

## 資料提供招請に関する公表

次のとおり物品の導入を予定していますので、当該導入に関して資料等の提供を招請します。

平成 23 年 5 月 19 日

独立行政法人国立高等専門学校機構本部

契約担当役 事務局長 後藤 宏平

調達機関番号 593 所在地番号 13

第 1 号

### 1 調達内容

(1) 品目分類番号 15、28

(2) 導入計画物品及び数量

高専統一認証基盤及びファイアウォール 一式

(3) 調達方法 借入

(4) 導入予定時期

平成 23 年度 3 月以降

(5) 調達に必要とされる基本的な要求要件

#### 1) 認証基盤

高専共通認証サーバ

(a)高専共通システムのアプリケーション等のユーザ認証が出来ること。

- ・LDAPv2 および v3 のプロトコルに対応すること。
- ・LDAP over SSL に対応し、任意の証明書が使用できること。
- ・任意 LDAP スキーマの拡張が可能なこと。

(b)高専共通のネットワークシステム等の認証が出来ること。

- ・RADIUS プロトコルに対応していること。
- ・RADIUS 認証において、PAP/CHAP によるユーザ認証が可能であること。
- ・RADIUS 認証において、MAC アドレスによる端末認証が可能であること。
- ・IEEE802.1X 認証に対応していること。
- ・ベンダ固有属性を登録して利用できること。

(c)全ての設定や管理が、HTTPS を用いた Web ブラウザより操作可能で、日本語化されていること。

(d)日本語マニュアルが提供されること。

(e)操作履歴を含むログの保存機能を有すること。

(f)データの保護やシステムの冗長化が行われていること。

(g)10,000 個以上のアカウントが利用できること。

(h)CSV や LDIF によるアカウント情報の管理が出来ること。

(i)各キャンパスおよび本部事務局からのアカウント情報の同期が可能なこと。

(j)停電時の対応が可能なこと。

各キャンパス用認証サーバ (55 キャンパス)

(a)キャンパス独自システムのアプリケーション等のユーザ認証が出来ること。

- ・LDAPv2 および v3 のプロトコルに対応すること。
- ・LDAP over SSL に対応し、任意に証明書が使用できること。
- ・任意の LDAP スキーマの拡張が可能なこと。

- ・ POSIX 認証に対応していること。
- (b)各キャンパスのネットワークシステム等の認証が出来ること。
- ・ RADIUS プロトコルに対応していること。
  - ・ RADIUS 認証において、PAP/CHAP によるユーザ認証が可能であること。
  - ・ RADIUS 認証において、MAC アドレスによる端末認証が可能であること。
  - ・ IEEE802.1X 認証に対応していること。
  - ・ ベンダ固有属性を登録して利用できること。
- (c)他の Active Directory や LDAP サーバへ指定したユーザの指定した属性の同期が可能なこと。
- (d)全ての設定や管理が、HTTPS を用いた Web ブラウザより操作可能で、日本語化されていること。
- (e)日本語マニュアルが提供されること。
- (f)操作履歴を含むログの保存機能を有すること。
- (g)データの保護やシステムの冗長化が行われていること。
- (h)2,000 個以上のアカウントが利用できること。
- (i)CSV や LDIF によるアカウント情報の管理が出来ること。
- (j)Shibboleth IdP の機能を有すること。
- (k)国立情報学研究所の学術認証フェデレーションで利用される Shibboleth IdP に参加できる機能・属性等を有すること。
- (l)高専共通用認証サーバへの指定ユーザのアカウント情報の同期が可能なこと。
- (m)停電時の対応が可能なこと。
- 本部事務局用認証サーバ
- (a)本部事務局独自システムのアプリケーション等のユーザ認証が出来ること。
- ・ LDAPv 2 および v 3 のプロトコルに対応すること。
  - ・ LDAP over SSL に対応し、任意の証明書が使用できること。
  - ・ 任意の LDAP スキーマの拡張が可能なこと。・ POSIX 認証に対応していること。
- (b)本部事務局のネットワークシステム等の認証が出来ること。
- ・ RADIUS プロトコルに対応していること。
  - ・ RADIUS 認証において、PAP/CHAP によるユーザ認証が可能であること。
  - ・ RADIUS 認証において、MAC アドレスによる端末認証が可能であること。
  - ・ IEEE802.1X 認証に対応していること。
  - ・ ベンダ固有属性を登録して利用できること。
- (c)他の Active Directory や LDAP サーバへ指定したユーザの指定した属性の同期が可能なこと。
- (d)全ての設定や管理が、HTTPS を用いた Web ブラウザより操作可能で、日本語化されていること。
- (e)日本語マニュアルが提供されること。
- (f)操作履歴を含むログの保存機能を有すること。
- (g)データの保護やシステムの冗長化が行われていること。
- (h)200 個以上のアカウントが利用できること。
- (i)CSV や LDIF によるアカウント情報の管理が出来ること。
- (j)Shibboleth IdP の機能を有すること。
- (k)国立情報学研究所の学術認証フェデレーションで利用される Shibboleth IdP に参加できる機能・属性等を有すること。

