Ｊ．本学からの問合せやシステム保守担当者からの課題提起をきっかけにシステムの設定変更等が必要となった場合、作業を実施すること。また、本システムが脆弱性の影響を受けることが発覚した場合、脆弱性対応を行うこと。

Ｋ．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連携先システムについて、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。移行に当たって連携先システムの設定や利用者の操作方法に変更が生じる場合、提案段階で明らかにすること。

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８年６月22日17時15分（郵送の場合は必着のこと。）

⑵　提供先　〒565―0871 大阪府吹田市山田丘１－１　大阪大学経理部経理契約課契約第三係　吉弘　周平　電話06―6879―4010

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21日から令和８年６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８年５月26日13時30分

⑵　開催場所　大阪大学Ｄ３センター吹田本館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

⑴　Classification of the products to be procured : 14

⑵　Nature and quantity of the products to be rent : OUID System 1 Set

⑶　Type of the procurement : products to be rent

⑷　Basic requirements of the procurement :

Ａ．This system consists of an Integrated ID Authentication System and an Integrated ID Management System.

Ｂ．The Integrated ID authentication infrastructure shall have the following functions.

Ｂ－１．Single Sign-On (SSO) Functions

ａ．A single sign-on function compliant with OASIS-SAML 2.0 and OIDC for services (web applications) that support authentication／authorization federation, including SPs participating in academic authentication federations.

ｂ．A portal site that lists links to systems that support single sign-on, and a user guideline web page that includes FAQs and other information.

ｃ．A single logout function that, when a user logs out from a federated SP／RP, logs the user out from all federated SPs／RPs.

Ｂ－２．Authentication Functions

ａ．Authentication functions including : password plus multi-factor authentication using a secondary factor with an ID or email address as the username ; passkey authentication ; certificate authentication ; and social account authentication.

ｂ．A function that allows users to change their passwords and secondary authentication methods by themselves.

ｃ．If authentication is not possible due to a forgotten password, etc., functions including : online password reset／reconfiguration by the user using a recovery email address and a My Number Card ; a temporary secondary-authentication bypass function when secondary authentication cannot be performed ; and a user self-service password reset function.

ｄ．A function to maintain authentication sessions between users and between SPs／RPs for a specified period of time.

Ｂ－３．Authentication Information Management Functions

ａ．A function to retain, for each ID, the attributes received via federation from the Integrated ID management infrastructure.

ｂ．A function to send to an SP／RP the attributes held by the ID linked to the username, using the username specified by the user at the time of authentication as the key.

ｃ．A function to control which SPs／RPs can be used according to the attribute information held by the ID used for authentication.

Ｂ－４．Administrator Functions

ａ．A function that allows administrators to add, modify, and delete SPs／RPs to be federated for authentication.

ｂ．A function to acquire user's authentication logs and allow administrators to view them.

ｃ．A function that allows administrators to reset user's authentication information.

Ｃ．The Integrated ID management infrastructure shall have the following functions.

Ｃ－１．ID Management Functions

ａ．A function to assign each user a unique ID within the University's systems.

ｂ．A function to manage role-specific information separately from user information when a user holds multiple positions (Role ID function).

ｃ．A function to manage attribute information linked to IDs and Role IDs, and in response to inquiries keyed by username, return the attributes held by one of the multiple Role IDs possessed by a user.

Ｃ－２．Data Import Functions

ａ．A function to automatically or manually import data (CSV) provided from source systems that serve as the origin of user information and register users. There are multiple source systems, and the key information differs depending on the system.

ｂ．A function to generate attribute information linked to IDs based on generation rules at the time of data import.

ｃ．A function to identify candidates that may refer to the same person when information for one user is registered in duplicate in the database at the time of data import (candidate record linkage function).

ｄ．If an administrator determines that entries in the record-linkage candidate list refer to the same person, a function to overwrite the user information while keeping role information separated.

Ｃ－３．Master Data Management Functions

ａ．For master data of attribute information to be granted to users (e.g., department master, position master), a function that allows administrators to register and update it via CSV import.

Ｃ－４．Workflow Application Functions

ａ．For users not included in the source systems, a function whereby designated staff apply for ID issuance and administrators approve it, thereby issuing, changing, or revoking IDs.

ｂ．A function that allows administrators and designated staff to search past applications.

ｃ．A function to grant application privileges to designated staff.