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。
令和８年５月７日
調達機関番号　415
所在地番号　15
第１号

1. 調達内容
   (1) 品目分類番号　71，27
   (2) 導入計画物品及び数量　新潟大学情報セキュリティ対策支援業務請負　一式
   (3) 調達方法　購入等
   (4) 導入予定時期　令和８年度第４・四半期以降
   (5) 調達に必要とされる基本的な要求要件
   新潟大学では、情報セキュリティ対策として、24 時間ネットワーク不正侵入監視、本学情報セキュリティポリシーに基づく情報インシデント等への対応業務、日々IPA・JPCERT/CC（Japan Computer Emergency Response Team Coordination Center）等のセキュリティ公的機関が発行する最新のセキュリティ情報を Web サイトなどで確認し、本学に必要と判断される情報を収集、整理し、学内に周知を行っており、これらの業務について、委託するものである。詳細は、導入説明書による。

   ① 24 時間ネットワーク不正侵入監視業務
   本業務においては、CISSP 認定資格、または、経済産業省が認定する情報処理システム監査技術者試験合格証を有する者が統括を行う体制であること。現場指揮にあたっては、CISSP 認定資格、または、経済産業省が認定する情報処理安全確保支援士試験、情報セキュリティスペシャリスト試験、システム監査技術者試験、ネットワークスペシャリスト試験のうち、2 種類以上の試験合格証を有する者が指揮する体制であること。また、上記の業務の統括を行う者及び現場指揮を行う者並びに日常の業務を行う情報セキュリティ相談員担当の情報セキュリティ技術者については、 本業務における総合的な判断及び業務遂行のため、 業務の再委託を禁止する。

   ② 日常の業務（情報セキュリティ相談員）
   本業務は、情報セキュリティ相談員が、本学情報セキュリティポリシーに基づき「A. セキュリティ・インシデント緊急対応・証拠保全及び分析」、「B. セキュリティ運用の対処法の提案」、「C. コンピュータウイルスの発見・感染状況集計業務及び管理者への対応手順通知」、「D. ファイル共有ソフト利用発見状況集計業務及び管理者への警告通知」、「E. 国立情報学研究所情報セキュリティ運用連携サービス（NII-SOCS）への対応」、「F. IT 資産管理システムの運用支援」及び「G. その他セキュリティ関連業務」の各業務を実施するものである。

   ③ 情報提供
   請負者は、日々IPA・JPCERT/CC（Japan Computer Emergency Response Team Coordination Center）等のセキュリティ公的機関が発行する最新のセキュリティ情報を Web サイトなどで確認し、本学に必要と判断される情報を収集、整理し、電子メールを利用し提供すること。提供先は、原則として本学が指定する配信宛先のみとする。配信は、原則として 2 週間に 1 回を基本とする。ただし、緊急度が高いものについては、即時配信とする。その際、それが緊急である旨を受信者が即時認識できることに留意し作成すること。なお、提供する様式に利用するソフトについては、事前に本学と打合せ、配信文書を作成し、提供すること。

   ④ セキュリティ業務支援
   本学担当職員と協議を行い、その指示に従い、セキュリティ相談員と同等程度の技術力を持つ技術者が、契約期間内に年間 120 時間の業務支援を行うこと。主な業務支援内容は下記とする。
   (a) 情報セキュリティ講習講師、講習資料作成
   (b) 情報セキュリティに関する資料作成・更新
   (c) 現地調査、ユーザ支援、計画停電やネットワーク設定変更に伴う立会いその他

   ⑤ 情報セキュリティ監査の実施
   「新潟大学情報セキュリティポリシー」を基に本学の実情にあった監査項目を抽出して助言型監査を実施すること。具体的には手順書に沿った業務運用状況を監査するための項目を抽出し 職員へのアンケートやヒアリング 現地視察等により業務で取り扱う情報資産が適切に運用・管理されているか専門的視点から監査すること。

   ⑥ 標的型攻撃メール訓練の実施
   本学のメール利用者に対して標的型攻撃メールを模したメールを送信し、標的型攻撃メールの訓練と訓練後の教育を行うこと。

   ⑦ 脆弱性診断の実施
   本学が用意する脆弱性診断ツール（nessus）を使用し、学内ネットワークに接続された機器の脆弱性を診断すること。診断の結果、緊急度の高い脆弱性については、機器の管理者に対して改善を通知すること。

   ⑧ ASM 診断の実施

   請負業者が用意するクラウド型の ASM ツールを使用し、本学が学外ネットワークに公開している機器の脆弱性を診断すること。脆弱性診断の結果、緊急性の高いものについては、機器の管理者に対して改善を通知すること。

