

滋賀県議会ファイル管理システムの提供および運用保守業務に関する仕様書

本仕様書は、滋賀県（以下「発注者」という。）が利用するファイル管理システム（以下「管理システム」という。）の提供および運用保守に係る業務に関して、管理システムの機能、性能および受注者が行う作業に係る基準を示すものである。

1. 調達の目的と前提条件

ペーパーレス化の推進をはじめ情報共有や議会審議の充実・深化のため、クラウドサービスによる管理システムの利用契約を行う。

議会関係資料（議案書、本会議・委員会・協議等の場での配布資料、滋賀県議会事務局（以下「事務局」という。）からの通知文書等）について、電磁的記録により作成した文書（以下「電子文書」という。）を管理システムに登録することにより共有を図り、タブレット端末を用いて閲覧できるようにすることで、本会議場、委員会室、会派控室等での審議、調査に資するとともに、委員会の県内・県外調査先等でも資料の活用が可能となるようにするものである。

なお、令和7年2月3日に滋賀県議会議員で構成する議会改革検討委員会から提出された検討結果報告書において、令和9年度以降の管理システムについては、公募型プロポーザル方式により選定することとされた。検討の過程では、同期機能を備えた管理システムにすべきとの意見があった一方、同期機能を必須要件とした場合には対象となるシステムが限定されることから、ペーパーレス化を実施する上での最低限の機能を要件とした上で、ファイル構成や同期機能その他の提案内容を含め、総合的に判断することとされた。

本調達は、こうした議会改革検討委員会における検討結果を踏まえ、令和9年度以降の議会運営において必要となる管理システムを調達するものである。

2. 調達内容および数量

調達内容および数量は、次の（１）から（４）までに掲げるとおりとする。

（１）管理システムの提供（一式）

管理システムは、150以上のライセンスに対応できること。

（２）初期設定作業（一式）

滋賀県議会において現在利用している管理システム（以下「現行システム」という。）から新たな管理システムへ円滑に移行し、運用を開始できるよう、必要な初期設定作業を実施すること。

（３）操作説明書等（任意様式）

次に掲げる操作説明書等を作成し、電子データにより発注者に提出すること。

ア 利用者操作説明書

記載に従って操作することにより、議員その他の管理システムを主に電子文書の

閲覧のために利用する者（以下「利用者」という。）が支障なく管理システムを利用できる内容であること。

イ 管理者操作説明書

利用者アカウントの登録、アクセス権限の設定その他の管理システムの運用を管理する者（以下「管理者」という。）の操作方法、利用者アカウントおよびその権限の管理に必要な作業手順その他必要な事項を記載すること。

ウ 編集者操作説明書

管理者から付与された権限の範囲内で、電子文書の登録、更新、削除その他の電子文書の管理に関する操作を行う者（以下「編集者」という。）の操作方法、電子文書の掲載手順その他必要な事項を記載すること。

エ ライセンス管理台帳

（４）現行システム掲載資料のデータ移行

現行システムに掲載されている資料について、必要なデータ移行を行うこと。

対象データは、ファイル数 52,600 個、データ容量 49,000MB 程度を想定する。なお、当該数量は令和 9 年 4 月 1 日時点の想定値であり、契約締結時または移行作業時点における実際の数量と異なる場合がある。

3. 契約期間等

（１）契約期間 契約締結日から令和 13 年 4 月 30 日

ア 初期設定作業等に向けた調整 契約締結日から令和 9 年 3 月 31 日

※初期設定作業等に向けた調整は発注者側で実施するが、必要に応じて受注者に助言等を求めることがある。また、受注者において必要と認める準備作業については、当該期間中の実施を妨げない。

イ 初期設定作業 令和 9 年 4 月 1 日から令和 9 年 4 月 30 日

※初期設定作業は受注者で実施すること。

ウ システム提供および運用保守支援 令和 9 年 5 月 1 日から令和 13 年 4 月 30 日

※運用保守支援は受注者で実施すること。

4. 契約方法

契約書のとおり

5. システム構成

インターネット回線を通じて提供されるクラウドサービスが「①クラウドサービス提供を行う組織が、ISO/IEC 27001 認証を取得していること、または ISMAP クラウドサービスリストに登録されていること。」「②準拠法、裁判管轄を日本国内に指定できること。」および「③クラウドサービス提供者が本県の情報を取り扱うに関して、その取り扱いを原則外

