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保守

Maintenance 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

一般仕様

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保守

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、上記整備で導入されたネットワーク機器の保守の仕様を定めたものである。

3. 業務内容

ネットワーク機器の保守	1 式

4. 保守対象機器

下記の機器について保守を行うこと。

(1) ディストリビューションスイッチ	1 台
(2) 端末認証装置	1 台
(3) 無線 LAN コントローラ	1 台
(4) フロアスイッチ	3 台
(5) 無線アクセスポイント	13 台

5. 保守期間

４項に記す保守対象機器の据付け調整作業開始時～令和 9 年 3 月 31 日

6. 保守対象機器の設置場所

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

7. 保守・支援体制

7.1 保守体制

障害発生による影響を最小限に抑えるため、保守の実施体制を構築すること。
また、故障や問合せなどの連絡先及び担当者（電話番号、メールアドレスなど）を保守連絡体制表として作成し提出すること。

7.2 保守内容

(1) オンサイト保守（24H365D）を原則とし、5 項に記す保守期間中対応すること。
(2) 機器の修理・交換・機器の再設定を可能とし、ハードウェア障害対応は遠隔又は現地で速やかに問題切り分け作業に着手することが可能であること。
(3) 切り分け後の保守交換部品の手配から現地到着までは原則 4 時間以内とする体制を構築すること。
(4) 対応後速やかに書面又は電子ファイル形式（Microsoft Word、Excel 又は PDF 形式等）にて保守作業実施報告書を作成し、QST に提出すること。書面の形式については特に指定しない。また、QST 側が報告内容について説明を求めた場合には迅速に対応すること。

8. 検査条件

保守期間中、7.2 項に記す保守内容を満足し、9 項に記す提出図書の確認をもって検査合格とする。

9. 提出図書

表 1 に記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	保守連絡体制表	契約後速やかに	3 部	不要
②	保守作業実施報告書	実施の都度	3 部	不要
③	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
④	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

(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。

「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。

10. 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。

11. 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。

12. 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。

13. 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。

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