サテライトトカマク事業のための外来研究者用ネットワークの構築

Establishment of a network for visiting researchers in the satellite tokamak project

仕様書

国立研究開発法人量子科学技術研究開発機構
那珂フュージョン科学技術研究所
先進プラズマ研究部 先進プラズマ統合解析グループ

1. 一般仕様

1.1 件　名

サテライトトカマク事業のための外来研究者用ネットワークの構築

1.2 目　的

国立研究開発法人量子科学技術研究開発機構（以下「QST」という。）那珂フュージョン科学技術研究所（以下「QST 那珂」という。）では、幅広いアプローチ活動のサテライトトカマク計画（「以下「STP」という。）において、JT-60SA のプラズマ加熱実験に向けた整備を実施している。

本仕様書は、STP に関連して QST 那珂に滞在する外来研究者等が使用するネットワーク及び端末認証システム整備の仕様を定めたものである。

1.3 業務内容

外来研究者用ネットワークの整備　　1 式

1.4 納　期

令和 8 年 9 月 30 日

1.5 納入場所及び納入条件

本件にて整備する機器の納入場所と納入条件は以下のとおりとする。

(1) 納入場所

茨城県那珂市向山 801 番地 1

QST 那珂　JT-60 制御棟 031 号室、JT-60 制御棟 1F 中央制御室及び計算機室他

(2) 納入条件

据付調整後渡しとする。

1.6 検査条件

2 項に記す調達機器の仕様、据付調整、機能設定、動作試験及び 1.8 項に記す提出図書の確認、機器の員数確認及び正常動作の確認（試験検査要領書に基づく動作試験を実施し、全ての試験項目において問題ないことを確認する。）をもって検査合格とする。

1.7 保　証

受注者は、本件に基づいて施工したものが、本仕様書の諸条件を完全に満たすことを保証するものとする。

1.8　提出図書

表 1 に示す図書を提出すること。

表１　提出図書一覧

図　書　名		提 出 時 期	部 数	確 認
①	作業工程表	契約後速やかに	3部	要
②	体制表（従事者、連絡先を含むこと。）	契約後速やかに	3部	要
③	方式設計書	要件協議後速やかに	3部	要
④	試験検査要領書	検査開始2週間前まで	3部	要
⑤	試験検査成績書	試験実施後1週間以内	3部	要
⑥	納入機器物品リスト	納入時	3部	不要
⑦	作業実施報告書	納入時	3部	不要
⑧	機器設定書	納入時	3部	不要
⑨	管理者向け操作マニュアル	納入時	3部	不要
⑩	ユーザ向け接続操作マニュアル	納入時	3部	不要
⑪	外国人来訪者票（QST指定様式）	入構の2週間前まで（外国籍の者、又は、日本国籍で非居住の者の入構がある場合に提出すること）	1部	要
⑫	再委託承諾願（QST指定様式）	作業開始2週間前まで（下請負等がある場合に提出すること）	1部	要
⑬	前記①～⑫の提出資料を格納した電子データ	試験終了後速やかに	2部(電子媒体)	不要

(提出場所)

QST 那珂　先進プラズマ研究部　先進プラズマ統合解析グループ

(確認方法)

提出書類の「確認」は次の方法で行う。

QST は、確認のために提出された図書を受領したときは、確認日を記載の上、受領印を押印して返却する。また、図書を提出後、期限日までに修正等を指示しないときには、確認したものとする。なお、「外国人来訪者票」は、QST の確認後、入構の可否を文書で通知する。「再委託承諾願」は、QST の確認後、書面にて回答する。

(電子媒体)

提出図書は、MS Word、MS Excel 等で作成し提出すること。また、電子媒体は CD-R 又は DVD-R を用いて提出すること。なお、電子媒体にはオリジナルファイルの他に PDF ファイルも添付すること。ただし、この方法によることができない電子データについては、QST の情報セキュリティ実施規程等を遵守し、QST と協議して提出方法を決定すること。

1.9　情報セキュリティの確保

情報セキュリティの確保については、別添 1『本契約において遵守すべき「情報セキュリティの確保」に関する事項』のとおりとする。

1.10　品質保証

(1) 本作業に係る全ての工程において、以下の事項について十分な品質管理を行う。

A. 管理体制

B. 設計管理

C. 外注管理

D. 現地作業管理

E. 物品管理

F. 工程管理

G. 試験・検査管理

H. 不適合管理

また、その計画については、品質保証計画書を提出し、QST より承認を受けること。設計管理については設計レビュー及び検証を行うこと。試験・検査管理については受注者により認定された検査員による検査及び試験を行うこと。すべての管理についての監査は受注者による定期的な内部監査を行うこと。

(2) 重大不適合が発生した場合、直ちにその内容を QST に報告するとともに、影響を最小限に抑え、要求された品質を維持するため、その処置方法を検討し、速やかに QST に提案し、その承認を得なければならない。