部委託しない。外部委託する場合は、事前に通知または公開されていること。」を満たすとともに、次のセキュリティ要件を満たすこと。

(1) 不正なアクセスを防止するためのアクセス制御

- ア ID 管理 (ID の作成から廃棄まで) とアクセス制御を実装すること。
- イ 本県職員のみが利用するセグメントにおいては本県が別途指定する IP アドレスおよび受注者の作業環境の IP アドレスにアクセス制限を行うこと。
- ウ 管理者特権を保有するクラウドサービス利用者に対し、ID およびパスワードによる認証に加え、端末認証その他これに類する認証方式を利用できること。
- エ クラウドサービス上に保存する情報やクラウドサービスの機能に対してアクセス制御を行うこと。
- オ クラウドサービス利用者によるクラウドサービスに多大な影響を与える操作の特定と誤操作の抑制ができること。
- カ インターネット等の外部の通信回線からクラウドサービス上に構築したシステムにログインする場合、適切なセキュリティ対策を行うこと。

(2) 取り扱う情報の機密性保護のための暗号化

- ア クラウドサービス内および通信経路全般において暗号化を行うこと。
- イ 取り扱う情報の機密性に応じた保護のための適切な暗号アルゴリズムを用いた暗号化処理を行うこと。

(3) 設計・設定および開発時におけるセキュリティ対策

- ア クラウドサービス上に他ベンダが提供するソフトウェア等を導入する場合、そのソフトウェアのクラウドサービス上におけるライセンス規定を確認し、管理を行うこと。
- イ 利用するクラウドサービス上の本システムのデータ容量の使用状況およびサービス稼働状況 (S L A の達成水準等) について、定期的に本県に報告すること。また、将来の利用拡大 (データ量や利用者数の増加等) に備え、必要なキャパシティ (プランの拡張性等) が十分に確保されていることを確認、担保すること。
- ウ リソース不足によるサービス停止に備えて、利用するデータ容量や稼働性能 (移植容易性) を監視し、業務が継続できるよう考慮すること。
- エ 利用するクラウドサービス上で保護データ等を取り扱う場合は、サービス停止に至る障害に備えて、可用性を考慮した設計とすること。

6. ファイル管理システムの基本要件

発注者が管理システムを通じて、クラウドサービスにおける SaaS に登録した電子文書を利用できるよう、受注者は、次のとおり機能提供および運用を行うこと。

(1) 基本性能

- ア 日本国内での利用を可能とすること。

- イ 次の OS を搭載したパソコン、タブレット端末からの利用を可能とすること。
 - ・ iOS26 以上
 - ・ Windows11
 - ・ Android
- ウ 24 時間 365 日の利用を可能とすること。(システムメンテナンス等でやむを得ずシステムを一時停止する場合を除く。)
- エ タブレット端末およびパソコンからは、専用アプリケーションまたはウェブブラウザ(Google Chrome, Safari, Edge)等を介し、登録されている電子文書の閲覧・ダウンロードができること。
- オ 利用者として 150 人以上が登録でき、そのすべてが同時にサービスに接続して登録文書を閲覧できること。
- カ クラウドサービスにおける SaaS に保存できる電子文書の容量は、60GB 以上とすること。
- キ 必要に応じ利用者の追加、保存容量の追加に対応できること。この場合において、別途費用が発生する場合は、提案書に記載すること。
- ク PDF 形式の電子文書が登録できること。
- ケ 利用者ごとにユーザーID およびパスワードを設定できること。また、ユーザーID およびパスワードの設定変更ができること。
- コ 管理者が利用者ごとに操作・閲覧権限を設定できること。また、操作を行う所属の範囲を限定できること。
- サ 管理者による操作が容易で管理者の負担が最小限となるように配慮されたシステムであること。
- シ 管理システムのバージョンアップが行われる場合は、管理システムに登録・管理されている電子文書に影響を与えないような措置を講じた上で、随時、最新版を提供すること。なおバージョンアップに係る費用は本業務の契約金額に含むものとする。

