

# NanoTerasu基幹LAN加速器NW境界ファイアウォール更新 仕様書

国立研究開発法人量子科学技術研究開発機構

NanoTerasuセンター

高輝度放射光開発研究部 加速器グループ

# 1 一般仕様

## 1.1 件名

NanoTerasu 基幹LAN加速器NW境界ファイアーウォール更新

## 1.2 目的

本件は、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。）が運用するNanoTerasuにおいて、基幹LANと加速器制御ネットワークとの通信制御を行う機器（以下「基幹LAN-加速器NW境界ファイアーウォール」という。）のメーカーサポートが終了するため、後継機種に更新するものである。

## 1.3 契約範囲

NanoTerasu 基幹LAN加速器NW境界ファイアーウォール更新

## 1.4 納期

令和9年3月31日(水)

ただし、現行機の外し、後継機の導入及び運用開始は夏の加速器停止期間(2026年8月8日~同年9月14日)のうちに完了するものとし、実際の現地作業日は受注後に協議にて決定する。

実運用開始後の不具合や設定調整が必要であることが判明した場合に、冬の加速器停止期間(2026年12月17日~2027年1月20日)または協議によって決定した日時に行うものとする。

## 1.5 納入物件

### (1) 納入図書

図書名	提出時期	部数
作業工程表	契約後速やかに	1部
システム設計書	作業前	1部
切り替え手順書	作業前	1部
試験検査要領書	試験検査1週間前	1部
試験検査報告書	納入時	1部
基幹LAN-加速器NW境界 ファイアーウォール パラメータシート	納入時	1部
起動停止手順書	納入時	1部
作業報告書	納入時	1部
上記を含む電子ファイルを納めた CD-ROM	納入時	1式

それぞれを指定の部数印刷したものを提出すること。文書についてはA4に印刷すること。A4では文字が判

読できない縮小図になる場合は、大型図面としA4に折り畳んで提出すること。

(納入場所)

NanoTerasuセンター

高輝度放射光研究開発部 加速器グループ

## (2) 納入品

2.1に示す機器、ソフトウェア

(納入場所)

国立研究開発法人量子科学技術研究開発機構

宮城県仙台市青葉区荒巻字青葉468-1

NanoTerasu 加速器サーバー室 及び 検証環境スペース

## 1.6 検査条件

1.5項に示す納入物件の確認およびQSTが仕様書に定める業務が実施されたと認めたことをもって、検査合格とする。

## 1.7 情報セキュリティ

- (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、QSTの情報セキュリティポリシーを遵守すること。
- (3) 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。
- (4) 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。
- (5) 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。
- (6) 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。
- (7) 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。
- (8) 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。

- (9) 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。
- (10) 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。
- (11) 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。
- (12) 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

## 1.8 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。

## 1.9 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。

## 1.10 善管注意義務

NanoTerasu加速器は、業務継続性の観点から高可用性および高信頼性を前提として運用されているユーザー施設である。受注者は、本業務が当該施設の運用継続に重大な影響を与え得ることを十分に認識したうえで、ネットワーク機器保守の専門事業者として通常要求される善良なる管理者の注意義務をもって業務を遂行しなければならない。また、仕様書に明示されていない事項であっても、専門事業者として当然に予見・回避すべきリスクについては、受注者の責任において適切な措置を講じること。

（要求者）

部課（室）名：NanoTerasuセンター

高輝度放射光研究開発部 加速器グループ

氏名：小原 脩平

## 2 技術仕様

現行の加速器制御ネットワークでは、DNS・NTP問い合わせや、NanoTerasu内における無線アクセスポイントの利用、外部ネットワークへのアクセス等のため、基幹ネットワーク（基幹LAN）側との通信が必須となるため、基幹LANと加速器制御系ネットワーク間の通信を制御するためのファイアーウォール装置を導入・運用中である。加速器制御系ネットワークの安定運用ため、現行機器の後継製品のなかで、同等以上の機能・性能を有する機器への換装を行う方針とする。なお、現行ファイアーウォール装置の撤去に併せて、加速器制御ネットワークと特定の外部ネットワークとのL2VPNの経路を廃止する。

### 2.1 対象機器

#### 2.1.1 現行機器（更新対象）

- |   |    |
|---|----|
| (1) Cisco Firepower 2130                      | 2式 |
| (2) Cisco FirePower 1120（外部ネットワークとのL2VPN接続用途） | 1式 |

#### 2.1.2 後継機器

相当品可とする。3式調達するが、うち1式は動作検証用途として導入する。

- |  |    |
|--|----|
| (1) Cisco Secure FireWall 3105（相当品可とする。） | 3式 |
|--|----|
- (ア) 形状は19インチ標準ラックマウントに収容可能で高さ1Uであること。奥行きが1,000mm以下であること。
- (イ) 電源は冗長構成とすること。
- (ウ) 電源はホットスワップ可能であること。
- (エ) 電源はC13またはC19アウトレットに接続できること。
- (オ) インターフェイスは下記を備えていることとする。
- ① 管理コンソールポート×1
  - ② 統合ネットワーク管理ポート 1/10G SFP×1
  - ③ 10M/100M/1GBASE-T イーサネット×8（RJ-45）
  - ④ 1/10G SFP×8
  - ⑤ USB3.0タイプA×1
- (カ) ホットスワップ可能なファンモジュールが2以上搭載できること。
- (キ) 静音ノイズが65 dBA@ 25C 74 dBA（最大）以下であること。
- (ク) 温度0～40℃で動作すること。
- (ケ) 湿度10～85%で動作すること。
- (コ) FW + AVC スループット（1024B）は10 Gbps以上であること。
- (サ) FW + AVC + IPS スループット（1024B）は10 Gbps以上であること。