   ⑨ IT 資産管理ツール運用支援
   本学が用意する IT 資産管理ツール（Tanium 社の Tanium）を使用し、以下の運用支援を行う。

(a) 脆弱性診断機能を用い、エンドポイントに対して脆弱性診断を実施し、緊急性が高いと判定された機器の管理者に対し、改善の実施を通知すること。
(b) エンドポイントにおける不審な活動を検知する機能を用い、急性の高いと判断された事象について、機器の管理者に対して改善を通知すること。

⑩ その他
(a) 月に 1 回以上、定例打ち合せ会を開催し、運用手順等を本学の担当者と協議すること。
(b) 定例打ち合せ会等で打ち合せた運用手順等は、書面（電子媒体含）で記録に残すこと。
(c) 契約期間内に、セキュリティ相談員の変更を行う場合、運用手順等の引継ぎのための適切な期間を設け、本学の担当職員にその内容を報告し、確認を得ること。
(d) 本契約の期間満了時ないし解約時には、本学と協議の上、必要なデータ資産、及び、運用手順書を全て電子媒体として提供すること。また、3 ヶ月前までにその時点での最新データ資産を電子媒体として提供すること。
(e) 本契約の期間満了時ないし解約時には、本学、及び、新しい業務請負者との打ち合せを綿密に行うこと。
(f) リモート作業は、本学の許可を得て、VPN 接続により実施すること。
(g) リモート作業を行う場合、作業端末は、本学の情報セキュリティ支援業務以外に、原則的に用いないこと。また、作業端末は、マルウェア対策ソフトウェアのインストールを含む情報漏洩等に対する十分なセキュリティ対策を施すこと。
(h) 保守用データを含む本学の情報データの持ち出しを行ってはならない。ただし、事前に持ち出しの内容、取り扱い方法、及び、そのセキュリティ対策について、定例打ち合わせ会等で本学セキュリティ担当教職員と協議し、本学情報基盤センター長の許可を得たものを除く。また、情報基盤センター長の事前許可を得た情報データを実際に持ち出す時は、情報データ移送書を書面で 2 部（大学保管用、及び、請負者保管用）作成し、本学セキュリティ担当教職員に提出すること。この移送書による記録のない情報データの持ち出しは、本学の許可を得ずに行った持ち出しとみなす。
(i) 定例打ち合わせ会時に、作業履歴リスト（作業内容、作業者、作業日時、作業端末等）を提出すること。

2. 資料及びコメントの提出方法

上記 1. ①～⑨に関する一般的な参考資料及び要求条件等に関するコメント並びに提供可能なライブラリに関する資料等の提供を招請する。

(1) 資料等の提供期限

令和８年６月８日　１７時００分（郵送の場合は必着のこと）

(2) 提出先　〒950-2181 新潟市西区五十嵐二の町 8050 番地　新潟大学財務部財務管理課　鈴木　美樹　電話 025-262-7674

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　令和８年５月７日から令和８年６月８日まで。

(2) 交付場所　上記 2 (2) に同じ。

4. 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。

5. Summary

(1) Classification of the products to be produced: 71,27

(2) Niigata University Information Security Measures Support Contract 1 Set

(3) Type of the procurement: Require

(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 Implementation of ASM Assessment

Using a cloud-based ASM tool provided by the contractor, assess the vulnerabilities of equipment exposed to the external network by the university. For vulnerabilities deemed high-priority, notify the equipment administrators of the need for corrective action.

⑨ IT Asset Management Tool Operation Support

Using the IT asset management tool provided by the university (Tanium, Inc.), provide the following operational support:

(a) Use the vulnerability assessment function to conduct vulnerability assessments on endpoints and notify the administrators of equipment deemed high-priority of the need for corrective action.

(b) Use the function to detect suspicious activity on endpoints and notify the equipment administrators of any deemed high-priority issues of the need for corrective action.

⑩ 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 (one for university storage and one for storage by the

contractor) and submit it to the faculty and staff in charge of security at the University. The removal of information data that is not recorded in this transfer form shall be deemed to be the removal of information data without the permission of the University.

i. At the regular meeting, submit a list of work history (work content, worker, work date and time, work terminal, etc.).

(5) Time limit for the submission of the requested material: 17:00,8 June 2026

(6) Contact point for the notice: Miki Suzuki, Financial Management section, Niigata University, 8050 Ikarashi 2-no-cho Nishi-ku Niigata-shi 950-2181 Japan, TEL 025-262-7674