

高専統一ネットワークシステム整備一式

仕様書

令和3年8月

独立行政法人 国立高等専門学校機構

目次

1. 調達件名	1
2. 本調達の概要	1
2.1 目的	1
2.1.1 本調達の背景と概要	1
2.2 契約期間	1
2.3 高専ネットワークシステムの概要	2
2.3.1 ネットワークの概要	2
3. 情報システム稼働環境	4
3.1 全体構成	4
3.1.1 全体構成	4
3.1.2 共通要件	4
3.2 ネットワーク機器個別要件	5
3.3 各高専個別要件	5
3.4 セキュリティ(UTM)機能個別要件	5
3.5 サーバ機器個別要件	6
3.6 ネットワーク基盤サービス個別要件	7
3.7 ユーザ認証基盤サービス個別要件	7
3.7.1 各キャンパス用及び機構本部用認証システム要件	7
3.8 その他サービス個別要件	11
3.9 eduroam 構築要件	11
3.10 SSL-VPN 構築要件	11
3.11 既存無線 LAN アクセスポイント追加要件	11
4. 接続作業	12
4.1 前提	12
4.2 現地調査・打合せ	12
4.3 接続作業	12
4.3.1 全般	12
4.3.2 本調達で必要なパッチケーブル	13
4.4 電源工事	14
4.5 ラックへの設置	14
4.6 無線 LAN アクセスポイントの設置	14
4.7 既設機器への対応	15

4.8 その他.....	15
5. 移行要件.....	16
5.1 移行業務要件.....	16
5.1.1 全般.....	16
5.1.2 移行計画の策定.....	17
5.1.3 移行設計.....	17
5.1.4 移行手順の作成.....	17
5.1.5 移行リハーサル.....	17
5.1.6 移行判定.....	17
5.1.7 移行作業.....	18
5.1.8 移行における体制.....	18
5.2 移行期間.....	19
5.2.1 移行・切替のスケジュール.....	19
5.2.2 移行単位.....	19
5.3 教育に関する要件.....	21
5.3.1 対象者.....	21
5.3.2 教育計画の策定.....	21
5.3.3 教育内容.....	22
5.3.4 マニュアル作成.....	22
5.3.5 教育時期.....	22
5.3.6 教育場所.....	23
6. 信頼性等の要件.....	24
6.1 信頼性要件.....	24
6.1.1 可用性.....	24
6.1.2 完全性.....	24
6.1.3 機密性.....	24
6.2 拡張性要件.....	24
6.3 上位互換性要件.....	24
6.4 システム中立性要件・事業継続性要件.....	24
7. 情報セキュリティ要件.....	25
7.1 共通方針.....	25
7.2 システムの情報セキュリティ対策.....	25
7.2.1 脆弱性対策.....	25
7.2.2 データ保護.....	25
7.2.3 アクセスログ管理.....	25
7.3 本調達業務の遂行等に係る情報セキュリティ対策.....	26
7.3.1 情報セキュリティ侵害が発生した場合の対処.....	26

7.3.2	機密保護	26
7.3.3	データ管理.....	26
7.3.4	その他のセキュリティ対策	26
8.	運用保守業務要件.....	27
8.1	運用保守業務の範囲.....	27
8.2	運用保守実施計画の策定.....	27
8.3	運用業務支援	27
8.3.1	サービスデスク業務要件.....	27
8.4	製品保守	28
8.4.1	製品保守共通要件	28
8.4.2	ハードウェア保守要件	29
8.4.3	ソフトウェア保守要件	30
8.5	各高専による保守・運用のオプション追加対応.....	30
9.	体制及び方法.....	32
9.1	作業実施体制	32
9.1.1	体制概要	32
9.1.2	体制内の役割	33
9.2	作業要員に求める資格等の要件	33
9.2.1	全般	33
9.2.2	統括責任者.....	33
9.2.3	各チームリーダー	34
9.2.4	各システム担当者	34
9.3	プロジェクト管理.....	34
9.3.1	全般	34
9.3.2	進捗管理	35
9.3.3	課題管理	35
9.3.4	QA 管理.....	35
9.3.5	品質管理	35
9.3.6	リスク管理.....	36
9.3.7	会議体.....	36
9.4	構築計画の策定.....	36
9.5	設計	36
9.5.1	全般	36
9.5.2	現状調査	37
9.5.3	基本設計	37
9.5.4	詳細設計	38
9.6	構築.....	39

9.6.1	事前構築	39
9.6.2	本番環境構築	39
9.7	本番切替	39
9.7.1	本番切替の要件	40
9.7.2	本節における本番切替の定義	40
9.8	導入支援	40
9.9	撤去	41
9.10	検収	42
9.11	作業場所	42
9.12	仕様書不適合責任	42
9.13	各高専による役務のオプション追加対応	43
10.	特記事項	45
10.1	役割分担	45
10.2	入札参加資格に係る事項	45
10.2.1	入札参加要件	45
10.2.2	応札者の実績	45
10.2.3	複数事業者による共同提案	45
10.3	知的財産権の帰属	46
10.4	遵守事項	46
10.4.1	契約条件	46
10.4.2	作業管理上の遵守事項	46
10.5	環境への配慮	47
10.5.1	グリーンコンピューティング（グリーン IT）への対応	47
10.6	下請負に関する事項	47
10.6.1	下請負の制限及び下請負を認める場合の条件	47
10.6.2	承認手続	47
10.7	その他特記事項	47

別 添 資 料

- 1 要件一覧（ネットワーク系）
- 1b 要件一覧（ネットワーク系／各高専個別）
- 2 要件一覧（UTM）
- 3 要件一覧（サーバ系）
- 3b ログ収集・バックアップ取得対象一覧
- 4 ネットワーク機器一覧
- 5 受託者の役割
- 6 全国高専キャンパス所在地一覧
- 7 用語集

1. 調達件名

「高専統一ネットワークシステム整備一式」

2. 本調達の概要

2.1 目的

2.1.1 本調達の背景と概要

平成 30 年度の高専統一ネットワークシステム整備では、全国 51 高専および機構本部において、ファイアウォールやスイッチ等のネットワーク機器、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、ネットワークのドメイン管理やユーザ認証管理等を行う各種サーバ、またこれら全ての機器の運用・保守にかかる役務の調達を行った。

今回の調達においても、前回同様、スケールメリットを活かした戦略的なネットワークシステムの整備や運用を求めて高専統一ネットワークシステム整備を行う。

本調達仕様書は、令和 5 年度を目途に実施されるこの次期「高専統一ネットワークシステム」の導入・移行・保守・運用等にかかる委託業務の内容を定めたものである。実際の導入・移行作業は、図 1 のとおり、令和 4 年度以降、約 1 年間をかけて段階的に行う計画とする。

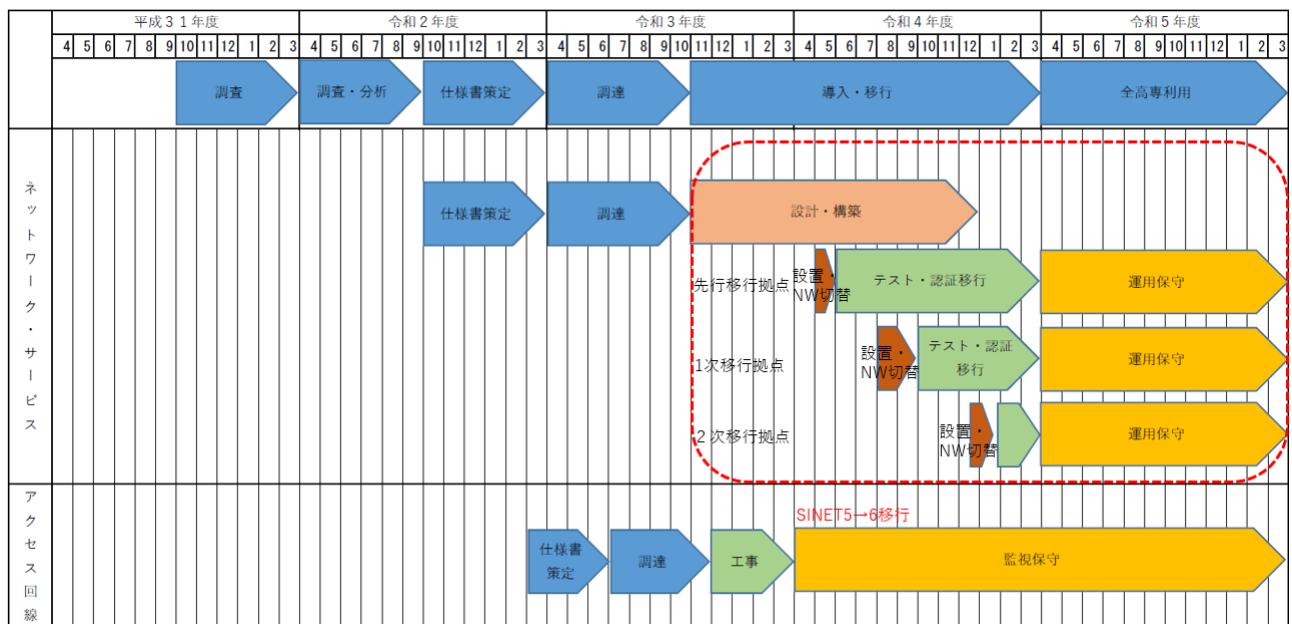


図 1.スケジュール概要

現行ネットワークシステムから次期ネットワークシステムへの移行は、令和 4 年度に三つのフェーズ（5 月連休、夏季休暇、冬季休暇）に分けて実施することを想定しているが、落札業者との協議により決定する。

2.2 契約期間

契約期間は、契約締結日から令和 10 年 3 月 31 日までとする。

なお、導入・移行作業については、契約締結日から令和 5 年 3 月 31 日までに完了させ、運用可能な状態にすること。

2.3 高専ネットワークシステムの概要

2.3.1 ネットワークの概要

(1) 現行ネットワークシステムの概要

現在、各高専におけるネットワークシステムは平成30年度の高専統一ネットワークシステム整備一式や SINET5 アクセス回線一式の調達を実施し、共通のネットワーク機器、標準化されたネットワーク構成、外部接続回線を導入した。ただし、VLAN の構成やネットワーク認証等の利用形態については特に統一されておらず、各校毎の実情に合わせて利用しているのが現状であり、ネットワークシステムの論理的設計やネットワーク認証等については高専毎に異なっている。

現行ネットワークシステムの例

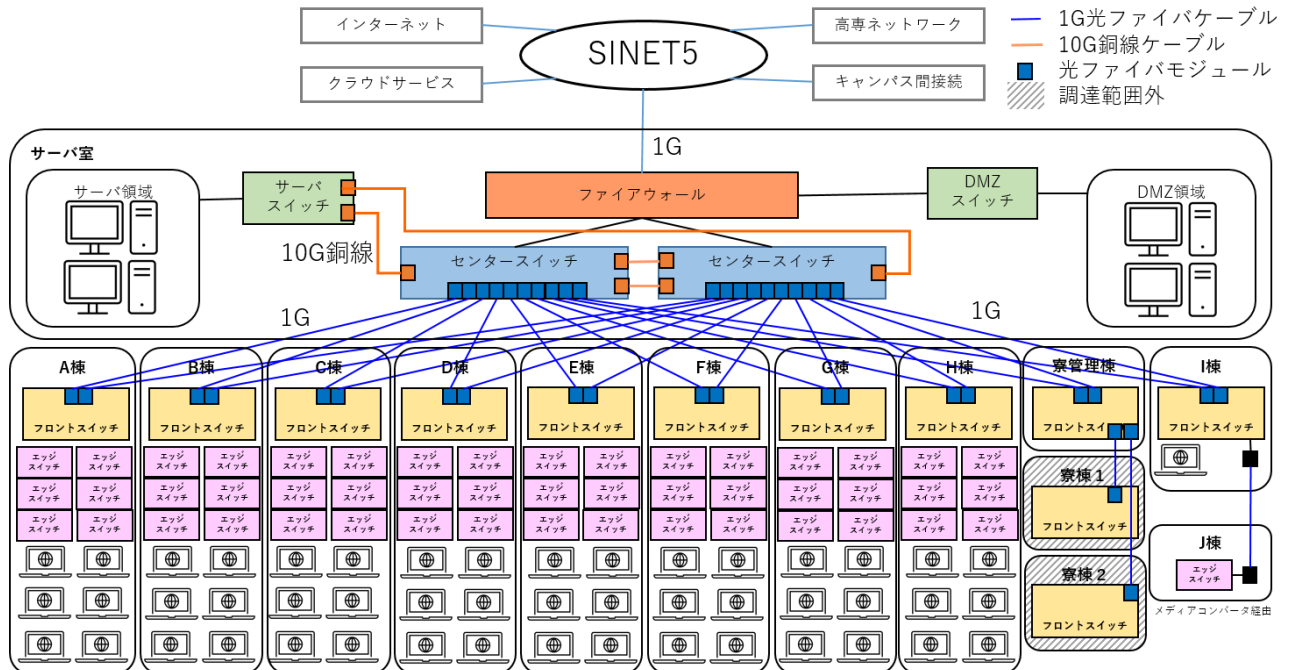


図 2. 現行ネットワークシステムの例

(2) 次期ネットワークの概要

機構では、現行ネットワークシステムにおける課題を整理した上で、GIGA スクール構想や情報セキュリティを高めたネットワーク、独立行政法人の情報セキュリティ対策の調整を行っている第二GSOCの基本サービスに対応していくことを検討し、高専統一ネットワークシステム整備の基本方針を定めていく。