(2) 利用者の管理

- ア 利用者をグループに分けて管理することができること。
- イ 各利用者を複数グループに登録ができること。
- ウ 利用者ごとやグループごとに、フォルダ単位およびファイル単位で電子文書の閲覧制限を容易に管理できること。

(3) セキュリティ対策

セキュリティについては、次の要件を満たすものとする。

- ア アクセスログを最低 12 か月間保管し、発注者の求めに応じて発注者に提示または提出すること。
- イ 端末による認証を行うこと。

- ウ 管理者権限での操作に関しては、IP アドレスによるアクセス制限を行えること。
- エ 不正アクセスがあった場合は、直ちに発注者に報告するとともに、被害の調査・対応、原因究明および再発防止対策を行うこと。
- オ 修正パッチ適用やバージョンアップ等を行う場合には、事前に検証環境において本システムの運用に影響が生じないことを十分に検証し、環境更新の事前評価を実施すること。
- カ サーバーと端末間の通信経路は、暗号化通信（SSL/TLS 方式）により端末からサーバーへリクエストする方式であり、通信に用いるプロトコルは https 通信であること。

7. 初期設定作業

受注者は発注者が現行システムから円滑に新たな管理システムへ移行し、運用を開始できるよう、必要な初期設定作業を行うものとする。

（1）初期設定作業の内容

初期設定作業には、次に掲げる作業を含むものとする。

- ア 管理システムの利用のために必要な設定
- イ 発注者が指定するフォルダ構成に基づくフォルダの作成
- ウ 利用者アカウントの登録および初期設定
- エ 管理者権限、編集者権限、閲覧権限その他必要な利用権限の設定
- オ 試験的な資料登録、配信および閲覧確認
- カ その他運用開始に必要な作業

（2）初期設定作業の実施時期

初期設定作業は、令和 9 年 4 月 1 日から令和 9 年 4 月 30 日までの間に実施するものとする。

ただし、令和 9 年 4 月 1 日以降の実施に向けて、受注者において必要と認める準備作業については、令和 8 年度中の実施を妨げない。

（3）設定値等の提供

作業に当たり必要な次に掲げる設定値等については、発注者が受注者に別途提供するものとする。

- ア 利用者情報
- イ 利用権限
- ウ フォルダ構成
- エ その他初期設定作業に必要な情報。ただし、本業務の実施に必要な範囲に限る。

8. 現行システム掲載資料のデータ移行

受注者は現行システムに掲載されている資料を新たな管理システムにおいて継続して利

用できるよう、必要なデータ移行作業を行うものとする。

(1) データ移行作業の内容

データ移行作業には、次に掲げる作業を含むものとする。

- ア 現行システムに掲載されている資料のファイル数、データ容量、フォルダ構成その他移行に必要な情報の確認
- イ 移行対象データ、移行方法、作業手順および作業スケジュールの整理
- ウ 発注者が提供する移行対象データの受領
- エ 新たな管理システムへのフォルダ構成の設定
- オ 新たな管理システムへの移行対象データの登録
- カ ファイル名、フォルダ構成、閲覧権限その他管理システムの利用に必要な設定
- キ 移行後のファイル数、データ容量および登録状況の確認
- ク 移行作業により不具合が生じた場合の修正および再確認
- ケ その他データ移行に必要な作業

(2) データ移行作業の実施時期

データ移行作業は、令和9年4月1日から令和9年4月30日までの間に実施するものとする。

ただし、令和9年4月1日以降の実施に向けて、受注者において必要と認める準備作業については、令和8年度中の実施を妨げない。

(3) データ移行の報告

受注者は、データ移行の計画を事前に発注者に報告するとともに、データ移行作業の完了後は、移行したファイル数、データ容量、移行作業の実施結果、不具合の有無および対応状況その他必要な事項について、発注者に報告するものとする。

