東京芸術大学

ファイアウォールシステム 一式

仕様書

令和 4 年 2 月

目次

1. 調達概要

1.1. 調達背景と概要

東京藝術大学(以下本学という)では、学内 LAN 環境からインターネット接続を実現するためのセキュリティ対策装置に次世代型ファイアウォールを導入している。本ファイアウォールは、教育研究系、事務系、サーバ系、DMZ 等のネットワークを装置内で論理的に分割してそれぞれのネットワーク環境に応じて情報セキュリティポリシーを適用している。そのため、本調達においても複数のネットワーク環境を論理的に分割してセキュリティポリシーをそれぞれに適用できる機能を持つ装置を調達する。また、昨今は WAN 回線速度の高速化が求められていることからも、10Gbps 接続に対応するファイアウォール装置を必要とする。

また、ファイアウォール装置は統合脅威管理機能を有し、セキリティ機能としてファイアウォール機能、アンチウィルス機能、不正侵入検知機能、コンテンツフィルタリング機能、アンチスパム機能を備えて、必要に応じてファイアウォールポリシーに適用できることが求められる。そして、現行のファイアウォール装置では SSI-VPN 機能が付随していることから、引き続きこれらの機能を利用して学外環境から学内 LAN への接続を可能にする。

ファイアウォール装置は、本学の基幹ネットワークやサーバシステムを制御する装置でもある事から、機機の更新時には既存の基盤サーバシステムとネットワークシステムを構築したそれぞれのベンターと連携した導入が求められる。

1.2. 調達方法

一般競争入札（最低価格落札方式）による調達、5 年間の借入れとする。但し、調達機器が借用期限以降に継続利用が必要になった場合は、借入期間を延長する場合がある。

1.3. 調達日程

本調達に係る調達関連の日程は以下のとおり。

①	入札公告日	令和 4 年 2 月 15 日
②	入札書受領期限	令和 4 年 4 月 7 日
③	開札日	令和 4 年 4 月 28 日
④	納入期限	令和 4 年 9 月 30 日

1.4. 調達内容及び範囲

本調達は、ファイアウォールシステム 一式(搬入、据付、配線、調整を含む)を上野キャンパスに導入する。また、本学には現行のファイアウォールシステム PaloAlto 社製 PA3020 が稼働している。受注者は現行機器と本調達システムの置き換えの作業(設定の移行)を行うこと。

調達物品は、ファイアウォール装置 2 台、ファイアウォールログ管理装置 1 台とする。

1.5. 落札者の決定方法

落札者の決定方法は、一般競争入札（最低価格落札方式）に基づいて行う。なお、以下の要件を満たさない場合は不合格となる。

[1]. 予定価格の制限範囲内で入札価格を提示した入札者であること。
[2]. 提案内容が仕様書の要件を満たす入札者であること。

落札者となるべき者が二人以上あるときは、直ちに当該競争加入者等にくじを引かせ、落札者を決定するものとする。また、競争加入者等のうち出席しない者又はくじを引かない者があるときは、入札執行事務に関係ない職員がこれに代わってくじを引き落札者を決定するものとする。

1.6. 調達に関すること

[1]. 本調達に関する機能、性能、技術等要件は「3. 調達物品の要件」に示す。
[2]. 調達物品・システムが備えるべき要件は、本学が必要とするシステムの要件である。入札機器及びシステムの性能がこれを満たさないと判定された場合は入札判定不合格になり、落札対象から除外される。
[3]. 入札機器及びシステム、ソフトウェアの機能・性能・技術が要件を満たすか否かの判定は、入札機器に関する技術仕様書を含む入札説明書が求める提出資料を審査して行う。
[4]. 提案する機器及びソフトウェアは原則、入札時点で製品化されていること。入札時点で製品化されていない機器やソフトウェアを応札する場合には、技術的要件を満たす証明及び納入期限までに製品化されて納入できることを保証する資料と確約書を提出すること。
[5]. 本調達物品の借用料はハードウェア及びソフトウェア、保守料金を含めること。
[6]. 本調達物品の設置、導入、設定に際してはこれらに関係する作業費用を含めること。

1.7. 留意事項

[1]. システム等の提案は、提案内容が本書の要件をどのようにして満たすのか、または実現方法を記載した資料添付して具体的に説明すること。提案の根拠が不明確なものや、説明が不十分の場合、審査過程で内容を審議した上で要件を満たしていないとする場合がある。
[2]. 提出する資料には照会先を明記すること。
[3]. 提出された資料の内容について、照会先に問い合わせる場合がある。
[4]. 提出資料は 1 部以上を用意すること。
[5]. 提出資料のうち、提案書や主要な資料提出は、電子データを追記書き込み不可の状態にした光ディスク媒体を郵送、またはインターネット経由で提出すること。デジタルデータは資料類をまとめた圧縮データファイルまたは ISO イメージファイルが望ましい。
[6]. 仕様書に記載すべき追加情報が発生した場合は、[10]の連絡窓口より提出資料の照会先に電子メールで連絡する。
[7]. 本仕様書に関する問い合わせは[10]の連絡窓口へ連絡すること。

