統合 ID 管理システム　一式

仕様書

令和 6 年 7 月

国立大学法人琉球大学

目次

Ⅰ 仕様書概要説明

1 調達件名等

1.1 調達件名

「統合 ID 管理システム一式」

1.2 調達者

国立大学法人琉球大学

1.3 調達内容

1. 統合 ID 管理システム　　1 式

2. SSO 認証基盤システム　　1 式

1.4 本調達の契約期間

契約締結日　～　令和 7 年 3 月 31 日

1.5 履行場所

本学及び担当者の指定する場所及び受注者の所有する作業場所

2 調達の背景及び目的

国立大学法人琉球大学（以下、本学という。）は、第 4 期中期計画において「情報化推進体制を整備し、新たな情報化推進計画に基づき、事務の効率化や情報基盤の整備、情報セキュリティ教育を推進し、デジタル・キャンパスを実現する」ことを目標としている。教育・研究活動の質向上、学生の PC 必携化や BYOD 推進に伴う ICT 環境構築、業務運営の改善及び効率化のため、情報セキュリティを考慮した情報基盤の整備が不可欠である。

このような背景のもと、琉球大学では、情報化推進計画の一環として、統合 ID 管理システムの導入を検討している。本システムは、統一された ID 管理を行うことで、利便性の向上と管理コストの削減を図るものである。また、セキュリティ強化を実現し、ユーザー認証の一元管理によるアクセスコントロールの最適化を目指す。これにより、学生や教職員の ICT 利用環境が一層向上し、業務効率化とセキュリティ確保が両立される。

3 技術的要件の概要

3.1 本調達物品に係わる性能、機能及び技術等（以下、「性能」という。）の要求要件(以下、「技術的要件」という。)は、「Ⅱ.調達物品に備えるべき技術的要件」に示すとおりである。

3.2 技術的要件は、全ての必須の要求要件である。

3.3 性能等が技術的要件を満たしているか否かの判定は,本学技術審査委員会において,応札仕様書,その他提出資料の内容を審査して行う。

3.4 技術的要件は，必要とする最低条件を示しており，これらを満たしていないとの判断がなされた

場合には不合格となり，落札決定の対象から除外する。

4 技術仕様等に関する留意事項

4.1 入札製品は、原則として入札時点で製品化されていること。入札時点で製品化されていない機器またはソフトウェアによって応札する場合には、技術的要件を満たすことの証明及び納入期限までに製品化され納入できることを保証する資料及び確約書等を提出すること。

4.2 提案システムのうち、納入期限までにバージョンアップが予想されるハードウェアまたはソフトウェアがある場合、その予定時期等が記載された資料を提出すること。

4.3 納入時における全てのソフトウェアは、最新バージョンで提供すること。

4.4 自社製品だけで仕様を満たせない場合、他社製品を使い仕様を満たしてもよい。

4.5 本仕様書に明示がない事項については、本学と協議し、誠実に対応すること。

5 提案に関する留意事項

5.1 提案が技術的要件を満たしていることを，応札仕様書のどの部分で証明できるかを技術的要件毎に，具体的かつわかりやすく，資料等を添付し参照すべき箇所を明示すること（技術的要件と入札機器に係る性能等を，対比表を作成して示すこと）。参照すべき箇所が，メーカーの仕様書，説明書，カタログ等である場合は，表中に参照資料番号を記入すると共に，資料中にアンダーラインを付したり，色付けしたり，余白に大きく矢印を付したりすることによって当該部分を分かり易くしておくこと。

5.2 記述内容が不明確である場合には，有効な応札仕様書とはみなさないので，留意すること。特に，審査に当たっては，「実現します」や「可能です」といった提案の根拠が不明確，説明が不十分であるなどで，技術審査に重大な支障があると本学技術審査委員が判断した場合は，技術的要件を満たしていないものとみなし不合格とし、落札決定の対象から除外される。

5.3 提案される内容等について，問い合わせやヒアリングを行うことがあるので、誠実に対応すること。

6 導入に関する留意事項

6.1 導入スケジュールは、本学担当者と協議し、その指示に従うこと。

6.2 導入システムを令和 7 年 3 月 31 日までに納品すること。

6.3 本調達の履行に当たり、受注者は、その計画・進捗状況・内容につき、本学との間でシステム導入に関する連絡会を適宜開催し、密接に連絡・協議するとともに、本仕様書に基づいて行う本学の指示・監督に従うこと。

6.4 本調達には、ハードウェア及びソフトウェアの調達・ライセンス費用を含むこと。

6.5 応札者は、調達機器の搬入、据え付け、配管・配線、調整及び既存機器との接続に要するすべての費用を負担すること。また、導入に際して、連携が必要な本学システム（ネットワーク・セキュリティを含む。）の既存機器への設定の追加・変更・調整等に係る費用も調達に含めること。

6.6 調達システムの安定稼働まで応札者が責任を持って行うこと。

7 その他留意事項

7.1 令和７年４月１日以降のハードウェア及びソフトウェアのライセンス及び保守は、別調達にて行う予定である。

II 調達物品に備えるべき技術的要件

（性能・機能に関する要件）

1 統合 ID 管理システムならびに SSO 認証基盤システム

現在、本学における ID 管理システムは、情報基盤統括センター（以下、「本センター」という。）が提供するキャンパス情報システムを利用するための ID 管理システムとして動作しているが、今回の調達において、統合 ID 管理システムとして発展させ、合わせてシングルサインオン（以下、SSO という。）認証基盤システムを構成し提供することで、利用者の利便性向上とセキュリティ環境の向上を図るものである。統合 ID 管理システムと SSO 認証基盤システムとの２つのシステムで構成することを理解し、両システムの親和性に考慮して構成すること。以下、本システムを構成する２つのシステムの要求仕様を記載する。

2 統合 ID 管理システム

2.1 統合 ID 管理システムの全体像

2.1.1 統合 ID 管理システムに求める構造を以下に示す。統合 ID 管理システムについては、パッケージ製品を主体とし、本学の求める機能を実装するために必要となる部分は外部開発モジュールによる実装も可とする。ただし、外部開発となるモジュールからは、採用するパッケージ製品のもつ API や、ファイルによる連携などを用いることで一つのシステムとして動作可能とすること。