(シ) NGIPS スループット (1024B) は10 Gbps以上であること。

(ス) 同時セッションの最大数は150 万以上であること。

(セ) 1 秒あたりの最大新規接続数は90,000以上であること。

(ソ) TLSは3.2 Gbps以上であること。

- |                      |    |
|----------------------|----|
| (2) 1000BASE-Tモジュール  | 3式 |
| (3) SFP-10G-SR モジュール | 6式 |

## 2.2 作業内容

### (1) 設計

#### (ア) 現行構成の確認・換装設計

- ① 現行機器の設定を確認すること。
- ② 既設機器を中心とした論理構成・物理構成を調査すること。なお、ラックマウント位置や電源接続構成も調査すること。
- ③ 現行加速器制御系ネットワークのルーティング設計を確認すること。
- ④ ホスト名、IPアドレスは現行を踏襲する方針とすること。なお、ファイアーウォールポリシー等についても現行設定を踏襲すること。
- ⑤ これらの設計内容を設計書としてまとめ、QSTと協議のうえ換装設計を確定させたうえで、成果物として納めること。

#### (イ) 切替計画の検討

- ① 切替手順を作成すること。
  - ・ 現行機器から後継機器への切替手順を作成
  - ・ 切替作業期間は1日を想定とし、最大3日間で予定を立てること。
  - ・ 現行機器から後継機器への移行検証を含む
- ② 切り戻し手順作成
  - ・ 作業失敗時又は異常発生時において、加速器停止期間中の許容できる作業日数内に解決の見通しが立たない場合には切り戻しを行うこと。
  - ・ 切り戻しに必要な時間及び前提条件を整理し、切り戻し手順及び切り戻し決定するタイミングを切替計画内に含めること。
  - ・ 切り戻しによって後継機種が運用開始できなかった場合には、受注者は切り戻しの原因分析及び対策を提示し、再度後継機種への切替計画を策定、作業日時をQSTと協議の上で実施すること。
  - ・ ただし施設運転の都合上、再度の切替作業が納入期限までに履行できないこと

が明らかとなった場合は、速やかにQSTと協議を行い、検収の取扱い、納入期限の見直し、暫定措置の適用等について、QSTの決定に従うこと。

## (2) 機器据付

### (ア) 現行機器のアンマウント

- ① ラックアンマウント、ケーブル抜線

### (イ) 後継機器の搭載

- ① ラックマウント、ケーブル配線・接続

## (3) 切替

### (ア) 作業場所

- ① 切り替え作業はNanoTerasu加速器サーバー室 及び 検証環境スペースにて実施する。

### (イ) 作業計画

- ① 作業はNanoTerasuの加速器運転停止期間に実施するため、運転スケジュールを考慮した計画を立てること。また8月28日~31日(予定)は建屋停電のために作業は不可とする。

### (ウ) 切り替え作業

- ① 作成した切り替え手順書に準拠した手順で実施する。

### (エ) 起動停止手順書

- ① 基幹LAN-加速器NW境界ファイアウォールの起動停止手順書を提供すること。

## (4) 関連作業

### (ア) ファイアウォール装置のパラメータシートの作成

### (イ) 動作検証用ファイアウォール（1式）の初期動作確認

- ① ファームウェアをQSTが指定するバージョンにすること。
- ② 起動確認等、初期不良の確認を行うこと。

### (ウ) 基幹LAN側スイッチにおける現行ファイアウォールに関連する設定の削除

- ① 現行ファイアウォールの置き換えにあたり、基幹LAN側スイッチで必要な設定がある場合は、作業対象に含めること。なお、基幹LANは仮想化されたネットワークであり、論理構成としてFabric Ethernetの一つであるSPB(Shortest Path Bridging)プロトコルを用いていることに留意すること。
- ② 現行ファイアウォールの撤去に併せて、加速器制御ネットワークと外部とのL2VPNの経路を廃止する。外部接続用のスイッチは基幹LAN側スイッチを使用しているため、廃止に伴い不要となる設定を基幹LAN側スイッチから削除すること。
- ③ 上記作業内容について、基幹LAN側スイッチのQST担当者及び保守業者への事前説

明を行い、基幹LAN側スイッチのQST担当者からの了承を得ること。

(エ) 新規ビームライン設備導入に向けた通信ポリシー・NAT設定の追加

- ① 2026年度後半に新規ビームラインの設備導入が計画されており、同ビームラインに関連する機器制御等のため、別途ネットワーク機器を導入・整備する予定である。ネットワーク機器の導入・運用に必要なファイアーウォールへの追加設定作業は、運転停止期間中に実施する必要があるため、QSTが指定するポリシー・NAT設定の追加を、本案件の範囲にて実施すること。

(オ) 内部ネットワークの各種アプライアンス機器のメール通知のための通信ポリシー・NAT設定の追加

- ① ファイルサーバー、無停止サーバー等のメール通知機能を備えている機種が、外部保守業者へメール通知が出来るよう、送信元NATで外部へSMTP通信できるよう追加設定を行うこと。送信元となる機器のIP及びポート番号、送信先メールサーバーのリストについては受注後にQSTより支給する。

(カ) 実稼働後の設定調整

- ① 2026年夏の後継機種に換装後、実運用状態と機器の性能との兼ね合い等、事前に想定し得ないもので設定内容に調整すべき箇所が判明した際に、再度設定調整を行うこと。
- ② 設定調整日時は冬の停止期間(2026年12月17日~2027年1月20日)又はQST担当者と協議の上決定した日時とし、作業調整期間は原則1日とする。

(5) プロジェクト管理、提出図書作成

(ア) 実施計画・工程検討、作業期間中の各種管理（工程、課題、等）

(イ) 提出図書は1.5に記載のとおり

以上