高専ネットワークシステム整備に関する基本方針を以下に示す。

- ① センタースイッチとフロントスイッチ間を 10Gbps 以上とする。
- ② フロントスイッチとエッジスイッチ及び PoE スイッチ間を 1Gbps 以上とする。
- ③ PoE スイッチと無線 LAN アクセスポイント間を 1Gbps 以上とする。
- ④ 全高専で校内ネットワーク接続時には何かの認証を行うことを必須とする。
- ⑤ 各高専の担当者の負荷の軽減に向けたネットワーク管理ツールの導入を行う。
ネットワーク管理ツールとしては次のことを単一または組合せにより実現する。
 - ・ダイナミック VLAN に対応した認証設定(.1x / PSK / WEB 各認証)
 - ・下記ネットワーク機器の SNMP 情報可視化・設定情報の可視化及び設定変更
 - センタースイッチ
 - フロントスイッチ
 - エッジスイッチ(非管理型エッジスイッチ除く)
 - サーバスイッチ/DMZ 用スイッチ
 - 無線 LAN アクセスポイント
 - PoE スイッチ
 - ・無線 LAN コントローラ(WLC)機能
 - ・MAC アドレス自動収集・登録機能
- ⑥ SINET データセンターにログ集約サーバを設置し、全高専の通信ログ、および IDS/IPS のログを集約する。
- ⑦ 指定された TAXII サーバから TAXII プロトコルを用いた IoC 情報を取得し、各高専の IDS/IPS 用に変換するシステムを導入する。TAXII バージョンは「1.1」に対応すること、STIX バージョンは「1.1.1(STIX1)」、「2.0(STIX2)」に対応すること。TAXII サーバに IoC 情報取得リクエストを HTTPS(443/TCP)を使って送信すること。
- ⑧ 上記に定める各種機能の利用・管理にあたって、ライセンスが必要な場合は、用意することとする。