2.1.2 本学の情報システムを利用する学生、教職員、その他構成員のアカウント情報を保管するためのリポジトリサーバを有すること。

2.1.3 本学の認証基盤となっている LDAP サーバや Active Directory サーバの存在、そして現状でも利用をおこなっている Shibboleth 認証環境にかんがみて、リポジトリサーバ自身も LDAP サーバで構成されることが望ましい。

2.1.4 メタサーバ（リポジトリサーバの中核となるアカウント情報の保管場所（リポジトリ）のサーバである。以下、「メタサーバ」という。）に保管されるアカウント情報の追加・更新・削除作業や、メタサーバのアカウント情報を利用して、今回調達する SSO 認証基盤システムを含む多数のシステムへのアカウントデータ連携（プロビジョニング）を実施できるプロセスサーバ（以下、プロセスサーバという。）を配置すること。

2.1.5 プロセスサーバに対して、管理者や利用者自身が情報のメンテナンスを行うための WebGUI を提供する Web アプリケーションサーバを構成すること。

2.1.6 プロセスサーバによって、アカウントデータを連携（プロビジョニング）させる対象としては、上述の認証基盤を構成する、LDAP サーバ、Active Directory サーバなどを対象とすること。連携（プロビジョニング）先のシステム群については後述する。

2.1.7 プロセスサーバから直接アカウントの連携を行うことができない場合を想定し、アカウントデータの間接連携に供するための CSV ファイルの出力も想定すること。さらに、アカウントの連携において、相手側のシステムに対してコマンド発行などを利用してアカウントの連携ができるようこの機能を備えること。連携対象となるものは、ユーザーアカウントに限らず、グループ情報や、ユーザーが利用するファイル領域も想定すること。

2.2 アカウント情報メンテナンスのための Web アプリケーションサーバ（以下、「管理者用 WebGUI 機能」という。）

2.2.1 管理者用 WebGUI 機能では、以下の機能を有すること。

(1) アカウント管理権限を持つユーザーをログイン機能によって認証選別し、管理権限の範囲によって、適切なメンテナンスメニューが提供可能であること。

(2) アカウント管理権限は、ログインした管理者によって、画面に表示される項目の有無の制御、項目に対しての更新や参照権限の設定、ユーザーアカウントの追加・更新・無効化・削除の実施の制限などが考えられる。本学は複数のキャンパス、複数の部局によって成立しているので、ログインを行った管理者に適切な属性値を設定することで、管理対象とできるユーザーの範囲（所属などをイメージ）を制限できるなど、実情にあった管理権限が定義できること。

(3) ユーザーアカウントの登録、更新、無効化、削除については、個別のユーザーアカウント単位の処理だけでなく、CSV などのファイルを利用した Web からのアップロード投入も実施可能で、かつその実施も権限によって制御できること。

(4) 個別ユーザーアカウントのメンテナンス画面においては、投入するユーザーアカウントの属性の特徴に応じて、フリーテキスト、プルダウンリスト、ラジオボタンなど編集モードが設定できること。

(5) 管理者操作のための画面構成について、GUI を用いた定義が行えること。画面によっては配置される属性の項目数の多少が考えられるので、タブで画面構成を分けるなどして、管理者の操作性に配慮できること。

(6) 管理者によって、利用者を検索し、当該ユーザーのパスワードの再発行ができる WebGUI も提供すること。ただし、この機能によって、発行されたパスワードの連携（プロビジョニング）範囲や、そのパスワードの有効期限は、後述する利用者自身によるパスワードの変更実施の場合とは区別され、制限できること。

(7) 学生については、本学の教務情報システムから提供される CSV などのファイル（発生源情報）による一括メンテナンスが実施できること。ただし、本システムでの ID 体系の分化については後述するので、発生源情報を一次加工するようなプロセスも想定すること。なお、入試形態

の多様化に伴い、CSV フォーマットの変異があることにも対応すること。

※ 本システムにユーザーを登録するための CSV などの情報を提供する教務情報システム、人事給与システム、システム管理者を発生源とする。

(8) 教職員については、本学の人事給与システムから提供される CSV などのファイル(発生源情報)による一括メンテナンスが実施できること。前項同様に本システムでの ID 体系の分化については後述するので、発生源情報を一次加工するようなプロセスも想定すること。

(9) 本学の情報システムを利用することになる教務情報システムに登録された学生以外及び人事給与システムに登録された教職員以外の本学構成員（以下、「その他構成員」という。）に対して、本センターにおいて、申請内容に基づき CSV ファイルを作成する運用にも対応すること。その他構成員を取り扱う CSV ファイルについても前項同様に、本システムでの ID 体系の分化については後述するので、発生源からの情報を一次加工するようなプロセスも想定すること。

(10) 発生源からの CSV ファイル（以下、「発生源データ」という。）の項目名称は発生源データにあらかじめ定義されている項目名がそのまま利用できること。

(11) 発生源データ上に表現される情報を利用して、変数や、定数あるいは参照ファイルを用いるなどの機能によって、関連する情報を補てんできる機能を有し、発生源データを加工する際の労力の低減とヒューマンエラーの低減が可能であること。また、投入される発生源データ上の項目状態を判断して、取込の除外が可能であること。

(12) 発生源データを用いた一括投入によってメタサーバにメンテナンスが実施された際には、引き続く処理として一括で、各連携先（プロビジョニング先）に反映が行われること。また、GUI による個別処理によってメタサーバに更新が行われた場合には、個別単位で、各連携先（プロビジョニング先)に対しての反映が行われること。CSV ファイルをアップロードしての実行が、本管理者用 WebGUI 機能を用いて、管理者の恣意的なタイミングで実施できるだけでなく、所定のフォルダに CSV ファイルを事前配置することで、時限を以って実行できるなどこれらをジョブ化しての実施も実現できること。各連携先（プロビジョニング先）への反映方法の詳細については、後述する。

(13) 管理者向け WebGUI 機能を定義する設計設定用 GUI を有すること。

(14) ユーザーアカウントの登録またはパスワード再発行処理において、発行したパスワードをユーザーに通知するための通知書（PDF 等）の出力ができること。また、通知書の内容を設定でき、変更が行えること。

