REC ネットワークセキュリティ強化用機器の保守契約

仕様書

令和 8 年 2 月

国立研究開発法人 量子科学技術研究開発機構
六ヶ所フュージョンエネルギー研究所
核融合炉システム研究開発部 BA計画調整グループ

1. 一般仕様

1.1件名 REC ネットワークセキュリティ強化用機器の保守契約

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「量研」という。)六ケ所フュージョンエネルギー研究所(以下「六ヶ所研」という。)では、国際核融合エネルギー研究開発センター(以下「IFERC」という。)事業の各活動に供する基盤ネットワークとして、IFERC ネットワークを整備し運用している。本件は、IFERC 事業計画における必要性を考慮し六ヶ所研 計算機・遠隔実験棟1階に導入されたファイアウォールを安定的に運用するための年間保守契約に関する仕様を定めるものである。

1.3提出図書

本契約において、以下の図書を各々の提出期日までに提出すること。

	図書名	様式指定	提出期日	部数	備考
1	障害時連絡体制対応表	指定なし	契約後及び変更の都度速やかに	3 部	
2	作業報告書 ・作業ごと及び保守期間終了時に年間分	指定なし	作業ごとの報告書は、 実施後速やかに提出	1 部	
	・書面及び電子ファイル形式	指定なし	作業報告書一式を保守期間終了時に提出	3 部	

1.4納入場所

青森県上北郡六ヶ所村大字尾駮字表舘2番地166 量研 六ヶ所研 管理研究棟 227号室

1.5契約期間

令和 8 年4月1日～令和 9 年3月31日

1.6検査条件

2.項に示す技術仕様を満足し、1.3項に示す作業報告書一式が提出されていることの確認をもって検査合格とする。

1.7特記事項

1.7.1 受注者の要件

受注者は、量研が量子科学技術の研究・開発を行う機関であるため、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し、日本国内法及び量研の規程等を遵守し、安全性に配慮した業務を遂行し得る能力を有すること。また、受注者は、既設のネットワーク機器を、迅速に修理・交換・機器の再設定を行うことができ、平日オンサイトでのハードウェア障害対応を問題の切り分け後4時間以内で着手可能であること。

1.7.2 技術情報の開示制限

受注者は、本契約を実施することによって得た技術情報を第3者に開示しようとするときは、あらかじめ書面による量研の承認を得なければならないものとする。量研が本契約に関し、その目的を達成するために受注者の保有する技術情報を了知する必要が生じた場合は、協議の上決定するものとする。

1.7.3 成果の公開

受注者は、本契約に基づく業務の内容及び成果について、発表若しくは公開し、又は特定の第3者に提供しようとするときは、あらかじめ書面による量研の承認を得なければならないものとする。

1.8 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。

1.9 グリーン購入法の推進

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。

1.10 その他

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、量研と協議の上、その決定に従うものとする。

2. 技術仕様

2.1保守に関する要求事項と概要

（1） 本契約が成立したら、速やかに障害時の連絡体制や対応について量研担当者と相談して決定し、「障害時連絡体制対応表」としてまとめ、書面にて量研担当者に提出すること。必要に応じて、「障害時連絡体制対応表」の改訂を行うこと。

（2） 2.2 項で示す機器に対して、オンサイト保守（24時間 365 日）を原則とし、1.5 契約期間に定める期間対応すること。オンサイト保守対応の駆けつけ時間は、原則問題切り分け完了後4時間以内とすること。ただし、量研六ヶ所研への到着時間が 17:00～翌朝 9:00 になる場合には、量研担当者に連絡し相談の上、翌営業日の午前中に訪問し、復旧のために必要な対応を行うこと。

（3） 2.2 項で示す機器に関する技術的な問合せへの対応を平日 9:00-17:00 で行うこと。

（4） 上記（2）の保守障害対応のために当該機器の監視システムを構築・運用すること。

（5） 障害対応後、障害発生から復旧までの作業内容及び障害の原因等について作業報告書を作成し、速やかに書面又は電子ファイル形式にて量研担当者に提出すること。また、量研担当者より説明を求められた場合には、説明を行うこと。

（6） 当該機器等のメーカー及び代理店等から、脆弱性情報、セキュリティパッチ提供、ファームウェアの更新及びリコール等の連絡及び発表があった場合には、量研担当者に対してその旨を通知し、量研担当者に対応に必要なソフトウェアを提供すること。

（7） （1）から（6）までの作業、保守及び修理時の交換部品、監視システム等構築及び運用費用等について、全ての費用を本契約に含むものとする。

2.2保守対象機器及びサービス

	機種名	型名	数量	備考
1	ファイアウォール	Palo Alto PA-1410 （脅威防御（ADV）, WildFire（ADV）ライセンスを含む）	1	
2	光トランシーバ	Palo Alto PAN-SFP-PLUS-SR	4	

以上

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、量研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、本件で取得した量研の情報を、量研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、本件で取得した量研の情報を、量研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、量研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、速やかに量研担当者に連絡し、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、量研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量研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、量研の許可無く量研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量研に提出し、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、量研に対しすべての責任を負うこと。
11）　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、量研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、その旨を量研担当者に届け出る。

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、直ちに量研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、これを量研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、直ちに量研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。

以上