	SDSW_48ポート	SDSW_SFP_1G-SX	SDSW_SFP_10G-SR	SDSW_SFP_10GBASE-T	SDSW_SFP_DAC	M/C_SX	M/C_LX	Repeater	Repeater_10G-SR	AP_本体	Injector	PSW_12ポート	PSW_24ポート	PSW_SFP_1G-SX	PSW_SFP_1G-LX	PSW_SFP_10G-SR	PSW_SFP_10G-LR	PSW_SFP_10G-RJ45
1	函館高専（次期）	1	0	2	0	0	0	2	2	2	0	0	0	2	18	0	0	9	0	0	0	18	0	0	8	15	1	0	0	0	0	0	0	1	0	2	0	0	0	0	0	0	60	4	9	0	0	0	0	0
2	苫小牧高専（次期）	1	0	2	0	0	0	2	2	2	0	6	0	14	0	0	4	6	0	0	0	12	0	0	0	6	2	8	0	0	0	0	0	1	0	2	0	0	0	0	0	0	60	3	1	6	0	0	0	0
3	釧路高専（次期）	1	0	2	0	0	0	2	2	2	2	0	0	26	2	4	0	12	2	0	0	24	2	0	0	3	4	7	4	0	7	0	0	1	0	2	0	0	0	0	0	0	50	5	6	3	0	0	2	0
4	旭川高専（次期）	1	0	2	0	0	0	2	2	2	0	0	0	30	0	0	0	13	0	0	0	26	0	0	0	2	4	1	0	0	0	0	0	1	0	2	0	0	0	0	0	0	50	10	6	0	0	0	0	0
5	八戸高専（次期）	1	0	2	0	0	0	2	2	2	8	0	0	2	18	0	4	16	0	0	0	28	0	0	0	17	27	0	0	0	0	0	0	1	0	2	0	0	0	0	0	0	50	25	6	0	0	0	0	0
6	一関高専（次期）	1	0	2	0	0	0	2	2	2	10	0	0	30	0	2	0	14	10	0	0	22	0	0	0	4	0	5	10	0	3	0	0	1	0	2	0	0	0	0	0	0	50	18	3	0	0	0	0	0
7	仙台高専（広瀬）（次期）	1	0	2	0	0	0	2	2	2	4	0	0	24	2	0	2	11	1	0	0	20	2	0	0	1	5	6	1	0	0	0	0	1	0	2	0	0	0	0	0	0	40	8	8	0	0	0	0	0
8	仙台高専（名取）（次期）	1	0	2	0	0	0	2	2	2	2	8	4	12	4	0	4	7	0	0	0	10	4	0	0	11	8	3	8	4	0	0	0	1	0	2	0	0	0	0	0	0	50	13	7	0	0	0	0	0
9	秋田高専（次期）	1	0	2	0	0	0	2	2	2	0	0	2	24	0	0	2	11	4	0	0	22	0	0	0	26	14	2	4	2	0	0	0	1	0	2	0	0	0	0	0	0	50	2	7	0	0	0	0	0
10	鶴岡高専（次期）	1	0	2	0	0	0	2	2	2	0	0	0	30	0	0	0	12	7	0	0	22	0	0	0	8	3	3	5	0	0	0	0	1	0	2	0	0	0	0	0	0	50	6	5	1	0	0	0	0
11	福島高専（次期）	1	0	2	0	0	0	2	2	2	0	3	1	24	0	2	4	11	0	0	0	22	0	0	0	6	1	1	3	2	0	0	0	1	0	2	0	0	0	0	0	0	60	23	6	0	0	0	0	0
12	茨城高専（次期）	1	0	2	0	0	0	2	2	2	2	2	2	20	6	0	0	13	2	0	0	18	6	0	0	4	5	2	4	2	0	0	0	1	0	2	0	0	0	0	0	0	60	9	5	2	0	0	0	0
13	小山高専（次期）	1	0	2	0	0	0	2	2	2	4	0	0	14	10	4	0	10	0	0	0	12	8	0	0	6	14	4	0	0	2	0	0	1	0	2	0	0	0	0	0	0	60	35	6	0	0	0	0	0
