公益財団法人私立大学退職金財団

事務基盤の更改及び運用保守業務

調達仕様書

公益財団法人私立大学退職金財団

令和 7(2025)年 9 月

目次

１．　概要

１－１　件名

公益財団法人私立大学退職金財団　事務基盤の更改及び運用保守業務

１－２　調達の背景

公益財団法人私立大学退職金財団（以下、「当財団」という）で利用している事務基盤は稼働開始から 4 年が経過し、使用中のハードウェア及びソフトウェアは、メーカーによるライフサイクル終了の対象となっている。特に仮想基盤に関しては、中小企業向けのライセンス販売がなくなり、継続的かつ安定的な運用を確保するために、新たな事務基盤の構築が必要となった。

１－３　目的

以下の要件を踏まえ、安定的かつ高いセキュリティを確保したうえで、効率的かつ柔軟性の高い事務基盤の構築を目的とする。

（１）急速に拡大するクラウドサービスの安全な利用を可能とし、パンデミック等の非常時においても業務継続が可能なリモートワーク環境を整備すること。

（２）政府情報システムにおける「クラウド・バイ・デフォルト原則」を参考とし、クラウドサービスの活用を基本方針とした業務環境の実現を目指すこと。

（３）インターネット接続による業務環境と、Web 閲覧やメール利用を行わず、個人情報等の重要情報を取り扱う環境とを分離するネットワーク構成（ネットワーク分離）を採用すること。

２．　調達範囲

現行事務基盤のうち暗号系基盤(参考資料 現行の事務基盤 参照)について、新しい事務基盤の構築対象とする。調達対象及びその範囲は以下の通りとする。

範囲	数	備考
Web 分離されたデスクトップ環境	10 台	マルウエア感染等による情報漏えいを防止するため、VDI 又は同等のセキュリティレベルを有すること。
サーバ機	必要数	３－1 項に定める各要件を満たすこと。
クラウドサービス	必要数	クラウドサービスを利用する場合、日本国内のリージョンを使用したサービスとすること。また、必要なサービス内容及び見積額を提示すること。 ※ISMAP 登録済みサービスであれば尚可。
データセンター		データセンターを利用する場合、日本国内に設置されており、Tier3 相当以上の設備を有すること。

３．　事務基盤の要件

事務基盤に求められる要件を以下の通り定義する。

３－１　機能要件

（１） セキュリティ環境

・VDI 接続又はこれと同等のセキュリティレベルを確保すること。
(ローカル端末からの情報漏えいリスクの軽減)

（２） Web 分離

・情報漏えい対策として、業務システムを除いた Web サイトの閲覧や電子メールの送受信を抑止する Web 分離環境又は同等のセキュリティ対策を行うこと。(マルウエアなどのウイルス感染対策及びウイルス感染時の情報漏えい対策)

（３） 業務システムとの連携

・インターネット経由で接続し業務システムを利用できること。(接続可能なサイトを限定すること)

（４） データ移動

・FAT PC から新環境へデータを移動できること。
・新環境から FAT PC へのデータ移動は、有権限者だけが行えること。

（５） 印刷機能

・新環境から当財団 LAN（新設）に接続された複合機に印刷できること。

（６） FAT PC

・通常系の移行で導入した「Microsoft Surface Pro（第 11 世代)」を利用することが望ましいが、ソフトウェアの制約等で使用できない場合は、推奨パソコンを提案すること。

（７） 使用可能アプリケーション

以下のアプリケーションを利用できること。なお、ソフトウェアのライセンスは当財団で用意する。

・Microsoft 365（Excel、Word、PowerPoint、Access）
・7-Zip
・TeraPad
・Microsoft Edge
・Just PDF6 Pro

（８） 以下のアプリケーションの使用を抑止すること。

・Teams
・Sharepoint
・Onedrive
・Microsoft Store

（９） ファイルサーバの要件

・オンプレミス又はプライベートクラウドとすること。

・保存データをアプリケーション又はファイルシステムレベルで暗号化すること。

・当財団 LAN や特定拠点からのみアクセスを許可すること。

・利用者ごとに読み取り・書き込み権限を細かく設定できること。

・保存容量は 1 テラバイト以上で冗長構成とすること。

・契約期間満了後、データを完全に消去(NIST SP 800-88 Rev.1 レベル)又は物理破壊し、不正な復元が不可能な状態にすること。

（１０）Dr.Sum の導入又は同等の機能を提供しデータ分析を行うことができること。

(Dr.Sum は Datalizer for Excel を使用し Excel からアクセスしている)

【Dr.Sum の使用状況】

① 1 テーブルの取り扱いデータ件数

600 万件(40 万件増/年)、100 万件(2 万件増/年)、60 万件(1 万件増/年)のテーブルがある。

② 1 データベースのテーブル個数

一つのデータベースに 69 個のテーブルが登録されている。

③ データベース登録個数

決算整理に必要な毎年度末の主要なデータを保存しているため、14 個のデータベースが登録されている。なお、毎年 1 個増加する。

④ データベースの内容

業務システム(t－マネージャ)で使用している主要データを複製して登録している。

⑤ データ更新

現在は、毎日自動処理によって更新を行っているほか、必要に応じて都度手動で対応している。

⑥ 主な使用目的

A. アクチュアリに収支予測を委託する際に必要なデータを抽出する。

B. Excel から抽出条件を指定して集計データを抽出する。また、必要に応じてドリルダウンし個別データを抽出する。

C. データ抽出条件を登録しておき、業務に必要なデータを抽出する。

D. 決算書作成に必要な集計データの抽出や決算説明に必要な分析を行うためのデータを抽出する。

【Dr.Sum のデータ更新について】

・新環境のデータ更新は、任意のタイミングで手動更新が行えるようにすること。データ更新の頻度は、自動更新で月 1 回（毎月 11 日）以上実施されることが望ましいが、手動更新のみでも差し支えない。

