仕 様 書

1　件名

クラウド型ファイル管理システム導入　一式

2　導入目的

独立行政法人国立高等専門学校機構（以下、「当機構」という）では、ファイルサーバーの利用終了に伴い、クラウド型ファイル管理システム（以下、「新システム」という）を導入する。クラウド型ファイル管理システムを利用し、各種業務において必要とされる情報セキュリティ対策を確保しながらデータをクラウド上へ保管し、各学校や外部へデータを安全に共有できることを目的とする。

3　業務期間

（1） 導入支援期間

契約締結日からから令和 9 年 3 月 31 日まで

（2） クラウドサービスのライセンス提供期間

① 令和 9 年 2 月 1 日から令和 14 年 3 月 31 日まで

② 令和 9 年 2 月 1 日にシステム本稼働するために必要な導入期間

（3） 保守サポート期間

① 令和 9 年 2 月 1 日から令和 14 年 3 月 31 日まで

② 令和 9 年 2 月 1 日にシステム本稼働するために必要な導入期間

4　契約概要

以下のシステムのライセンスの提供、導入支援、及び保守サポートを提供すること。

- システム名：クラウド型ファイル管理システム
- 利用人数　：210 名（外部利用者の数は含まない）
- 別紙に示す要件を満たすこと

5　本業務の受注者の要件

- 行政機関（中央省庁、都道府県、市町村）における 200 人以上の全職員での導入並びに保守の実績を有していること。
- ISO/IEC27001 による認証を取得していること。

6　本調達の内容

本業務の内容は、下記のとおりである。下記のうち、提案するサービスを導入する上で必要な工程については当機構と協議の上決定し、導入支援を行うこと。

（1） ライセンスの提供

（ア）ライセンスは令和 9 年 2 月 1 日から令和 14 年 3 月 31 日まで利用可能とすること。

（イ）教職員 210 人が利用するにあたり必要なライセンスを用意すること。また、利用人数分のライセンスの他に、システム運用に必要なシステムアカウントが必要な場合は、ライセンス数に含めること。

（2） 導入支援

（ア） 管理者向けの管理コンソールの説明と設定支援

対面もしくはオンラインにて以下の内容について実施すること。また、設定作業についてリモートでの対応も可とする。その場合の当機構にてアクセス権の設定を行う。

① テナント設計

主要機能、及びフォルダ構成、設定方法について説明し、最適な基本設定、フォルダ構成の設計を支援し、設定作業を行うこと。

また、ユーザーログインに際しては Entra ID の資格情報を利用したシングルサインオンによる運用を想定するため、新システム側の設定について適切な説明および支援を行うこと。なお、Entra ID 側の設定については当機構で実施する。

② セキュリティ・ガバナンス設定

初期設定において、必要なセキュリティやガバナンスに関連する設定事項については、機能説明を実施した上で当機構の要件をヒアリングし、設定値を提案、設定作業を行うこと。

③ 運用設計

運用事例等の情報を提供し、当機構にヒアリングをしたうえで、当機構が新システム導入後の運用を行えるよう運用手順書を作成すること。ただし、運用設計の範囲は今回導入する新システムの範囲内とする。

（イ） データ移行設計及びデータ移行

現行ファイルサーバーの状況を調査した上で、データを新システムへ移行するための移行方法の提案及びデータ移行を行う。データ移行時の要件は下記の通り。

① 現行ファイルサーバー（容量：13TB、ファイル数：960 万、フォルダ数：160 万、主なファイル形式：docx/pdf/xlsx/pptx/mp4 など）について調査し、現行ファイルサーバーから新システムへ移行した際に権限の削減が起こる場合には、削減している箇所を一覧にまとめて報告すること。

