JLAN 用 Web アプリケーションファイアーウォール装置賃貸借仕様書

1. 件名　JLAN 用 Web アプリケーションファイアーウォール装置賃貸借

2. 目的

J-PARC センターでは、大強度陽子加速器施設（J-PARC）の基幹ネットワークシステム（以下「JLAN」という）の整備と運用を行っている。

JLAN のセキュリティ向上を図るため、ネットワークレベルで管理する従来型ファイアーウォールに加えて、Web サーバのアプリケーションレベルでセキュリティ管理を行う Web アプリケーションファイアーウォール(WAF)装置を導入し、JLAN 上の Web サーバのセキュリティを強化している。今年度末で、現用の Web アプリケーションファイアウォール装置の賃貸借契約が終了となる。このため、Web アプリケーションファイアーウォール装置を更新し、Web サーバへのセキュリティ強化の維持を図ることとした。

本仕様書は、JLAN 用 Web アプリケーションファイアーフォール装置の賃貸借調達について定めたものである。

3. 導入物品等の仕様

JLAN 用 Web アプリケーションファイアーウォール装置　　一式

JLAN 用 Web アプリケーションファイアーウォール装置として、以下を満たす Barracuda 社製 Web Application Firewall 861 相当品 ×1 台 であること。

(1) ハードウェア及びソフトウェア要件

1) Web サーバ及び Web アプリケーションを保護する専用 OS を搭載したアプライアンス装置であること。
2) 電源ユニットが冗長構成でホットスワップ対応であること。
3) スループットが 1Gbps 以上であること。
4) セキュリティ監視用のネットワーク接続インタフェースとして、1000BASE-T (Gigabit Ethernet Cupper)を 2 ポート以上装備していること。
5) セキュリティ監視用ポートの接続配置形態は、透過型プロキシによるインラインブリッジ構成、およびリバースプロキシ構成が可能であること。
6) インラインブリッジ構成は、L2 トランスペアレントブリッジとして動作し論理的なネットワーク体系の変更を必要とせずに接続配置できること。
7) セキュリティ監視用のネットワーク接続インタフェースがバイパス機能を有し、インラインブリッジ構成での障害発生時に WAF 監視機能をバイパスする Fail Open 機能を有すること。
8) WAF 装置管理用のネットワーク接続インタフェースとして、10/100/1000BASE-T を 1 ポート以上装備していること。
9) WAF 装置管理用のネットワーク接続インタフェースは、接続元 IP アドレスによりアクセス制御が可能であること。
10) 30 台以上の Web サーバを同時に WAF 監視可能であること。
11) SSL オフローダを搭載し、SSL/TLS 暗号化通信の検査が行えること。
12) インラインブリッジ構成およびリバースプロキシ構成のどちらにおいても、SSL/TLS 暗号化通信の検査について、RSA および DHE/ECDHE 方式の鍵

交換を用いた暗号スイートの復号に対応できること。また、RSA の公開鍵長 2048bit 以上に対応できること。

13) アプライアンス装置メーカ自身が、Web サイト攻撃や Web アプリケーションの脆弱性に関するシグネチャ及びセキュリティポリシーを提供するために、最新の脅威を分析し、定期的及び適時にセキュリティ機能のアップデートを提供できること。
14) Web アプリケーションセキュリティとして、 SQL インジェクション、OS コマンドインジェクション、クロスサイトスクリプティング(XSS)、クッキー改ざん、フォームフィールド改ざん、パスワードリスト攻撃、Web サイトクローキング、不正な Web サイトスクレイピングを防御できること。
15) OWASP Top 10:2021 Web アプリケーションセキュリティリスク について対策が行えること。
16) IP レピュテーションデータベースを利用した匿名プロキシ（発信元偽装)、Tor（発信元隠蔽）からの通信の遮断、および Geo IP によるアクセス元制御が行えること。
17) Web サーバから送信されるレスポンスに、個人情報や機密情報などが含まれていないか検査し、パケット遮断やデータの書き換えなどにより、データ漏出を防止する機能を有すること。
18) サービス不能攻撃(DDoS)対策が行えること。
19) 過検知を回避するポリシーチューニングを、各 Web サーバについて独立に行えること。
20) Web プロトコルとして、HTTP(S) 1.0/1.1/2.0 、WebSocket、XML に対応すること。
21) タグ VLAN（IEEE802.1Q）のパケットを扱えること。
22) IPv4 及び IPv6 に対応すること。
23) 運用・管理において、以下の機能を有すること。
    ① ユーザロールを定義し、ユーザアカウントの権限を制限できること。
    ② Web ブラウザから管理用 WebUI によりリモートでの管理が可能なこと。管理用 WebUI は日本語に対応していること。
    ③ WAF セキュリティイベントのログ、および Web サービスへのアクセスログを記録し管理用 WebUI から確認できること。また、これらのログを syslog サーバへ転送できること。
    ④ レポート機能を有し、PDF 形式のレポートファイルを電子メールで配信できること。
    ⑤ 設定やログ情報閲覧などの管理に係わる通信は全て暗号化して行われること。