14	群馬高専（次期）	1	0	2	0	0	0	2	2	2	2	0	0	20	0	0	0	9	6	1	1	18	0	0	0	20	18	0	10	1	0	0	0	1	1	2	0	0	0	1	0	0	40	24	3	0	0	0	0	0
15	木更津高専（次期）	1	0	2	0	0	0	2	2	2	4	0	0	6	24	4	0	13	0	0	0	2	24	0	0	7	43	7	0	0	0	0	0	1	0	2	0	0	0	0	0	0	60	30	8	0	0	0	2	0
16	東京高専（次期）	1	0	2	0	0	0	2	2	2	1	0	0	26	4	2	0	15	0	0	0	24	4	2	0	0	0	5	0	0	0	0	0	1	0	2	0	0	0	0	0	0	60	9	8	1	0	0	0	0
17	長岡高専（次期）	1	0	3	0	0	0	2	2	2	2	0	0	20	0	0	4	10	2	0	0	18	0	0	0	3	9	8	0	0	0	0	0	1	0	2	0	0	0	0	0	0	59	6	17	1	0	0	0	0
18	富山高専（本郷）（次期）	1	0	2	0	0	0	2	2	2	0	0	0	16	2	0	2	8	3	2	1	14	4	2	0	0	8	9	4	2	0	0	0	1	0	2	0	0	0	0	0	0	40	15	6	3	4	0	0	0
19	富山高専（射水）（次期）	1	0	2	0	0	0	2	2	2	0	0	0	30	0	0	2	15	2	0	0	30	0	2	0	0	3	18	2	2	0	0	0	1	0	2	0	0	0	0	0	0	40	19	1	4	0	0	0	0
20	石川高専（次期）	1	0	2	0	0	0	2	2	2	0	10	2	18	8	0	0	10	3	0	0	12	8	0	0	11	11	3	2	0	4	0	0	1	0	2	0	0	0	0	0	0	60	4	13	3	0	0	0	0
21	福井高専（次期）	1	0	3	0	0	0	2	2	2	0	0	0	26	0	0	0	12	2	2	2	24	0	0	0	5	19	0	2	0	0	0	0	1	0	2	0	0	0	0	0	0	60	15	9	0	0	0	0	0
22	長野高専（次期）	1	0	3	0	0	0	2	2	2	0	0	0	20	2	0	4	10	0	0	0	18	2	0	0	7	0	2	6	0	0	0	0	1	0	2	0	0	0	6	0	0	60	6	12	0	0	0	0	0
23	岐阜高専（次期）	1	0	2	0	0	0	2	2	2	2	0	0	24	0	0	0	10	2	0	0	20	0	0	0	11	17	1	3	0	0	0	0	1	0	2	0	0	0	0	0	0	60	18	11	3	0	0	0	0
24	沼津高専（次期）	1	0	2	0	0	0	2	2	2	0	0	0	22	0	0	0	9	4	0	0	18	0	0	0	8	20	0	4	0	0	0	0	1	0	2	0	0	0	0	0	0	60	19	8	0	0	0	0	0
25	豊田高専（次期）	1	0	2	0	0	0	2	2	2	0	0	0	26	0	0	2	7	4	0	0	14	0	0	0	7	19	1	12	0	0	0	0	1	2	2	0	0	0	6	0	0	60	24	6	0	0	0	0	0
26	鳥羽商船（次期）	1	0	2	0	0	0	2	2	2	0	2	2	16	4	0	2	9	0	0	0	14	4	0	0	4	7	10	2	2	0	0	0	1	0	2	0	0	0	0	0	0	40	18	4	0	0	0	0	0
27	鈴鹿高専（次期）	1	0	2	0	0	0	2	2	2	0	2	0	26	0	0	4	12	5	0	0	22	0	0	0	5	19	11	3	0	2	0	0	1	0	2	0	0	0	2	0	2	4	60	14	8	0	0	0	0	0
28	舞鶴高専（次期）	1	0	2	0	0	0	2	2	2	0	0	0	22	2	0	4	11	3	0	0	20	2	0	0	5	9	0	2	0	0	0	0	1	0	2	0	0	0	0	0	0	50	20	6	0	0	0	0	0