(3) QST は、受注者に対して事前に通知することにより、受注者の品質保証に係る受注者監査を実施できるものとする。

(4) 受注者は、本契約の履行状況を確認するため、QST 側が認める者に対して特定した作業場所に立ち入る権利（立入り権）を有することに同意すること。
また、作業場所への立入りは、検査等への立会い及び定期的会合への参加の他、受注者に対して事前に通知することにより、必要に応じて実施することができるものとする。

(5) 受注者は、本契約の適切な管理運営を証明するために必要な文書及びデータを提供すること。

(6) QST は、受注者が本契約の履行に当たって、契約書等の要求事項を満足できないことが認められる等、必要な場合は、受注者に作業の停止を命じることができる。

(7) 受注者は、QST から作業停止命令が発せられた場合には、可及的速やかに当該作業を停止し、QST の指示に従い要求事項を満足するよう必要な措置を講ずるものとする。

(8) 受注者は、本契約一般条項の規定に従い、下請負人に対し本契約の一部を履行させる場合、本仕様に係る一切の義務を受注者の責任において当該下請負人者に遵守させるものとする。

1.11 契約不適合責任

契約不適合責任については、契約条項のとおりとする。

1.12 グリーン購入法の推進

(1) 本契約において、グリーン購入法（国等による環境物品等の調達の推進等に関する法律）に適用する環境物品（事務用品、OA 機器等）が発生する場合は、これを採用するものとする。

(2) 本仕様に定める提出図書（納入印刷物）については、グリーン購入法の基本方針に定める「紙類」の基準を満たしたものであること。

1.13 協議

本仕様書に記載されている事項及び本仕様書に記載のない事項について疑義が生じた

場合は、QST と協議の上、その決定に従うものとする。

1.14　その他

（1）受注者は、QST が量子科学技術の研究・開発を行う機関であり、高い技術力及び高い信頼性を社会的に求められていることを認識するとともに、QST の規程等を順守し、安全性に配慮しつつ業務を遂行しうる能力を有する者を従事させること。

（2）受注者は、本件業務を実施することにより取得したデータ、技術情報、成果その他のすべての資料及び情報を QST の施設外において、発表若しくは公開することはできない。ただし、あらかじめ書面により QST の承認を受けた場合はこの限りではない。

（3）受注者は、異常事態等が発生した場合、QST の指示に従い行動するものとする。

2. 技術仕様（ネットワークの整備）

本項では、サテライトトカマク事業外来研究者用ネットワークの整備に関する技術仕様を述べる。

2.1 概要

QST 那珂では、滞在する外来研究者等が業務を行うためのオフィスネットワーク環境の構築を進めている。外来研究者用オフィスネットワーク環境構築にあたっては、外来研究者のネットワーク利用時の利便性の向上を図ることと同様に、ネットワークセキュリティの確保も必要不可欠な要素となる。

このため、端末認証装置を導入し接続許可のない端末の接続を制限することで、セキュリティ対策の不十分な機器の持ち込みを防ぎ、セキュアなオフィスネットワーク環境を構築すると共に、外来研究者の利便性にも配慮した接続環境の円滑な運用を図る。

2.2 調達機器の仕様

本契約で調達する機器とその仕様一覧を表 2 に示す。表 2 に示す各機器について、2.3 項に示す据付調整及び機能設定を実施すること。

表 2 調達機器一覧と仕様

No	品名(型番)	仕様	数量
①	ディストリビューションスイッチ (Cisco Catalyst C9300X-24HX：相当品可)	・SFP+/SFP28 ポート x8 以上のネットワークモジュールを備えること。 ・10GBASE-T RJ-45 ポート x24 以上備えること。 ・ホットスワップ対応冗長電源を備えること。 ・DHCP relay 機能を備えること。 ・DNA Advantage ライセンスが付属すること。	1 台
②	端末認証装置 (Cisco Identity Service Engine アプライアンス：相当品可)	・EAP-TLS (IEEE 802.1X)によるクライアント証明書インストール方式のネットワークアクセスコントロール（NAC）認証を、無線/有線端末に対して統一的に適用可能であること。 ・証明書を内部 CA にて発行できること。ユーザデータを内部 DB で管理できること。	1 台

		・クライアント証明書が未インストールの BYOD 端末が接続されると EAP-TLS 認証が失敗し、dACL により証明書プロビジョニングに必要なサービス以外へのアクセスを禁止できること。上記は、２．フロアスイッチより下流にイーサネットハブ等がさらに接続される場合（L2 多段接続）に対しても、端末を特定して機能すること。 ・ユーザが現地で SCEP に基づく証明書プロビジョニングを行う前に、管理者によるユーザ事前登録を必須とする運用を実現できること。 ・100 端末まで利用可能とすること。 ・完全に英語での UI に対応すること。	
③	無線 LAN コントローラ (Catalyst 9800-L-C：相当品可)	・無線 AP を 30 台以上制御できること。 ・RRM によるカバレッジ最適化を自動実行可能であること。 ・端末認証装置(Cisco Identity Service Engine アプライアンス)と連携した証明書ベース NAC 認証（Central WebAuth、BYOD プロビジョニング）が実装可能であること。 ・EAP-TLS 認証、WPA2/WPA3 Transition モード、複数 SSID/VLAN 制御、QoS 機能をサポートすること。	1 台
④	フロアスイッチ (Cisco Catalyst 9200L-24PXG-4X：相当品可)	・SFP+ 10GBASE-SR ポート x4 以上を備えること。 ・1GBASE-T 以上の PoE 給電ポート x 24 以上備えること。 ・ホットスワップ対応冗長電源を備えること。 ・DNA Advantage ライセンスが付属すること。 ・QoS を利用可能であること。	3 台
⑤	無線アクセスポイント (Catalyst 9166I：相当品可)	・最大 5Gbps のマルチギガビット接続に対応すること。 ・フロアスイッチ(Cisco Catalyst 9200L-24PXG-4X)からの PoE 給電で動作すること。	13 台