[8]. 借用開始期間の借用物品搬入、並びに借用期間満了時、解約時には借用物品を撤去すること。その際に発生する撤去作業費用等の費用は本調達に含まれる。

[9]. 本仕様書に関する連絡窓口は次の通り。

〒110-8714 東京都台東区上野公園 12-8

東京藝術大学 芸術情報センター「情報基盤・システム」担当

電話 050-5525-2474 メール: net-admin@ml.geidai.ac.jp

2. 全体要件

2.1. 納入場所及び納入期限

[1]. 納入場所は、本学上野キャンパスとする。
[2]. 本システムの納入期限は令和 4 年 9 月 30 日、借り入れ開始は令和 4 年 10 月 1 日とする。
[3]. 指定する期日までに設定作業等を完了し、キャンパスネットワークを稼働できる状態にすること。

2.2. 機器の搬入・設置・撤去について

[1]. 本調達システムに係る物品の搬入、据え付け、配線、調整およびこれらに付帯する工事は受注者が行い、その諸経費は受注者が負担とすること。
[2]. 借入期間の満了時ないしは解約時には借入れ物品を撤去し、撤去に係る全ての費用は本調達に含めること。
[3]. 搬入、設置に際しては、本学の業務に支障がないよう留意し、本学の施設に損傷を与えないように注意を払うこと。万が一、本学の施設に損傷を与えた場合は、受注業者の責任で現状復帰すること。
[4]. 本システムの設計、工事、納入に関する計画・工程は、本学の担当者と協議しその内容に従い構築を進めること。
[5]. 本システムの設置場所への搬入、据付、配管、配線、ネットワーク及び既存設備との物理的接続・調整、ソフトウェアのインストールを行い、各機器、ネットワークの動作試験を行うこと。試験実施前には試験内容を本学の担当者に提出し、試験後はその結果を動作試験結果報告書として成果物に含めること。
[6]. 本システムの設置は、本学サーバ室（上野キャンパス）に、EIA 規格準拠の 19 インチラックに設置すること。

2.3. 設定情報の移行

[1]. 現行のシステムから本調達のシステムに移行すること。その際、基本的には現構成に基づいて移行するが、構築・設計の中でネットワーク体系や構成を見直す場合がある。その際は設定変更に応じること。
[2]. 設定の移行時は、本学担当者と協議して設計・構築すること。なお、移行に必要な既存のネットワーク構成や設定情報は本学が提示する。

2.4. 保守・役務の条件

本調達が導入する機器に適用する保守条件は以下の通り。故障により機器の交換が発生した場合は交換機器の設定内容を復元する作業を交換機器発送前、もしくは到着後に実施すること。そ

の場合の機器設定費用は本調達に含まれる。

[1]. 5 年間平日 9-17 時オンサイト

[2]. 導入したシステム、ソフトウェアに深刻なセキュリティホールが発見された場合は、本学の担当者と調整の上、対応すること。

[3]. オンサイト対応が必要な場合の交通費等の諸経費は受注者側が負担すること。

[4]. 本学は本調達以降、2 件の大規模 ICT 関連の更新(全学ネットワークシステム及びサーバ等基盤システム)を控えている。それぞれの案件ではシステム更新に伴う論理ネットワーク構成の変更等に伴う機器への設定の追加・削除等の作業が発生する。そのため、2 つ大規模 ICT 関連案件が完了する 2023 年 5 月末までの間に機器の設定等変更が発生した場合は、その内容について協議しオンサイトでの対応を行うこと。なお、オンサイト対応が難しい場合は詳細な設定手順を速やかに提示し、本学による作業のサポートを行うこと。

2.5. 完成図書

本調達における設計、構築、検証の過程で作成した各ドキュメントを提出すること。

① 落札機器価格内訳書

② 基本設計書

③ 詳細設計書

④ 動作試験結果報告書

⑤ 想定される障害の復旧処置手順・連絡手順を記載した障害対応手順書

2.6. 情報セキュリティ等要件

[1]. 受注者は、本調達案件及びで知り得た一切の情報について、故意又は過失にかかわらず、本調達に関わる従事者以外に情報を漏らさないこと。

[2]. 本調達の履行に関連して知り得た機密情報の加工、改ざん、複写、複製等をしてはならない。ただし、保守範囲内のものやバックアップを目的とするものはこの限りではない。

[3]. 本システムのリース契約終了後は、案件に関する情報を返却又は破棄すること。

[4]. 受注者において秘密情報の漏えい等の事故が発生した場合は、直ちに本学へ報告し、受注者が責任をもって対応すること。

[5]. 受注者が情報システムを構成する要素(ソフトウェア、ハードウェア)として採用した機器等について、不正な変更が加えられていないことを検査する体制(機器に不正が見つかったときの追跡(トレーサビリティ)等)が受注者において確立していること。