29	明石高専（次期）	1	0	2	0	0	0	2	2	2	0	0	0	20	4	0	0	9	0	0	0	14	4	0	0	1	21	10	2	0	2	0	0	1	0	2	0	0	0	0	0	0	50	11	3	1	0	0	0	0
30	奈良高専（次期）	1	0	2	0	0	0	3	3	2	0	8	6	24	2	0	0	17	4	0	0	20	2	8	38	7	5	5	10	6	0	0	0	0	0	2	0	0	0	0	0	10	60	18	8	0	0	0	2	0
31	和歌山高専（次期）	1	0	2	0	0	0	2	2	2	0	0	0	26	2	0	4	13	0	0	0	24	2	0	0	2	2	0	0	0	0	0	0	1	0	2	0	0	0	2	0	0	50	11	8	0	0	0	0	0
32	米子高専（次期）	1	0	2	0	0	0	2	2	2	0	12	0	2	0	0	4	7	18	0	0	0	0	0	0	9	8	0	12	0	0	0	0	1	0	2	0	0	0	0	0	0	60	4	8	0	0	0	0	0
33	松江高専（次期）	1	0	0	2	0	0	2	2	2	0	0	2	0	16	0	0	8	0	1	0	22	0	24	0	6	0	0	0	2	0	0	0	1	0	0	0	0	0	0	1	0	60	1	4	2	0	0	6	0
34	津山高専（次期）	1	0	2	0	0	0	2	2	2	0	0	0	10	15	0	0	7	0	0	0	5	10	21	0	15	6	7	0	0	3	3	22	0	0	2	0	0	0	0	0	0	50	34	3	0	0	0	0	0
35	広島商船（次期）	1	1	2	0	0	0	2	2	2	0	0	0	12	6	0	4	8	5	1	1	10	6	5	0	5	3	2	6	1	0	0	0	0	1	2	2	0	5	1	0	0	40	12	6	0	0	0	0	0
36	呉高専（次期）	1	0	2	0	0	0	2	2	2	0	0	0	16	18	2	0	15	1	0	0	10	18	2	0	1	4	7	1	0	0	0	0	1	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
37	徳山高専（次期）	1	0	2	0	0	0	2	2	2	0	0	0	14	2	0	4	7	0	0	0	12	2	0	0	8	5	12	8	0	0	0	0	1	0	2	0	0	0	0	0	0	40	8	6	0	0	0	0	0
38	宇部高専（次期）	1	0	2	0	0	0	2	2	2	0	0	0	28	0	0	2	13	0	0	0	26	0	0	0	2	7	4	0	0	0	0	0	1	0	2	0	0	0	0	0	0	60	31	6	0	0	0	0	0
39	大島商船（次期）	1	0	2	0	0	0	2	2	2	0	2	0	16	4	0	0	7	3	0	0	10	4	0	0	15	7	0	12	0	0	0	0	1	0	2	0	0	0	0	0	0	40	8	6	0	0	0	0	0
40	阿南高専（次期）	1	0	2	0	0	0	2	2	2	0	2	4	2	32	0	0	14	0	2	0	28	0	0	0	12	11	2	0	0	0	0	0	1	0	2	1	0	0	0	0	0	50	11	9	0	0	0	0	0
41	香川高専（高松）（次期）	1	0	2	0	0	0	2	2	2	0	8	8	8	24	0	0	8	3	0	0	16	0	0	0	7	29	0	5	4	0	0	0	1	0	2	0	0	0	0	0	0	50	22	6	3	0	0	0	0
42	香川高専（詫間）（次期）	1	0	2	0	0	0	2	2	2	0	0	0	12	8	0	2	9	2	0	0	10	8	0	0	5	4	6	2	0	0	0	2	1	0	2	0	0	0	0	0	0	40	14	4	0	0	0	0	0
43	新居浜高専（次期）	1	0	2	0	3	0	2	2	2	0	0	0	20	0	3	0	8	4	0	0	16	0	2	1	18	14	0	6	0	2	0	1	1	0	2	0	0	0	6	0	0	60	11	9	0	0	0	0	1