		・IEEE 802.11ax 対応、トライバンド対応であること。 ・RRM, CleanAir をサポートすること。 ・EAP-TLS 認証、WPA2/WPA3 Transition モードをサポートすること。	
⑥	光トランシーバモジュール(Cisco 10/25GBase-LR：相当品可)	・10/25GBASE-LR SFP28 光トランシーバ ・LC-LC OS2 光パッチケーブルに対応すること。	2 個
⑦	光トランシーバモジュール(Cisco 10GBase-SR：相当品可)	・10GBASE-SR SFP+光トランシーバ ・LC-LC 光パッチケーブルに対応すること。	6 個
⑧	光パッチケーブル（AFP2-DLC/DLC-SM-10：相当品可）	・シングルモード(OS2)光パッチケーブル 10m ・LC-LC Duplex コネクタ（クリップ付）	2 本
⑨	光パッチケーブル（AFP2-DLC/DLC-OM4-03：相当品可）	・マルチモード(OM4)光パッチケーブル 3m ・LC-LC Duplex コネクタ（クリップ付）	6 本

2.3　据付調整及び機能設定

下記に指定する各設置場所に機器を据付けること。なお、ラックマウントキット、電源ケーブルなど、機器の据付けや動作に必要な部材、物品類は全て本仕様に含めること。

また、指定する機器について、機能を実現する設定を実施すること。 設定に際し、必要な機微情報の共有は契約後の要件協議によることとし、設定機能の詳細や構築内容等については、機器設計書に詳細に記載の上、提出すること。

2.3.1 JT-60 制御棟 031 号室への機器の据付及び機能設定

(1) 機器の据付

① 既設 19 インチサーバーラック内への機器の設置

- 既設 19 インチサーバーラック内に表 2 中の No.①ディストリビューションスイッチ、No.②端末承認装置、No.③無線 LAN コントローラを据付け、あるいは格納すること。図 1 に JT-60 制御棟 031 号室ラック内機器据付概略図を記す。
- 設置、格納位置については、QST の指示に従うこと。なお、機器の電源ケーブルは、本仕様の範囲内とする。

② 光トランシーバモジュールの装着

- 19 インチサーバーラック内に据付けたディストリビューションスイッチに表 2 No.⑥、⑦(3 個)の光トランシーバモジュールを装着すること。
- 装着するポートについては、QST の指示に従うこと。

③ ディストリビューションスイッチの接続

- JT-60 制御棟 031 号室内に設置される既設光成端箱とディストリビューションスイッチ間を表 2 No.⑧の光パッチケーブルにて接続すること。
- 光パッチケーブルを用いて接続するディストリビューションスイッチのポート及び光成端箱の接続箇所については、QST の指示に従うこと。

④ 端末承認装置、無線 LAN コントローラ及びフロアスイッチの接続

- 19 インチサーバーラック内に設置された端末承認装置及び無線 LAN コントローラとディストリビューションスイッチを接続すること。なお、機器間の接続に使用する UTP ケーブルは、本仕様の範囲内とする。

⑤ 各フロア用光成端箱との接続

- 19 インチサーバーラック内に設置された JT-60 制御棟 1F EPS 室用、中央制御室用及び計算機室用の各光成端箱とディストリビューションスイッチ間を表 2 No.⑨の光パッチケーブルにて接続すること。
- ディストリビューションスイッチの接続ポート及び光成端箱の接続箇所については、QST の指示に従うこと。

(2) 機能設定

① ディストリビューションスイッチ

- QST の指示に従い VLAN 設定及び IP 設定を行うこと。
- QoS 設定として、音声パケット（DSCP 46）に低遅延キュー（LLQ）に割り当てるポリシーを定義し、QST が指定するポートに適用すること。
- QST が指定するサーバへシスログを送信するように設定を行うこと。
- 構築するゲストネットにおける DHCP Relay として機能し、DHCP メッセージ（Discover / Request 等）を QST が指定する DHCP サーバ及び 端末認証装置に中継する（DHCP Probe）ように設定すること。
- DHCP メッセージ中の各種 DHCP オプション（Fingerprint 情報を含む）が保持されたまま端末認証装置に到達し、ISE による端末プロファイリング（Endpoint Profiling）が適切に行われる設定を行うこと。

