B－3　User authentication shall be possible from all PCs. It is desirable that the product support authentication in conjunction with an HTTPS server and automatic renewal of server certificates using ACME.

B－4　The switch shall provide MAC address-based authentication functionality for servers, IoT devices, and other equipment.

B－5　The authentication function shall authenticate each terminal connected through an existing switch connected to this switch.

B－6　The switch shall have a function for assigning VLANs to devices in coordination with the authentication function.

B－7　Access lines using 1,000 BASE-LX shall be provided to each room in the Aramaki Campus.

B－8　Access lines using UTP shall be provided to each room at the other locations (Showa, Kiryu, Ota, and affiliated schools).

C　Large-Scale NAT Device

C－1　The device shall be capable of performing NAT or NAPT at high speed for 2,000 or more subnets and converting the entire University network to private IP addressing.

C－2　Based on communication logs and other information, it shall be possible to easily trace and identify an internal IP address from an external IP address, while minimizing the number of possible candidates during identification. For this purpose, it is desirable that the device implement an IP address mapping (translation) method that limits the number of internal IP addresses simultaneously associated with a single external IP address.

D　Off-Campus Connection Security System

D－1　The system shall provide access control using firewall functionality.

D－2　The system shall be capable of virus detection and countermeasures against targeted attacks.

D－3　The system shall be capable of detecting security anomalies in on-campus systems.

D－4　The system shall provide DNS filtering capable of refusing to resolve DNS queries for malicious sites.

D－5　The system shall provide VPN connectivity. For VPN connections, based on the VLAN attribute associated with the user ID, the system shall allow access to the relevant VLAN through access-list control or by assigning the connection to that VLAN.

D－6　Multi-factor authentication shall be available for VPN authentication. It is desirable that the system integrate with the University's SSO (Shibboleth) and support the University's two-factor authentication using OTP and FIDO.

D－7　Secure remote configuration changes shall be possible. It is desirable that the system provide an API enabling integration with independently developed management systems and similar systems.

D－8　The system shall provide throughput of 10 Gbps or more.

D－9　It is desirable that the product have a proven track record of promptly providing firmware updates after vulnerabilities become publicly known. It is also desirable that firmware updates be easy to perform and that the product provide a mechanism allowing easy rollback to the previous version in the event of a problem. As this requirement is particularly important for VPN functionality, the VPN functionality may be implemented using a separate, independent device.

D－10　It is desirable that the product allow VPN connections from various Internet access environments, including those available at business travel destinations. If HTTPS is used for this purpose, the product shall support automatic renewal of server certificates using ACME.

D－11　The system shall have redundant connection functionality that allows communication to continue during maintenance or failure of one system.

E　Network Management and Monitoring System

E－1　The system shall be capable of managing and monitoring the network.

E－2　Access logs shall be collectable in coordination with the authentication switches.

F　Wireless LAN System

F－1　The equipment shall provide comfortable operation in environments where many users connect simultaneously, such as classes. It is desirable that each access point support 50 or more simultaneous users.

F－2　Access points shall support both PoE and external power supplies. Energy-efficient products capable of operating within the power supplied under IEEE 802.3af or IEEE 802.3at are desirable.

F－3　The system shall provide a configuration supporting IEEE 802.1X authentication and allowing connection using the ID and password of a university-wide authentication account.

F－4　For devices that do not support IEEE 802.1X authentication, the system shall provide a configuration enabling connection through HTTPS using a web browser and authentication with the ID and password of a university-wide authentication account. The system shall also support automatic renewal of server certificates using ACME.

F－5　For connections of IoT devices and similar equipment, it is desirable to provide a configuration that enables connection authentication and identification of the responsible administrator while ensuring sufficient security, without directly storing the administrator's personal ID and password in the device.

F－6　The system shall provide a configuration that allows access point settings to be changed collectively.

F－7　Products with monitoring functions covering terminal connection status, radio conditions, access point connection status, and similar information are desirable.

G　Other Requirements

G－1　The proposed network equipment shall support IPv6.

G－2　The system shall provide a configuration that assigns one subnet to each of approximately 2,000 University laboratories and allows access control for inter-subnet communications.

G－3　The wired and wireless authenticated networks shall be capable of supporting 15,000 University members.

G－4　When server certificates on equipment installed within the University are automatically renewed using ACME, it is desirable that the system be configured to minimize the exposure of such equipment to external networks.

(5)　Time limit for the submission of the requested material: 17:00　21 December, 2026

(6)　Contact point for the notice: Kiyoko Yuasa, Procurement Section, Accounting Division, Gunma University, 4—2 Aramaki-machi Maebashi-shi 371—8510 Japan, TEL 027—220—7066

意見招請に関する公示

次のとおり調達に関する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。

令和８年11月９日

支出負担行為担当官

デジタル庁会計担当参事官　甲元　信宏