44	弓削商船（次期）	1	0	2	0	0	0	2	2	2	0	0	0	21	4	2	0	11	1	0	0	18	4	0	0	6	31	0	1	0	1	0	0	0	0	2	0	0	0	0	0	0	40	40	0	0	0	0	0	0
45	高知高専（次期）	1	0	2	0	0	0	2	2	2	0	0	2	24	0	0	0	12	0	0	0	22	0	0	0	14	1	0	0	2	0	0	0	1	0	2	0	0	0	16	0	0	50	30	4	0	0	0	0	0
46	久留米高専（次期）	1	0	2	0	0	0	2	2	2	0	0	10	12	18	2	0	14	0	0	0	10	16	2	0	12	16	1	0	10	0	2	0	0	0	2	0	0	0	0	0	0	40	19	3	0	0	0	0	0
47	有明高専（次期）	1	0	2	0	0	0	2	2	2	0	0	0	12	12	4	2	11	2	0	0	10	12	0	2	15	23	0	2	0	0	0	0	1	0	0	0	2	0	0	0	0	60	0	12	0	0	0	0	0
48	北九州高専（次期）	1	2	0	0	0	2	2	2	2	0	32	0	0	0	0	0	15	20	10	0	0	24	0	0	11	12	1	0	0	0	0	0	1	0	2	0	0	0	0	0	0	60	3	13	0	0	0	0	0
49	佐世保高専（次期）	1	0	2	0	0	0	2	2	2	0	0	12	2	24	0	4	12	3	2	3	24	1	0	0	22	5	1	3	10	0	0	0	1	0	2	2	0	1	0	0	0	50	4	10	2	0	2	0	0
50	熊本高専（熊本）（次期）	1	0	2	0	0	0	2	2	2	0	0	0	10	10	0	4	7	7	0	4	10	0	0	0	8	32	3	8	0	0	0	0	1	0	2	0	0	0	2	0	0	40	0	8	0	0	0	0	0
51	熊本高専（八代）（次期）	1	0	0	0	0	0	2	2	2	4	0	0	12	10	0	0	11	4	0	0	12	10	0	0	5	7	9	4	0	0	0	0	1	0	2	0	0	0	0	0	0	40	26	3	0	0	0	0	0
52	大分高専（次期）	1	0	2	0	0	0	2	2	2	0	0	0	14	6	0	0	9	4	1	1	12	6	0	0	4	7	0	5	1	0	0	0	1	0	2	0	0	0	1	0	0	60	7	10	0	0	0	0	0
53	都城高専（次期）	1	0	2	0	0	0	2	2	2	2	0	0	20	0	4	0	8	0	0	0	18	0	0	0	2	21	1	4	1	0	0	0	1	0	2	0	0	0	4	1	0	50	14	10	0	0	0	0	0
54	鹿児島高専（次期）	1	0	2	0	0	0	2	2	2	0	0	0	30	8	0	0	18	2	0	0	28	8	0	0	3	1	1	2	0	0	0	0	1	0	2	0	0	0	0	0	0	60	15	8	0	0	0	0	0
55	沖縄高専（次期）	1	0	1	0	0	2	2	2	2	0	0	4	0	25	0	0	12	0	0	0	24	0	0	0	19	15	7	0	4	0	0	0	1	0	2	0	0	0	0	0	0	50	50	1	0	0	0	0	0
	機構本部事務局（八王子:竹橋）（次期）	1	0	2	0	0	0	2	2	2	0	0	0	8	0	0	0	2	0	0	0	4	0	0	0	2	4	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	26	0	6	0	0	0	0	0
		56	6	104	2	3	2	113	113	110	49	97	61	945	356	35	78	597	143	22	776	352	47	69	425	609	192	192	56	24	7	23	13	56	4	110	9	2	48	4	2	4	2825	806	369	32	4	2	6	6	1