3. 情報システム稼働環境

3.1 全体構成

3.1.1 全体構成

本調達の全体構成を下図に示す。

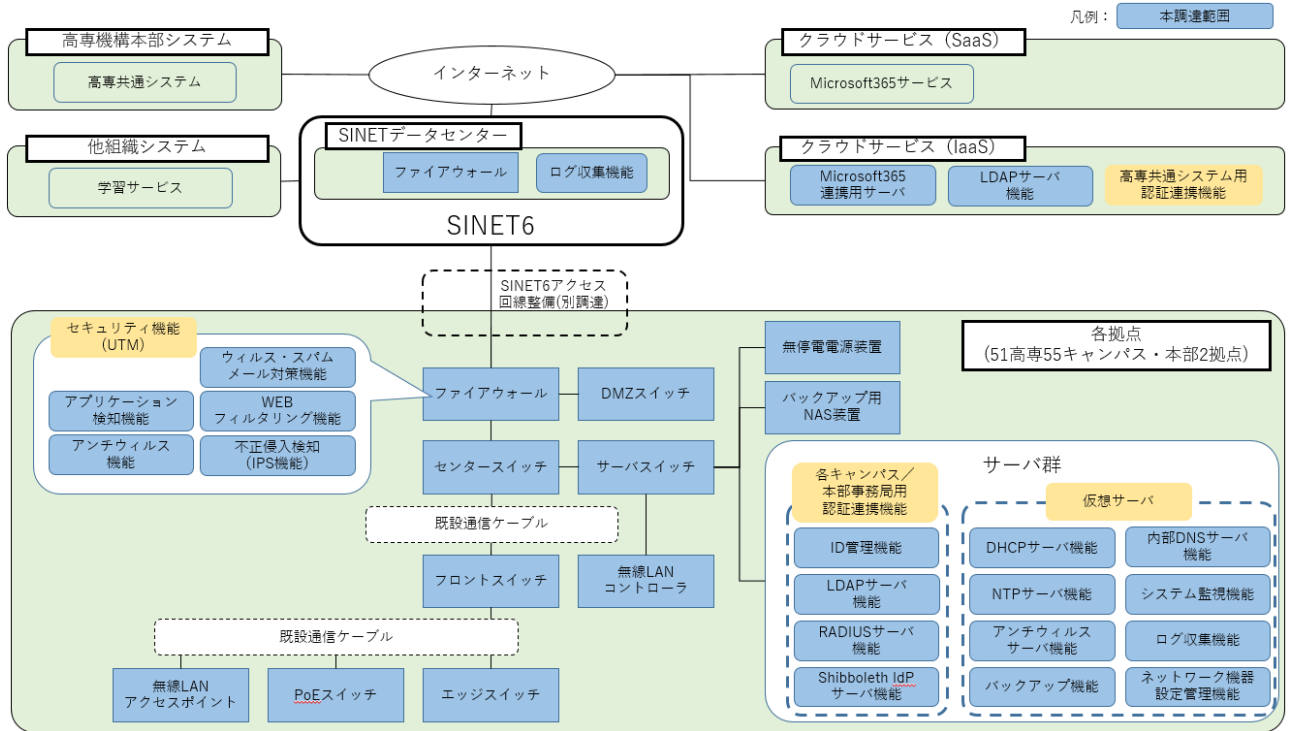


図 3.全体構成

3.1.2 共通要件

(1) ネットワーク機器共通要件

別添資料 1 「要件一覧(ネットワーク系)」を参照のこと。

(2) 無線 LAN システム機器共通要件

別添資料 1 「要件一覧(ネットワーク系)」を参照のこと。

(3) サーバ機器共通要件

別添資料 3 「要件一覧(サーバ系)」を参照のこと。

3.2 ネットワーク機器個別要件

要件については別添資料1「要件一覧(ネットワーク系)」を参照のこと。

また導入機器の高専毎の員数については別添資料4「ネットワーク機器一覧」を参照のこと。

3.3 各高専個別要件

特定の高専については固有の要件が存在する。別添資料1「要件一覧(各高専個別)」を参照のこと。

3.4 セキュリティ(UTM)機能個別要件

ファイアウォールに搭載を想定する機能としてのセキュリティ(UTM)は別添資料2「要件一覧(UTM)」を参照のこと。

3.5 サーバ機器個別要件

以下に各キャンパス及び本部事務局用のサーバ関連の全体システム構成を示す。
要件内容は別添資料3「サーバ機器一覧」を参照のこと。

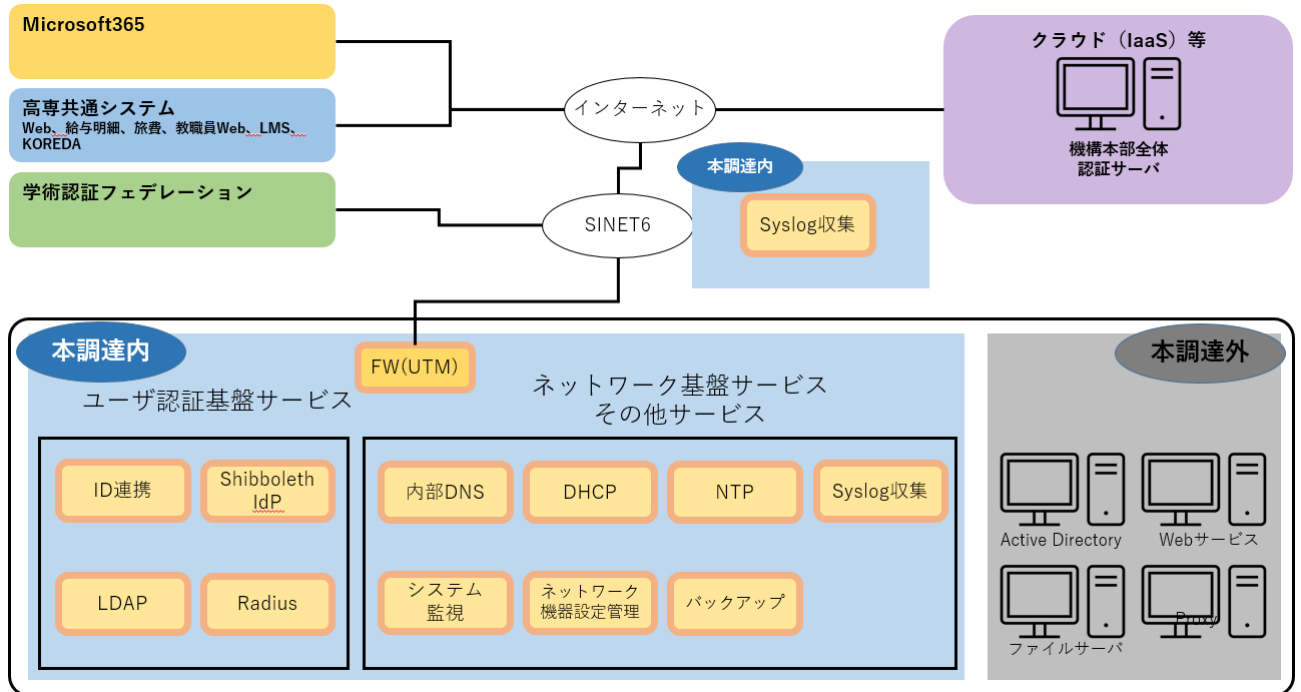


図 4 全体システム構成（サーバ系）

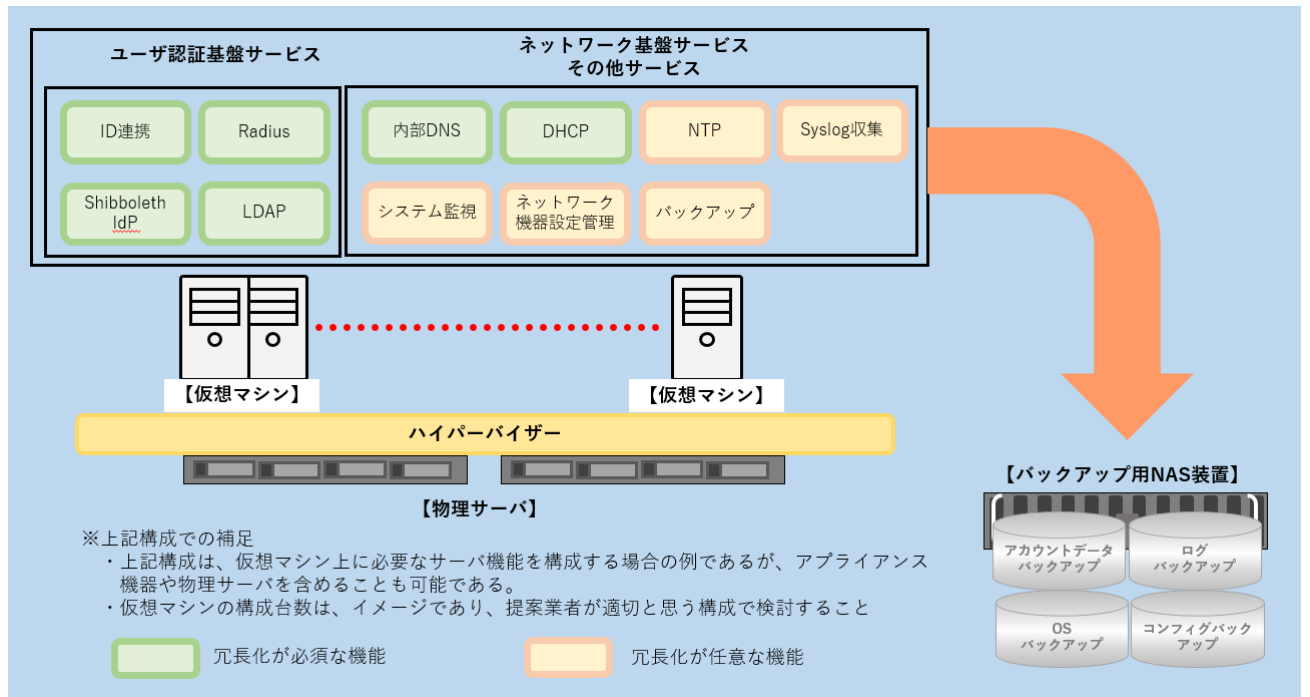


図 5 各キャンパス及び本部事務局配置サーバの想定構成

3.6 ネットワーク基盤サービス個別要件

別添資料3「サーバ機器一覧」を参照のこと。

3.7 ユーザ認証基盤サービス個別要件

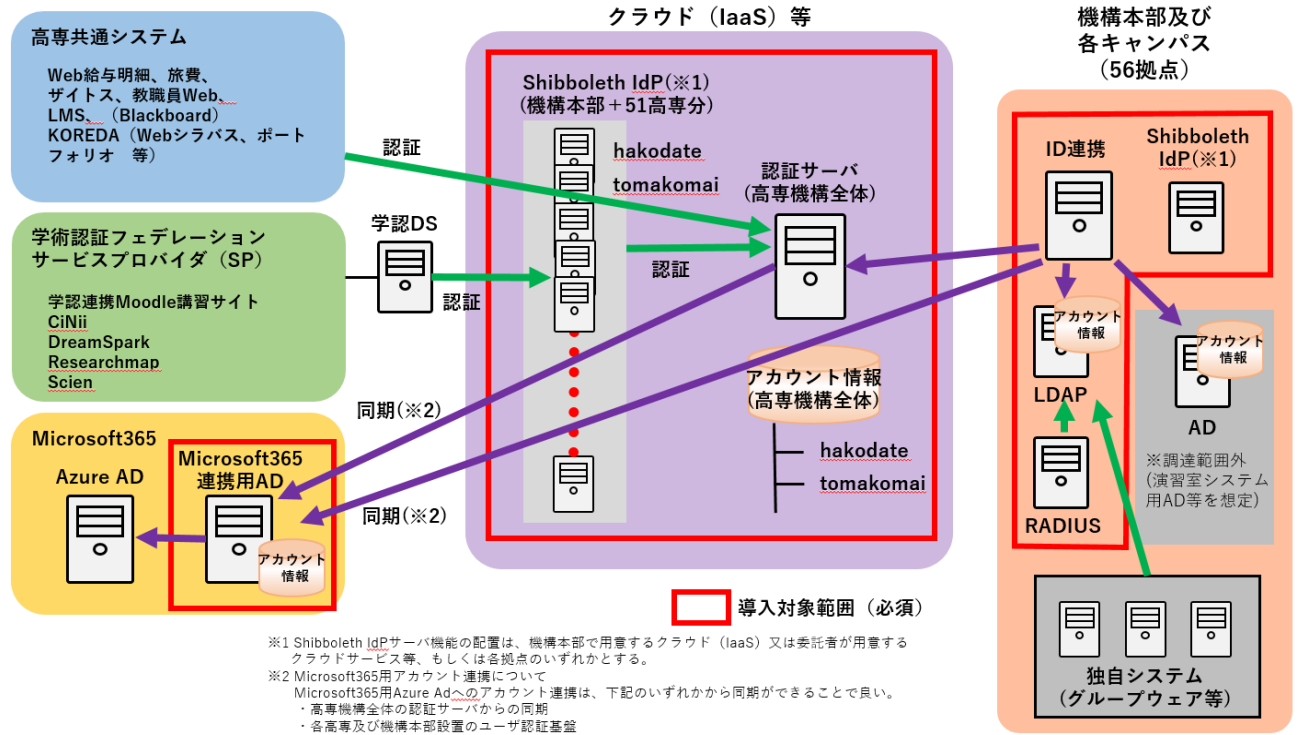


図 6 認証連携の全体システムイメージ

3.7.1 各キャンパス用及び機構本部用認証システム要件

各キャンパス及び本部事務局に設置するユーザ認証基盤システムに必要な要件を記載する。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はないため、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。

内容は別添資料3「サーバ機器一覧」を参照のこと。

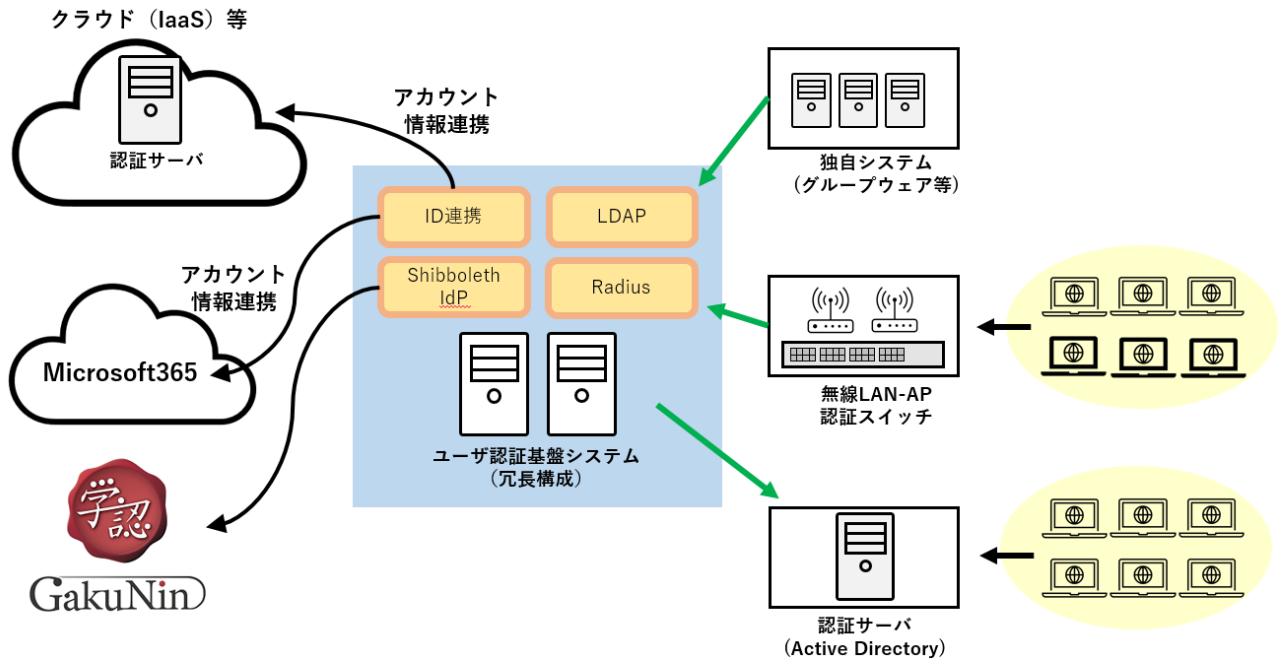


図 7.認証サーバ構成 (各キャンパス及び機構本部用) 共通要件

(1) 共通要件

別添資料 3 「サーバ機器一覧」を参照のこと。

(2) 認証機能要件

別添資料 3 「サーバ機器一覧」を参照のこと。

(3) ネットワーク認証機能要件

別添資料 3 「サーバ機器一覧」を参照のこと。

(4) 国立情報学研究所の学術認証フェデレーション連携要件 (Shibboleth IdP 要件)