② 実際に移行を行う環境下で現行ファイルサーバーのデータを新システムへ移行する「トライアル移行」を実施し、その実績に基づいた移行計画を

策定すること。

③ トライアル移行時は複数のフォルダ(合計 1TB 程度)を移行し、エラーが起きた場合にはエラーの一覧をまとめて報告すること。

④ データ移行に際しては、専用ツールを提案することも可とする。その場合は専用ツールも本調達に含めること。

（ウ） 教職員向けのサービス利用説明会の開催

対面もしくはオンラインにて以下の内容について説明会を 1 回開催し、説明会の録画データを当機構に提出すること。

① 利用開始手順（初期アカウントの設定、ログイン方法など）

② 基本操作方法（フォルダ作成/アップロード/バージョン管理/検索等）

③ その他（業務での利活用方法のアドバイス、利用上の注意点）

7 保守・運用サポート

提供するサービスの保守・運用に関して、以下の内容を実施すること。

（1） 管理者及びエンドユーザーより以下のような問い合わせに対し、平日 9：00～17:00 の間で Web フォームまたはメールによる保守サポートをすること。

(ア)機能仕様や操作手順に関する問い合わせ

(イ)サービスの機能を利用する上で発生した事象に関する問い合わせ

（2） 問い合わせ受付後、2 営業日以内を目安に初回回答をすること。

8 納品物

下記資料を、指定された提出時期にそれぞれ納品すること。

項番	資料名	提出時期	概要
1	要件定義書	令和 8 年 12 月	新システム導入における目的、対象範囲、権限管理、保存・などの要件を定義
2	基本設計書	令和 8 年 12 月	利用対象ユーザー・デバイス、サイト設定、フォルダ設計方針などを記載
3	方式設計書	令和 8 年 12 月	データ移行ツールによる移行手順、切替スケジュール、リスク・エラー対応を整理・定義
4	詳細設計書	令和 8 年 12 月	Enterprise 設定・オプション機能の設定値（Enterprise 設定シート）、およびフォルダ設計におけるフォルダ階層・権限・所有者の定義（フォルダ構成テンプレート）を記載

5	テスト仕様書	令和 8 年 12 月	各種機能や機能設定などに関する動作確認シナリオを記載
6	運用手順書	令和 9 年 3 月	運用に関わるユーザー・グループ管理、フォルダ管理、および各種棚卸しの作業手順を記載
7	管理者向けマニュアル	令和 9 年 3 月	標準で作成しているものの納入も可とする。
8	ユーザー向けマニュアル	令和 9 年 3 月	標準で作成しているものの納入も可とする。
9	ユーザー説明会資料	令和 9 年 3 月	ユーザー説明会用の資料を提供すること。
10	データ移行トライアル結果報告書	令和 9 年 2 月	データ移行トライアルの結果を記載
11	データ移行手順書	令和 9 年 2 月	データ移行の手順を記載
12	データ移行報告書	令和 9 年 4 月	データ移行作業の実施内容を網羅的に記載

9　支払方法

（1） 導入支援

当機構による検収後、受託者の請求に基づき支払うこととする。

（2） クラウドサービスのライセンス提供

当機構による年度ごとの検収後、受託者の請求に基づき支払うこととする。

（3） 保守サポート

当機構による年度ごとの検収後、受託者の請求に基づき支払うこととする。

10　サプライチェーン・リスクマネジメント

受注者は、サプライチェーン・リスクの要因となる脆弱性を発生させない又は増大させないための管理体制を構築し、応札時に当機構に提示すること。また、報告する体制には以下の情報を含めること。

・管理体制図
・受注者の資本関係、役員等の情報
・事業の実施場所
・事業従事者の所属、専門性（情報セキュリティに係る資格・研修実績等）
・事業従事者の実績及び国籍に関する情報

また、上記体制が変更になった場合は速やかに当機構へ報告を行うこと。

11　機密保持

（1）　受注により知り得た全ての情報について守秘義務を負うものとし、これを第三者に漏らし、又は他の目的に使用しないこと。

（2）　受注により知り得た情報については、契約期間はもとより、契約終了後においても第三者に漏らさないこと。

（3）　正当な理由があってやむを得ず第三者に開示する場合、書面によって事前に当機構の承諾を得ること。また、情報の厳重な管理を実施すること。

（4）　当機構が提供した資料は、原則として全て複製禁止とすること。但し、業務上やむを得ず複製する場合であって、事前に書面にて当機構の許可を得た場合はこの限りではない。なお、この場合にあっても使用終了後はその複製を当機構に返納又は焼却・消去する等適切な措置をとり、機密を保持すること。