別紙１－２　ネットワーク機器一覧（前回導入時）

2021/3/11

#	拠点名	ファイアウォール	センタースイッチ							フロントスイッチ					エッジスイッチ								サーバスイッチ					DMZスイッチ					メディアコンバータ		無線LAN						VPNルータ
			24ポート	SFP_1G-RJ45	SFP_1G-SX	SFP_1G-LX	SFP_10G-SR	SFP_10G-LR	10G銅線	48ポート	SFP_1G-SX	SFP_1G-LX	SFP_10G-SR	SFP_10G-LR	8ポート	24ポート	48ポート	SFP_1G-SX	SFP_1G-LX	非管理型8ポート	非管理型16ポート	非管理型24ポート	48ポート	SFP_1G-SX	SFP_1G-LX	SFP_10G-SR	SFP_10G-LR	8ポート	24ポート	48ポート	SFP_1G-SX	SFP_1G-LX	メディアコンバータ(SX)	メディアコンバータ(LX)	コントローラー	AP	屋外用AP	POEスイッチ	インジェクタ	24ポート
1	函館高専	1	2	2	1	14	0	0	4	9	1	14	0	0	1	24	0	0	0	0	0	0	2	0	0	0	0	1	0	0	0	0	0	0	1	40	0	7	5	0
2	苫小牧高専	1	2	2	16	0	0	0	2	6	10	0	0	0	0	5	3	8	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	6	7	0
3	釧路高専	1	2	2	20	2	0	0	4	11	22	2	2	0	1	5	6	2	0	0	0	0	2	0	0	0	0	0	1	0	0	0	0	0	1	40	0	6	8	0
4	旭川高専	1	2	2	26	0	0	0	2	13	26	0	0	0	3	1	3	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	40	0	6	14	0
5	八戸高専	1	2	10	0	16	0	0	2	11	0	22	0	0	0	47	0	0	8	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	4	22	0
6	一関高専	1	2	8	28	0	0	0	2	12	27	0	0	0	2	2	6	7	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	6	9	0
7	仙台高専（広瀬）	1	2	9	20	2	0	0	2	11	21	2	0	0	0	5	6	1	0	0	0	0	2	0	0	0	0	0	0	1	0	0	0	0	1	40	0	7	8	0
8	仙台高専（名取）	1	2	4	22	2	0	0	2	7	14	0	0	0	0	19	3	8	2	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	7	9	0
9	秋田高専	1	2	2	22	2	0	0	2	11	26	0	0	0	0	42	0	4	2	0	0	16	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	5	12	0
10	鶴岡高専	1	2	2	26	0	0	0	2	11	26	0	0	0	7	4	5	7	0	0	0	0	2	3	0	0	0	0	1	0	0	0	0	0	1	40	0	6	6	0
11	福島高専	1	2	2	25	2	0	0	4	11	25	0	0	0	3	3	1	2	2	0	0	0	2	0	0	0	0	0	0	1	0	0	2	0	1	40	0	5	14	0
12	茨城高専	1	2	4	20	8	0	0	2	13	19	6	0	0	3	4	2	3	2	0	0	3	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	6	8	0
13	小山高専	1	2	4	14	6	0	0	2	9	14	4	0	0	0	18	6	0	2	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	2	30	0
14	群馬高専	1	2	2	18	0	0	0	2	9	23	1	0	0	5	32	0	9	1	0	0	0	1	1	0	0	0	0	1	0	0	0	1	0	1	40	0	3	24	0
15	木更津高専	1	2	2	0	24	0	0	4	12	0	24	0	0	0	54	1	0	0	0	0	0	2	0	0	0	0	0	1	0	0	0	0	0	1	40	0	5	18	0
16	東京高専	1	2	4	20	4	0	0	2	5	10	0	0	0	3	5	6	10	4	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	8	5	0
17	長岡高専	1	2	4	18	0	0	0	2	10	18	0	0	0	0	11	9	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	7	7	0
18	富山高専（本郷）	1	2	4	14	2	0	0	2	8	20	3	0	0	0	29	8	8	3	0	0	0	3	1	2	0	0	1	0	0	0	0	1	0	1	40	0	6	15	0
19	富山高専（射水）	1	2	4	28	0	0	0	2	15	28	0	0	0	0	6	26	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	4	19	0
20	石川高専	1	2	2	17	6	0	0	6	10	18	4	0	0	0	26	1	3	2	0	0	0	3	0	0	0	0	0	1	0	0	0	0	0	1	40	0	7	1	0
21	福井高専	1	2	2	24	0	0	0	2	12	25	0	0	0	5	18	0	1	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	6	12	0
22	長野高専	1	2	4	16	2	0	0	2	10	16	2	0	0	6	1	2	6	0	0	0	0	1	0	0	0	0	0	1	0	0	0	6	0	1	40	0	6	11	0
23	岐阜高専	1	2	2	22	0	0	0	2	9	18	0	0	0	0	31	0	2	0	0	0	0	2	2	0	0	0	0	1	0	1	0	0	0	1	40	0	3	25	0
24	沼津高専	1	2	2	18	0	0	0	2	9	19	0	0	0	0	27	1	7	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	40	0	6	10	0
25	豊田高専	1	1	1	4	0	12	0	0	7	9	0	10	0	0	30	2	12	0	0	0	0	1	2	0	2	0	0	0	0	0	0	5	0	1	40	0	4	22	0
26	鳥羽商船	1	2	2	20	0	0	0	2	9	18	0	0	0	1	8	10	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	40	3	3	23	2
27	鈴鹿高専	1	2	4	22	0	0	0	2	12	25	0	0	0	0	22	14	4	0	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0	1	40	0	5	19	0
