(l) Server can synchronize account information of designated users with the KOSEN common authentication server.
(m) Server can respond to power outages.

③ 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.

④ 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.

⑤ 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)
① 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
② Firewall has eight or more 10／100／1000 Mbps Ethernet ports.
③ Firewall is IPv4／IPv6 dual-stack, and offers various path control methods and functions such as NAT／PAT.
④ Security functions support IPv6.
⑤ 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.
⑥ 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.
⑦ Firewall provides sufficient throughput and concurrent sessions for ordinary network use, when supposing that 1,000 clients are connected to the internal network.
⑧ Firewall can maintain a three-month log, and offers log analysis／reporting functions.
⑨ Various settings, operating status, and statistics information can be browsed through a web GUI supporting Japanese.
⑩ Firewall can respond to power outages.
⑪ 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 Hachioujishi Tokyo 193—0834 Japan, TEL 042—662—3137

意見招請に関する公示

次のとおり調達物品の仕様書案の作成が完了したので、仕様書案に対する意見を招請します。

平成23年5月19日

財務省大臣官房会計課長　松村　武人

◎調達機関番号　015　◎所在地番号　13

1　調達内容
(1)　品目分類番号　71、27
(2)　購入等件名及び数量
国庫収支事務オンラインシステムの改修に係る設計・開発及びシステム移行業務　一式

2　意見の提出方法
(1)　意見の提出期限　平成23年６月９日17時30分（郵送の場合は必着のこと。）
(2)　提出先　〒100—8940 東京都千代田区霞が関３－１－１財務省入札説明室（Ｂ東—84号室）
(3)　問い合わせ先　〒100—8940 東京都千代田区霞が関３－１－１　財務省大臣官房会計課契約第一係　濱田　賢吾　電話03—3581—4111　内線2140

3　仕様書案の交付
(1)　交付期間　平成23年５月19日から平成23年６月８日まで。
(2)　交付場所　上記２(2)に同じ。

4　仕様書案の説明会
(1)　開催日時　平成23年５月27日14時00分から
(2)　開催場所　財務省理財局応接室（中—402号室）