② 端末認証装置

a. 統一認証方式

- BYOD 端末の接続を想定し、有線と無線の証明書ベースのクライアント端末認証（EAP-TLS (802.1X)）に統一すること。
- 証明書は端末認証装置内部 CA にて発行すること。
- ユーザデータは端末認証装置内部データベースで管理すること。

b. 証明書発行プロセス

- 接続にはユーザによる事前申請を必須とし、管理者が申請情報に基づく Guest Account 登録を実施し、現地でユーザが端末証明書インストールを行うためにアクセスすることになる Guest Portal へのログインに必要なパスワード等を発行する処理フローを実現できること。
- BYOD 端末のオンボーディング機能を有し、SCEP 方式による証明書プロビジョニングを可能とすること。
- SCEP にネイティブ対応しない Linux 端末についても、秘密鍵がネットワークに流れない方式での証明書インストール手段を提供すること。
- 管理者が発行したパスワード等による Guest Account 認証（Guest Portal ログイン）後に証明書プロビジョニングが行われるように設定すること。
- Guest Portal へアクセスできる Guest Account の有効期限を設定可能とし、使用後は失効処理が可能であること。証明書の有効期限を設定可能であること。
- 同一証明書での有線・無線両方での接続を可能とすること。

c. 未認証端末のアクセス制御

- 未認証端末が接続する Onboarding VLAN は、認証後接続可能となる VLAN と同一とする。ただし未認証端末に対しては、ダイナミック ACL (dACL) によりアクセス先を DNS、DHCP、NTP、証明書プロビジョニングポータルのみに限定すること。
- アクセススイッチに L2 多段接続（例：イーサネットハブ）を許容し、ハブを介して有線接続される端末についても、dACL に基づき端末を特定したアクセス制御を可能とすること。

d. 端末プロファイリング機能

- ディストリビューションスイッチから送信される DHCP Relay（DHCP Probe）等を受信し、端末プロファイリング（Endpoint Profiling）に利用できること。
- フロアスイッチから送信される DHCP Probe, DHCP SPAN Probe, RADIUS Accounting 情報等を受信し、Endpoint Profiling に利用できること。
- 無線 LAN コントローラから送信される RADIUS Accounting 情報等を受信し、Endpoint Profiling に利用できること。

- DHCP Relay及びDHCP SPAN Probe から得た DHCP Fingerprint と RADIUS Accounting 情報等を総合し、Endpoint Profiling が適切に行われるよう ISE のプロファイル設定を構成すること。接続される端末とそのプロファイル情報を総合して Endpoint Database として把握し、更新をログとして保全すること。

e. ログ及び監査

- ISE のログ（認証ログ・Endpoint Profiling ログ）は QST が指定する Syslog サーバへ、Syslog や pxGrid 等により送信するように設定すること。

f. 端末証明書の更新

- 端末証明書の更新は、毎回申請・承認手続きと管理者による Guest Portal へのアクセス許可操作を必須とする運用とし、SCEP により自動更新されない設定が可能であること。

③ 無線 LAN コントローラ

- BYOD 端末の接続を想定し、証明書ベースのクライアント端末認証（EAP-TLS (802.1X)）を端末認証装置によって行えるように相互の設定を行うこと。認証方式は EAP-TLS のみ許可する設定とする。
- 未認証端末が接続された場合、端末認証装置と連動してダイナミック ACL (dACL) を適用し、証明書プロビジョニングに必要なアクセス先以外にはアクセスできないように設定すること。
- 端末認証装置側でセッション監視、ログ保存、ポリシー変更時のセッション再認証や切断を行えるように設定すること。
- 無線クライアントの接続情報（MAC アドレス、端末種別、アクセスポイント情報、セッション情報など）を RADIUS Accounting として端末認証装置（Cisco ISE）へ送信できるよう適切に設定すること。
- 動作ログは QST が指定する Syslog サーバへ送信するように設定すること。