2.3 利用者のための Web アプリケーション機能（以下、「利用者用 WebGUI 機能」という。）

2.3.1 利用者用 WebGUI 機能では、以下の機能を有すること。

(1) 利用者によるログインによって、利用者自身の属性情報（パスワード変更を含む。）を変更可能とすること。

(2) ログインした利用者の持つ属性の値を判断して、提供されるメニュー構成などが変化できること。

(3) パスワードポリシーが定義可能であること。パスワードポリシーは本学管理者との協議によっ

て定めることとするが､Windows 環境におけるパスワードの複雑性と同等の定義が行えること。

(4) 利用者がパスワードを変更する際は、既存パスワードの入力と新しいパスワードの入力、新しいパスワードの確認入力が実施できるものとし､入力された新しいパスワードの強度が啓蒙的な情報として表示可能であること。

(5) 本アプリケーションにおいては、本学のロゴなどを表現できること。

(6) 本アプリケーションによって､メタサーバに対して行われた更新情報は､速やかに各連携先(プロビジョニング先）に対しても反映されること。反映方法の詳細については後述する。

(7) 利用者向け WebGUI 機能を定義する設計設定用 GUI を有すること。

(8) 機能として、「パスワード変更」､「UNIX 情報の変更」となる。それぞれの内容は、以下のとおりである。

・パスワード変更・・・利用者自身でパスワード変更するものである

・UNIX 情報の変更・・・UNIX で動作している教育用サーバ（実習室 Linux 含む)、研究用サーバの shell を変更できる機能である。

2.4 プロセスサーバの機能について

メタサーバに対してのユーザーアカウント情報の反映機能や、アカウントの連携先（プロビジョニング先）に対して、連携における必要機能や本プロセスサーバで実施が必要な機能を以下に記載する。

2.4.1 メタサーバに対しての情報反映

(1) WebGUI アプリケーションからのメンテナンス情報に基づいて、メタサーバへの反映が実施できること。CSV や GUI からの情報をもとにして、メタサーバの属性をマッピングして反映を行うことを基本とするが､CSV や GUI からの属性情報に対して、定数や変数を加えることや、CSV や GUI からの属性値を条件として条件分岐を行い､メタサーバに対しての反映値を制御できること。

(2) メタサーバのユーザーを削除する場合は、いったん無効化処理を行って、OU の移動なども併用し保管したのち、物理削除が実施できること。

(3) メタサーバのユーザー属性の状態を判断条件として､メタサーバのユーザー属性情報を変更可能であること｡および､その条件に則ったユーザーを選択的に反映先システムに対して連携(プロビジョニング）を行う機能を有すること。

(4) メタサーバは、レプリケーション構成を保持し、冗長性を確保すること。

2.4.2 本プロセスサーバ自身の機能について

(1) 前述のように､メタサーバに保管されているユーザーアカウントの情報が一定の条件を満たした場合に、処理を行って、その結果を各連携先に反映できること。例として、非常勤の教職員や、科目等履修生のように、アカウントの有効期限を有する場合に、有効期限を判断して、自動的に削除や無効化などが実施できること。

(2) パスワード有効期限や、上記のような有効期限を保持させる場合に、有効期限の到来前に、該当ユーザーに対して警告メールを送信する機能を有すること｡なお､この場合のメール本文は、

送信事象に合わせて設定可能であること。

(3) 本プロセスサーバ自身はコンソール機能を有すること。このコンソール機能を用いることで、本項で記載している各種の設定について GUI にて定義が行えること。

(4) 本プロセスサーバからパスワードなど本学が重要と認めた情報をメタディレクトリに保管する場合には、本学が指定する任意の属性に対して暗号化やハッシュ化などの措置を行って、安全に保管されること。また、連携先にこれらの情報が必要となる場合には、ハッシュ化を行って連携反映を実施できること。なおハッシュ関数は、MD5,SHA-1、SHA-2、SMD-5、SSHA などに対応可能であること。Active Directory に対しては、ADSI を用いて適切にパスワード連携が行えること。

(5) メタサーバにユーザーアカウント情報を保管する場合の属性名称については、一般属性名（cn,uid など)、本システム固有のシステム属性名称の他に、本学固有の属性名称を使えることとして、管理者の理解を助ける設計が可能であること。

(6) 本プロセスサーバが、メタサーバに対してメンテナンスの実行や各連携先への反映の実行部分を担うことから、本プロセスサーバの実行時のログは実行時にリアルタイムで表示され、かつ実行後においてもログの検索の実施が行える GUI を備えること。また、ログについては、別段の Syslog サーバや、Windows のイベントログへの格納も行えること。

(7) 統合 ID 管理システムの運用においては夜間のバッチ処理的な動作の実行も必要であり、バッチ処理設定が行えることに加えて、この場合にエラーの発生など、ログの条件によっては、管理者に対してエラー発生を警告するためのメールを送信可能であること。

2.4.3 キャンパス情報システム Active Directory サーバへの連携

(1) 本学の Active Directory サーバは、情報基盤統括センター系ドメインと、事務系ドメインの２式の Active Directory サーバを運用している。

情報基盤統括センター系ドメイン・・パソコン室の PC 認証および管理、Microsoft365 の利用における ADFS 認証の資源

事務系ドメイン・・Microsoft365 の利用における ADFS 認証の資源

今回の調達において、事務系ドメインを情報基盤統括センター系ドメインに統合する。提案者においては、この構成に配慮を行って、２種の Active Directory ユーザーを安全に収斂させる方策を提案すること。

(2) 現状において、同一人物が、別の UPN (User Principal name。ActiveDirectory におけるユーザー名の１つである。）を利用して２つの Active Directory に配置されている場合が存在するが、新システムにおいては、このようなユーザーは管理 ID からの分割を行って、別のアカウントとして管理を行う方針とするので、このことに対応すること。

(3) メタサーバに存在するアカウントの中から、Active Directory に対して連携を行うユーザーの範囲を設定して、アカウント連携を行うこと。連携対象とするユーザーをメタサーバから抽出する際のフィルター条件を設定し抽出を行って、CSV ファイルなどの中間ファイルを用いることなく、Active Directory 側の対応する範囲のユーザーを抽出して自動的に差分反映を行うこと。