9. 運用保守支援

受注者は、管理システムの安定的な運用を確保するため、次に掲げる運用保守支援を行うものとする。

- (1) データのバックアップを少なくとも1日に1回取得すること。
- (2) 異常な入力または処理を検出し、管理システムに登録されたデータの滅失または改変を防止するための対策を講じること。
- (3) システム運用中に障害・トラブル等が発生した際に原因追求が可能となるよう、操作ログやアクセスログ等のシステムログ、例外事象の発生に関するログ等を取得・保管し、発注者から求めがあった場合は、管理画面からの出力または受注者による抽出・提供により、必要な範囲のログを提示または提出すること。
- (4) 受注者は、管理システムが正常に利用できる状態にあることを確認するため、サービスの稼働状況、保存容量の使用状況その他受注者が提供するクラウドサービスにおいて確認可能な項目について、必要な監視または確認を行うこと。

(5) サポート体制は、次のとおりとすること。

ア 管理システムおよびサービス全般についての問い合わせに対応すること。

イ 通常の問い合わせ対応は、土曜日、日曜日、祝休日および年末年始（12月29日から1月3日まで）を除く月曜日から金曜日の午前8時30分から午後5時15分とし、電話または電子メールにより対応すること。

ウ イに定める時間以外の時間（以下「発注者業務時間外」という。）であっても、管理システムの全部または主要な機能が利用できない場合、電子文書の閲覧または登録に重大な支障が生じている場合、データの滅失、毀損もしくは改変のおそれがある場合、不正アクセスまたは情報漏洩のおそれがある場合その他の議会運営に重大な支障が生じるおそれがある場合は、緊急の場合として、電話による対応を行うこと。

エ システム障害の際には、次のとおり対応すること。

(ア) 発注者が障害を検知して受注者に連絡した場合、連絡から速やかに電話または電子メールで障害対応状況、復旧見込み等について回答すること。発注者業務時間外の場合には、障害の程度により適宜協議すること。

(イ) 受注者が障害を検知した場合、速やかに発注者に連絡の上、遅滞なく電話または電子メールで障害対応状況、復旧見込み等について回答すること。発注者業務時間外の場合には、障害の程度により適宜判断して報告すること。

(ロ) 障害があった場合、復旧のための体制をとり、原則として、発注者からの連絡または受注者による検知から12時間以内に、発注者業務時間外においては24時間以内に復旧すること（機器設備交換を必要とする障害の場合を除く。）。

(ハ) 障害を復旧した場合、復旧後に、障害状況・発生原因・事後対策等についての報告を行うこと。

10. その他

(1) 守秘義務

受注者（本業務の契約者、保守員等）が本業務中に知り得た情報は、本業務の実施に必要な範囲内において利用するものとし、情報漏洩防止のため取り扱いには十分注意するとともに、これを第三者に漏らしてはならない。これは本契約期間の終了または解除後も同様とする。また、業務上扱うデータは、本業務に必要な範囲において使用するものとする。

(2) 善管注意義務

本業務に従事する者は、善良な管理者の注意をもって業務の実施に当たるものとする。

(3) 契約内容の変更

ライセンス数、保存容量等の変更が必要になった場合は、その契約変更の対応を迅速に行うこと。なお、費用については協議の上、別途決定するものとする。

(4) 業務の終了

受注者は、本契約の満了または契約の解除により本業務が終了する場合において、発注者が管理システムに登録した電子文書、フォルダ構成、利用者情報、権限設定その他発注者が管理システムを利用するために登録したデータについて、PDF、CSV、その他の汎用的な形式または発注者および受注者が協議して定める形式により、本契約終了日までに発注者に引渡すものとする。なお、引渡し完了後は、保管されている情報はすべて抹消することとし、発注者に対し、書面等により報告するものとする。

(5) 仕様書に記載のない事項

本仕様書に記載のない事項および疑義の生じた事項については、発注者と協議の上、処理するものとする。