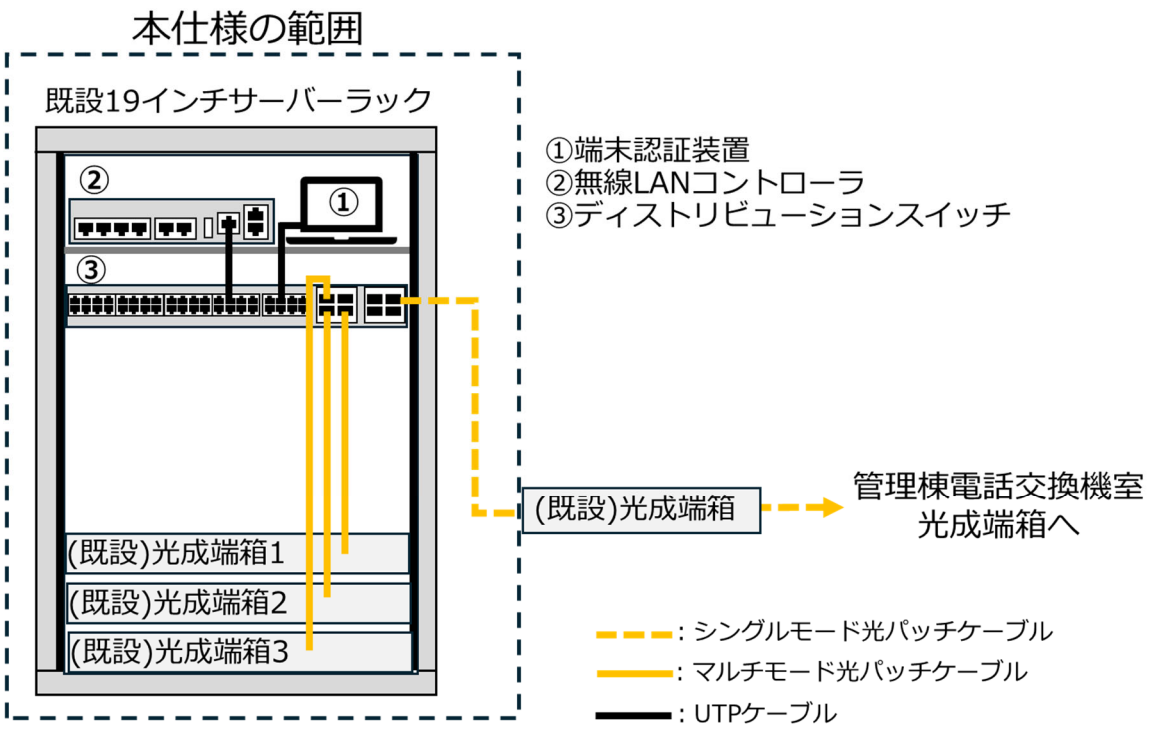

図 1　JT-60 制御棟 031 号室ラック内機器据付概略図

2.3.2 JT-60 制御棟中央制御室、計算機室への機器の据付及び機能設定

(1) 機器の据付

① フロアスイッチの設置

- JT-60 制御棟中央制御室及び計算機室内の既設 19 インチサーバーラックに各々 1 台を据付けること。図 2 に JT-60 制御棟中央制御室及び計算機室内の機器据付概略図を示す。
- 据付位置については、QST の指示に従うこと。なお、機器の電源ケーブルは、本仕様の範囲内とする。

② 光トランシーバモジュールの装着

- 各 19 インチサーバーラック内に据付けたフロアスイッチに表 2 No.⑦の光トランシーバモジュール各 1 個を装着すること。
- 装着ポートについては、QST の指示に従うこと。

③ ネットワーク機器の接続

- 各 19 インチサーバーラック内に据付けたフロアスイッチと同ラック内据付けられている光成端箱を表 2 No.⑨の光パッチケーブルで接続すること。
- 光パッチケーブルを用いて接続するフロアスイッチのポート及び光成端箱の接続箇所については、QST の指示に従うこと。

④ 無線アクセスポイントの据付

- JT-60 制御棟中央制御室及び計算機室に各 3 台を据付けること。
- 据付位置については、電波調査を導入前に行い、QST と協議の上、決定すること。
- 各 19 インチサーバーラック内に組み込んだフロアスイッチと無線アクセスポイントを Cat6A の UTP ケーブルにて PoE 接続すること。
- 機器間の接続に必要となる UTP ケーブル及び UTP ケーブルの布設は本仕様の範囲内とする。

(2) 機能設定

①フロアスイッチの設定

- 端末接続情報（MAC アドレス、インターフェース情報、セッション情報など）を RADIUS Accounting として端末認証装置（Cisco ISE）へ送信できるよう設定すること。
- DHCP Probe, DHCP SPAN Probe 及び RADIUS Accounting による端末接続情報を、端末認証装置（Cisco ISE）へ送信できるよう設定を行い、端末プロファイリング（Endpoint Profiling）が適切に行われるよう調整すること。

②無線アクセスポイントの設定

- 異なる VLAN に属する複数の SSID を扱うため、無線アクセスポイントとの接続は trunk 設定とする。
- 無線暗号化方式は WPA3/WPA2（EAP-TLS 802.1X）Transition Mode を採用すること。
- BYOD 端末の接続を想定し、証明書ベースのクライアント端末認証（EAP-TLS (802.1X)）を、端末認証装置（Cisco ISE）によって行えるように相互の設定を行うこと。認証方式は EAP-TLS のみ許可する設定とする。
- 未認証端末が接続された場合、端末認証装置と連動してダイナミック ACL (dACL) を適用し、証明書プロビジョニングに必要なアクセス先以外にはアクセスできないように設定すること。
- 端末認証装置側でセッション監視、ログ保存、ポリシー変更時のセッション再認証や切断を行えるように設定すること。
- 動作ログは QST が指定する Syslog サーバへ送信するように設定すること。
- JT-60 制御棟 031 号室に設置される無線 LAN コントローラ(Catalyst 9800-L-C) 及び端末認証装置(Cisco Identity Service Engine アプライアンス)に本無線アクセスポイントの設置情報を反映させること。