(4) メタサーバに保管されるアカウントの属性と Active Directory 側の属性をマッピングして、アカウント情報の連携を行うこと。ただし、メタサーバ側の属性情報に対して、定数や変数を加えることや、メタサーバの属性の値によって、条件分岐を行なって反映する値を制御できること。Active Directory 側のパスワードを変更しないで、他の一般属性を変更する場面においても、Active Directory 側のパスワードに関わる属性に変化を与えないこと。(例えば、パスワード変更回数や、パスワード期限情報の更新はパスワード変更の際にだけ行われること。)

(5) Active Directory 側のユーザーを削除する場合、いったん無効化処理を行って、OU の移動なども併用して保管したのち、物理削除が実施できること。

(6) メタサーバ側のユーザーの身分や所属学部などを分類のための情報として利用し、カテゴリに分け、セキュリティグループの作成やメンバの更新、グループの削除が実施できること。

(7) 利用者によるパスワードの変更については、利用者用 WebGUI 機能からの操作を基本とすること。

(8) 本センタードメインの Active Directory サーバを認証基盤として利用している各システムによって必要とされる属性情報がメタサーバからの情報によって充足されること。

(9) Active Directory サーバは、Microsoft365 を利用するためのアカウント資源情報を提供することになるので、Microsoft365 側へのアカウント連携を行うための必須属性や、Microsoft365 A3 および AI の各機能を制限するためのライセンス情報のための属性値を正しく連携し反映させること。

2.4.4 キャンパス情報システム LDAP サーバへの連携

(1) 本センターで有している LDAP サーバ（以下、「本 LDAP サーバ」という。）に対してアカウントの連携を実施すること。現状の OU 構造などを観察し、同じ構成となるように連携する OU をコントロールできること。(現状の OU 構造を維持すること。)

(2) 本 LDAP サーバにアカウントを反映すべきユーザーについては、メタサーバの属性情報をもとにして、対象者を抽出するためのフィルター条件が定義でき、抽出を行い、CSV ファイルなどの中間ファイルを用いないで、本 LDAP サーバ側の対応する範囲のユーザーを抽出して自動的に差分反映を行うこと。

(3) メタサーバに保管されるアカウントの属性と本 LDAP サーバ側の属性をマッピングして、アカウント情報の連携を行うこと。ただし、メタサーバ側の属性情報に対して、定数や変数を加えることや、メタサーバの属性の値によって、条件分岐を行なって反映する値を制御できること。本 LDAP サーバ側のパスワードを変更しないで、他の一般属性を変更する場面においても、本 LDAP サーバ側のパスワードに関わる属性に変化を与えないこと。

(4) 本 LDAP サーバ側のユーザーを削除する場合は、いったん無効化処理を行って、OU の移動なども併用して保管したのちに、別して物理削除が実施できること。

2.4.5 SSO 認証基盤システムリポジトリへの連携（プロビジョニング）

(1) SSO 認証基盤システム側においても、アクセス制限や認証手段をユーザーの属性情報に応じて制御を行うこととなり、このためのユーザーリポジトリを有することとなる。このリポジトリに対応するための属性情報をメタサーバに保有し、連携（プロビジョニング）を行うこと。

(2) 連携（プロビジョニング）を行う属性の中に、パスワード情報を含む場合は、SSO 認証基盤サーバ側の仕様に沿ったパスワードの安全な連携方式を採用すること。

(3) SSO 認証基盤側で、ユーザーの有効、無効の制限が可能である場合には、統合 ID 管理システム側からも、有効、無効の制御のための属性値の連携（プロビジョニング）を実施できること。

(4) SSO 認証基盤システムにおいて、ユーザー単位における SSO 対象 SP の利用可否選別が、ユーザー属性情報に基づいて実施可能となるように、利用可否選別情報についても連携が可能であること。

2.4.6 キャンパス情報システム ユーザー向けファイルサーバシステムへの連携（プロビジョニング）

(1) 本学において、ユーザーの発生に伴い、ユーザーが利用可能な Linux 環境でのファイル格納用フォルダ領域と、Windows 環境でのファイル格納用フォルダ領域を用意している。ユーザーの新規作成時においては、この両方のフォルダ領域の作成が実施できること。

(2) 作成した領域において適切なセキュリティ設定が実施できること。

(3) また、ユーザーが離籍する場合においては、後述する 2.7.1.(6)項のアカウントライフサイクルの削除運用期日に基づき、離籍したユーザーの当該フォルダ領域の削除を実施できること。

2.4.7 学内の多種システムに対しての CSV 連携（プロビジョニング）

(1) 本学において、ここまでに示した Active Directory や、LDAP サーバを認証基盤として利用しつつ、そのローカルシステム内部にユーザー情報を保持する必要のあるシステムが多数存在している。したがって、これらのシステムに対して、必要なユーザーの範囲や、必要な属性項目を調整して CSV ファイルを出力することが求められる。これらの CSV ファイルについては、最大で 3 フォーマットが可能となるように構成すること。

- ・登録者全件データ CSV
- ・教職員・その他構成員データ CSV
- ・学生データ CSV

(2) 出力した CSV は、ActiveDirectory サーバや LDAP サーバを認証基盤として利用している本学の各システムが SFTP や FTP などで取得し、利用できる構成を行うこと。また、認証基盤を利用しているシステムごとに接続用の ID を作成し、どのデータを取得できるか制限ができるよう構成できること。

2.5 Microsoft EntraID に対する連携について

2.5.1 前述の Active Directory に保管されるユーザー情報、グループ情報を資源として、Microsoft Entra Connect を用いて、適切な連携状態となるよう設計実施すること。

2.5.2 グローバルアドレスリストへの表示、非表示など、Microsoft Entra Connect の詳細設定については本学担当者と協議を行って設定すること。

2.5.3 本学における、EntraID へのユーザー登録は、現状の ID 管理システムからの PowerShell コマンドによる実装にて実現している。認証環境については、ADFS での利用を行っている。提案者においては、この環境を理解し、ユーザーの利用環境に影響を与えないように、Microsoft Entra Connect によるアカウント同期動作を実現すること。

2.5.4 Active Directory と、EntraID との間でのユーザーの一意キーとなる、ImmutableID については、Active Directory の壊滅的な破損にも対応できるように、本 ID 管理システムにおける属性値計算機能を用いて、Micrrosoft 社の規定に則った ImmutableID を計算保持し、復元可能とすること。

