⑹　Contact point for the notice : Academic Computing and Communications Center, University of Tsukuba, 1―1―1 Tennodai Tsukuba-shi 305―8577 Japan, TEL 029―853―6219, E-mail accc@un.tsukuba.ac.jp

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21日

国立大学法人大阪大学総長　熊ノ郷　淳

◎調達機関番号　415　◎所在地番号　27

○第２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　ＯＵＩＤシステム一式

⑶　調達方法　借入

⑷　導入目的　大阪大学に関わるすべての人が一意な生涯ＩＤ（ＯＵＩＤ）の利用を通じて大阪大学のリソース・学びにアクセスできる環境の実現のため、統合的なＩＤ認証・管理基盤を提供し、学内外の様々な情報システムとの認証連携・データ連携を実現するものである。

⑸　導入予定時期　令和10年10月以降

⑹　調達に必要とされる基本的な要求要件

Ａ．本システムは、統合ＩＤ認証基盤と統合ＩＤ管理基盤から構成される。

Ｂ．統合ＩＤ認証基盤は以下の機能を有すること。

Ｂ－１．シングルサインオン機能

ａ．認証・認可連携に対応したサービス（Webアプリケーション）に対して、OASIS-SAML2.0、ＯＩＤＣに準拠したシングルサインオン機能。連携先に学術認証フェデレーション参加ＳＰを含む。

ｂ．シングルサインオン可能なシステムのリンク集を掲載するポータルサイトおよびＦＡＱ等を掲載する利用者向けガイドラインWebページ。

ｃ．連携先ＳＰ／ＲＰからログアウトした場合、すべての連携先ＳＰ／ＲＰからログアウトした状態にするシングルログアウト機能。

Ｂ－２．認証機能

ａ．ＩＤまたはメールアドレスをユーザ名としたパスワード及び二次認証による多要素認証、パスキー認証、証明書認証、ソーシャルアカウント認証機能。

ｂ．利用者自身によるパスワードおよび二次認証変更機能。

ｃ．パスワード忘れ等により認証ができない場合の、リカバリ用メールアドレス、マイナンバーカードを用いた利用者自身によるオンラインパスワードリセット・再設定機能、および、二次認証が出来ない場合の二次認証一時解除機能。利用者自身で利用者自身によるパスワードリセット機能。

ｄ．所定の時間、ＳＰ／ＲＰの認証セッションを維持する機能。

Ｂ－３．認証情報管理機能

ａ．統合ＩＤ管理基盤からの連携を受け、ＩＤごとに持つ属性を保持する機能。

ｂ．認証時に利用者が指定したユーザ名をキーとして、ユーザ名に紐づくＩＤが持つ属性をＳＰ／ＲＰに送信する機能。

ｃ．利用者が認証に用いたＩＤが持つ属性情報に応じて、利用可能なＳＰ／ＲＰを制御する機能。

Ｂ－４．管理者向け機能

ａ．管理者が、認証連携するＳＰ／ＲＰを追加・変更・削除する機能。

ｂ．利用者の認証ログを取得し、管理者が認証ログを閲覧する機能。

ｃ．管理者が利用者の認証情報をリセットする機能。

Ｃ．統合ＩＤ管理基盤は以下の機能を有すること。

Ｃ－１．ＩＤ管理機能

ａ．１利用者に対して、大学のシステム内で一意となるＩＤを付与する機能。

ｂ．１利用者が複数の身分を有する場合に、１利用者としての情報とは別に、身分ごとの情報を管理する機能（ロールＩＤ機能）。

ｃ．ＩＤ、ロールＩＤに紐づく属性情報を管理し、ユーザ名をキーとした問合せに対して１利用者が持つ複数ロールＩＤのうち１つのロールＩＤが持っている属性を回答する機能。

Ｃ－２．データ取込み機能

ａ．利用者情報の源泉となるシステムから提供されるデータ（ＣＳＶ）を自動または手動により取込み、ユーザ登録を行う機能。源泉システムは複数あり、システムによってキーとなる情報が異なる。

ｂ．データ取込み時、生成ルールを基にＩＤに紐づく属性情報を生成する機能。

ｃ．データ取込み時、１利用者の情報が重複してデータベースに登録される際、同一人物である可能性を候補する機能（名寄せ候補機能）。

ｄ．名寄せ候補の一覧に対して管理者が同一人物と判定した場合は、ロールの情報は分岐したまま１利用者の情報を上書きする機能。

Ｃ－３．マスタ管理機能

ａ．所属マスタ、役職マスタ等、利用者に付与する属性情報のマスタについて、管理者がＣＳＶインポートにより登録、更新する機能。

Ｃ－４．ワークフロー申請機能

ａ．源泉システムに含まれない利用者について、特定の職員がＩＤ発行を申請し、管理者が承認することでＩＤの発行、変更、失効を行う機能。

ｂ．管理者および特定の職員が、過去の申請の検索を行う機能。

ｃ．特定の職員に申請の権限を付与する機能。

Ｃ－５．管理者向け機能

ａ．管理者が利用者の情報を検索し、個別に編集する機能。

ｂ．管理者が利用者の情報を検索し、特定の帳票形式およびＣＳＶで出力する機能。

ｃ．管理者が利用者のパスワード、二次認証をリセットする機能。

ｄ．管理者アカウントに応じた権限管理を設定する機能（全体管理、ユーザ登録担当、パスワードリセット担当等）。

ｅ．サーバへのリモートアクセスを制御・管理する機能。

Ｃ－６．証跡機能

ａ．利用者情報に対する操作履歴や、プロビジョニング記録を証跡ログとして保存する機能。

ｂ．管理者が利用者ごとの証跡ログを検索・参照・出力する機能。

Ｃ－７．利用者向け機能

ａ．利用者が自身の属性情報を編集する機能。

ｂ．利用者が自身のパスワードを編集・リセットする機能。

Ｃ－８．ＩＤプロビジョニング機能

ａ．更新された利用者情報をシステムごとの連携条件に応じて取得・加工し、同期する機能。

Ｄ．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。

Ｅ．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。）

Ｆ．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に退避が可能なこと。

Ｇ．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。

Ｈ．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。

Ｉ．本学からのシステム保守担当者への質問・問い合わせに対応すること。