28	舞鶴高専	1	2	2	20	2	0	0	4	10	20	0	0	0	1	14	0	0	2	0	0	0	2	0	0	0	0	0	1	0	0	0	0	0	1	40	0	6	13	0
29	明石高専	1	2	2	16	4	0	0	2	9	14	4	0	0	1	28	10	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	40	0	5	11	0
30	奈良高専	1	2	2	22	4	0	0	2	10	20	0	0	0	0	8	8	2	4	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	40	0	5	15	0
31	和歌山高専	1	2	2	22	2	0	0	2	12	22	2	0	0	1	1	0	1	0	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	1	40	0	6	12	0
32	米子高専	1	2	2	12	0	0	0	2	7	17	0	0	0	5	13	0	11	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	6	8	0
33	松江高専	1	2	2	2	14	0	0	2	7	0	14	0	0	0	13	1	4	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	40	0	5	14	0
34	津山高専	1	2	2	4	12	0	0	2	8	5	12	0	0	0	29	0	5	1	0	0	0	1	2	1	0	0	0	1	0	0	0	0	0	1	40	0	0	0	0
35	広島商船	1	2	2	10	6	0	0	2	8	15	7	0	0	2	6	3	6	1	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0	1	40	0	6	12	0
36	呉高専	1	2	4	14	14	0	0	2	14	11	14	0	0	0	14	3	1	0	0	0	0	2	2	0	0	0	0	1	0	0	0	0	0	1	40	0	8	0	0
37	徳山高専	1	2	2	10	2	2	0	4	7	11	4	2	0	4	9	17	2	2	0	0	0	2	1	0	0	0	0	0	0	0	0	0	0	1	40	0	6	8	0
38	宇部高専	1	2	2	24	0	0	0	2	12	24	0	0	0	0	7	6	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	3	23	0
39	大島商船	1	2	2	16	4	0	0	2	7	13	4	0	0	9	15	0	15	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	6	10	0
40	阿南高専	1	2	2	0	24	0	0	4	12	0	24	0	0	1	21	2	0	0	0	0	0	2	0	0	0	0	0	1	0	0	0	0	0	1	40	0	5	18	0
41	香川高専（高松）	1	2	2	4	16	0	0	2	8	6	12	0	0	1	34	0	6	4	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	6	12	0
42	香川高専（詫間）	1	2	2	10	8	0	0	2	9	12	8	0	0	8	3	11	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	40	0	2	30	0
43	新居浜高専	1	2	2	16	0	0	0	2	8	21	0	0	0	7	25	0	9	0	0	0	0	1	0	0	0	0	0	1	0	0	0	4	0	1	40	0	6	11	0
44	弓削商船	1	2	2	18	4	0	0	2	12	19	4	0	0	0	38	0	1	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	0	40	0
45	高知高専	1	2	2	20	2	0	0	2	11	20	0	0	0	26	1	1	0	2	0	0	0	1	0	0	0	0	0	1	0	0	0	16	0	1	40	0	4	20	0
46	久留米高専	1	2	2	10	28	0	0	2	15	10	18	0	0	5	26	0	0	10	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	5	19	0
47	有明高専	1	2	2	10	12	0	0	2	10	11	10	0	0	0	38	0	2	0	0	0	0	2	1	2	0	0	0	0	0	0	0	0	0	1	40	0	8	0	0
48	北九州高専	1	2	2	20	10	0	0	2	15	20	10	0	0	0	27	3	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	8	2	0
49	佐世保高専	1	2	2	12	12	0	2	2	7	6	8	0	3	7	25	5	11	4	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0	1	40	0	6	10	0
50	熊本高専（熊本）	1	2	2	14	0	0	0	4	6	16	0	0	0	0	42	3	7	0	0	0	0	3	3	0	0	0	0	1	0	0	0	2	0	1	40	0	8	0	0
51	熊本高専（八代）	1	2	2	12	8	0	2	4	10	13	8	0	2	0	12	14	5	0	0	0	0	2	0	0	0	0	0	1	0	0	0	0	0	1	40	0	3	26	0
52	大分高専	1	2	2	10	6	0	0	4	8	14	7	0	0	3	6	2	5	1	0	0	0	2	0	0	0	0	1	0	0	0	0	1	0	1	40	0	7	10	0
53	都城高専	1	2	2	18	0	0	0	4	8	18	0	0	0	2	21	1	5	0	1	14	12	3	2	0	0	0	0	1	0	0	0	1	0	1	40	0	6	11	0
54	鹿児島高専	1	2	2	24	8	0	0	4	16	26	8	0	0	0	0	8	2	0	0	0	0	2	0	0	0	0	0	1	0	0	0	0	0	1	40	0	4	19	0
55	沖縄高専	1	2	2	0	16	0	0	2	6	0	12	0	0	18	26	1	0	4	37	0	28	1	0	0	0	0	0	1	0	0	0	0	0	1	40	0	7	4	0
56	機構本部事務局（八王子-竹橋）	1	0	0	0	0	0	0	0	2	0	0	0	0	0	0	7	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	17	0	3	0	0
	合計	**56**	**109**	**150**	**851**	**310**	**14**	**4**	**136**	**546**	**862**	**274**	**14**	**5**	**141**	**981**	**227**	**210**	**63**	**38**	**15**	**59**	**79**	**21**	**5**	**2**	**0**	**3**	**40**	**2**	**1**	**0**	**42**	**0**	**56**	**2217**	**3**	**296**	**721**	**2**