2.5.5 本学においては、ExchangeOnline のメールシステムの活用も行っているので、そのための必要属性についても本 ID 管理システムにおいて管理を行い、適切に Microsoft Entra Connect にて連携対象属性として設定されること。UserPrincipalName だけでなく、mail、mailNiuckName、proxyAddresses の各属性についても適切に管理設定されること。

2.6 ユーザーID に関する実装方針

統合 ID 管理システムで登録が開始される以前に登録されたユーザーのログイン ID は、統合 ID 管理システム稼働後も変更せず同じものを利用できるようにする。2.6.1 項以降の実装方針は、統合 ID 管理システムで登録が開始された後の実装方針ある。

2.6.1 本システムにおいては、以下のようなユーザーID を保持して、それぞれの場面でユーザーの識別を行えるようにシステム全体を整えること。

- ・発生源 ID　→　アカウントとしての実体を表すための ID
- ・管理 ID　→　本 ID 管理システム上の主キー
- ・ログイン ID（ノーマル）　→　ユーザー自身が認識している ID
- ・ログイン ID（ショート）　→　ユーザー自身が認識している ID

2.6.2 本システムで管理対象となるアカウントは大きく学生・教職員・その他構成員の３種に大別される。

2.6.3 学生の場合は、学籍番号が発生源 ID となる、教職員の場合は教職員番号が発生源 ID となる。その他構成員の場合は、本センターで発生源 ID を附番する。発生源 ID は、学部生の内部進学や非常勤職員の常勤化などで同一人物において変更となることがあるので、システムとしてこれに対応すること。

2.6.4 管理 ID とは、統合 ID 管理システムにおいて附番を行う ID でシステム上の主キーとなる。発生源 ID が変化する場合においても、管理 ID は変化しない。同一人物が、異なる身分で同時にアクティブである必要な場面においては、同一人物に対してことなる発生源 ID のもと、ことなる管理 ID を発行する。この場合、後述するログイン ID（ノーマル)、ログイン ID（ショート）も同様に別 ID が発行される。

管理 ID の附番ルールについては、本学担当者と協議を行い、ユニークかつ判読性のある体系を提案すること。

2.6.5 ログイン ID（ノーマル)、ログイン ID（ショート）については、いずれもユーザーが本学のシステムにログインを行うための主キーである。原則変更を行わないが、なんらかの事情によって変更せざるを得ないと管理者が認めた場合、管理者によって変更可能とする。ノーマルとショートの違いは桁数で、ショートは全体として 10 桁となるように整備される。ショートを有する理由は、現存する本学の内部システムにおいて、ログイン桁数が 10 桁で制限されているシス

テムが存在していることがその理由で、将来的にはログイン ID（ノーマル）に収斂される見込みであるが、当面併用することとなる、この２つの ID の附番体系は以下の通りとする。

・ログイン ID（ノーマル）

苗字ローマ字＋記号（_）＋識別記号（教職員・学生・その他）＋重複しない文字列 3 文字（数字・英文字）

→したがって、ログイン ID（ノーマル）の桁数はバリアブルとなる。

・ログイン ID（ショート）

苗字ローマ字（先頭 6 文字以内）＋識別記号（教職員・学生・その他）＋重複しない文字列 3 文字（数字・英文字）

→したがってログイン ID は 10 文字以内となる。

学籍番号を持つ学生は、以下のとおりとする。

学部生：e+学籍番号数字 6 桁、　大学院生：k+学籍番号数字 6 桁

非正規学生：f+学籍番号 7 桁（非正規学生）

→したがって、ログイン ID（ショート）の桁数は 10 桁以内に限定される。

2.7 ユーザーアカウントの登録・管理に関する実装方針

2.7.1 ユーザーアカウントライフサイクルと権限設定について

ユーザーはそれぞれ身分を有することで、その身分に応じたアカウントライフサイクルならびに、権限設定がなされることが必要である。以下の記述内容の実装を行うこと。

(1) ユーザーに与えられる身分は、人事給与システム及び教務情報システムから登録された身分以外に本センターで定めを有しており、種別としては 20 種程度が現状の種別である。この種別のことを「身分識別」と呼称し、身分識別に応じてユーザーのライフサイクル定義や、初期の権限設定が実行できること。将来において、身分識別の種別が増加した場合にも、識別情報の追加を行うことで、対応可能であること。

例）　身分識別コード　身分識別　　人事給与システム・教務情報システムの身分

１	⇒	教員	⇒	教授、准教授、講師、助教、大学院担当教授等
２	⇒	事務職員	⇒	部長、課長、課長代理、係長、主任、一般事務職員等
７	⇒	技術補佐員	⇒	技術補佐員、医員など
９	⇒	学部生	⇒	学部生
１１	⇒	非正規学生	⇒	研究生、特別研究学生

(2) 権限は、ユーザーアカウントで利用できるシステム等のことである。現在、以下のものがある。

・Microsoft365　・パソコン室の PC　・無線 LAN　・VPN 接続

・計算機サーバ（UNIX 系サーバ）　・個人アカウントの Web 公開　・WebClass

・本センター管理外システムの認証　・学術認証フェデレーション

2.7.1.(1)項の「身分識別コード」をもとにユーザーアカウントの登録時に有効化する権限を定め（以下、初期権限という。）、ユーザーの登録時に「身分識別コード」に沿った権限を有効化すること。「身分識別コード」ごとの初期権限については、システム構築時に決定すること

とする。

(3) ユーザーアカウントに初期で有効化されなかった権限について、システム管理者が権限を指定し有効化できること。

(4) システム管理者がユーザーアカウントに付与された権限を指定し、無効化できること。

(5) 権限の無効化において「パソコン室の PC」、「計算機サーバ」などの利用者のデジタル資産を有する場合、無効化処理を行うことで利用者のデジタル資産を削除することなく権限の使用を制限できること。

(6) ユーザー識別情報において、以下のようなアカウントライフサイクルの定義が行えること。無効化実施の可否、無効化実施までの期間、無効化が実行されてから完全無効化（履歴 OU への移動）実施までの期間。

・無効化・・ユーザーアカウントを利用できない状態にすること

・無効化実施までの期間・・設定された利用期限ですぐに停止するのではなく、一定の猶予期間を設けたのちユーザーアカウントを無効化するまでの期間である。

・完全無効化・・無効化したユーザーアカウントを一定の猶予期間を設けたのち機能を削除（利用者のデジタル資産の削除を含む。）し、ユーザーアカウント情報を履歴 OU に移動することである。