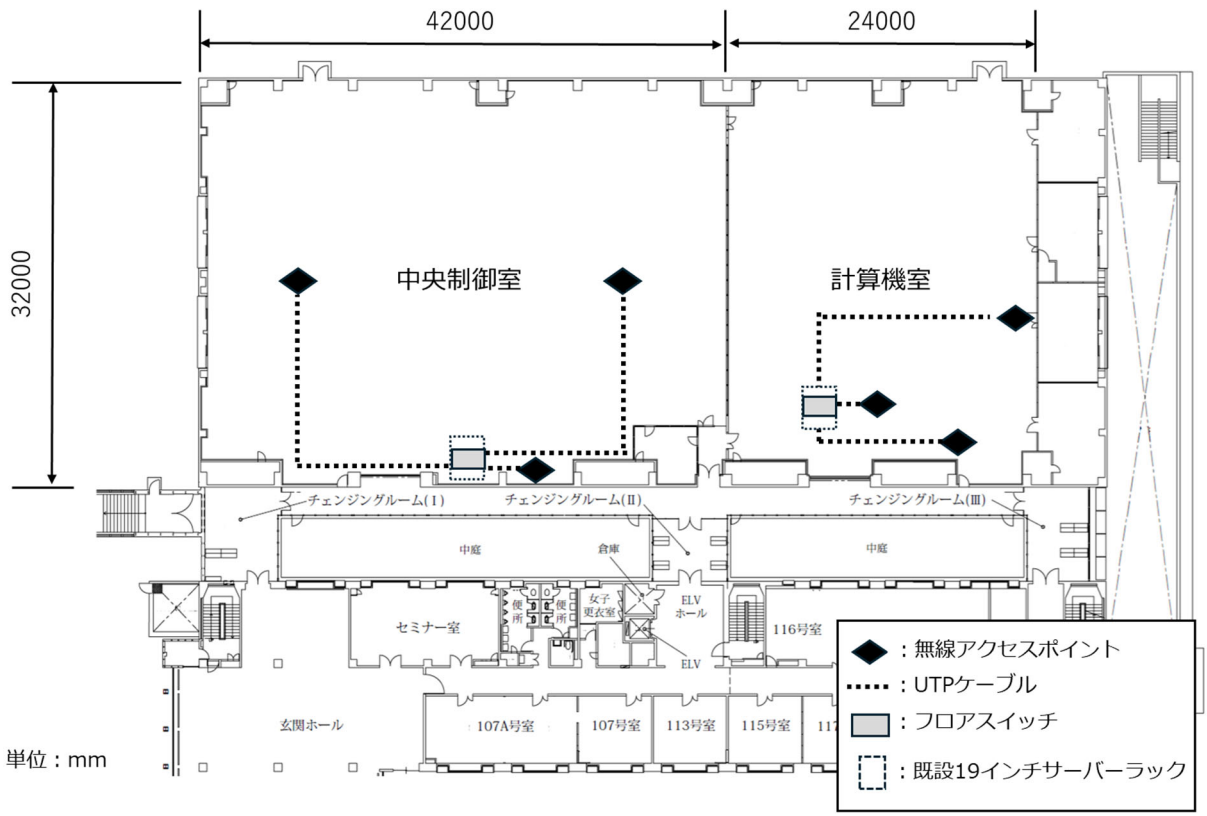

図 2 JT-60 制御棟中央制御室及び計算機室内の機器据付概略図

2.3.3 JT-60 制御棟 1F、 2Ｆへの機器の据付及び機能設定

(1) 機器の据付

① フロアスイッチの設置

- JT-60 制御棟 1F EPS 室内の既設ラックに据付けること。図 3 に JT-60 制御棟 1F 及び２Ｆの機器据付概略図を示す。
- 据付位置については、QST の指示に従うこと。なお、機器の電源ケーブルは、本仕様の範囲内とする。

② ネットワーク機器の接続

- ラック内に据付けたフロアスイッチと同ラック内据付けられている光成端箱を表２No.⑨の光パッチケーブルで接続すること。
- 光パッチケーブルを用いて接続するフロアスイッチのポート及び光成端箱の接続箇所については、QST の指示に従うこと。

③ 無線アクセスポイントの据付

- JT-60 制御棟 2F の会議室、居室及び廊下側面に計 7 台を据付けること。なお、据付位置については、電波調査を導入前に行い、QST と協議の上、決定すること。

- JT-60 制御棟 1F EPS 室内に据付けたフロアスイッチを起点とし、Cat6A の UTP ケーブルを布設し、PoE 接続すること。なお、機器間を接続する UTP ケーブルの布設作業も本仕様に含めるものとする。

④ 情報コンセントの据付け

- 無線アクセスポイントと同様に JT-60 制御棟 1F EPS 室内に据付けたフロアスイッチを起点に JT-60 制御棟 2F に Cat6A の UTP ケーブルを布設し、情報コンセントを 6 箇所に据付けること。据付位置については、QST と協議の上、決定すること。
- 情報コンセントの据付け、UTP ケーブルの布設作業及び UTP ケーブルは、本仕様に含めるものとする。