（別紙２）更新作業スケジュール

2027 年度

4 月

日	月	火	水	木	金	土
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

5 月

日	月	火	水	木	金	土
						1 本部 東京高専
2 本部 東京高専	3 本部 東京高専	4 本部 東京高専	5 本部 東京高専	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

6 月

日	月	火	水	木	金	土
		1	2	3	4	5
6	7	8	9	10	11	12 長野高専
13 長野高専	14 長野高専	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

7 月

日	月	火	水	木	金	土
				1	2	3 都城高専
4 都城高専	5 都城高専	6	7	8	9	10
11	12	13	14	15	16	17 茨城高専 秋田高専
18 茨城高専 秋田高専	19 茨城高専 秋田高専	20	21	22	23 釧路高専	24 釧路高専
25 釧路高専	26	27	28	29	30	31

8 月

日	月	火	水	木	金	土
1	2	3	4	5	6 沼津高専	7 沼津高専 函館高専
8 沼津高専 函館高専	9 岐阜高専 函館高専	10 岐阜高専 苫小牧高専	11 岐阜高専 苫小牧高専	12 苫小牧高専	13 富山高専 石川高専	14 富山高専 石川高専
15 富山高専 石川高専	16 富山高専 明石高専	17 富山高専 明石高専	18 富山高専 明石高専	19	20 大分高専	21 大分高専 有明高専
22 大分高専 有明高専	23 仙台高専 有明高専	24 仙台高専 舞鶴高専	25 仙台高専 舞鶴高専	26 仙台高専 舞鶴高専	27 仙台高専 熊本高専	28 仙台高専 熊本高専
29 沖縄高専 熊本高専	30 沖縄高専 熊本高専	31 沖縄高専 熊本高専				

9 月

日	月	火	水	木	金	土
			1 熊本高専	2 大島商船	3 大島商船	4 久留米高専 大島商船
5 久留米高専	6 久留米高専	7 鳥羽商船	8 鳥羽商船 宇部高専	9 鳥羽商船 宇部高専	10 宇部高専	11 高知高専
12 広島商船 高知高専	13 広島商船 高知高専	14 広島商船 呉高専	15 呉高専	16 香川高専 呉高専	17 香川高専	18 香川高専 津山高専
19 香川高専 津山高専	20 香川高専 津山高専	21 香川高専	22 群馬高専	23 群馬高専	24 群馬高専 奈良高専	25 徳山高専 奈良高専
26 徳山高専 奈良高専	27 徳山高専	28	29	30		

10 月

日	月	火	水	木	金	土
					1	2
3	4	5	6	7	8	9 北九州高専 佐世保高専
10 北九州高専 佐世保高専	11 北九州高専 佐世保高専	12	13	14	15 松江高専	16 松江高専 米子高専
17 松江高専 米子高専	18 米子高専	19	20 小山高専	21 小山高専	22 小山高専 長岡高専	23 長岡高専
24 長岡高専	25	26	27	28	29 鹿児島高専	30 鹿児島高専
31 鹿児島高専						

11 月

日	月	火	水	木	金	土
	1 鈴鹿高専	2 鈴鹿高専	3 木更津高専 鈴鹿高専	4 木更津高専	5 木更津高専 一関高専	6 福井高専 一関高専
7 福井高専 一関高専	8 福井高専	9	10	11	12	13 福島高専
14 福島高専	15 福島高専	16	17	18	19	20 八戸高専 和歌山高専
21 八戸高専 和歌山高専	22 八戸高専 和歌山高専	23	24	25	26	27
28	29	30				

12 月

日	月	火	水	木	金	土
			1	2	3	4
5	6	7	8	9	10 豊田高専	11 豊田高専
12 豊田高専	13	14	15	16	17	18 旭川高専 阿南高専
19 旭川高専 阿南高専	20 旭川高専 阿南高専	21	22	23	24	25 鶴岡高専 新居浜高専
26 鶴岡高専 新居浜高専	27 鶴岡高専 新居浜高専	28	29	30	31	

1 月

日	月	火	水	木	金	土
						1
2	3	4	5	6	7	8 弓削商船
9 弓削商船	10 弓削商船	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

2 月

日	月	火	水	木	金	土
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29				

3 月

日	月	火	水	木	金	土
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

（別紙3）各拠点及び機構本部所在地一覧

番号	高専名	住所
01	函館高専	北海道函館市戸倉町14-1
02	苫小牧高専	北海道苫小牧市字錦岡443
03	釧路高専	北海道釧路市大楽毛西2-32-1
04	旭川高専	北海道旭川市春光台2条2-1-6
05	八戸高専	青森県八戸市大字田面木字上野平16-1
06	一関高専	岩手県一関市萩荘字高梨
07	仙台高専（広瀬）	宮城県仙台市青葉区愛子中央4-16-1
07	仙台高専（名取）	宮城県名取市愛島塩手字野田山48
08	秋田高専	秋田県秋田市飯島文京町1-1
09	鶴岡高専	山形県鶴岡市井岡字沢田104
10	福島高専	福島県いわき市平上荒川字長尾30
11	茨城高専	茨城県ひたちなか市中根866
12	小山高専	栃木県小山市大字中久喜771
13	群馬高専	群馬県前橋市鳥羽町580
14	木更津高専	千葉県木更津市清見台東2-11-1
15	東京高専	東京都八王子市椚田町1220-2
16	長岡高専	新潟県長岡市西片貝町888
17	富山高専（本郷）	富山県富山市本郷町13
17	富山高専（射水）	富山県射水市海老江練合1-2
18	石川高専	石川県河北郡津幡町北中条タ1
19	福井高専	福井県鯖江市下司町
20	長野高専	長野県長野市徳間716
21	岐阜高専	岐阜県本巣市上真桑2236-2
22	沼津高専	静岡県沼津市大岡3600
23	豊田高専	愛知県豊田市栄生町2-1
24	鳥羽商船	三重県鳥羽市池上町1-1
25	鈴鹿高専	三重県鈴鹿市白子町
26	舞鶴高専	京都府舞鶴市字白屋234
27	明石高専	兵庫県明石市魚住町西岡679-3
28	奈良高専	奈良県大和郡山市矢田町22
29	和歌山高専	和歌山県御坊市名田町野島77
30	米子高専	鳥取県米子市彦名町4448
31	松江高専	島根県松江市西生馬町14-4
32	津山高専	岡山県津山市沼624-1