12　再委託の禁止

受注者は本業務を自ら履行するものとし、本業務の全部を第三者に委託、又は請け負わせてはならない。ただし、本業務の一部を第三者に委託する場合であり、かつ、当機構に書面によって外部委託の詳細を提出し許可された場合は、この限りではない。なお第三者委託を許可された場合であっても、受注者は契約による責任を免れることはできない。

13　その他

・当初に業務を開始するにあたって十分協議および調整を行うこと。また、この仕様書に定めのない事項は、当機構と受注者の双方との協議により決定するものとする。

・システムに当機構の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、当機構と請負者が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

・受注者は、情報セキュリティインシデントが起こった際の対応手順を、応札時に当機構に提示すること。

・情報セキュリティ侵害発生時には、当機構の情報セキュリティ監査を受け入れること。

・受注者は、本業務における情報セキュリティ対策(作業端末のソフトウェアの更新等)が適切に履行されていることを、毎月末に書面にて当機構に提出すること。また、情報セキュリティ対策が不十分だったことが判明した場合、受注者の責において、適切な対策を講ずること。

・受注者は、業務完了後、本件に係る情報を返却または抹消し、そのことを当機構に書面で報告すること。

以上

別紙　新システムに関する要件書

1　基本要件

（1） インターネット上で利用できるクラウドサービスを提案すること。

（2） 保存容量を制限なく利用できること。容量従量課金及び設定変更等に伴う容量追加は認めない。

（3） クラウドストレージ上のフォルダに対して他の教職員を招待し、アクセス権を限定したファイルおよびフォルダの共有が可能な機能を有すること。

（4） フォルダやファイルのアクセス権は、グループまたはユーザーごとに設定可能な機能を有すること。 なお、組織内・外のユーザー単位で不要な操作を行わせないために細かなアクセス権限が選択可能であること。イメージとしては以下の 7 つに分けた権限の付与を想定している。

①フォルダの所有者と同程度の権限

②アップロード、ダウンロード、プレビュー、共有リンク(当該ファイルを共有するためのリンク）の取得、ファイル編集、削除

③アップロード、ダウンロード、プレビュー、共有リンクの取得、ファイル編集

④アップロード、プレビュー

⑤ダウンロード、プレビュー、共有リンクの取得

⑥プレビュー

⑦ アップロード

（5） 管理者にて、ユーザーの登録・削除、特定のフォルダへのアクセス権限の設定を行えること。

（6） 専用ツールを提案することも可とする。その場合は必要なライセンス数等も本調達に含めること。

2　機能要件

（1） 利用者の OS は Windows・MacOS・iOS の、常にそれぞれ直近 2 つのメジャーバージョンをサポートしていること。

（2） 各ブラウザ（Microsoft Edge、Firefox、Google Chrome、Safari)の最新のバージョンに対応すること。

（3） 利用者が場所（機構内外）を問わずアクセス可能で、PC、タブレット端末などデバイス問わずブラウザベースでの利用ができ、接続時、機器に最適なレイアウトで表示されること。

（4） 最大で 150GB の単一ファイルの保存ができること。

（5） 編集可能な形式ファイル（Word、Excel 等）であれば Web ブラウザ上のエディタで開くとともに、編集ができること。(当機構所有の Online 編集可能な Office フ

ァイルで連携した利用を想定。）

（６） Web ブラウザ上で、ファイル（docx、xlsx、pdf、pptx 等）のダウンロードを必要としないファイルプレビューができること。

（７） 任意のフォルダに対して指定の日付にフォルダや共有リンクを削除する自動処理の設定が可能なこと。

（８） 作成/編集を行ったユーザー情報が記録されること。

（９） バージョン管理機能を有しており、過去に遡ってすべてのバージョンのファイルを復元できること。

（１０）フォルダ招待及び共有フォルダへのリンク（URL）指定により、有効期限を設定したうえで、ファイル共有が可能であること。

（１１）指定したフォルダ上にあるファイルもしくは特定のメタデータを有するファイルについて、指定した期間はフォルダ内に保持し、経過した後自動的に削除する機能を有すること。

（１２）クラウドサービス機能に標準で電子署名を付与する機能が実装されていること。なお、検証等を行う際を考慮し、利用できるユーザーを限定できる等の設定が可能であること。

