F．マスターデータベースシステムは以下の機能を有する。
(ｱ) 学内情報源システム（学務情報システム、人事給与システム）より得られるＣＳＶ形式のデータにより利用者の属性情報を登録可能とする機能。
(ｲ) (ｱ)で登録した利用者の属性情報を編集でき、利用者自身による情報の最新化を促す機能。
(ｳ) 利用者に対してＩＤなどの情報を配付するための帳票出力機能。
(ｴ) マスターデータベースシステムに対して管理者権限設定など必要なアクセス制御ができる機能。
G．基幹系ユーザ情報配付システムは、学内基幹系システム（ＤＢＭＳ、ＬＤＡＰ、Active Directory）などに対して、安全な通信手段を用いて直接属性情報を提供する機能を有する。
H．ワークフローシステムは以下の機能を有する。
(ｱ) 全学ＩＴ認証基盤サービスに関連する各ワークフロー申請（個人ＩＤ申請、所属変更、入力代行設定）に関する機能をWebブラウザで提供すること。
(ｲ) 各申請情報をマスターデータベースシステムと連携して処理を行う機能。
(ｳ) 利用者の属性情報を基にワークフローの利用権限を設定できる機能。
Ⅰ．ネットワークシステムの要件は、以下のとおりである。
(ｱ) 本システムを構成する機器を通信遅延が発生しない方法でネットワーク接続すること。
(ｲ) 必要に応じて本学学内ＬＡＮネットワーク機器に接続すること。
(ｳ) 構成上必要とされる接続規格及びポート数を用意すること。
J．システムの障害時において、サーバ・ネットワークの冗長化等により、本システムのサービスを停止させないための対策を実施すること。
K．各種ログを採取・集約し、本学の求めに応じて集計レポートを作成する機能を有すること。
L．システムの障害を防止するための十分な保守体制、障害発生時の迅速な対応及びシステム運用に関するサポート体制を提供できること。
M．遠隔保守の実施にあたっては、ＳＮＭＰ等による監視および重要サービスの死活確認等の障害検知の機能を有すること。また、保守時はアクセス元のＩＰ・端末の制限、あるいはセキュリティトークンの利用など、セキュリティに十分な配慮を行った仕組みを導入すること。
N．サーバ上での作業用アカウント、データ連携用アカウントについてはセキュリティの観点から不要な操作権限を制限すること（必要な制限事項は本学と協議し実施すること。）
O．システム管理用の特権ＩＤについて、運用担当者ごとのアクセスコントロールや、操作証跡保存、監査機能、振舞いでの異常検知等が可能であること。
P．緊急度の高い脆弱性を有するソフトウェアがあるマシンのチェックやレポート機能、パッチ管理機能を有すること。
Q．定期的に各サーバのバックアップデータの取得を行い、災害等非常時のため取得バックアップデータの退避が可能なこと。
R．現在稼働中の全学ＩＴ認証基盤システムと認証連携及びデータ連携を行なっている学内システムについて、次期システムで同等の連携を行うための移行作業を実施すること。

2　資料及びコメントの提供方法　上記１(2)の物品に関する一般的な参考資料及び同(6)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。
(1) 資料等の提供期限　令和３年６月21日17時15分（郵送の場合は必着のこと。）
(2) 提供先　〒565―0871 大阪府吹田市山田丘１―１　大阪大学財務部契約課政府調達係　道木　宏晴　電話06―6879―4006
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３年５月17日から令和３年６月21日まで。
(2) 交付場所　上記２(2)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。
(1) 開催日時　令和３年５月20日13時30分
(2) 開催場所　大阪大学サイバーメディアセンター本館２階大会議室
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
(1) Classification of the products to be procured : 14
(2) Nature and quantity of the products to be rent : Campus-wide IT Authentication Platform System 1 Set
(3) Type of the procurement : products to be rent
(4) Basic requirements of the procurement :
A．The system consists of SSO (Single Sign-On) System, Personal ID Management and Federation System and Network System.
B．SSO System consists of SSO System in Campus and SSO System for Gakunin (The Academic Access Management Federation in Japan).
C．SSO System in campus must provide the following requirements.
(1) SSO function conform to OASIS-SAML2.0 for campus-wide service corresponding to the SSO authentication and authorization federation.
(2) Function to link the user attribute information in Master database system with the campus-wide service applications in support of SSO authentication federation.
(3) Function that allows users to delegate their operating privileges to other users (or allows them to input data as other users) for campus-wide service application corresponding to SSO authentication federation.
D．SSO System for Gakunin must provide the following requirements.
(1) Function that enable the authentication federation with Service Providers (SP) are provided by participating universities and companies of Gakunin.
(2) Function that enable generating attribute information defined in System Administration Standards for the GakuNin (Ver. 2.5) using the user attribute information managed by the master database system.
(3) Function that present list of the user attribute information to be transferred on web browser and confirm to provide to third-party, when members in Osaka University first access to Service Providers (SP) in Gakunin.
E．Personal ID Management and Federation System consists of Master Database System, Mission-critical Identity Management System and Workflow System.
F．Master Database System must provide the following requirements.
(1) Function to register user attribute information for staff and students of Osaka University using CSV format data obtained from the registration authority in office.
(2) Function that edit user attribution informations are registered in (1) and update some of attribute information by themselves.
(3) Function for report (print) output to distribute system information such as Personal ID to users.
(4) Function that enable access control to Master Data System such as administrator authority setting.
G．Mission-Critical Identity Management System must provide the function to transmit user attribution informations to mission-critical systems in campus (DBMS, LDAP, Active Directory) in secure communication.