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１⑸①～⑨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。
⑴　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）
⑵　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。
⑴　交付期間　令和８年５月７日から令和８年６月８日まで。
⑵　交付場所　上記２⑵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
⑴　Classification of the products to be produced : 71, 27
⑵　Niigata University Information Security Measures Support Contract 1 Set
⑶　Type of the procurement : Require
⑷　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