(l)高専共通用認証サーバへの指定ユーザのアカウント情報の同期が可能なこと。

(m)停電時の対応が可能なこと。

高専共通用認証サーバと各キャンパス用認証サーバ及び本部事務局用認証サーバの同期

(a)各キャンパス用認証サーバ及び本部事務局用認証サーバで管理されている指定されたユーザ(教職員等)の指定されたアカウント情報を，高専共通用認証サーバに同期可能なこと。

(b)高専共通用認証サーバ内でユーザ ID の重複を回避し，ユーザ ID の唯一性が保証されること。

高度化再編高専の各キャンパス用認証サーバの同期

(a)通常の各キャンパス用認証サーバの機能に加え，次の対応を行うこと。・複数キャンパスを合わせたアカウント数が利用できること。

・いずれのキャンパスからもアカウント情報の管理が可能なこと。

・いずれのキャンパスからのアカウント操作も，他のキャンパスの認証サーバに反映可能なこと。

## 2) ファイアウォール (54 キャンパス)

セキュリティ機能として，以下の機能を有すること。

(a)ファイアウォール機能

(b)VPN 機能

(c)不正侵入検知機能

(d)アンチウイルス機能

(e)アンチスパム機能(f)コンテンツフィルタリング機能

(g)アプリケーション制御機能

10/100/1000Mbps の Ethernet インタフェースを 8 ポート以上有すること。

IPv 4 / IPv 6 デュアルスタックで，各種経路制御方式，NAT/PAT 等の機能を有すること。

セキュリティ機能においても IPv 6 に対応していること。

内部ネットワークをグループ化(たとえば，教育研究系，教員系，事務系など)し，グループ毎に異なるポリシー設定が可能であること。

本調達の認証基盤によるユーザ認証方式に対応し，コンテンツフィルタリング機能やアプリケーション制御機能においてユーザグループに応じたポリシー設定が可能であること。

内部ネットワークに 1,000 台のクライアントが接続されていることを想定したとき，通常のネットワーク利用に十分なセッション数・スループット性能等を有すること。

3 か月分のログ収集が可能で，保存したログの分析・報告の機能を有すること。

日本語対応した Web GUI にて各種設定，稼働状態ならびに統計情報の閲覧ができること。

停電時の対応が可能であること。

日本語マニュアルが提供されること。

## 2 資料及びコメントの提供方法

上記 1 (2)の物品に関する一般的な参考資料及び同(5)の要求要件等に関するコメント並びに提供可能なライブラリーに関する資料等の提供を招請する。

(1) 資料等の提供期限 平成 23 年 6 月 20 日 17 時 00 分 ( 郵送の場合は必着のこと。)

(2) 提供先 〒193 - 0834 八王子市東浅川町 701 番 2

独立行政法人国立高等専門学校機構本部財務課財務システム係 鈴木 隆  
電話 042-662-3137

## 3 説明書の交付 本公表に基づき応募する供給者に対して導入説明書を交付する。

(1) 交付期間 平成 23 年 5 月 19 日から平成 23 年 6 月 20 日まで。

(2) 交付場所 上記 2 (2)に同じ。

## 4 説明会の開催 本公表に基づく導入説明会を開催する。

(1) 開催日時 平成 23 年 5 月 26 日 10 時 00 分

(2) 開催場所 独立行政法人国立高等専門学校機構本部会議室

## 5 その他 この導入計画の詳細は導入説明書による。なお、本公表内容は予定であり、変更することがあり得る。

## 6 Summary

(1) Classification of the products to be procured : 15, 28

(2) Nature and quantity of the products to be rent : Unified Authentication infrastructure and Firewalls for all National Colleges of Technology 1 Set

(3) Type of the procurement : Rent

(4) Basic requirements of the procurement :

1)Authentication infrastructure

KOSEN common authentication server

(a)Server can authenticate users of applications,etc. of KOSEN common system.

・ Server supports LDAP v2 and v3 protocols.

・ Server supports LDAP over SSL, and allows use of arbitrary certificates.

・ Server allows extension of arbitrary LDAP schemas.

(b)Server can authenticate KOSENs' common network system, etc.

・ Server supports RADIUS protocol.

・ Server can authenticate users by using PAP/CHAP in RADIUS authentication.

・ Server can authenticate terminals based on MAC address in RADIUS authentication.

・ Server supports IEEE802.1X authentication.

・ Server allows registration and use of vendor-specific attributes.

(c)Server settings and management can be operated entirely through a Web browser using HTTPS and in Japanese.

(d)A Japanese manual is available.

(e)Server has the function to maintain logs including operation history.

(f)Server offers data protection and system redundancy.

(g)Server allows use of 10,000 or more user accounts.

- (h)Server allows management of account information in CSV and LDIF formats.
- (i)Server can synchronize account information provided from the respective campuses and the Headquarters Secretariat.
- (j)Server can respond to power outages.