無効化の実施前にユーザー及びシステム管理者にメールにて事前に通知できること。完全無効化の実施前にもシステム管理者にメールにて事前通知できること。

(7) その他構成員は、毎年度において次年度に向けた年次更新処理を行うので年次更新の状況もユーザー属性に保管することで、適切に有効・無効の管理が実施できるように設計を行うこと。

2.7.2 発生源によるユーザーアカウントの登録・管理に関する実装方針

(1) 発生源である人事給与システム及び教務情報システムから FTP 接続し提供される CSV ファイルを受け取れること。システム管理者が登録する CSV ファイルについては、統合 ID 管理システムの所定のフォルダに格納する。

(2) 発生源から提供される発生源データ（以下、「発生源データ」という。）を用いて、発生源 ID をもとにユーザーアカウントの登録・更新・無効化が行えること。登録に際して、発生源 ID の発生に伴いもたらされたデータセットの中に、英字姓、英字名が存在しない場合、半角カナ文字の姓名情報から、ヘボンタイプでローマ字変換を行い、英字姓、英字名を設定できること。

(3) ユーザーアカウントの登録に際し、2.6 項のユーザーID に関する実装方針に沿った管理 ID の附番、ログイン ID の附番を行うこと。

(4) 人事給与システム及び教務情報システムからの発生源データにおいて、半角カナ文字またはローマ字が誤って提供されることがある。誤って登録されたユーザーアカウントについて、システム管理者が登録されたユーザーアカウントを削除し、半角カナ文字またはローマ字を修正し、再登録できるようにするかユーザーID の変更にて対応できるよう配慮したシステムにすること。

(5) 人事給与システムにおいては、学生のアルバイトや雇用期間が短い短期雇用職員、教務情報シ

ステムにおいては、学部生が大学院の講義を聴講するために付与される身分について、ユーザーアカウント自体が不要だったりすでにユーザーアカウントを持っていたりするため新しいアカウントの発行が不要な構成員が存在する。人事給与システム及び教務情報システムからの発生源データとの連携において、特定の職種・身分の構成員のユーザーの登録を行わないよう設定できること。ただし、本ケースにおいてもユーザーアカウントの作成が必要とすることがあり、その対応として、当該ユーザーをその他構成員として登録することで対応する。この場合の必要要件については、2.7.2.(13)項を参照すること。

(6) 人事給与システムから提供される発生源データは、教職員の全件データとなり項目は次の通りとする。教職員のデータは、常勤教職員と非常勤教職員の 2 つのデータが提供される。

職員番号、氏名、半角カナ、所属、所属コード、職種、職種コード、官名、官名コード、生年月日、採用日、退職日、任免区分、任免区分コード、係名称、係コード、データ更新日

(7) 教務情報システムから提供される発生源データは、学生の年度内の全件データで項目は次の通りとする。

学籍番号、氏名、半角カナ、ローマ字、所属コード、学生等区分（身分コード)、現況区分（在籍状態)、生年月日、入学日付、卒業予定日、有無効フラグ、更新日（YYYY/MM/DD）

(8) システム管理者から提供される発生源データは、本学担当者と調整し決めることとする。システム管理者が登録するユーザーは、その他構成員が主となるが、人事給与システム及び教務情報システムを発生源とする教職員及び学生の一部をシステム管理者が先行して登録を行うことがある。また、システム管理者が提供する発生源データには、必ず利用期限（年度内）を設定することとする。本ケースにおける先行して登録を行うユーザーは、一旦、その他構成員として登録を行い、その後、正式情報の到来をシステム管理者が認識したタイミングで、発生源 ID の変更を行うものとする。正式情報の到来の判断については、2.7.2.(11)項及び 2.7.2.(12)項記載の機能によって、発見が行えるものとする。

(9) システム管理者が登録した教職員及び学生のユーザーアカウントで発生源である人事給与システム及び教務情報システムからの発生源データに同じ発生源 ID が発生した場合、その発生源データをもとに更新・無効化が行えること。

(10) 発生源データをもとに登録・変更・停止のあったユーザーの情報について、システム管理者にメールで通知を行うかログで確認することができる機能を有すること。

(11) ユーザーアカウントの登録時、発生源データのいくつかの項目を組み合わせ（例えば、「氏名＋生年月日」)、個人識別キーを作成し、登録できること。本学では、教職員では非常勤講師等、学生では科目等履修生等で複数部局にわたり同一人物が登録されることがあり、同一人物への複数ユーザーへのユーザーアカウント発行を防ぐために利用する。

(12) ユーザーアカウントの登録時、発生源 ID が違うが 2.7.2.(11)項の個人識別キーが同じ登録者がいた場合、ユーザーアカウントの登録をエラーとして処理し、登録を行わないこと。システム管理者が、同一人物ではないと確認した場合、システム管理者によりユーザーアカウントの登録が行えること。本ケースにおいて、個人識別キーが一致するユーザーを別のユーザーアカウントとして、登録を行う場合、一旦、その他構成員として登録を行い、その後、システム

管理者が、発生源 ID の変更を行うものとする。本ケースにおいてのその他構成員登録の必要要件については、2.7.2.(13)項を参照すること。

(13) その他構成員として取り扱うユーザーアカウントは、2.2.1.(9)項のその他構成員以外に、2.7.2.(5)項のユーザーアカウント、2.7.2.(8)項のユーザーアカウント、2.7.2.(12)項のユーザーアカウントが存在する。特に 2.7.2.(5)項のユーザーアカウント及び 2.7.2.(12)項のユーザーアカウントは、本来登録対象でないユーザーアカウントであるが、特例対応措置として登録を行う。このため、その他構成員を扱う CSV ファイルでの処理およびシステム管理者による WebGUI での処理において、以下の 2 種のフラグ情報を設けてこの特例措置への対応を可能とし、これらのフラグが ON となっている場合において、判定を回避して特例登録が行えること。

1) 登録除外となる身分識別コードの判定を回避するフラグ

2) 同一個人識別キーを有するアカウントの存在判定を回避するフラグ

(14) システム管理者が変更前後の発生源 ID を提示することで該当ユーザーアカウントの発生源 ID の変更が行えること。

(15) 離籍情報について、発生源の種別により以下のように処理が可能であること。

1) 人事給与システムが発生源の場合、人事給与システム側から提供される発生源データと本システムのリポジトリから出力される現アカウント CSV の比較により抽出される削除対象レコードを以って離籍処理を行う。

