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４年３月22日から令和４年５月９日まで。
⑵　交付場所　上記２⑵に同じ。
4　説明会の開催　本公表に基づく導入説明会を開催する。
⑴　開催日時　令和４年３月28日11時00分
⑵　開催場所　山形大学医学部第二会議室
5　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。
6　Summary
⑴　Classification of the the products to be procured : 22, 31
⑵　Nature and quantity of the products to be purchased : Surgical Navigation System 1 Set
⑶　Type of the procurement : purchase
⑷　Basic requirements of the procurement :
A　The system should consist of a monitor cart and a camera cart.
B　The monitor cart should have a 32-inch 4K UHD display.
C　The display should have a multi-touch screen monitor.
D　The system should have the function of digital integration with the equipped microscope, and shall be able to provide image support through augmented reality (AR) functions in the microscope views.
E　The system should be able to be used in an intraoperative MRI operating room and use the intraoperative MRI images as update images.
F　The preoperative planning software should be applicable to craniotomy and stereotactic neurosurgery.
G　A superior maintenance system should be in place.
⑸　Time limit for the submission of the requested material : 11 : 00　28 March, 2022
⑹　Contact point for the notice : Kazuyuki Kakizaki, Procurement Section, Accounting Division, Department of Iida Campus services, Yamagata University, 2―2―2 Iidanishi Yamagata-shi 990―9585 Japan, TEL 023―628―5028

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４年３月22日
国立大学法人東京大学総長　藤井　輝夫
◎調達機関番号　415　◎所在地番号　13
○第16号
1　調達内容
⑴　品目分類番号　14
⑵　導入計画物品及び数量　全学セキュリティファイアウォール　一式
⑶　調達方法　購入等
⑷　導入予定時期　令和４年度１月以降
⑸　調達に必要とされる基本的な要求要件
A　ＩＰアドレス、ポート番号を用いた通信可否のアクセスリストを設定することができること。
B　通信を解析することでアプリケーション識別が可能であり、アプリケーション単位での通信可否を設定することができること。
C　ＩＰアドレスやＵＲＬ、ドメインネーム、ファイルシグネチャ等のブラックリストおよびホワイトリストを保持することができ、一定時間ごとに自動的にリストを更新する機能を有すること。また、管理者が独自のブラックリストおよびホワイトリストを定義できること。
D　ＡＰＩを用いて上記１～３の機能を設定できること。
E　IPv４とIPv６どちらのプロトコルにも対応し、どちらのプロトコルにおいても同等の機能が利用できること。
F　ダウンロードおよびアップロードするファイルを隔離環境にて検査するためのサンドボックス機能を有すること。
G　Webアプリケーションに対する侵入行為やクロスサイトスクリプティングを用いた攻撃、ソフトウェアの脆弱性を用いた攻撃を防御できること。
H　現在100Gbps２回線、将来的に400Gbps以上の帯域で外部と接続される本学のキャンパスネットワークのセキュリティを確保できる、十分な性能を持った設備であること。
I　データセンターに設置され、複数のキャンパスからの通信がすべて経由する装置となるため、単一障害に対応する可用性を有すること。
J　IPsecを用いた拠点間ＶＰＮを設定でき、ＶＰＮ上を流れる通信に対しても通常のイーサネット接続と同様のセキュリティ機能を提供できること。
K　ＤＨＣＰ機能およびルータ機能を有すること。ルータ機能には経路制御プロトコル（OSPFv２／ｖ３）を含むこと。
L　インシデント検出結果や通信記録などのログをsyslog等で外部に転送できること。
M　インシデント検出結果や通信記録などのログをクラウド上のログ検索システムに転送し、クラウド上にてログの検索機能を提供すること。
N　認証基盤と連携し、通信をユーザ単位で識別する機能を提供できること。
O　１台の物理システムの中に複数台の仮想的なシステムを構築でき、それぞれの仮想システムが別の管理者によって別のシステムとして機能できること。
2　資料及びコメントの提供方法　上記１⑵の物品に関する一般的な参考資料及び同⑹の要求要件等に関するコメント並びに提供可能なライブラリー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４年４月22日17時00分（郵送の場合は必着のこと。）
⑵　提出先　〒277―0882　千葉県柏市柏の葉６－２－３　東京大学情報システム部情報戦略課会計チーム　志村　正規　電話　080―9452―3828
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４年３月22日から令和４年４月22日まで。
⑵　交付場所　上記２⑵に同じ。
4　説明会の開催　本公表に基づく導入説明会を開催する。
⑴　開催日時　令和４年３月29日15時00分
⑵　開催場所　Zoomによるオンライン開催
5　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。
6　Summary
⑴　Classification of the products to be procured : 14
⑵　Nature and quantity of the products to be purchased : University-wide Security firewall 1 Set
⑶　Type of the procurement : Purchase
⑷　Basic requirements of the procurement :
A　This system must have ACL (Access Control List) functions based on IP address and port number.
B　This system must identify applications by analyzing network traffic and have ACL functionality based on the application flows.
C　This system must have blacklists and whitelist functions of IP addresses, URLs, domain names, and file signatures. The lists must be updated periodically and automatically. Also, An administrator must configure the original blacklists and whitelists.
D　The functions in 1―3 above must be configured using APIs.
E　This system must provide the same functions on both IPv4 and IPv6.
F　The system must have a sandbox function to quarantine upload and download files in an isolated environment.
G　The system must protect web applications against brute-force, cross-site scripting, and vulnerability attacks.
H　The system must have sufficient performance to ensure the security of the University's campus network, which is currently connected to the Internet using 100Gbps×2 lines and will be upgraded to 400Gbps line or more in the future.
I　The system is located in a datacenter and it accommodates the lines from main campuses, so the system must have high-availability against single failures.