別添資料 3 「サーバ機器一覧」を参照のこと。

(5) Microsoft365 連携要件

Microsoft365 連携の例を以下に示す。

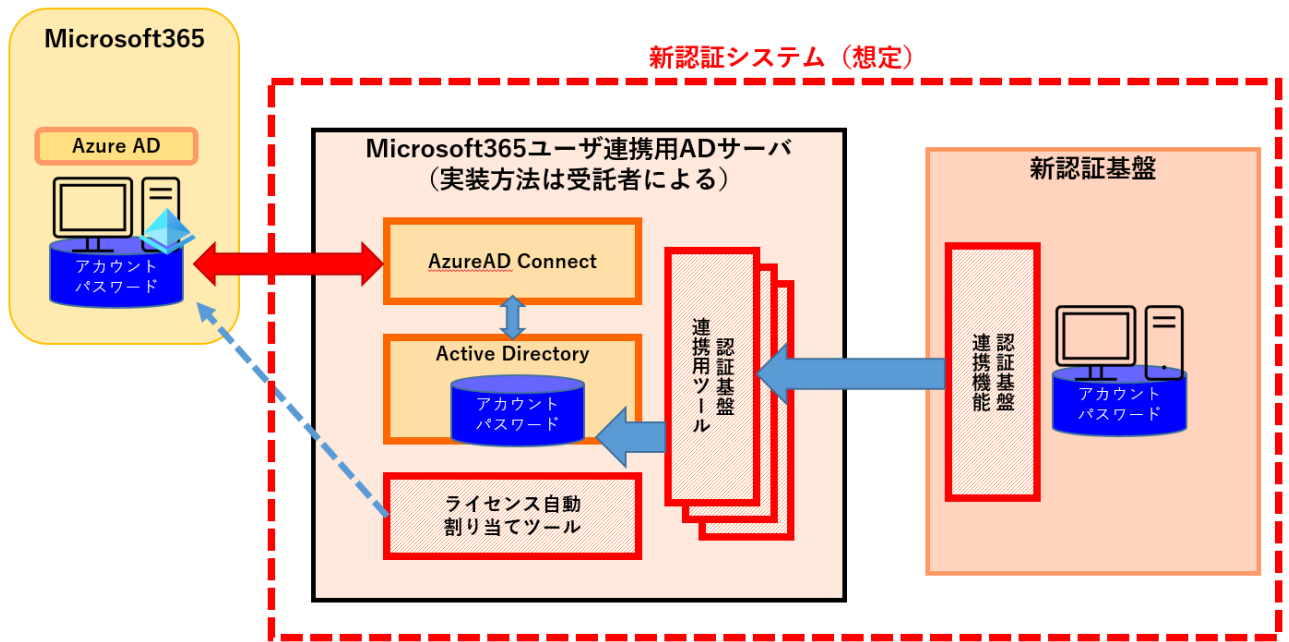


図 8. Microsoft365 連携

Microsoft365 のアカウント名については、各高専のアカウント名と同一だが、ドメイン名は基本違う。

例えば、

高専側アカウント： hoge@aaa-nct.ac.jp

Microsoft365 アカウント： hoge@aaa.kosen-ac.jp

のようになる。

また、高専機構本部のように同じドメインの高専も数高専ある。

高専側アカウント： hoge@bbb-nct.ac.jp

Microsoft365 アカウント： hoge@bbb-nct.ac.jp

Microsoft365 アカウントについては、ほぼ全アカウントで多要素認証を行っている。

(6) 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以下に図を示す。

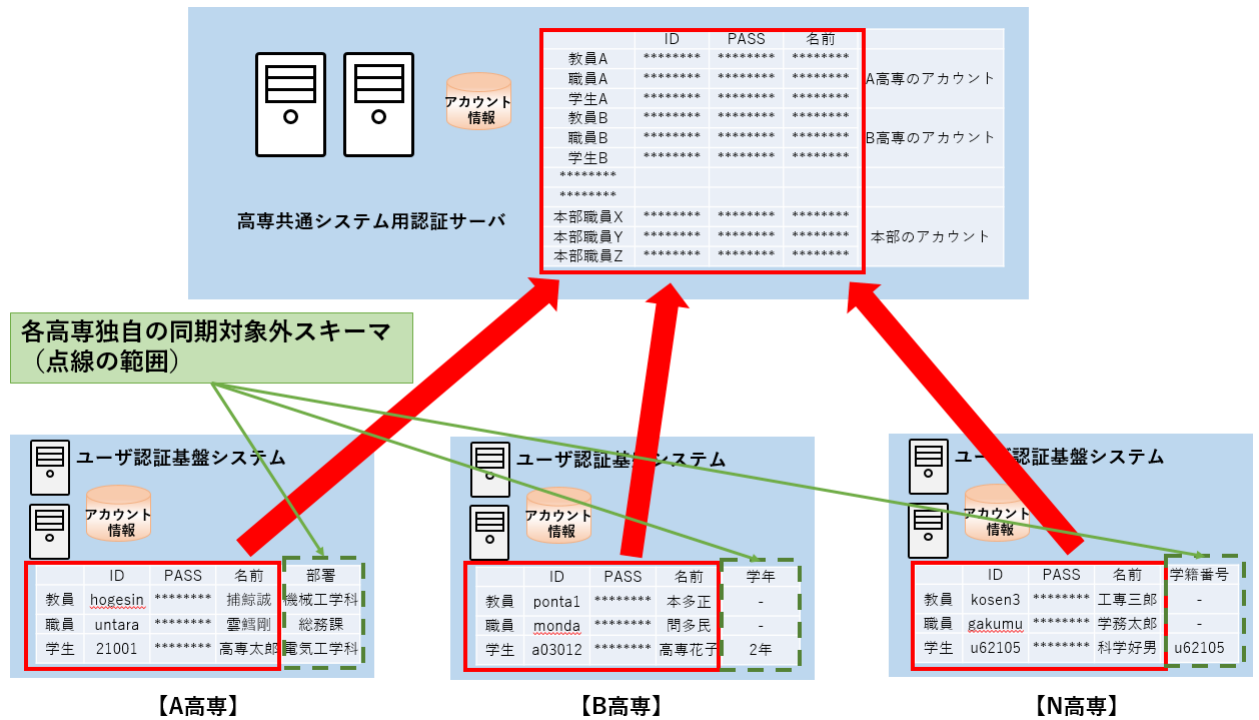


図 9. 認証サーバ間の同期

また併せて、高度化再編校の同期についての補足図を以下に示す。

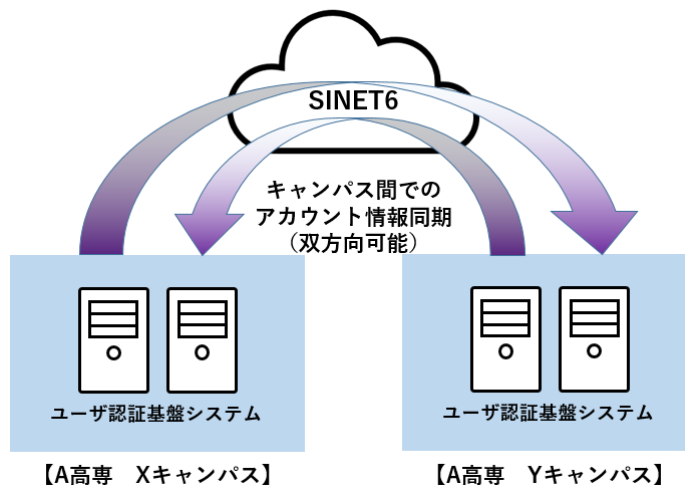


図 10. 複数キャンパスサーバ間の同期 (高度化再編校)

3.8 その他サービス個別要件

別添資料3「サーバ機器一覧」を参照のこと。

3.9 eduroam 構築要件

eduroam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、各キャンパス及び本部事務局に設置するユーザ認証基盤システム及び各スイッチ、無線 LAN アクセスポイントについて eduroam の設定を行うこと。ただし、eduroamJP の参加申請は各キャンパスの担当者が行っているものとし、SINET より eduroam 用の IP アドレスを取得しているものとする。

その他の要件については、機構本部と別途協議を行うこととする。

3.10 SSL-VPN 構築要件

各高専担当者やネットワーク管理者が学外からネットワークの設定等を行えるように、各キャンパス及び本部事務局に設置するファイアウォールについて SSL-VPN を利用できる設定を行うこと。認証については、ユーザ認証基盤システムで認証するように設定し、多段階認証を行える拠点担当者用のユーザを2～3名分作成すること。ただし、設定後に利用可能とするか利用停止とするかは各高専と調整を行うこと。

3.11 既存無線 LAN アクセスポイント追加要件

現在、各高専に導入されている無線 LAN アクセスポイント (CISCO Aironet1832i) および無線 LAN コントローラー (CISCO WLC2504) について、無線 LAN コントローラーの RADIUS サーバ設定の変更作業及び本調達の RADIUS サーバのクライアント追加設定作業により、既存の無線 LAN アクセスポイントが利用できるマニュアルを作成し、機構本部に提供すること。

上記について、導入時に現地にて既存機器の設定変更及び本調達の RADIUS サーバの追加設定を行う場合は加点とする。(10 数高専程度の予定)

4. 接続作業

本調達においては配線工事が完了していることを前提とする。本調達の範囲内で必要となる接続作業について記載する。

4.1 前提

- ① センタースイッチとフロントスイッチ間の光配線、及び UTP ケーブル・無線 AP 用 UTP ケーブルについては各高専にて敷設が完了していることを前提とする。
- ② 本調達の受託者による現地調査の結果、ケーブル配線に不足や問題があることが判明した場合は、各拠点担当者への報告を行うこと。各高専の責任において不足や問題への対応を本調達の導入に合わせて実施する。
- ③ ラック・設置スペースについては受託者の策定する設置仕様に基づき各高専で用意・準備する。
- ④ サーバ室の空調は各高専のサーバ室へ設置済のものを用いる。受託者の現地調査の結果容量の不足が懸念される場合は、適宜各拠点担当者へ報告を行い各高専の責任において対応の判断を行う。

4.2 現地調査・打合せ

- ① 高専毎に機器の設置場所・設置形態は様々である。接続作業の実施にあたっては事前に現地調査を実施すること。
- ② 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。
- ③ 現地調査の結果に基づき各拠点別の計画を策定し、拠点担当者の承認を得ること。

4.3 接続作業

4.3.1 全般

- ① 導入した各種機器間の接続に必要な接続作業及び整線を行うこと。
- ② 上記接続に必要な部材（ケーブル、端子等）については受託者で準備すること。現地調査の結果、各高専既設部材の利用が可能な場合は、既設部材の利用を行うことでよい。建屋あるいは部屋をまたぐ配線は敷設が完了していることを前提とする。
- ③ 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受託者で準備すること。光スプライスボックスは、各拠点にて設置されていることを前提とし、現地調査時にコネクタ形状を確認して準備すること。
- ④ 各パッチケーブルは各高専の設計条件に合わせて適切な製品・数量を導入すること。光パッチケーブルはシングルモード（SM）またはマルチモード（OM3、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 6 またはカテゴリ 6A を準備すること。
- ⑤ 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。

4.3.2 本調達で必要なパッチケーブル

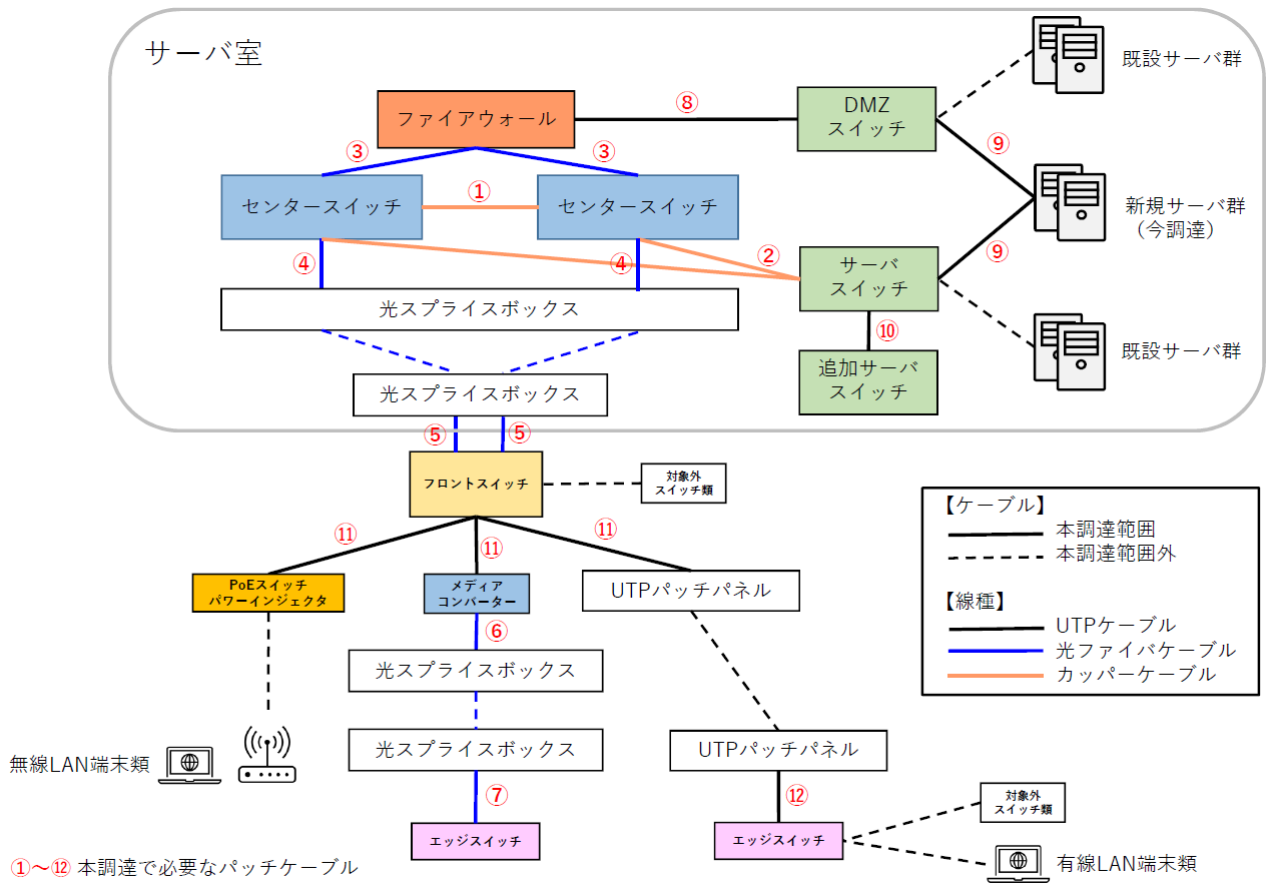


図 10-1 本調達で必要なパッチケーブル

- ① センタースイッチ～センタースイッチ間が7m以内になる場合は仮想化用のケーブルを準備すること。
- ② センタースイッチ～サーバスイッチ間が7m以内になる場合は適合するカッパーケーブルを準備すること。
- ③ トランシーバ及びメディアコンバーターと光スプライスボックスを接続する光パッチケーブルを準備すること。また、本調達により新たにジャンパー用光ケーブルが必要な部分に対してはこれを準備すること。
- ④ メディアコンバーターと各スイッチを接続する UTP パッチケーブルを準備すること。
- ⑤ PoE スイッチと各スイッチを接続する UTP パッチケーブルを準備すること。
- ⑥ パワーインジェクターと各スイッチを接続する UTP パッチケーブルを準備すること。
- ⑦ 現状構成においてセンタースイッチが単一構成である高専の場合、センタースイッチの冗長化に合わせてファイアウォールとセンタースイッチ間の追加される UTP パッチケーブルを準備すること。
- ⑧ 現状構成において DMZ スイッチ及びそれに類する機器が無く、本調達において新たに DMZ スイッチがファイアウォールと同室内に配備される高専の場合、ファイアウォールと DMZ スイッチ間の追加される UTP パッチケーブルを準備すること。

- ⑨ 本調達により配備されるサーバ類(無停電電源装置を含む。)と各スイッチを接続する UTP パッチケーブルを準備すること。
- ⑩ サーバ類接続用のサブポートとしてサーバスイッチにエッジスイッチが追加されている高専においては、サーバスイッチとサブポート用エッジスイッチを接続する UTP パッチケーブルを用意すること。
- ⑪ ケーブル長は必要十分なものを準備すること。
- ⑫ その他の配線を含むパッチケーブルは既存ケーブルを利用すること
- ⑬ 各スイッチ間を接続するパッチケーブルを準備し接続すること。その際に、光スプライスボックスあるいは UTP パッチパネル経由で接続することになる場合は、各スイッチから光スプライスボックスあるいは UTP パッチパネルに接続するパッチケーブルも準備すること。

4.4 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。各高専の責任において電源配線工事を実施する。

4.5 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高専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。各高専の責任において、受託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が行われることを前提とする。
- ④ 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、拠点担当者に報告を行うこと。各高専の責任において、受託者の機器設置までに対応が行われることを前提とする。
- ⑤ ラックマウントが不可能な機器については、耐震ベルト等の転倒防止対策を行うこと。

4.6 無線 LAN 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高専作成の配置図に基づき設置すること。
- 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。

4.7 既設機器への対応

- 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、各拠点担当者の指示に従い取り外すこと。
- ② 取り外した既設機器については各拠点担当者の指示に従い、同一キャンパス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、その考慮を行うこと。

4.8 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。
- ② 受託者側の管理上必要な管理ラベルについては、受託者にて貼付すること。