番号	高専名	住所
33	広島商船	広島県豊田郡大崎上島町東野4272-1
34	呉高専	広島県呉市阿賀南2-2-11
35	徳山高専	山口県周南市学園台
36	宇部高専	山口県宇部市常盤台2-14-1
37	大島商船	山口県大島郡周防大島町大字小松1091-1
38	阿南高専	徳島県阿南市見能林町青木265
39	香川高専(高松)	香川県高松市勅使町355
39	香川高専(詫間)	香川県三豊市詫間町香田551
40	新居浜高専	愛媛県新居浜市八雲町7-1
41	弓削商船	愛媛県越智郡上島町弓削下弓削1000
42	高知高専	高知県南国市物部乙200-1
43	久留米高専	福岡県久留米市小森野1-1-1
44	有明高専	福岡県大牟田市東萩尾町150
45	北九州高専	福岡県北九州市小倉南区志井5-20-1
46	佐世保高専	長崎県佐世保市沖新町1-1
47	熊本高専(熊本)	熊本県合志市須屋2659-2
47	熊本高専(八代)	熊本県八代市平山新町2627
48	大分高専	大分県大分市大字牧1666
49	都城高専	宮崎県都城市吉尾町473-1
50	鹿児島高専	鹿児島県霧島市隼人町真孝1460-1
51	沖縄高専	沖縄県名護市字辺野古905
52	高専本部(八王子)	東京都八王子市東浅川町701-2
52	高専本部(竹橋)	東京都千代田区一ツ橋2-1-2　学術総合センター11F

（別紙４）

用語集

調達仕様書及び別紙に記述する主な用語を以下に示す。

No.	用語	定義
1	エッジスイッチ	建屋各フロアに設置され、各フロア設置機器とフロントスイッチを中継するスイッチ。アクセススイッチともいう。
2	NII	独立行政法人国立情報学研究所（National Institute of Informatics）の略称。大学共同利用機関法人情報・システム研究機構を構成する機関の一つであり、「SINET」の運営組織。
3	各拠点	本調達仕様書では、実際に機器が導入される 51 国立高専の 55 キャンパスを指す。
4	機構本部	本調達仕様書では、高専機構本部事務局を指す。
5	既設設備	各拠点及び機構本部が保有しているシステム及び機器等。
6	高専機構	本調達仕様書では、独立行政法人国立高等学校機構にて本プロジェクトの管理・運営を実施する部門を指す。
7	高専共通システム	主に教職員が利用する Web 給与明細、旅費等の各種アプリケーション。
8	高専統一ネットワークシステム	高専機構における機器や構成、サービス等を標準化したネットワークシステム。令和 10 年 4 月運用開始に向けて更新する。
9	高度化再編校	平成 21 年、宮城、富山、香川、熊本の 4 地区において、近隣の二つの高専が統合され、二つのキャンパスを持つ高専が誕生した。これを高度化再編校という。高度化再編校は、以下の 4 校となる。 ・仙台高専（広瀬キャンパス、名取キャンパス） ・富山高専（本郷キャンパス、広瀬キャンパス） ・香川高専（高松キャンパス、詫間キャンパス） ・熊本高専（熊本キャンパス、八代キャンパス）
10	サーバスイッチ	キャンパス内部向けサービスを、提供するサーバ群を束ねるスイッチ。
11	SINET	NII が運営している日本全国の大学、研究機関等の学術情報基盤ネットワーク網。
12	SINET アクセス回線	各拠点及び機構本部のネットワークを外部ネットワーク SINET に接続するための回線。
13	SINET データセンタ	SINET の地域拠点となる接続施設。
14	センタースイッチ	各拠点の LAN の中心にあり、同一セグメント内通信以外の全ての通信を中継するスイッチ。コアスイッチともいう。

No.	用語	定義
15	データセンタ	SINET データセンタ又は SINET データセンタと相互接続する IaaS 又は SaaS 等データセンタを指す。
16	DMZ スイッチ	DMZ 領域に配置されたサーバ群を束ねるスイッチ。
17	フロントスイッチ	各建屋に 1 台ずつ置かれ、センタースイッチとエッジスイッチを中継するスイッチ。ディストリビューションスイッチともいう。