(2) 機能設定

前項 2.3.2 JT-60 制御棟中央制御室及び計算機室への機器の据付 (2)機能設定 無線アクセスポイントの設定に同じ。

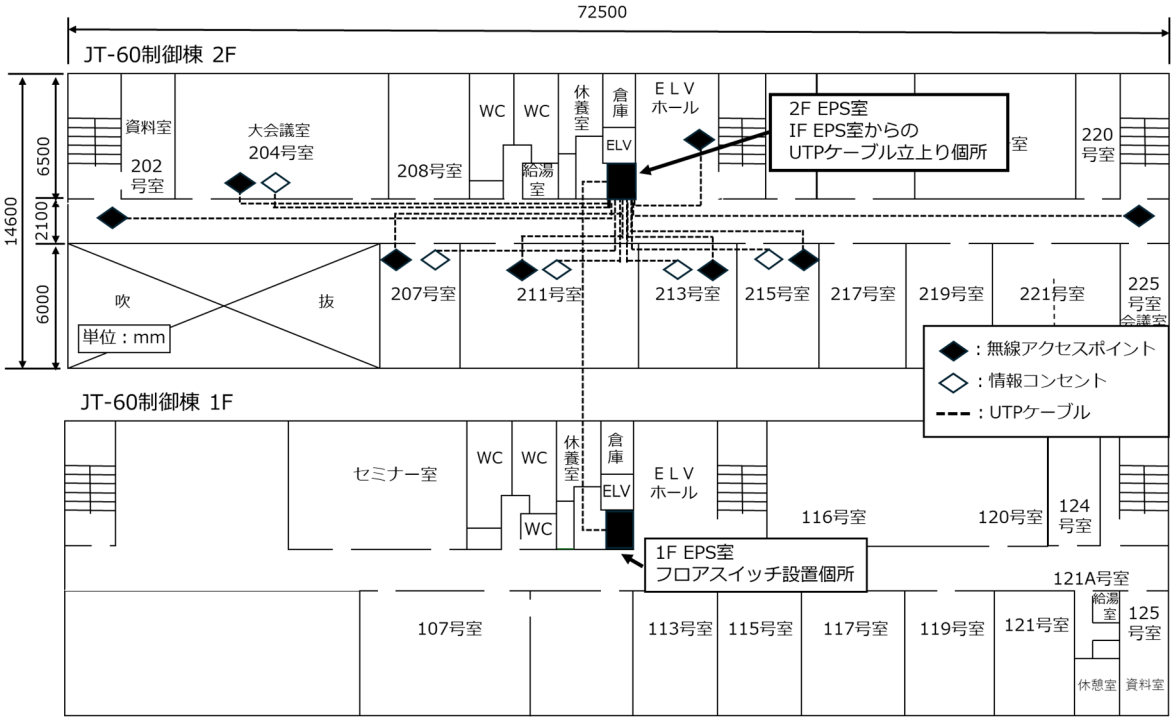

図 3 JT-60 制御棟 1F 及び 2 F の機器据付概略図

2.4 動作試験

本契約において構築整備した機能について、試験検査要領書を作成し、必要な機能確認試験を実施すること。試験検査要領書は、実施前に QST 担当者に提出し、確認を得ること。なお、試験に必要な端末は QST が提供する。

別添 1　本契約において遵守すべき「情報セキュリティの確保」に関する事項

1）　受注者は、QST の情報セキュリティポリシーを遵守すること。
2）　受注者は、本件で取得した QST の情報を、QST の許可なしに本件の目的以外に利用してはならない。本件の終了後においても同様とする。
3）　受注者は、本件で取得した QST の情報を、QST の許可なしに第三者に開示してはならない。本件の終了後においても同様とする。
4）　本件の履行に当たり、受注者は従業員又はその他の者によって、QST が意図しない変更が加えられることのない管理体制を整えること。
5）　本件の履行に当たり、情報セキュリティ確保の観点で、受注者の資本関係・役員等の情報、本件の実施場所、業務を行う担当者の所属・専門性(情報セキュリティに係る資格・研修実績等)・実績及び国籍に関する情報を求める場合がある。受注者は、これらの要求に応じること。
6）　本件に係る情報漏えいなどの情報セキュリティインシデントが発生した際には、速やかに QST 担当者に連絡し、その指示の元で被害拡大防止・原因調査・再発防止措置などを行うこと。
7）　受注者は、QST から本件で求められる情報セキュリティ対策の履行状況を QST からの求めに応じて確認・報告を行うこと。またその履行が不十分である旨の指摘を受けた場合、速やかに改善すること。
8）　受注者は、機器、コンピュータプログラム、データ及び文書等について、QST の許可無く QST 外部に持ち出してはならない。
9）　受注者は、本件の終了時に、本件で取得した情報を削除又は返却すること。また、取得した情報が不要となった場合も同様とする。
10）本件で作成された著作物（マニュアル、コンピュータプログラム等）の所有権は、QST に帰属するものとする。
11）本件の履行に当たり、その業務の一部を再委託するときは、軽微なものを除き、あらかじめ再委託の相手方の住所、氏名、再委託を行う業務の範囲、再委託の必要性及び金額等について記載した書面を QST に提出し、承諾を得ること。その際受注者は、再委託した業務に伴う当該相手方の行為について、QST に対しすべての責任を負うこと。
12）本契約において、特に下記の点について遵守すること。