5. 移行要件

5.1 移行業務要件

5.1.1 全般

① 受託者は、以下の作業を実施すること。

- ア) 移行計画書の作成
- イ) 移行手順の作成
- ウ) 移行リハーサルの実施
- エ) 移行判定
- オ) 移行作業の実施

移行の流れを以下に示す。

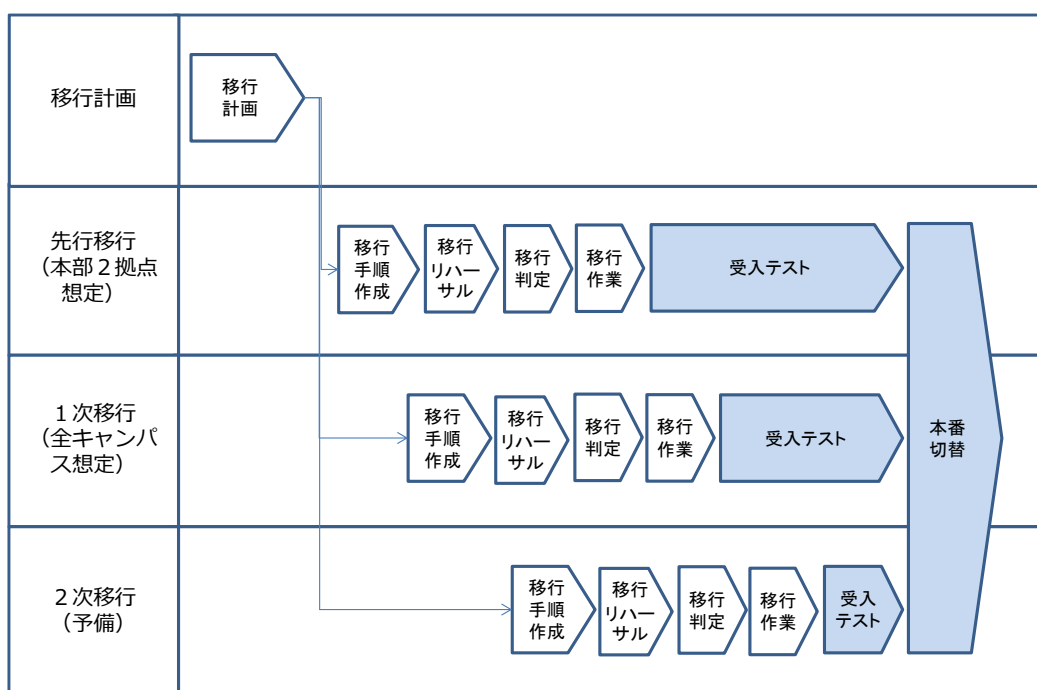


図 11 移行の流れイメージ

表 1 移行の概要

移行フェーズ	概要	対象キャンパス
先行移行	令和4年5月～6月の調整可能な期間に構築及びテストを実施する。移行判定後、受入テストの実施並びに本部での全国高専展開前の確認を行う。	本部事務局2拠点
1次移行	令和4年7月～11月における構築及びテスト完了後に移行を行う。	全キャンパス(想定)
2次移行	令和4年12月～令和5年1月(冬期休暇)における構築及びテスト完了後に移行を行う。	1次移行が不可能なキャンパス及び予備

5.1.2 移行計画の策定

- ① 受託者は、移行計画書を作成し機構本部の承認を得ること。
- ② 移行計画書には、少なくとも以下を記載すること。
 - ア) 体制及び役割
 - イ) 移行範囲・対象
 - ウ) 移行スケジュール
 - エ) 移行方式
 - オ) 移行判定基準
- 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。
- ④ 移行日程については、受託者と各拠点の担当者との協議のうえ調整を行うこと。

5.1.3 移行設計

- ① 移行計画書に基づいて、移行設計を行うこと。

5.1.4 移行手順の作成

- ① 移行計画書に基づいて、移行手順書を作成すること。
- ② 移行手順書には、少なくとも以下を記載すること。
 - ア) 体制及び役割
 - イ) 連絡先
 - ウ) 移行作業、操作手順
 - エ) 移行タイムチャート、想定時間
 - オ) 切り戻し手順

5.1.5 移行リハーサル

- ① 受託者は移行リハーサル計画を策定し、拠点担当者の承認を得ること。なお、移行リハーサルとは、移行・受入支援チームの担当者が、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 受託者は計画に基づき、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、各拠点の承認を得ること。

5.1.6 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 受託者は、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と受託者とする。
- ③ 移行判定は、移行・切替作業の実施が否決された場合でも、本番稼働への影響がない日程で実施すること。
- ④ 移行判定会議は拠点別に実施するものとする。最終的な移行の判定は各拠点責任者が行う。

5.1.7 移行作業

- ① 移行手順書に基づいて、移行作業を行う。
- ② 移行作業の実施状況は拠点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、受託者の責により一部機能が利用できない等の場合は、代替機能を受託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判断した場合には、各拠点担当者と協議の上、現行ネットワークシステムへの切り戻しを行うこと。切り戻し作業は受託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、拠点担当者及び機構本部に報告すること。
- ⑤ 移行作業後、必要に応じて稼働立ち合いを行い、問合せやトラブルに対応すること。
- ⑥ 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。またその体制について提案すること。

5.1.8 移行における体制

- ① 本書「9.体制及び方法」にて記載する。左記に追加して、各拠点での作業においては統括管理組織・責任者との密な連携を行える体制を整えること。

5.2 移行期間

5.2.1 移行・切替のスケジュール

- ① 移行の想定スケジュールを下記に示すが、必要に応じ受託者にてスケジュールを立案すること。

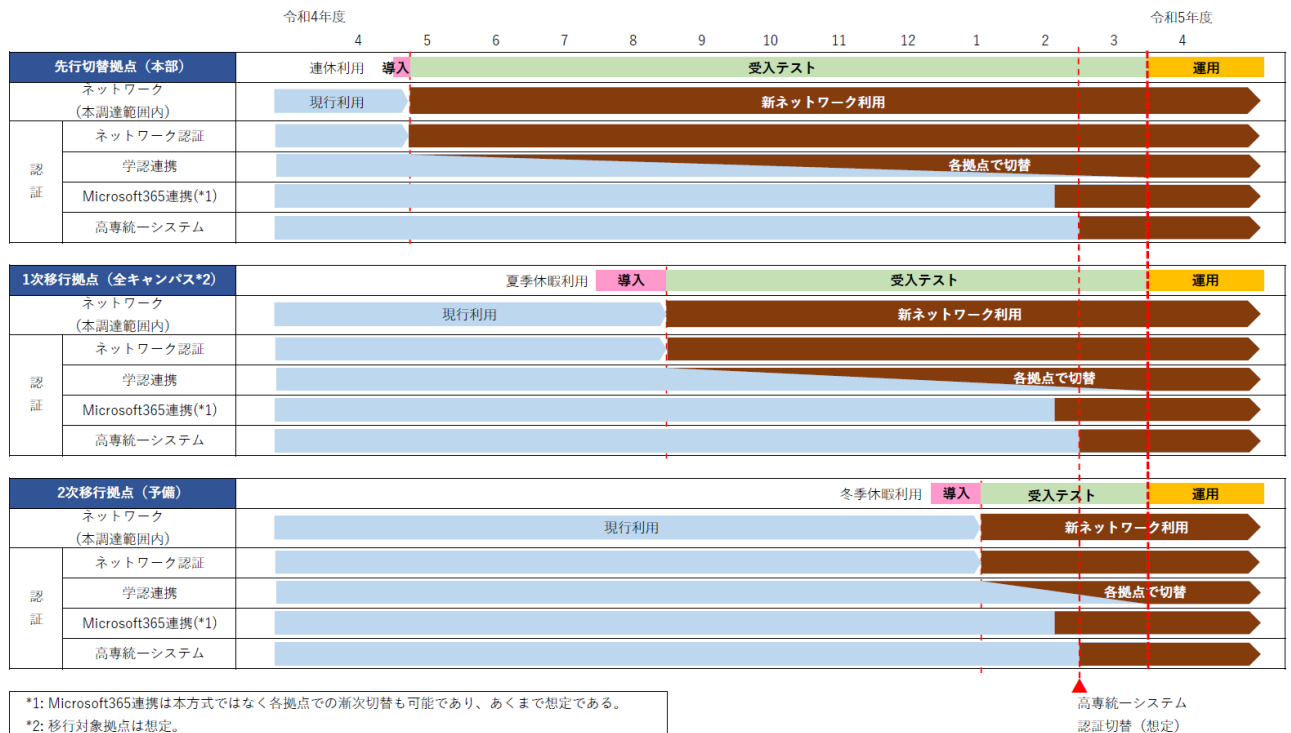


図 12 想定移行・切替スケジュール

5.2.2 移行単位

本システムの移行は大きく以下の移行領域に分類される。

(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。

ア) ネットワーク

- ・各種スイッチ
- ・ファイアウォール
- ・無線 LAN

イ) ネットワーク基盤サービス

- ・内部向け DNS
- ・DHCP
- ・NTP

ウ) 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、休暇期間中の切替を想定している。実際の各拠点の実施時期は拠点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 学生寮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が使用される。これらについては各拠点担当者に対して可能な範囲での技術支援を行うこと。

(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。

- ① 関わる機器の設置に関しては上記(1)ネットワーク等の移行に先行または同時に終了している必要がある。
- ② 既存の認証システムは、完全に認証システムが切り替わる令和4年度末(令和5年3月)まで並行しての利用が必要である。受託者はこれらの利用について考慮すること。
- ③ アカウントデータ及び RADIUS 認証用の MAC アドレスの登録は拠点担当者が行う。ただし、拠点担当者からの依頼により、オプション役務が発生する可能性がある。
(例：演習室等の機器認証情報の登録等)

以下に各領域の想定を記載する。

(ア) ネットワーク接続の認証

- ① 本調達で導入するスイッチや無線 LAN に接続する際の認証は、本調達導入ネットワークの利用の最初から本調達導入の認証システムを用いることを前提とする。
- ② 学生寮など本調達範囲外のネットワークについての変更が必要な場合は、拠点担当者が設定変更を行うことを前提とする。

(イ) 学認連携の移行

- ① 学認連携の切り替えは、各高専担当者が各高専独自のスケジュールで行う。
- ② 上記切り替えが行われるまでは、既存の認証システムが学認連携に用いられる。
- ③ 受託者は、本切替に対して技術支援を行うこと。

(ウ) Microsoft365 連携の構築

- ① 受託者は Microsoft365 の連携のために必要な機能を実装すること。
- ② 実装の方式により移行の方法が異なると想定される。本項では連携用 AD サーバを新設する方式を想定するが、応札者が本方式以外を用いる場合は方式についての記載を行うこと。
- ③ 実行基盤として想定している Azure は機構本部が保有するものを利用する。応札者は必要と想定される利用量について示すこと。認証の個別要件は「3.7.1 各キャンパス用及び機構本部用認証システム要件」を参照のこと。
- ④ 各高専では各高専担当者が、認証サーバの導入後令和5年1月末(想定)までに、新認証システムへアカウントデータを投入する。受託者は連携切替までに連携用 AD サーバに各高

専のアカウントデータが同期されていることを確認し、機構本部及び各高専担当者と調整のうえ不具合の解消を行うこと。

- ⑤ 必要があれば、受託者は Microsoft365(AzureAD)へ新しい AD 連携サーバに接続する。
- ⑥ Microsoft365 のライセンス・利用状況・グループ設定が現状から適切に引き継がれる方法を提案し、機構本部と協議のうえ実施すること。

※注 マイクロソフト社 Microsoft365 認証連携の仕様を確認して設計・構築を行うこと。

(エ) 高専共通システム等の認証の移行支援

- ① 高専共通システム等、上記に記載したもの以外の連携切替は、全高専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、機構本部担当者によって行われる。受託者は情報提供と技術支援を行うこと。

5.3 教育に関する要件

受託者は、機構本部、各高専担当者への教育訓練を実施すること。

5.3.1 対象者

想定される対象者を以下に示す。

表 2 教育訓練の対象者

対象者	対象人数	場所	想定時間	概要
各拠点担当者	5名～10名程度	各拠点	1～2時間	導入時に物理的な事項を中心に、実際の機器を用いて教育を実施する。十分な教育訓練が出来ることを前提に Web 会議ツール等によるオンラインでの教育も可とする。
機構本部	5名程度	機構本部	2時間	機構本部のシステム管理者向けに教育訓練を行うことを想定。十分な教育訓練が出来ることを前提に Web 会議ツール等によるオンラインでの教育も可とする。

5.3.2 教育計画の策定

- ① 教育訓練を実施するにあたって、以下の内容を含む教育計画書を提出し、機構本部の承認を得ること。
 - ア) 教育目的
 - イ) 体制/役割
 - ウ) 教育方法
 - エ) 教育スケジュール