2) 教務情報システムが発生源の場合、教務情報システム側から提供される発生源データの有効無効フラグを用い、このフラグが無効状態となった場合を以って、離籍処理を行う。

3) その他構成員については、有効期限経過後、もしくはシステム管理者が、その構成員削除用の CSV ファイルを作成し、そのレコードを以って離籍処理を行う。

(16) 2.7.2.(15)項の離籍情報が発生するので、これらに含まれる発生源 ID をもとにユーザーアカウントの無効化を行うこと。無効化処理については、2.7.1.(6)項の「ユーザーアカウントのライフサイクル」をもとに処理を行うこと。

(17) システム管理者が発生源 ID を指定し、ユーザーアカウントの利用停止処理が行えること。この利用停止処理は、緊急の無効化処理（利用停止）となり 2.7.1.(6)項の「ユーザーアカウントのライフサイクル」を無視して利用停止できること。

(18) 2.7.2.(17)項で利用停止されたユーザーアカウントについて、システム管理者が発生源 ID を指定し、利用停止を解除できること。

(19) 発生源データをもとに離籍した教職員及び学生が、再度、採用または入学し、ユーザーアカウントが無効化状態であれば、ユーザーアカウントの無効化を解除し利用できる状態にすること。パスワードは停止前のパスワードが利用できるようにすること。ユーザーアカウントが完全無効化されていた場合、新しく登録できること。

(20) 発生源 ID とは別項目として、発生源 ID を可逆暗号化方式である Blowfish 方式で暗号化した値をユーザーアカウントに情報として有すること。

(21) システム管理者から変更前後のログイン ID が示された場合、該当ユーザーアカウントのログイン ID の変更が行えること。

(22) 2.7.1.(6)項の「ユーザーアカウントのライフサイクル」をもとにユーザーアカウントの完全無効化が行えること。

(23) システム管理者が登録したその他構成員のユーザーアカウントの年次更新処理として、発生源 ID をキーとして、利用期限の更新が行えること。

3 SSO 認証基盤システム

3.1 SSO 認証基盤システムの全体像

本学として利用するサービスや ICT システム（以下、「SP」という。）に対して、シングルサインオン環境を提供する機能製品を納品すること。認証方式については、以下の方式に対応していること。SAML、WS-Federation、OpenID Connect、OAuth、またこれらの方式に対応できていない SP を対象として、リバースプロキシーサーバを併用することで、代理認証方式や、リバースプロキシ認証方式にも対応できること。ユーザーブラウザの Add-On を用いる方法で、SAML に対応していないシステムも SSO 利用が可能となること。今回の計画の範囲においては、学認あるいは、SAML によるフェデレーション認証による SP を対象とするが、SAML 以外の上記の認証構造にも対応可能であること。

3.1.1 SSO 対象システム

以下のシステムを本計画における SSO 対象システムとする。

- 本学の学術認証システム環境における各 SP
- ローカル Shibboleth サーバ（本学図書館が利用）
- Microsoft365 の各システムやサービス
- 導入予定であるデジタル職員証システム
- クラウドの動画配信システム

なお SSO 対象システムは今後も増加することに配慮すること。

3.1.2 SSO 対象人数と同時接続数

SSO 対象人数としては、学内教職員・学生・その他構成員の 20,000 名以上とし、同時アクセスユーザー数として同一秒間 50 接続を見込む。また、SSO 利用者のアクセス経路として、本学ネットワーク内からのアクセスに加えて、インターネット経由でのアクセスも可能とし、アクセス経路に応じた適切な通信暗号化が行われること。

3.1.3 SSO ポータルサーバ

SSO 利用者と、SSO システム管理者を区別することが可能な WebGUI 機能として提供し、SSO 利用者に対して、統合 ID 管理システムから連携（プロビジョニング）されるユーザー情報に含まれるユーザー種別を判断して、そのユーザーが利用可能な SP のアイコンが表示できること。これらのアイコンを用いてシステムランチャーとして機能すること。SSO システム管理者の場合は、本 SSO システムの各種設定を行う Web アプリケーションとして機能すること。

3.1.4 SSO IdP サーバ（Shibboleth IdP 兼用）

認証をつかさどるための IdP サーバとして構成されていること。本 IdP サーバは Shibboleth 認証サーバとしても動作を行うことが可能であること。Shibboleth 認証機能を兼ねる場合には、

学認環境で提供されている、uApprove 機能（送信属性許可機能）と同等機能を有すること。

3.1.5 SSO リバースプロキシーサーバ

SAML などのフェデレーション認証機構に対応していない SP のため、リバースプロキシーサーバの利用が可能な製品であること。

3.1.6 SSO リポジトリサーバ

LDAP サーバ（SSO システムリポジトリ）と同じサーバであり、本 SSO システムのユーザーリポジトリとしての機能と、SSO システム側で定義される利用者の制御情報を格納するための制御用リポジトリとして動作すること。

3.1.7 SSO ログサーバ

本 SSO システムへのユーザーアクセスログとユーザーがどの SP を利用したのかを確認できるログ情報を保管するサーバとして機能すること。ログ情報の検索については、SSO システム管理者が、3.1.3 項の SSO ポータルサーバを用いて実施可能であること。閲覧可能なログには「ログイン ID」「認証方式」「アクセス先」「アクセス時間」が出力され、かつそれらの条件でフィルター検索可能であること。

3.1.8 多要素認証機能

多要素認証機能を有すること。多要素認証のトークンとしては、すくなくとも以下の２種には対応すること。Google や Microsoft 社の Authenticator アプリの利用や、メールによる送信。多要素認証トークンの設定については、利用者が SSO ポータルから実施できること。

3.1.9 ユーザーアクセス制御機能

SSO システムの管理者が利用者の種別に応じてアクセスを許可する SP を定義する機能を提供すること。また、SSO システム配下の SP の利用権限を個別に利用者に割り当てる機能を提供すること。利用者のアクセス元 IP アドレスや、利用対象の SP によって、多要素認証に必要性を定義できる機能を提供すること。上記の設定を、WebGUI 機能で実施可能なこと。