(2) 保守及び技術支援の要件

1) 本仕様書に関する機器保守は、平日 9:00～17:00 のオンサイト保守とする。なお、部品交換に要した費用は本仕様に含むものとする。
保守のために代替機を用いる場合には、同一製品もしくは機能・性能が同等以上の製品とすること。情報が記録されたストレージデバイス等については、返却不要の保守対応とする。
2) 障害保守を実施した場合には、障害復旧後、障害原因及びその対応について詳細に書かれた障害報告書（日本語記述）を速やかに 1 部提出する

こと。

3) ソフトウェアアップデート（セキュリティ機能アップデート、OS バージョンアップデートなど）をインターネットからのダウンロードにより随時提供すること。
また、本仕様書の契約期間中にリリースされたソフトウェアの新バージョン提供についての費用は本仕様に含むものとする。

4) 平日 9:00～17:00 に、技術情報の提供、技術支援を電子メールや電話で受付し、対応すること。

5) 本仕様書の保守・技術支援に関する体制及び連絡先を記載した説明資料を 1 部提出すること。

(3) 装置の移行に係わる要件

現用 WAF 装置において監視を行っている Web サーバについて、メーカが推奨する標準的な WAF ポリシーにより監視を行えるよう、導入する WAF 装置へ設定を実施すること。

なお、現用の WAF 装置について確認が必要な場合、入札公告公示後に守秘義務遵守に関する誓約書を受領した後、現用の WAF 装置の機種名、設定情報等のうち移行に必要な情報を開示する。