- オ) マニュアル・教材の内容
- ② 追加費用の発生しない範囲で、本調達の特성에応じた教育訓練が提案できる場合は記載すること。

5.3.3 教育内容

- ① 本調達においては拠点担当者が設定を変更する可能性があるため、基本的な設定変更を含む通常想定される運用全般について教育を行うこと。以下の内容を想定するが機構本部と協議の上決定すること。
 - ア) システム操作方法
 - イ) 各機器の設定方法
 - ウ) 障害時の対応方法
 - エ) システム運用方法
- ② 教育に用いる教材・資料の提供を行うこと。教育訓練実施後は機構本部経由で各高専担当者に配布することを想定している。

5.3.4 マニュアル作成

- ① 受託者は、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。
 - ア) スイッチ各種
 - イ) 無線 LAN コントローラ、無線 LAN アクセスポイント
 - ウ) ファイアウォール
 - エ) 認証基盤
 - オ) その他各種サーバ
- ② マニュアルの内容として、基本的な設定変更を含む通常想定される運用全般について記載すること。以下の内容を想定するが機構本部と協議の上決定すること。
 - ア) システム操作方法
 - イ) 各機器の設定方法
 - ウ) 障害時の対応方法
 - エ) システム運用方法（システム立ち下げ時および立ち上げ時の操作方法等）
- ③ 教育訓練は本マニュアルを以って行うこと。

5.3.5 教育時期

- ① 教育時期については、以下の内容を想定しているが、機構本部と協議の上決定すること。
 - ア) 運用開始前の導入教育（機構本部を含む各拠点で実施。各1回ずつを想定）
 - イ) 定期教育（年1回程度開催）
- ② 上記「イ)定期教育」については本調達の範囲外とする。ただし、本調達の範囲内とすることが望ましい。

5.3.6 教育場所

- ① 教育場所については、各拠点で実施すること。ただし、十分な教育訓練が出来ることを前提に Web 会議ツール等によるオンラインでの教育も可とする。
- ② 各拠点での教育にあたっては導入済み機器を用いてもよい。他に各拠点で用意する必要がある設備・部材については各拠点担当者と事前に調整を行うこと。

6. 信頼性等の要件

6.1 信頼性要件

6.1.1 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 過去に出荷・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を選定すること。

6.1.2 完全性

- ① サーバのストレージ装置（内蔵 HDD）は RAID1/RAID5/RAID6/RAID10 等の冗長構成とすること。
- ② サーバのストレージ装置（内蔵 HDD）についてはバックアップが取得できる機器構成・運用とすること。

6.1.3 機密性

- ① 本書「7 情報セキュリティ要件」を参照のこと。

6.2 拡張性要件

- ① サービスに著しく影響を与えない範囲で機能の拡張が可能であること。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ことが望ましい。
- ② 無線 LAN アクセスポイントについては、導入されるコントローラの範囲内で追加の余地があること。
- ③ 追加可能なアクセスポイントの数量や利用形態について制約がある場合は明示すること。

6.3 上位互換性要件

- ① 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、本調達の間期間を通して、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。

6.4 システム中立性要件・事業継続性要件

- ① 特定の事業者・製品に依存することなく次々ネットワークシステムの更改が可能であること。
- ② 併せて各高専で運用・保守を継続することが可能なシステム構成であること。

7. 情報セキュリティ要件

7.1 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主体的に実施すること。

- ① 受託者は、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 受託者は、情報セキュリティに関する問題が発生した場合には、速やかに機構本部に報告し、必要な対策を講じること。また、事前に連絡方法・対応手順等を明示して機構本部の承認を得ること。
- ③ 情報セキュリティ対策の実施に当たっては、機構本部で策定しているセキュリティポリシー群に準拠すること。

7.2 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、以下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、「3 情報システム稼働環境」に詳しい記載があるので参照すること。

7.2.1 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 重大な影響のあるサーバ、FW、コアスイッチ等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機構本部へ報告すること。
- 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、アンチマルウェ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。

7.2.2 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の防止を考慮した対策を講じること。
- 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。

7.2.3 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。なお、高度なログ分析ツールのようなものは不要とする。
- ③ アクセスログは、最低 1 年間分は本調達で導入するストレージ上に保管可能であること。
- ④ ファイアウォールのアクセスログ・IDS/IPS のログについては、データセンター内に設置

する集約ログサーバにも転送すること。

7.3 本調達業務の遂行等に係る情報セキュリティ対策

本調達に係る業務を遂行するに当たり、受託者は以下のセキュリティ対策を実施すること。

7.3.1 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、機構本部及び各高専の情報資産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、速やかに機構本部へ報告すること。
- ② 上記機構本部及び各高専の情報資産とは以下のことである。
 - ア) 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
 - イ) 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
 - ウ) 電子、紙媒体に係らず機構本部及び各高専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
 - エ) その他機構本部及び各高専の所有に帰属するもの

7.3.2 機密保護

- ① 機構本部から受託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機構本部の承認を得ること。

7.3.3 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 受託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は、国立情報学研究所の UPKI 電子証明書発行サービスを利用する想定であり、証明書発行サーバの導入は不要である。また、証明書発行手続きは、高専側で行うものとする。

7.3.4 その他のセキュリティ対策

- ① 受託者は本調達業務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 ネットワークシステムの設計・構築工程において、業務の一部を外部業者に再委託する場合は、再委託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託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、機構本部及び高専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。

8. 運用保守業務要件

8.1 運用保守業務の範囲

本調達の運用保守領域としては「運用業務支援」及び「製品保守」が主なものとなる。

- ① 運用保守の体制について提案すること。

8.2 運用保守実施計画の策定

本運用保守業務における運用保守実施計画の策定について以下に記載する。

- ① 受託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、機構本部の承認を得ること。
- ② 運用保守業務実施計画書に係る記載内容の詳細については落札後に機構本部と協議のうえ決定とするが、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。
 - 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

8.3 運用業務支援

本運用保守業務における運用業務支援要件について以下に記載する。

8.3.1 サービスデスク業務要件

(1) 受付業務

- ① 受託者は機構本部及び各高専担当者に対し、問合せ及び保守対応等の依頼を一元的に受付ける問合せ窓口を設置すること。ただし、学生・教職員からの問合せについては、各高専担当者または機構本部にて対応を行うものとする。
- 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、ソフトウェア製品とする。
- ③ 問合せは電話及び電子メール等の日本語による受け付けを行うこと。
- ④ 電話による受付時間については平日(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 9:00～17:30 を最低限対応すること。本対応時間を上回ることが望ましい。
- ⑤ 休日夜間帯においても電子メールによる受け付けは行い、翌営業日より迅速な対応を開始できる仕組みを導入すること。
- ⑥ ログ、コンフィグ、パッチ等のファイルを、拠点担当者、機構本部担当者と受託者の間で授受する仕組みとして、機構が保有する Microsoft365 の利用を考えている。応札者が提供できる仕組みで、より適切と思われるサービスがあれば提案すること。
- ⑦ 受託者は機構本部及び各高専担当者からの依頼を受け、依頼内容、対応進捗及び対応結果等、受け付け対応の履歴管理を行うこと。
- ⑧ 受託者は上記以外に機構本部より依頼を受けた場合、対応内容について協議の上、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。

(2) 問合せ対応業務

- ① 受託者は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に係る問合せに対し、問合せ受付け、調査及び製品ベンダ問合せ等を実施し、問合せに対する回答を行うこと。
- ② 問合せに対する回答は日本語で行うこと。
- ③ 受託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) アナウンス業務

- ① 受託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、機構本部及び各高専担当者向けにアナウンスを行うこと。

(4) 報告業務

- ① 本調達の範囲にて受託者は受付け対応及び対応作業履歴から定期報告書の作成を実施し、機構本部へ下記頻度で対面で報告を行うこと。
 - ア) 令和5年度までは半年に1回
 - イ) 令和6年度以降は1年に1回
- ② 機構本部への定期報告書に係る内容の詳細については落札後に機構本部と協議のうえ決定とするが、定期報告書には少なくとも以下の内容を含めること。
 - ア) 問合せ及び保守対応履歴、対応ステータス
 - イ) メンテナンス情報
 - ウ) 修正プログラムリリース情報
 - エ) 各高専の状況概要
- ③ 受託者は各拠点担当者へ年1回以上の簡易的な報告を対面もしくはオンラインで行うこと。内容の詳細については機構本部と協議の上決定とする。

8.4 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。

8.4.1 製品保守共通要件

- ① 本調達では、高専毎に異なる令和4年度の機器導入時から令和5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9年度末(令和10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ことが望ましい。
- 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、「9.9 撤去(2)データ消去」に記載された通りとする。

8.4.2 ハードウェア保守要件

(1) ハードウェア問合せ対応支援業務

- ① 受託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、最低限平日 9:00～17:30 のハードウェア問合せ対応支援を行うこと。
- ② 受託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。

(2) ハードウェア保守業務

(ア) 全体

- ① ハードウェア保守業務対応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問合せ対象外とする。
- 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。
 - ア) 平日 9:00-17:30 オンサイトまたはそれを上回る保守サービスが必要な機器
 - ・ センタースイッチ
 - ・ ファイアウォール
 - イ) 先出 SENDバックまたはそれを上回る保守サービスが必要な機器
 - ・ 上記以外の納入されるハードウェア製品
- ③ 設定の復旧については各高専担当者が実施可能なこと。復旧手順については、「5.3 教育に関する要件」に記載に従いマニュアルを作成し各高専担当者に周知すること。
- ④ 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ことが望ましい。

(イ) 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。
- ② 全拠点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 冗長化されているハードウェア製品については、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。
- ④ 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 4 時間以内のオンサイト対応が望ましい。
- ⑤ 受託者は保守作業後設定の復旧を行うこと。設定は各拠点担当者により変更される可能性があるため、設定情報については拠点担当者より入手すること。

(ウ) 先出 SENDバック保守

- ① 先出 SENDバック保守は、各高専担当者から故障連絡後、置き換え対象機器を受託業者・製造元または代理店から送付し、各拠点の担当者が接続変更を行った後に故障機器を送り返すことをいう。

- ② 先出センドバック保守時の各高専担当者の切替え作業にあたって、ライセンス変更受付け等の作業時間制約がある場合は明記すること。
- ③ センドバック保守対応を行うにあたり、各高専からの保守対応依頼日を起点として、発送までのリードタイムを提示すること。
- ④ 無停電電源装置の定期バッテリー交換を含む。
- ⑤ 上記の機器送付リードタイム低減措置において、予備機を各高専に配置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・数量及び対象高専を明示すること。

8.4.3 ソフトウェア保守要件

(1) ソフトウェア問合せ対応支援業務

- ① 受託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、最低限平日 9:00～17:30 のソフトウェア問合せ対応支援を行うこと。
- ② ソフトウェア問合せ対応支援業務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、各高専に既存のソフトウェアについては問合せ対象外とする。
- ③ 受託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。

(2) 修正プログラム提供業務

- ① 受託者は本調達で納入されたファームウェア、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。メジャーリリースおよ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 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。
- ③ 修正プログラムにより作成したマニュアルに変更がある場合は、マニュアルを更新すること。

(3) 各高専担当者の実施する修正プログラム

- ① 各高専担当者が実施する必要があるプログラム更新については修正プログラムと合わせて適用マニュアルも提供を行うこと。
- ② 各高専担当者のスキルレベルには差があることを考慮し、十分に簡易と考えられるプログラム更新の手順とすること。本件について考慮が必要な点とその対応がある場合は提案を行うこと。

8.5 各高専による保守・運用のオプション追加対応

運用・保守の必要項目やレベルは各高専の事情により様々であるため、本調達で導入される全高専に共通の運用・保守は必要最低限のものとする。

- ① 各高専と受託者が協議の上、双方が合意した場合は費用負担により、保守レベルを個別に上げることができること。
- ② 各高専と受託者が協議の上、双方が合意した場合は費用負担により、運用支援業務のサー

ビスレベルや、支援作業を個別にオーダーできること。

- ③ これら各高専費用負担による追加は、本調達の契約とは別に、高専毎の発注及び契約とする。
- ④ 各高専の事情により追加オーダーを受託者以外に発注もしくは競争入札にかける場合は、設定する上で必要な情報提供を行うこと。
- ⑤ 上記対応の各高専担当者からの依頼や問合せが可能な窓口を運用期間を通じて用意すること。サービスデスクからのエスカレーションを想定するが、本問合せ独自の窓口でもよい。
- ⑥ これらの目的を達するためのサービス提供形態・契約体系及び体制など、応札者が重要と考える点について提案すること。