III性能、機能以外に関する要件

1 サーバ

1.1 Ⅱ.２項の統合 ID 管理システム及びⅡ.３項の SSO 認証基盤システムを動作させるサーバは、専用ハードウェアが必要な場合、機器、ライセンスを本調達に含むこと。専用ハードウェアが必要ない場合、本センターが管理する仮想基盤の仮想サーバを使用し構築すること。

2 大学保有の既存システムとの連携および設定変更

2.1 調達システムを導入するにあたり、本学が有するキャンパス情報システムと連携が必要になる。連携するシステムについて、本学担当者と調整し、業務に影響がでないよう本学システムの設定の追加・変更・調整等を行うこと。また、追加・変更・調整等に係る費用について、この調達に含むこと。ただし、発生源である人事給与システムおよび教務情報システムからの提供される発生源データの生成および提供に係るシステムの設定の追加・変更・調整等は除く。

2.2 Ⅲ.1.1 項で導入するサーバについて、本学が有するネットワーク機器、セキュリティ機器の設定および変更が必要な場合、技術支援を行うこと。技術支援に係る費用について、この調達に含むこと。

2.3 今回調達する統合 ID 管理システムにおいて、ユーザーのメールアドレスを Microsoft365 に統一するため、キャンパス情報システムで導入したオンプレのメールシステムとの連携（プロビジョニング）は行わないが、統合 ID 管理システム稼働前に登録されたユーザーアカウント（以下、「既存ユーザーアカウント」という。）は、キャンパス情報システムで導入したオンプレのメールシステムのメールアカウントを Microsoft365 に統一するまで引き続き利用する必要がある。そのため、既存のユーザーアカウントにオンプレのメールアカウントを利用できるための情報を保持し、統合 ID 管理システム稼働後もオンプレのメールアカウントを利用できるようにすること。

3 現行システムからの移行について

3.1 現行システムからのユーザーアカウントの移行は、本調達に含む。移行作業は、本学業務に支障をきたすことなく円滑に行うこと。

3.2 調達システムが稼働する前のユーザーアカウントで利用できる権限（メールアドレス等）は、変更することなく利用できるようにすること。

4 構築体制

4.1 業務内容を円滑に推進し、確実な稼働につながる体制を整備すること。

4.2 トラブルが発生した場合に対応できるバックアップ体制を確保すること。

4.3 導入を円滑に進めるため、進捗状況管理を適切に行うこと。

4.4 導入のスケジュールを開始時に提出し、本学の承認を得ること。

4.5 導入で想定されるリスクを管理し、スケジュールおよび費用に影響を与えないよう対応すること。

4.6 導入が完了するまで定期的または必要に応じて、進捗状況の報告等を行うための打ち合わせを実施すること。打ち合わせを行った際、議事録を作成し、本学担当者の承認を得ること。

4.7 進捗状況に遅延が発生しそうな場合、速やかに増員等の特別な対応を行い本学に報告すること。増員等の特別対応に係る費用は、調達費用で行い、追加費用が発生しないようにすること。

4.8 課題等の懸念事項を明確化にし、本学と共有すること。また、実現可能な解決策を主体的に提案し迅速に対応すること。

4.9 導入そのものに影響を及ぼすトラブルが発生した際は、必要に応じて本学が開催する緊急会議に、来学またはリモートにて参加すること。

4.10 受注者（構築に携わる構成員すべてを含む。）は、本調達にあたり後述のⅢ.7 項の「受注者の守秘義務」を順守すること。

4.11 障害が発生した場合、速やかにシステム復旧、原因調査、再発防止策及び調査報告を行うこと。障害の原因箇所がシステムである場合、受注者が責任を持って回復措置をとること。障害復旧作業完了後、完了報告書を本学担当者に提出し、内容確認を得ること。

5 運用管理・支援体制

5.1 システムの円滑な運用を計るため、研修資料一式を作成し、本学担当者に対する必要な教育、指導を行うこと。研修テキストは、受注者で人数分用意すること。

5.2 応札者が提案したシステムに関する具体的なセキュリティに配慮したサービス、アーキテクチャ、ソフトウェア等の導入及び管理策等を提案すること。

5.3 応札者が提案したシステムに関して質問や問い合わせがある場合は、テレビ会議システム、電話・電子メールによる問い合わせ窓口を有し、迅速かつ適切に対応すること。

5.4 本センターが行う開発、性能・機能向上に伴う作業、プログラムの移植、及び機器の接続に関して、必要な技術情報を提供し、作業の支援を行うこと。

5.5 システム運用に必要な情報・障害対策について、必要な情報・資料を随時提供すること。また、本学の要求に応じて必要な技術情報を速やかに提供すること。

6 ドキュメント類の提供

6.1 調達するシステムに関して製造元が発行するハードウェアマニュアル及びソフトウェアマニュアルを種類ごとに日本語版または英語版のいずれか一方を提供すること。ただし、オンラインマニュアルしか存在しない場合、オンラインマニュアルで良い。

6.2 調達するシステムの運用・保守マニュアル、システム構成図、操作マニュアルを日本語で提供すること。

7 受注業者の守秘義務

受注業者は、案件および案件に関連する役務過程において知り得た案件に関する一切の情報(以下「案件に関する情報」という。）について、次の義務を順守すること。

7.1 故意または過失にかかわらず、案件に直接従事する担当者であることを本学が書面にて認めた者以外の者(以下「他者」という。）に案件に関する情報を漏らさないこと。

7.2 案件の履行に関連して知り得た本学の秘密情報の加工、改ざん、複写または複製等をしてはならない。ただし、安全管理上必要なバックアップを目的とするものはこの限りではない。

7.3 契約中は、案件に関する情報の取扱いに十分留意し、他者に情報を開示しないこと。

7.4 契約終了後は、案件に関する情報を返却または確実に破棄するとともに、本学の書面による許可なく案件に関する情報を他者に開示しないこと。

7.5 案件に関する情報を知り得た者が、異動、転職、退職等の事由によって案件と無関係になった場合でも、本学の書面による許可なく案件に関する情報を他者に開示させないこと。

7.6 万が一受注業者先において秘密情報の漏えい等の事故が発生した場合には、直ちに本学へ報告し、また、受注業者先が責任をもって対応すること。

7.7 その他、本学の指示に基づいて守秘義務を全うすること。

以上