（１３）クラウドサービス機能に標準で AI（単一ファイルの要約や情報の抽出、クラウドサービスで利用できるメモアプリ等で利用可能な生成 AI 機能を想定）機能が実装されていること。なお、検証等を行う際を考慮し、利用できるユーザーを限定できる等の設定が可能であること。

（１４）削除されたファイル・フォルダについて、一定期間はごみ箱に残り、ごみ箱に残っている場合には復元が可能なこと。

3　セキュリティ要件

（1）当該クラウドサービスで取り扱うデータを保管するデータセンター（バックアップセンターを含む。）は日本国内にあること。

（2）サービス側でバックアップ、もしくはレプリケーションがされており、データセンターの被災等でデータが消失した場合でも復旧し、ファイルにアクセスすることができること。

（3）管轄裁判所を日本国内の裁判所とすること。

（4）当該クラウドサービスの提供者が、下記いずれかの認証を取得していること。

ア　ISO/IEC27017 による認証

イ　ISO/IEC27018 による認証

（5）「政府情報システムのためのセキュリティ評価制度」に定める「ISMAP クラウドサービスリスト」に登録されたクラウドサービスであること。

（6）IP アドレス制限機能を有すること。

（７）二要素認証の機能を有していること。
（８）クライアント証明書を所有した特定端末でしか利用できないなどのアクセス制御機能があり、管理者が利用端末を制限できる機能を有すること。
（９）不正アクセス検知のため、特定の地域からのアクセスや、複数の国から同時アクセスがあった場合に検知ができること。
（１０）ウイルス感染を防ぐため、ファイルアップロード時にウイルススキャンが実行され、悪意のあるファイルが検出された場合、管理者へ通知できること。
（１１）マルウェア等を検知した際に、自動的にダウンロードを制限する機能を有すること。
（１２）ユーザーの誤操作等による情報漏えいを防止するために、クラウドストレージ上にアップロードされたファイルに対して､特定の分類ラベルを付与することでファイル単位でのアクセス制御を可能にすること。
（１３）サービス提供期間は､24 時間 365 日とするとともに､99.9%以上の可用性を提供すること。（システムメンテナンスは除く）
（１４）管理画面上からアクセスログ（ファイルの閲覧、編集、ダウンロード等のユーザーの操作履歴）が取得できること。なお、アクセスログは、管理画面上から過去１年分以上の取得が可能であること。
（１５）AI 機能においては、LLM が学習しない仕組みを前提とし、AI 機能による情報漏洩対策や、AI が参照する範囲についてユーザーのアクセス権等が十分に考慮されていること。

4　ID プロビジョニング機能要件

（１） ユーザー管理

（ア）IDM（Active Directory / Microsoft Entra ID）の情報に基づき、新システムへのユーザー登録・更新・削除をプロビジョニングできること。また、連携対象／非対象のユーザーの制御ができること。

（イ）ユーザー削除時の動作を、即時削除・段階削除の各パターンから選択可能であること。

（ウ）ユーザー作成時に個人フォルダの自動作成およびアクセス権付与、ユーザーの削除時に指定場所へ個人フォルダの自動退避ができること。

（２） グループ管理

（ア）IDM（Active Directory / Microsoft Entra ID）のグループ情報に基づき、新システムのグループ作成・更新・削除をプロビジョニングできること。また、IDM 側のグループ名を変更した場合、新システム側のグループ名に変更が反映されること。（新規グループとして登録されないこと。）

（イ）IDM（Active Directory / Microsoft Entra ID）上の入れ子（ネスト）グループ構

造をシステム側に反映できること。

（ウ）グループ削除時の動作を、即時削除・段階削除から選択可能であること。

（3） 同期制御・運用管理

（ア）本番反映前にシミュレーション機能により対象データを事前確認できること。

（イ）実行結果をログファイル等で出力できること。

（4） 一括操作機能要件

（ア）フォルダ・グループの一括作成・変更・削除・移動ができること。

（イ）CSV ファイルをパラメータとした一括処理が可能であること。

（5） その他の要件

日本語によるマニュアル・サポートが提供されること。

以上