(4) Basic requirements for the procurement: As information security measures, Niigata University provides 24-hour network intrusion monitoring, response to information incidents based on the university's information security policy, and daily IPA, JPCERT／CC (Japan Computer Emergency Response Team Coordination Center) and other security public institutions check the latest security information on websites, collect and organize information that is judged necessary for the University, disseminate it to the university, and outsource these tasks. (Details are according to the introductory instructions.)

① 24-hour network intrusion monitoring

This work must be supervised by a person who has a CISSP certification qualification or an information processing system audit engineer examination certificate certified by the Ministry of Economy, Trade and Industry. The on-site command must be led by a person who has a CISSP certification qualification or two or more of the following examinations: Information Processing Security Assurance Support Specialist Examination, Information Security Specialist Examination, System Audit Engineer Examination, and Network Specialist Examination certified by the Ministry of Economy, Trade and Industry. In addition, those who supervise the above operations, those who supervise the site, and the information security engineers in charge of information security consultants who perform daily operations are prohibited from re-outsourcing their work in order to make comprehensive judgments and perform their duties in this work.

② Daily work (information security consultant)

Based on the University's Information Security Policy, the Information Security Consultant provides "A Security Incident Emergency Response, Evidence Preservation and Analysis", "B Proposal of Countermeasures for Security Operations", "C Notification of Computer Virus Detection and Infection Status Aggregation and Response Procedure to Administrator", "D Aggregation of File Sharing Software Usage Discovery Status and Warning Notification to Administrator", "E Responding to the National Institute of Informatics Information Security Operation Collaboration Service (NII—SOCS)", "F Operational support for IT asset management systems" and "G Other security-related operations".

③ Provision of information

The Contractor shall check the latest security information issued by public security organizations such as IPA, JPCERT／CC (Japan Computer Emergency Response Team Coordination Center) on a daily basis, collect and organize information deemed necessary by the University, and provide it by e-mail. As a general rule, the information will be provided only to the distribution address designated by the University. In principle, delivery is based on once every two weeks. However, if the amount is urgent, it will be delivered immediately. In doing so, keep in mind that the recipient can immediately recognize that it is urgent. Regarding the software to be used for the form to be provided, the university must discuss with the university in advance and prepare and provide the distribution document.

④ Security business support

In consultation with the staff in charge of the University, engineers with technical skills equivalent to those of security consultants shall provide 120 hours of operational support per year within the contract period. The main business support contents are as follows.

A Information security lecture instructor and preparation of training materials

B Preparation and update of information security materials

C Field surveys, user support, witnessing planned power outages and network configuration changes, etc.

⑤ Implementation of information security audits

Based on the Niigata University Information Security Policy, conduct advisory-type audits by extracting audit items that match the actual situation of the University. Specifically, items for auditing the status of business operations in accordance with the procedure manual should be extracted, and audited from a professional perspective to ensure that information assets handled in business are properly operated and managed through questionnaires, interviews, on-site inspections, etc.

⑥ Implementation of targeted e-mail attack drills

To send e-mails simulating targeted attack e-mails to e-mail users of the University, and to conduct training and post-training education on targeted attack e-mails.

⑦ Implementation of vulnerability assessments

Use the vulnerability assessment tool (nessus) provided by the University to diagnose vulnerabilities in devices connected to the University network. If the diagnosis results indicate a vulnerability with a high degree of urgency, notify the device manager of the improvement.

⑧ Other Notices

A Hold regular meetings at least once a month to discuss operational procedures, etc. with the person in charge of the University.

B Operational procedures, etc. discussed at regular meetings, etc. shall be recorded in writing (including electronic media).

C If a security consultant is to be changed within the contract period, an appropriate period shall be established for the transfer of operational procedures, etc., and the details shall be reported to the staff in charge of the University for Confirmation.

D Upon expiration or termination of this Agreement, all necessary data assets and operating procedures shall be provided in electronic form in consultation with the University. In addition, the latest data assets at that time must be provided as electronic media at least three months in advance.

E Upon expiration or termination of this Agreement, close meetings shall be held with the University and the new contractor.

F Remote work shall be carried out with the permission of the University via VPN connection.

G When working remotely, the work terminal shall not be used for any purpose other than the University's information security support work. In addition, work terminals should take sufficient security measures against information leakage, including the installation of anti-malware software.

H You must not take out the University's information data, including maintenance data. However, this excludes cases in which the contents of the take-out, how to handle it, and the security measures thereof have been discussed with the faculty and staff in charge of security at regular meetings, etc., and permission has been obtained from the director of the Information Technology Center of the University. In addition, when actually taking out information data with the prior permission of the Director of the Information Technology Center, prepare two copies of the information data transfer form