Authentication server for each campus (55 campuses)

- (a)Server can authenticate users of applications, etc. of the campus-specific system.

- Server supports LDAP v2 and v3 protocols.
- Server supports LDAP over SSL, and allows use of arbitrary certificates.
- Server allows extension of arbitrary LDAP schemas.
- Server supports POSIX authentication.

- (b)Server can authenticate the network system, etc. of each campus

- Server supports RADIUS protocol.
- Server can authenticate users by using PAP/CHAP in RADIUS authentication.
- Server can authenticate terminals based on MAC address in RADIUS authentication.
- Server supports IEEE802.1X authentication.
- Server allows registration and use of vendor-specific attributes.

- (c)Server can synchronize designated attributes of designated users with another Active Directory or LDAP server.

- (d)Server settings and management can be operated entirely through a Web browser using HTTPS and in Japanese.

- (e)A Japanese manual is available.

- (f)Server has the function to maintain logs including operation history.

- (g)Server offers data protection and system redundancy.

- (h)Server allows use of 2,000 or more user accounts.

- (i)Server allows management of account information in CSV and LDIF formats.

- (j)Server offers the functions of Shibboleth IdP.

- (k)Server offers functions, attributes, etc. for participating in the Shibboleth IdP used by the Academic Authentication Federation of the National Institute of Informatics.

- (l)Server can synchronize account information of designated users with the KOSEN common authentication server.

- (m)Server can respond to power outages.

Authentication server for the Headquarters Secretariat

- (a)Server can authenticate users of applications, etc. of the Headquarters Secretariat-specific system.

- Server supports LDAP v2 and v3 protocols.
- Server supports LDAP over SSL, and allows use of arbitrary certificates.
- Server allows extension of arbitrary LDAP schemas.
- Server supports POSIX authentication.

- (b)Server can authenticate the network system, etc. of the Headquarters Secretariat.

- Server supports RADIUS protocol.

- Server can authenticate users by using PAP/CHAP in RADIUS authentication.
  - Server can authenticate terminals based on MAC address in RADIUS authentication.
  - Server supports IEEE802.1X authentication.
  - Server allows registration and use of vendor-specific attributes.
- (c)Server can synchronize designated attributes of designated users with another Active Directory or LDAP server.
- (d)Server settings and management can be operated entirely through a Web browser using HTTPS and in Japanese.
- (e)A Japanese manual is available.
- (f)Server has the function to maintain logs including operation history.
- (g)Server offers data protection and system redundancy.
- (h)Server allows use of 200 or more user accounts.
- (i)Server allows management of account information in CSV and LDIF formats.
- (j)Server offers the functions of Shibboleth IdP.
- (k)Server offers functions, attributes, etc. for participating in the Shibboleth IdP used by the Academic Authentication Federation of the National Institute of Informatics.
- (l)Server can synchronize account information of designated users with the KOSEN common authentication server.
- (m)Server can respond to power outages.

Synchronization between the KOSEN common authentication server and the authentication server for each campus.

- (a)Designated account information of designated users (school staff, etc.) managed by the authentication server for each campus or the authentication server for the Headquarters Secretariat can be synchronized with the KOSEN common authentication server.
- (b)KOSEN common authentication server prevents user ID collisions within the server, and ensures the uniqueness of each user ID.

Synchronization of the authentication server for each campus of the new reorganized KOSENs

- (a)Server for a new reorganized KOSEN will satisfy the following requirements in addition to the requirements for the regular authentication server for each campus.
- Server allows use of a sufficient number of user accounts to cover multiple campuses.
  - User information can be managed from any KOSEN campus. • Account operation from any KOSEN campus can be reflected in the authentication servers of other campuses.

## 2)Firewalls (54 campuses)

Firewall offers the following security functions.

- (a)Firewall function
- (b)VPN function

(c)Unauthorized access detection function

(d)Anti-virus function

(e)Anti-spam function

(f)Contents filtering function

(g)Application control function

Firewall has eight or more 10/100/1000 Mbps Ethernet ports.

Firewall is IPv4/IPv6 dual-stack, and offers various path control methods and functions such as NAT/PAT.

Security functions support IPv6.

Firewall can form groups (e.g., educational and research group, school staff group, and administrative group) in the internal network, and set different policies for each group.

Firewall supports the user authentication methods adopted by the authentication infrastructure procured this time, and can set different policies according to the user group for its contents filtering function and application control function.

Firewall provides sufficient throughput and concurrent sessions for ordinary network use, when supposing that 1,000 clients are connected to the internal network.

Firewall can maintain a three-month log, and offers loganalysis/reporting functions.

Various settings, operating status, and statistics information can be browsed through a web GUI supporting Japanese.

Firewall can respond to power outages.

A Japanese manual is available.

(5) Time limit for the submission of the requested material : 5 : 00 PM 20, June, 2011

(6) Contact point for the notice : Suzuki Takashi, Finance Division, Institute of National Colleges of Technology, Japan, 701-2 Higashiasakawamachi Hachioji-shi 193 - 0834 Japan, TEL 042 - 662 - 3137