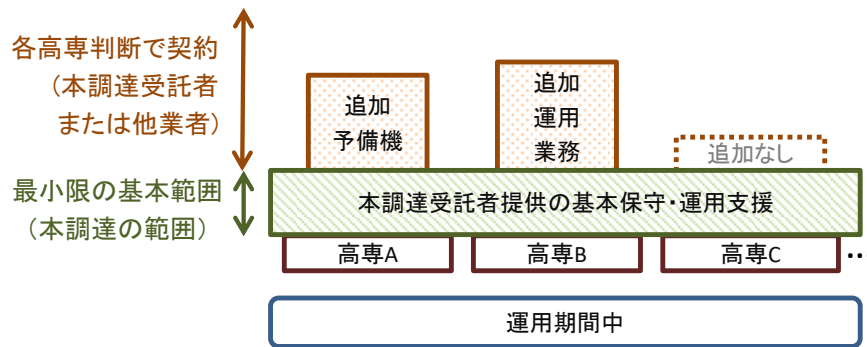


図 13 運用・保守オプション追加のイメージ

表 4 想定される保守・運用オプションの例(本調達には含まれない)

No.	想定される追加保守・運用項目例	区分
1	サービスデスク受付の時間・曜日延長(24 時間 365 日化)	運用支援
2	オンサイト保守作業時間の 24 時間 365 日化	保守
3	UTM 機器のオンサイト保守化	保守
4	オンサイト保守の駆け付け時間短縮 (翌営業日→4 時間以内 等)	保守
5	リモート保守対応 (認証システム)	保守 運用支援
6	リモート保守対応 (N/W 基盤サービス)	保守 運用支援
7	リモート保守対応(UTM)	保守 運用支援
8	運用個別業務の追加	運用支援
9	運用・保守の有償相当のスポット対応業務	運用支援 保守

9. 体制及び方法

9.1 作業実施体制

9.1.1 体制概要

プロジェクトの推進体制及び請負者に求める作業実施体制は次の図及び表のとおりである。受託者のチーム編成については想定であり、受託者決定後に協議の上、見直しを行う。なお、システム稼働前と稼働後の体制は別に作成すること。また、受託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。

- ① 応札者はプロジェクト実施体制及び役割を明記すること。
- ② 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。
- ③ 作業工程やタスク毎に必要な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託者の範囲を以下の体制図に示す。

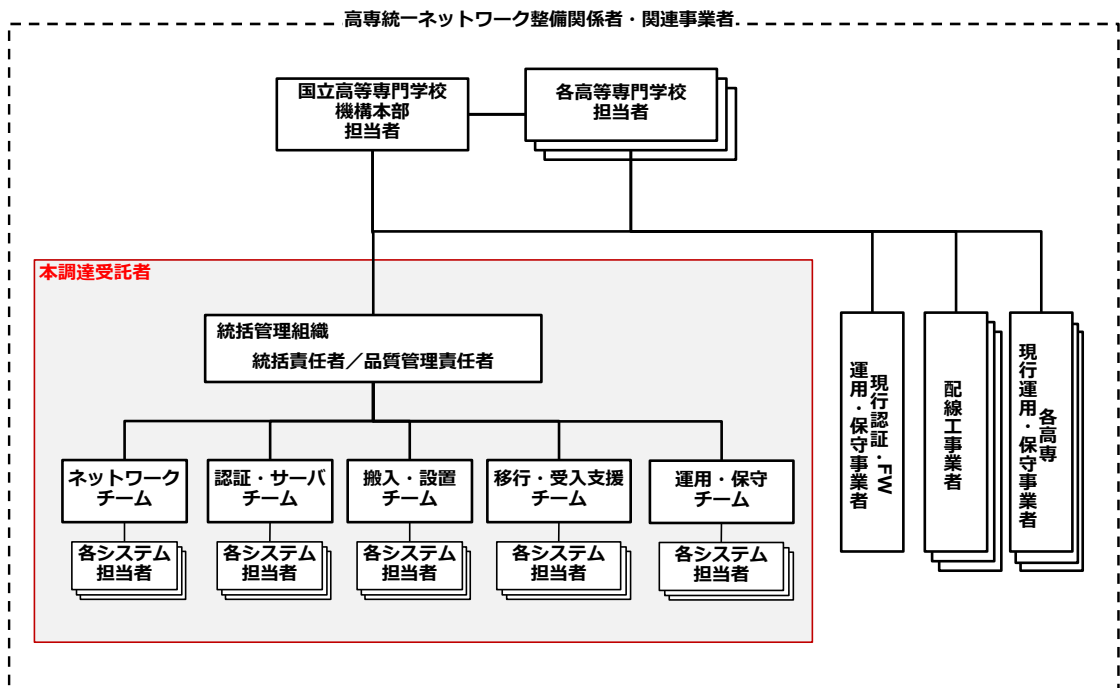


図 14 体制図

9.1.2 体制内の役割

体制図における想定する役割と要件について以下に示す。

表 5 体制

No.	役割	要件
1	統括管理組織	① 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こと。 ② 統括管理組織は、高専機構本部に対して決定事項等の報告を行い、承認を得ること。
2	統括責任者	③ 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、機構本部の承認に基づき、各チームの作業を統括管理すること。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こと。
3	チーム体制	④ 統括管理組織の下に、チームリーダーと各システム担当で構成されるチームを設置すること。 ⑤ 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。受託者の設置チームについて明示すること。 ⑥ チームリーダーはプロジェクト全体で2名以上とし、チームの兼務を認めるが、システム担当者との兼務は認めない。
4	品質管理責任者	⑦ 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名以上設置すること。なお、品質管理責任者が、他の作業を兼務することは認めない。

9.2 作業要員に求める資格等の要件

9.2.1 全般

- ① 作業要員は、本仕様書に示す要件を円滑に遂行できる能力を有すること。
- ② 要員の交代の必要があると判断したときは、1週間前までに受託者に通知の上、交代させるものとする。
- ③ ここに述べる以外に資格について必要性がある場合は、応札者は提案を行い、それに対応した要員配置を行うこと。

9.2.2 統括責任者

- ① 作業要員は、本仕様書に示す要件を円滑に遂行できる能力を有すること。
- ② 「ITスキル標準 (Ver3.0)」のプロジェクトマネジメント(専門分野：指定しない、達成度指標：レベル5以上)に該当し、チームのリーダーとして10年以上の経験を有すること。
- ③ 過去5年以内において、教育研究機関(大学等)におけるキャンパス全体のネットワーク更新プロジェクトのマネジメントを実施した経験を有していること。

- ④ 設計・構築・移行期間中は、本調達に係る作業に専任すること。
- ⑤ 統括責任者は以下のいずれかの資格を有すること。
 - ア) PMP (Project Management Professional)
 - イ) 情報処理技術者 (プロジェクトマネージャ)
- ⑥ 上記以外に、本調達の特性に応じて統括責任者に必要とする要件があれば提案し、それに対応した体制とすること。

9.2.3 各チームリーダー

- ① 「IT スキル標準 (Ver3.0)」の担当する職種(専門分野：担当する分野、達成度指標：レベル4以上)に該当し、チームのリーダーとして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)におけるキャンパス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 導入する担当の機器・ソフトウェア等に精通していること。
- ④ ネットワーク設計チームリーダーは、以下の資格又は同等の資格を有すること。
 - ア) 情報処理技術者 (ネットワークスペシャリスト)
- ⑤ 上記以外に、本調達の特性に応じてチームリーダーに必要とする要件があれば提案し、それに対応した体制とすること。

9.2.4 各システム担当者

- ① 「IT スキル標準 (Ver3.0)」の担当する職種(専門分野：担当する分野、達成度指標：レベル3以上)に該当し、各機器等の設計・構築担当者として3年以上の経験を有すること。
- ② 導入する担当の機器・ソフトウェア等に精通していること。

9.3 プロジェクト管理

9.3.1 全般

- ① 受託者は、契約締結後2週間以内にプロジェクト計画書を提出し、機構本部の承認を得ること。
- 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。
 - ア) プロジェクト概要
 - イ) 実施内容
 - ウ) スケジュール
 - エ) 成果物
 - オ) 実施体制と役割
 - カ) プロジェクト運営
 - キ) 管理方法
 - 進捗管理
 - 課題管理
 - QA 管理
 - 品質管理

- 貸与物品管理
- ドキュメント管理
- リスク管理
- 人的資源管理
- セキュリティ管理

ク) 会議体・コミュニケーション方法

- ③ 受託者は、プロジェクト進捗管理を行うとともに定例会議、個別検討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機構本部に報告し、協議の上問題解決に努めること。
- ④ 本調達の特性を考慮した有用な管理手法やツールがある場合は提案を行うこと。

9.3.2 進捗管理

- ① 受託者は、プロジェクト進捗管理を行うとともに定例会議、個別検討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機構本部に報告し、協議の上問題解決に努めること。
- ② WBS (Work Breakdown Structure) 及び EVM (Earned Value Management) 等による進捗管理を行うこと。

9.3.3 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。
 - ア) 課題内容
 - イ) 影響
 - ウ) 優先度
 - エ) 発生日
 - オ) 担当者
 - カ) 対応状況
 - キ) 対応策
 - ク) 対応結果
 - ケ) 解決日
- ② 起票・検討・対応・承認といっ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。

9.3.4 QA 管理

- ① 機構本部及び各高専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。

9.3.5 品質管理

- ① 作業工程毎に品質評価基準を定め、次工程に推移する際は機構本部の承認を得ること。
- ② 受託者内に品質管理を専門とした部門、または担当者が存在し、品質レビューを定期的に

実施すること。

9.3.6 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 上記①で整理したリスクについて、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。

9.3.7 会議体

- ① 統括責任者は、機構本部に対し定例会議を開催し、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。
- ② 構築期間中の定例会議は月 1 回以上、個別検討会議は週 1 回程度を想定している。実際の開催頻度は、プロジェクト計画書に明記すること。
- ③ 定例会議の開催頻度は、設計・構築作業の進捗状況により必要に応じて変更されるものとする。
- ④ 各チームリーダーは、総括責任者と共に会議体を開催し、高専機構本部に決定事項を報告の上、承認を得ること。
- ⑤ 開催する会議体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。
- ⑥ その他必要な会議体については、機構本部と協議を行い設置すること

9.4 構築計画の策定

- ① 受託者は、構築計画書を作成し、機構本部の承認を得ること。
- ② 構築計画書には少なくとも以下を記載すること。
 - ア) ネットワーク構築方法
 - イ) サーバ構築方法
 - ウ) スケジュール
 - エ) 体制及び役割
 - オ) 制約条件及び前提条件
- ③ 受託者は、構築計画書に基づいて、高専統一ネットワークシステムの構築を行うこと。
- ④ 構築完了後、構築結果報告書を作成し、機構本部に報告すること。
- ⑤ 構築結果報告書は先行移行、1次移行、2次移行のそれぞれについて行うこと。

9.5 設計

9.5.1 全般

- ① 受託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、機構本部の承認を得ること。

9.5.2 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、高専毎に定められている「配線概要図」及び、各高専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、最新の情報を精査すること。
- ② 現地調査の前に必要な情報の収集のために、受託者の責で調査票を作成し機構本部の許可を得ること。各高専への調査票配布・回収は機構本部を通して行う。
- ③ 受託者は現地調査のスケジュールを作成し、各高専との調整を受託者が行うこと。その際各高専の日程都合を尊重すること。
- ④ 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すること。
- ⑤ 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、適宜最新状況の確認や各高専の状況の把握・フォローを行うこと。有用な手法があれば提案を行い、機構本部と協議のうえ対応すること。
- ⑦ 全高専現状調査の結果、別添資料4「ネットワーク機器一覧」に記載される高専毎員数と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、高専毎の導入員数の調整を行うこと。
 - ア) 調整の際は、受託者の責で別添資料4「ネットワーク機器一覧」を更新し本部の承認を得ること。検収の際は更新後機構本部の承認がなされた「ネットワーク機器一覧」が用いられる。

9.5.3 基本設計

- ① 受託者は、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機構本部の承認を得ること。
- ③ ネットワークに関しては、必要に応じて各高専担当者と設計内容に関して協議を行い設計を行うこと。
- ④ 記載内容は受託者の提案を元に機構本部と協議の上決定する。少なくとも以下について記載があること
 - ア) 全体方式設計
 - イ) 全体物理構成
 - ウ) 全体論理構成
 - エ) ネットワーク論理構成図
 - オ) サーバ論理構成図
 - カ) 命名規則
 - キ) 各システム方式設計
 - ク) 可用性設計・冗長化設計

