REC ネットワークのセキュリティ強化改修

仕様書

令和 7 年 10 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

仕様書

1. 件名
REC ネットワークのセキュリティ強化改修

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。）六ヶ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、幅広いアプローチ活動協定に基づき、国際核融合エネルギー研究開発センター（以下「IFERC」という。）事業における基盤ネットワークとして、SINET6に接続したネットワークシステムを整備し運用している。
本仕様書は、ITER 遠隔実験センター活動におけるサービスの重要性の増大及び IT セキュリティを取り巻く環境の変化を考慮して、REC 関連外部向けサービスのセキュリティのさらなる強化を目的として行うシステム改修の仕様を定めるものである。

3. 納期
(1)5. に示す導入機器の設置、設定等
令和 8 年 2 月 27 日
(2)6. に示す保守
導入機器の検査後、令和 8 年 3 月 31 日まで

4. 納入場所
〒039-3212 青森県上北郡六ヶ所村大字尾駮字表舘2番地166
QST 六ヶ所研 計算機・遠隔実験棟 1 階 特殊設備室

5. 調達物
5.1 導入物品
(※相当品可とする。)

No	品名/型番	仕様	数量
1	ファイアウォール /Palo Alto PA1410	・アプリケーションレベルでの識別・制御が可能な次世代（L7）ファイアウォールであること。アプリケーションを識別する App-ID は毎月更新されること。自社開発アプリケーションにカスタム App-ID を割り当て可能であること。 ・10G SFP+ポートを4つ以上備えること。 ・Threat Prevention のスループットが 4.5Gbps 以上であること。 ・冗長電源を備えること。 ・マネジメントポートを備え、アウトオブバンド管理により管理プレーンとデータプレーンを完全に分離可能であること。 ・Advanced Threat Protection ライセンス、WildFire ライセンスを備えること。 ・既存機器との組み合わせを考慮する必要があるため、相当品を提案する場合には、事前に可否を問い合わせること。	1
2	SFP+モジュール/ Palo Alto PAN-SFP-PLUS-SR	・10GBASE-SR SFP+ 光トランシーバ ・LC-LC 光ファイバケーブルに対応すること。 ・1. のファイアウォールで使用可能であること。	4

3	L3 スイッチ /Yamaha SWX3220-16TMs	・10G SFP+ポートを 6 口以上を備えること。 ・10GBASE-T（RJ-45）ポート 4 口以上を備えること。 ・リンクアグリゲーション、ポートミラーリング、L3 ACL をサポートすること。	1
4	SFP+モジュール /Yamaha YSFP-10G-SR	・10GBASE-SR SFP+ 光トランシーバ ・LC-LC OM4 光ファイバケーブルに対応すること。 ・1. のファイアウォールで使用可能であること。	6
5	スイッチ付 PDU /APC AP7900B	・ネットワーク経由でアウトレット毎の ON/OFF を操作可能であること。 ・インプットプラグ：NEMA 5-15P、アウトレット：NEMA 5-15R 8 口以上を備えること。 ・100V に対応、許容入力電流 15A 以上であること。 ・ラック内への固定器具を含むこと。	2
6	光ファイバケーブル	・LC-LC OM4 Duplex 光ファイバケーブル ・長さ 1m	6

5. 2 据付調整

・導入機器は QST が指定する 19 インチ情報ラック内に設置すること。設置位置等詳細は QST 担当者と協議の上決定すること。機器のラック内設置位置や電源への接続情報は方式設計書に記載すること。

・導入機器の電源は可能な限り互いに異なる 5. のスイッチ付 PDU に接続し、PDU はそれぞれ異なる UPS に接続して可用性を確保すること。

・ネットワーク停止を伴う導入作業は、QST 担当者と日程を協議・調整の上実施すること。

・その他のラックマウントキット、電源ケーブルなど、設置に必要な部材類は、本契約内で用意すること。

・QST の既存ファイアウォールを「FW1」、1. ファイウォールを「FW2」、3. L3 スイッチを「中間 SW」として、-FW1-中間 SW-FW2-内部既存 L2 スイッチ（2）の順に、10G 光ファイバ2本の LAG で直列に接続すること（図1）。