A.　情報セキュリティ教育の実施

受注者は、作業担当者に対する適切な情報セキュリティ教育を実施すること。

B. 不正プログラム感染防止

受注者は、本業務に使用するパソコン等の端末において、不正プログラムの感染を防止するため、次の事項を遵守すること。

① 不正プログラム対策ソフトウェア等により不正プログラムとして検知された実行ファイルを実行せず、データファイルをアプリケーション等で読み込まないこと。

② 不正プログラム対策ソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル、使用 OS、インストールアプリケーション等について、これを常に最新の状態に維持すること。

③ 不正プログラム対策ソフトウェア等による不正プログラムの自動検査機能を有効にすること。

④ 不正プログラム対策ソフトウェア等により定期的にすべての電子ファイルに対して、不正プログラムの有無を確認すること。

⑤ 外部からデータやソフトウェアをパソコン等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること。

⑥ 不正プログラム感染の予防に努めること。具体的には、以下を例とする不正プログラム対策を講ずること。

a） 不審なウェブサイトを閲覧しないこと。

b） アプリケーション利用において、マクロ等の自動実行機能を無効にすること。

c） プログラム及びスクリプトの実行機能を無効にすること。

d） 安全性が確実でないプログラムをダウンロードしたり実行したりしないこと。

⑦ 作業者は、パソコン等の端末（支給外端末を含む）が不正プログラムに感染したおそれのある場合には、感染したパソコン等の端末の通信回線への接続（LAN ケーブル等）を速やかに取り外し、QST 担当者にその旨を報告すること。

C. アカウント及びパスワード等の管理

① 作業者は、自己に付与されたアカウント以外の識別コードを用いて、情報システム を利用しないこと。

② 作業者は、自己に付与されたアカウントを適切に管理すること。

a） 自己に付与されたアカウントを他者に付与及び貸与しないこと。

b） 自己に付与されたアカウントを、それを知る必要のない者に知られるような状態で放置しないこと。

c） 業務のためにアカウントを利用する必要がなくなった場合は、その旨をQST 担当者に届け出る。

③ 作業者は、管理者権限を持つアカウントを付与された場合には、管理者としての業務遂行時に限定して、当該アカウントを利用すること。

④ 作業者は、自己の管理するパスワード等の利用者認証情報の管理を徹底すること。

a） パスワード等を用いる場合には、以下の管理を徹底すること。

(1) 仮のパスワード等は、最初のログイン時点で変更すること。

(2) 自己のパスワード等を他者に知られないように管理すること。メール等で送信しないこと。

(3) 自己のパスワードを内容が分かる状態でメモや付箋等に記入し、モニタ、端末本体及びその周辺に貼付するようなことがないようにすること。

(4) 自己のパスワード等を他者に教えないこと。

(5) パスワード等を忘却しないように努めること。

(6) パスワード等を設定するに際しては、十分な長さ（英数記号交じり 13 桁以上）とし、文字列は容易に推測されないものにすること。

(7) 端末に、パスワード等を記憶させない、または暗号化等を行うことによって他人がパスワードを読めないようにすること。

b） IC カード等（所有による利用者認証）を用いる場合は、以下の管理を徹底すること。

(1) IC カード等を本人が意図せずに使われることのないように安全措置を講じて管理すること。

(2) IC カード等を他者に付与及び貸与しないこと。

(3) IC カード等を紛失しないように管理すること。紛失した場合には、直ちに QST 担当者にその旨を報告すること。

(4) IC カード等を利用する必要がなくなった場合には、これを QST 担当者に返還すること。

c） パスワード等及び IC カード等の利用者認証情報が他者に使用され、またはその危険が発生した場合には、直ちに QST 担当者にその旨を報告すること。

D. 物理的セキュリティ及びログの保全

本契約で使用する作業用端末やハードウェアトークンは、不特定多数の者が作業端末にアクセス又は持ち出しができないよう、端末等にアクセスした人間を特定できる適切な物理的セキュリティ対策や入退管理の対策を講ずること。また、ログイン操作の記録を必要に応じて確認できるようログを保全する対策を講ずること。

E. 通信の暗号化

本契約作業に係るアクセスは全て SSH, HTTPS 等の暗号化可能なプロトコルに基づき行うこと。暗号化のなされていないメール等で機微情報を送受信しないこと。

F. 本契約で取り扱う情報やソフトウェアは、QST の許可なしに第三者に開示してはならない。本件の終了後においても同様とする。

以上