- ケ) インフラ運用設計
- コ) セキュリティ設計
- サ) 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）

9.5.4 詳細設計

- ① 受託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。
- ② 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いる。
- ③ ネットワーク(UTM 機能を含む)に関しては、各拠点の現行ネットワークの設定踏襲を基本とし、拠点担当者と設計内容に関して協議を行うこと。
<各拠点向けに設定が必要と想定される項目>
 - ア) IP アドレス
 - イ) VLAN
 - ウ) アクセスコントロール設定
 - エ) 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）
 - オ) UTM のセキュリティ設定
 - カ) その他必要と考えられる項目
- ④ サーバに関しては、標準構成を基本とし各拠点毎のパラメータは必要最小限の設計とする。
<各拠点向けに設定が必要と想定される項目>
 - ア) 各機器の IP アドレス
 - イ) 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
 - ウ) 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
 - エ) その他拠点配置に依存する項目
- ⑤ 詳細設計書の記載内容は機構本部と協議の上決定するが、少なくとも以下について記載すること。
 - ア) 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）
 - イ) ネットワーク機器パラメータ設計
 - ウ) サーバ機器パラメータ設計（仮想サーバ設計含む）
 - エ) 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）
 - オ) ユーザ認証機能設計
 - カ) ファシリティ設計（ラック構成図、電源接続図、結線図等）

9.6 構築

9.6.1 事前構築

- ① 事前構築では、単体テスト、結合テスト(受託者提案による)を実施し、機能の正常性を担保すること。
- 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 受託者は外部の人およ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。
- ④ 事前構築で必要となる検証機器や作業場所等は、受託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、全て受託者の負担とすること。

9.6.2 本番環境構築

(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、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、連係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、応札者の考える要点とその対応について提案すること。

(2) 搬入設置

- ① 搬入については、事前に申請し許可を得ること。
- ② 各高専担当者の指示する場所に搬入・設置を行い、養生品、梱包等は撤去すること。
- ③ 受託者が個別に各拠点担当者に連絡し、搬出入のルート、養生は、各拠点担当者の指示に従うこと。また、必要な手続及び打合せについては、受託者が遅滞なく行うこと。手続きおよび打ち合わせはオンラインおよびリモートにて行うこと。
- ④ 施設内で作業を行う際は、社員証や各拠点担当者に指定された名札等を常に目に見えるように携帯すること。
- 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担当者と協議すること。
- ⑥ 機器の移設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、受託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影響がある場合は、作業内容、影響範囲、影響時間等明確にし、事前に各拠点担当者に対して承認を得ること。

9.7 本番切替

移行の詳細については「5. 移行要件」を参照のこと。

9.7.1 本番切替の要件

- ① 受託者は、本番切替判定基準を作成すること。
- ② 本番切替判定基準として、少なくとも以下を確認すること。
 - ア) 事前のテストが完了し、すべて合格していること。
 - イ) 障害対策が実施されていること。また影響範囲が明確になっていること。
 - ウ) システムの運用や操作の手順が明確になっていること。
 - エ) 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。
- ③ 本番切替判定会議を開催すること。参加者は受託者と拠点担当者とする。
- ④ 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。

9.7.2 本節における本番切替の定義

(1) ネットワーク切替

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。そのため本節では受入テスト開始をネットワークの本番切替と捉える。

DNS、DHCP などネットワーク基盤サービスについても同様とする。

(2) 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。

- ア) 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。
- イ) 各高専担当者が行う学認の認証切替
→ 受託者の範囲外のため本節の対象外とする。
- ウ) 機構本部が行う想定の高専共通システム認証切替
→ 機構本部が主体となり実施を行うため本節の対象外とする。
- エ) 受託者及び本部が行う想定 Microsoft365 認証連携切替（受託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。

9.8 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、その各高専担当者に積極的な技術支援及びアドバイスをを行うこと。
- ② 本調達機器以外のシステム等における設定作業等は、各拠点の担当者又はシステム等納入業者・保守業者が行うが、受託業者は適宜連携・情報共有を行うこと。
- ③ 各拠点の既存システム等との接続を円滑に行うため、各拠点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、各高専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、各高専担当者に積極的な技術支援及びアドバイスをを行うこと。
 - ア) 本調達外の既存機器等の設定変更

イ) 認証基盤に係るアカウントの移行

ウ) 以下の機能における、各拠点に合わせた設定（導入時は全拠点共通の標準設計に基づいた設定にて導入する。）

- 内部 DNS 機能
- DHCP 機能
- NTP 機能
- 各キャンパス用認証機能
- 各キャンパス用アカウント管理機能
- 本部事務局用認証機能
- 本部事務局用アカウント管理機能
- システム監視機能
- ネットワーク機器設定管理機能

9.9 撤去

(1) 撤去

- 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、各拠点担当者の指示に従い、受託者の責において受託者が納入した機器の撤去作業を行うこと。ただし、次々期システム展開作業後、撤去作業まで期間、撤去機器の保管場所の確保は各拠点で行う。
- ② ①の実現にあたって 受託者は、不要となる機器（以下「不要機器」という。）を事前に把握するために現地調査を実施し、不要機器の保管場所及び機器の一覧を作成し、各組織に確認を行い、各拠点担当者から承認を得ること。
- ③ 撤去・搬出・廃棄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、全て受託者の負担とすること

(2) データ消去

- ① 契約満了時又は解除時後のデータ消去は受託者の責任において行い、設置されている各拠点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機類、無線 LAN 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。
- 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、受託者の負担で用意すること。
- ④ データ消去作業終了後、受託者は、データの消去完了を明記した証明書を機構本部に提出すること。

(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、受託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。

ア) 受託者は、「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。

イ) 廃棄作業完了後、受託者は、廃棄作業が適法に完了したことを示す廃棄完了証明書または廃棄作業報告書を各拠点担当者に提出すること

ウ) 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。

9.10 検収

- ① 本調達の受託者は、各拠点に納品される成果物等については拠点担当者に内容の説明を行い、拠点担当者の確認を受けること。
- ② 受託者は納品期日までに全拠点担当者の確認を受け、これを以って機構本部担当者から検収を受けること。
- ③ 検収の結果、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、変更点について機構本部及び各拠点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。

9.11 作業場所

- ① 本調達において各拠点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、受託者の責任において用意すること。また、必要に応じて機構本部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 各拠点において作業場所が必要と受託者が判断する場合は、要件を明示すること。各拠点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 各拠点において、作業を行う場合には拠点担当者の指示に従うこと。

9.12 仕様書不適合責任

- ① 受託者は、本調達について検収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、その不適合が機構本部の指示によって生じた場合を除き（ただし、受託者がその指示が不相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。）、受託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機構本部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機構本部の承認を受けること。
- ② 前項の仕様書不適合責任期間経過後であっても、成果物等の不適合が受託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。

高専機構は、前各項の場合において、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、不適合を修正してなお生じる損害に対しても同様とする。

9.13 各高専による役務のオプション追加対応

役務の必要項目や作業レベルは各高専の事情により様々であるため、本調達で導入される全高専に共通の導入時の役務は必要最低限のものとする。

- ① 各高専の判断と費用負担により、本調達範囲外の役務を個別にオーダーできること。
- ② 各高専の判断と費用負担により、本調達範囲内の役務について作業範囲の拡大等を個別にオーダーできること。
- ③ これら各高専費用負担による追加は、本調達の契約とは別に、高専毎の発注及び契約とする。
- ④ 各高専の事情により追加オーダーを受託者以外に発注もしくは競争入札にかける場合は、適切な情報提供を行うこと。
- ⑤ 上記対応の各高専担当者からの依頼や問合せが可能な窓口を用意すること。サービスデスクからのエスカレーションを想定するが、本問合せ独自の窓口でもよい。
- ⑥ これらの目的を達するためのサービス提供形態・契約体系及び体制などについて、応札者が重要と考える点について提案すること。

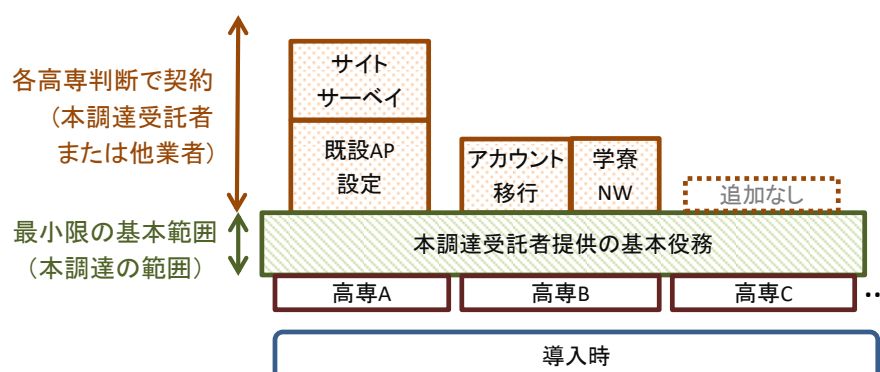


図 15 役務のオプション追加イメージ

表 6 想定される役務オプションの例(本調達には含まれない)

No.	想定される役務項目例	区分
1	無線 LAN のサイトサーベイ	調査
2	無線 LAN アクセスポイントの配置設計	設計
3	IPv6 への新規対応 (従来からの IPv6 利用部分は除く)	設計
4	セキュリティ診断	テスト
5	無線 LAN アクセスポイント設置後のサイトサーベイ	テスト
6	各高専既存の認証アカウント移行	移行

No.	想定される役務項目例	区分
7	各高専の独自の認証連携の切り替え作業	移行
8	標準構成の範囲をこえるネットワーク基盤サービス(DNS、DHCP 等)の設定移行	移行
9	受入テスト期間のオンサイトサポート	導入支援
10	学生寮ネットワークの設定変更・テスト	範囲外対応
11	既存無線 LAN の設定変更・テスト	範囲外対応
12	10G モジュールの追加	機器構成
13	サーバスイッチの追加及びスタック化	機器構成
14	無線 LAN アクセスポイントの追加	機器構成
15	無線 LAN コントローラの付加機能追加	機能追加
16	各高専での追加の個別教育実施	教育
17	各高専固有事情を反映したマニュアルの作成	教育

10. 特記事項

10.1 役割分担

別添資料5「受託者の役割」を参照のこと。

10.2 入札参加資格に係る事項

10.2.1 入札参加要件

(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（公財）日本情報処理開発協会による JIS Q27001 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。

10.2.2 応札者の実績

- 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・構築方法論を受託者自身が有し、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、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ことが望ましい。
- ③ 全国いずれかの高専もしく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ことが望ましい。
- ④ 本作業遂行において、高専機構本部及び各高専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、継続的实施に必要な組織、要員、設備及び施設を有していること。

10.2.3 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、全ての応札条件を満たすこと。

10.3 知的財産権の帰属

- ① 受託者は、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若しく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 受託者は、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 受託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、受託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、受託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、受託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、速やかに受託者に通知することとする。

10.4 遵守事項

10.4.1 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、受託者には履行義務・成果物作成義務が発生する。
- ③ 受託者は、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 高専機構本部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、担当職員との協議に応じること。

10.4.2 作業管理上の遵守事項

- ① 受託者は、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、本業務の遂行、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、機構本部担当者と協議・検討の上実施すること。
- ③ 本業務の契約履行期間の満了、全部もしくは一部の解除、又はその他契約の終了事由の如何を問わず、本業務が終了となる場合には、受託者は高専機構が継続して本業務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。

10.5 環境への配慮

10.5.1 グリーンコンピューティング（グリーン IT）への対応

- ① 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。

10.6 下請負に関する事項

10.6.1 下請負の制限及び下請負を認める場合の条件

- ① 本調達の受託者は、業務の全部を第三者に下請負することはできない。
- ② 受託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 受託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、受託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託者の責任とする。
- ⑤ 高専機構本部の求めに応じて、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 高専機構本部の求めに応じて、受注事業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。

10.6.2 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、下請負の必要性等について記載した別添の下請負承認申請書を高専機構本部に提出し、あらかじめ承認を受けること。
- ② 本調達の受託者は、業務の一部でも下請負する場合、下請負の内容、含まれる情報、下請負先及び下請負に対する管理方法等を事前に高専機構本部と協議の上、承認を得ること。
- ③ 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本部に提出し、承認を受けること。

10.7 その他特記事項

- ① サプライチェーンリスクマネジメントについて
 - ア) 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。
 - イ) 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。

ウ) 本業務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。

エ) 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。

- ・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

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。