4. 調達方法

借入 （リース）

借料には、搬入据付、現地調整、付帯工事等の導入諸経費 及び賃貸借期間における保守等に要する対価を含める。

5. 賃貸借期間等

納入期限　 令和８年３月３１日
賃貸借期間 令和８年４月１日から 令和１４年３月３１日まで（７２ヶ月）

6. 納入場所及び納入条件

(1) 納入場所

茨城県那珂郡東海村白方白根 2 番地の 4
日本原子力研究開発機構 原子力科学研究所
計算センター建家 101 号室

(2) 納入条件

据付調整後渡し

7. 据付調整等

(1) 当機構担当者立ち会いの下に、受注者が搬入設置を実施すること。

1) 作業責任者は作業を監督し、当機構の作業安全に係わる規程、規則等を遵守し、災害発生防止に努めること。

2) 指示された搬入経路から搬入し、受注者が設置作業すること。

3) 当機構担当者が指定する 19 インチラックにラックマウントし、指定する電源コンセントより本装置へ通電すること。

4) 本装置を当機構担当者の指示に従い、JLAN へ接続すること。これに必要な LAN ケーブル等は受注者が用意するものとする。

5) 他の機器、設備に損傷を与えないよう注意して作業すること。損傷等の事故が発生した場合は遅滞なく当機構担当者へ報告し、その指示に従い

速やかに原状に復すること。

(2) 受注者は、以下に示す本装置の導入調整作業を実施し、Web アプリケーションファイアーウォールとしてのセキュリティ監視を正常に動作させること。

1) 導入調整作業は全て現地オンサイトチューニングとする。
2) 作業責任者は作業を監督し、情報セキュリティ管理を行うこと。
3) 導入調整作業実施に当たり当機構担当者と事前に打ち合わせし、作業工程表を含む作業要領書を作成し、確認を得た後に作業すること。
また、導入調整作業完了後に設定パラメータシートを含む作業報告書を提出すること。
4) 透過型プロキシ方式を用いたインラインブリッジ構成で導入すること。
5) WAF 監視外トラフィックについては、通信を遮断せずに透過的な機器としてふるまうように設定を行うこと。
6) WAF 装置の障害発生時に、Fail Open 機能により WAF 監視機能がバイパスされるように調整すること。
7) HTTP(S)リクエストを受け付ける WAN 側の仮想 IP アドレスを、監視対象の Web サーバの IP アドレスと同一に設定し、Web サーバの通信を監視できるよう調整すること。
8) 現用 WAF 装置において監視対象に設定されている全ての Web サーバについて、導入する WAF 装置の標準的な WAF ポリシーで監視を行うよう設定すること。
9) 監視対象の Web サーバについて、それぞれ独立にポリシーチューニングできるように設定すること。
10) DHE 鍵交換の暗号化方式を利用した SSL/TLS 通信を複号して監視できるように設定すること。
11) ログを JLAN に接続された syslog サーバへ転送する設定を行うこと。
12) アラート検知などの通知メールが正常に送信されるように調整すること。

(3) 受注者は、導入調整と併せてオンサイトで以下の説明講習を実施すること。

1) 装置の起動、停止などの操作手順
2) WebUI 等による運用・管理手順
3) Web サーバの監視設定追加方法
4) ポリシーチューニング（過検知の回避）方法
5) その他のシステム運用管理に係わる基本操作

8. 検査

検査は現地完成検査を当機構担当者立会の下で実施する。検査の内容・方法については、以下のとおりとする。

(1) 現地完成検査

現地据付け調整が完了し受注者の自主検査によって正常動作を確認後、当機構担当者立ち会いの下に、予め承認を受けた検査要領書により実施すること。

(2) 検査項目

員数検査（保守サービス契約及びソフトウェアライセンスの証書などを含む)、外観検査、据付け配線検査、機能検査を行う。

9. 支給品等

現地据付け搬入及び試験等に必要な電力等は、無償で支給する。

10. 提出図書

(1)	作業要領書（据付調整 2 週間前までに）	２部（要確認）
(2)	作業員名簿（作業開始前までに）	１部
(3)	検査要領書（検査 2 週間前までに）	２部（要確認）
(4)	検査成績書（検査後速やかに）	２部（要確認）
(5)	作業報告書（設定パラメータシート含む）	１部
	＊作業報告書については電子媒体でも１式提出すること。	
(6)	保守・技術支援体制表（検収時）	２部
(7)	その他必要な書類	２部

11. 検収条件

第 6 項に示す納入場所に納入し据付調整後、員数検査、外観検査、据付け配線検査、機能検査及び提出図書の合格をもって検収とする。

12. 委任又は下請負等の届出

委任又は下請負がある場合に限り、契約開始 2 週間前までに当機構指定様式で 1 部提出し、承認を得るものとする。なお、2 週間以内に当機構から変更請求をしない場合は、自動的に承認したものと見做す。

13. 特記事項

(1) 受注者は業務を実施することにより取得した当該業務及び作業に関する各データ、技術情報、成果その他のすべての資料及び情報を当機構の施設外に持ち出して発表もしくは公表し、または特定の第三者に対価をうけ、もしくは無償で提供することはできない。ただし、あらかじめ書面により当機構の承認を受けた場合はこの限りではない。

(2) 受注者は原子力機構内施設へリース物件を設置する際に異常事態等が発生した場合、原子力機構の指示に従い行動するものとする。また、契約に基づく作業等を起因として異常事態等が発生した場合、受注者がその原因分析や対策検討を行い、主体的に改善するとともに、受注者による原因分析や対策検討の結果について機構の確認を受けること。

14. 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）の採用が可能な場合は、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。

15. 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、当機構と協議のうえ、その決定に従うものとする。