[6]. 調達する機器に対して、不正な変更が加えられないように製造者等が定めたセキュリティ確保のための基準等が整備されており、その基準等が当該機器等に適用されていること。

3. 調達物品の要件

本章では、調達する機器およびシステムが備えるべき要件を示す。

3.1. ファイアウォール装置

3.1.1. 基本要件

[1]. ファイアウォール装置を 2 台用意すること。
[2]. ファイアウォール装置は冗長構成で構築すること。
[3]. 1GbE に対応した RJ-45 ポートを 10 ポート(管理ポート含む)以上備えること。
[4]. 1GbE に対応した SFP ポートを 8 ポート以上備えること。
[5]. 10GbE に対応した SFP+ポートを 2 ポート以上備えること。
[6]. 筐体のサイズは 1U であること。
[7]. 19 型ラックに搭載可能であること。
[8]. 既存の学内スイッチとファイアウォール装置は 10GbE で接続すること。

3.1.2. 機能要件

[1]. 装置にはセキリティ機能としてファイアウォール機能、VPN 機能、アンチウィルス機能、不正侵入検知機能、コンテンツフィルタリング機能、アンチスパム機能を備えていること。
[2]. アンチウィルス機能、不正侵入検知機能、コンテンツフィルタリング機能、アンチスパム機能はすべて自社で開発したシグネチャを利用していること。
[3]. VPN 利用時のユーザー認証は RADIUS、LDAP、Tacacs+をサポートすること。
[4]. 本調達に VPN の利用に必要な SSL 証明書の更新作業を 5 年分含めること。なお、更新に必要な SSL 証明書は本学が用意する。
[5]. SNMPv1/v2c/v3 による管理機能を備えていること。
[6]. ファイアウォールのポリシー等の設定は WEB GUI で設定できること。
[7]. IEEE802.1Q VLAN タギングに対応していること。
[8]. 論理的な仮想ファイアウォールを標準で 5 以上設定できること。
[9]. ファイアウォール機能として NAT および NAPT を利用できること。
[10].不正侵入検知機能により WAN 側の DoS 攻撃から防御できる機能を備えていること。
[11].不正侵入検知機能としてセキュリティポリシー毎にシグネチャの適用できること。
[12].ウィルスパターンファイルの更新は、自動でアップデートできること。
[13].コンテンツフィルタリング機能は、70 以上のカテゴリ(危険なサイトや不適切な Web サイト等を制限すべきデータベース)が用意されているとともに、各カテゴリに設定するポリシーグループは許可/監視、ブロック等の個別設定ができること。
[14].リモートアクセスのための SSL-VPN 機能を利用できること。
[15].SSL-VPN は、同時に 300 クライアント以上接続できること。
[16].SSL-VPN を利用するためのクライアントライセンスは無制限であること。
[17].ファイアウォール装置の冗長構成は、アクティブ-アクティブ、アクティブ-パッシブ、クラスタリングから選択できること。なお、冗長構成の選択にあたっては、設計時に本学と協議

すること。

3.1.3. 性能要件

[1]. ファイアウォールスループットは UDP パケットにおいて 36Gbps 以上に対応すること。
[2]. ファイアウォール同時セッション(TCP)は 8,000,000 以上に対応すること。
[3]. ファイアウォールに設定可能なポリシー数は 10,000 以上できること。
[4]. IPSec VPN スループットが 20Gbps 以上であること。
[5]. SSL-VPN のスループットは 7Gbps 以上であること。
[6]. IPS を有効にした際のスループットは 10Gbps 以上で利用できること。
[7]. 次世代型ファイアウォール機能のスループットは 9.5Gbps 以上で利用できること。
[8]. 脅威保護機能を有効にした際のスループットは 7Gbps 以上で利用できること。

3.2. ファイアウォール専用ログ管理システム

3.2.1. 基本要件

[1]. ログ管理システムを 1 式用意すること。
[2]. ログ管理システムは、ファイアウォール装置と連携してログデータを取得できること。
[3]. ログを保存するためのストレージ容量は実効容量 8TB 以上を備えること。
[4]. ログデータの保存期間は必要に応じて 1 年以上の保存に対応すること。
[5]. 本システムを利用するためのライセンス（サポート及び更新含む）は、構築期間中を含めサービス開始から 5 年分を費用に含めること。
[6]. 本システムの保守サービスは祝日、年末年始を除く平日 9:00-17:00 オンサイト修理対応とし、構築期間中含めサービス開始から 5 年分を費用に含めること。

3.2.2. 機能要件

[1]. ファイアウォール装置からデータを収集することで、ネットワーク全域にわたってセキュリティの可視性を向上できること。
[2]. Web GUI のダッシュボードを備え、カスタマイズ可能なレポートテンプレートを利用できること。
[3]. ファイアウォールから収集したログを自動的に分析してレポートを生成する機能を備えること。
[4]. ファイアウォールから収集したログからレポートを作成する際は、あらかじめ用意されたレポートテンプレートが利用できること。

以上