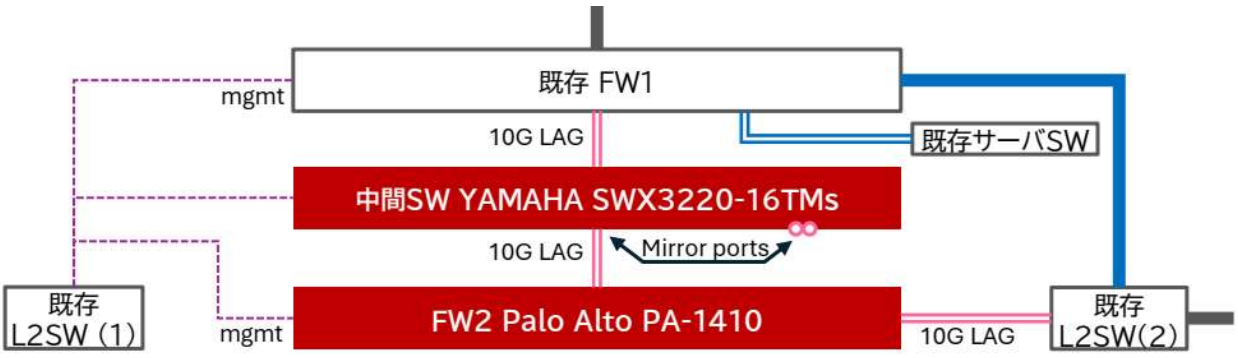

図1 物理結線のイメージ

・中間 SW、FW2 への管理アクセス用配線を上記 10G LAG とは独立に行うこと。

・スイッチ付 PDU は既存 LAN ケーブルを利用して、QST が指示するネットワークに接続すること。

・各ケーブルには、接続元と先を示すタグを付けること。

5. 3 機能設定

5.1 節の導入機器について、下記の機能を実現する設定を実施すること。

（1）VPN 終端、DMZ 等の外部と通信するセグメントは、これまで通りに FW1 で管理すること。

（2）FW1 と FW2 の間は単一の Transit VLAN により通信を行うように設定すること。

（3）内部セグメント間の通信は FW2 で掌握し App-ID に基づくアプリケーション制御を徹底可能な設定とすること。これにより、万一 FW1 を掌握された場合にも、FW2 で保護された内部セグメントへは既定の通信以外は不可能な多層防御構造を実現すること。

（4）FW2 の Advanced Threat Protection、WildFire の機能を有効にすること。SSL 復号処理の要否は、個々のサービスに対応した通信許可ごとに設定可能とすること。

（5）FW2 の管理アクセス、監視及び Syslog 送信、NTP サーバとの同期等は全てマネジメントポート経由で実施するように設定すること。また Transit VLAN の interface などデータプレーンにおける FW2 自身の IP 宛通信は全て拒否すること。

（6）FW2 と下流既存 L2SW(2)の接続は trunk 設定とすること。設定する VLAN 等の機微情報は契約締結後に提示する。

（7）図1における FW1 と下流既存 L2SW(2)の間の接続（青線）は当面維持して、青線を通って稼働中の FW1 管理下のサービスを、都合の良いタイミングで FW2 管理下セグメントへ移してピンクの線を通る動作へと移行できるよう、運用の自由度に配慮した設定とすること。

（8）FW2 の App-ID の更新確認・適用が可能な限り簡便に実施できるように設定すること。

（9）中間 SW において、Transit VLAN のミラーポートを設定すること。

（10）スイッチ付 PDU によりネットワーク越しに FW1、中間 SW、FW2 の電源を遮断可能とすること。

5. 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。試験に必要な端末は QST が準備する。

6. 保守

6. 1 運用時の保守

本契約で導入する装置の内 5.1 節の 1 の機器については、オンサイト保守（24 時間 365 日）を原則とし、令和 8 年3月31日まで対応すること。

保守は、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速やかに着手可能であること。

保守作業は、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）にて報告書を作成し、QST 担当者に提出すること。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。

6. 2 保守体制

保守の実施体制を構築すること。特に、QST 担当者が故障や問合せなど最初に連絡する連絡先及び担当者（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. 提出図書

下記の書類を提出すること。

図書名	提出時期	部数	確認
作業工程表	契約後速やかに	3部	要
作業体制表	〃	3部	要
再委託承諾願 （QST 指定様式）	〃（※再委託がある場合に提出。）	1部	不要
方式設計書	要件協議後速やかに	3部	要
物理ネットワーク配線図	〃	3部	要
試験検査要領書	検査着手前	3部	要
打合せ議事録	打合せ後速やかに	3部	要
試験検査成績書	試験実施後1週間以内	3部	要
納入機器物品リスト	納入時	3部	不要
実施作業報告書	〃	3部	不要
機器設定書	〃	3部	不要
管理者向け操作マニュアル	〃	3部	不要
保守連絡体制表	〃	3部	不要
電子データ	〃	3部	不要

（提出場所）

QST　六ヶ所研　核融合炉システム研究開発部　BA 計画調整グループ

8. 検査条件

（1）5. に示す導入機器の設置、設定等

5に示す物品・サービスの導入、機能設定、据付調整、動作試験、6に示す提出書類確認、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。

（2）6. に示す保守

保守期間中、6. に示す仕様を満足し、報告書が提出されていることの確認をもって検査合格とする。

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。

10. 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、成果その他の全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。

（4）受注者の故意又は過失により QST 又は第三者に損害を与えた場合、賠償等の措置を取ること。

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。

（要求者）
部課（室）名：六ヶ所研　BA 計画調整グループ
氏名：徳永　晋介

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) また本契約において、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。

①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。

②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。

③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。

①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。

a） 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。

b） 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。

c） 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。

d） 自己のパスワード等を他者に教えないこと。

e） パスワード等を忘却しないように努めること。

f） 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。

g） 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。

② 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。

a） 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。

b） IC カード等を他者に付与及び貸与しないこと。

c） 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。

d） 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。

③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