３－２　非機能要件

（１） 対象利用者数は 10 名とする。

（２） 業務で利用する時間は平日８時～18 時まで(最大 22 時まで)とする。

（３） システムの稼働率は、定期保守や自然災害による停止を除き、99.9%以上を目安とする。

（４） 納品されるすべての機器、サービス、機能、ソフトウェア等については、構成、設定、利用方法、保守等に関するマニュアル及びドキュメントを作成し、電子媒体（原本の電子ファイル及び PDF 形式の２種類）で提出すること。

３－３　セキュリティ要件

（１） 不正侵入及び不正利用を防止するため、適切な利用者認証等の対策を講じること。

（２） 利用者には、役割や業務に応じたアクセス権を付与すること。

（３） ウイルス対策ソフト等を活用し、不正プログラムへの対策を行うこと。

（４） 機器を導入する場合、冗長性を考慮すること。

（５） 利用期間中、メーカーのサポートを適切に受けられるよう、サポート対象のバージョンを維持し、必要に応じてアップデートを実施すること。

（６） システムの脆弱性情報が公表された場合、必要に応じて修正パッチを適用すること。

（７） インシデント発生時に状況を把握できるよう、必要な内容及び期間のログを適切に記録・保存すること。

（８） リソースの利用状況を監視し、必要に応じて警告を発する機能を設けること。

（９） 各サーバ及びファイルサーバのデータについてバックアップを取得すること。また、世代管理を行うこと。

（１０）バックアップデータは暗号化しクラウド又は遠隔地に保存すること。

（１１）クラウド上のコンポーネントについてはクラウドサービス上で提供しているバックアップサービスを使用する想定だが、別途バックアップが必要である際は提案すること。

（１２）営業時間外にシステムが利用された場合、当財団へのアラート通知機能を設けること。

（１３）事務基盤の構築後、セキュリティ専門サービスを提供する第三者による診断を実施し、セキュリティ上の問題の有無を確認したうえで、当財団に報告書を提出すること。また、運用に支障がないと当財団が認めた軽微な脆弱性、及び当財団が許容したものを除き、それ以外の脆弱性については対応を行うこと。

（１４）受注者が実施する作業、構築するシステム及びネットワークが影響を及ぼす可能性について、当財団に対して本調達仕様書の要件に基づくセキュリティ対策の提案を行うこと。

（１５）受注者は事務基盤の構築中であるか完成であるかといった状態にかかわらず、信頼性とセキュリティに十分に考慮して、システムへの不正侵入や攻撃、ウイルス感染等への防止に万全を期すこと。

（１６）セキュリティ事件、事故及びセキュリティの違反が生じた場合、速やかに当財団へ報告を行うこと。

３－４　運用・保守要件

運用業務

（１） 毎月、運用保守実績、障害報告、問い合わせ対応内容等、運用保守業務に係る報告書を作成し、報告会議を開催すること。

（２） 運用業務で生じた課題について改善提案を行うこと。

（３） セキュリティインシデント発生時には対応支援を行うこと。

（４） 障害発生時には、復旧作業及び原因調査を実施すること。

（５） システムリプレイス時には、導入支援（情報提供、設定変更等）を行うこと。

（６） 事務基盤の異常を検知した際には、障害対応を行うこと。

（７） 機器の増設・入れ替えが行われた際には、監視設定の変更を行うこと。

（８） ネットワーク関連機器の構成管理を行うこと。

（９） 端末及びユーザアカウントの最適な管理方法を提案すること。

（１０）運用保守用のユーザアカウントを管理すること。

（１１）情報資産台帳を作成・管理すること。

（１２）本稼働開始以降の運用・保守のため、専門知識を有する要員を確保し、遠隔保守又は現地対応の体制を保持すること。

保守業務

（１） ハードウェアを導入した場合には、定期点検、障害対応、障害要因に基づく設定変更作業及び交換作業等を実施すること。

（２） 仮想サーバを導入した場合には、各仮想サーバに対する設定の提案及び設定変更作業等を実施すること。

（３） ファームウェア及びソフトウェアに係る設定変更作業、再インストール作業等を実施すること。

（４） ファームウェア及びソフトウェアのバージョンアップに係る検討、提案、実施作業等を行うこと。

（５） 各保守業務に伴い、関連するドキュメントの更新を行うこと。

４．　構築作業体制

（１） プロジェクト管理方法を明示し、当財団の了承を得ること。

（２） プロジェクトの体制を整え、責任者を明示すること。また、当財団との連絡体制を明示すること。

（３） 定例報告会を開催し、進捗状況を報告すること。

（４） 品質管理方針に基づき、品質管理を実施すること。

（５） 運用・保守業務に必要なドキュメントを作成すること

（６） データ移行に際して、当財団に対して必要な支援を行うこと。

５．　移行、研修

（１） 現暗号系システムのデータはすべて新事務基盤へ移行すること。

（２） データの移行は令和 8(2026)年 8 月中に行うこと。

（３） 事務基盤の切り替えは当財団の休日の間(土日祝日及び当財団が定める夏季休業日(3 日間))に行い、営業日に影響を与えないこと。

（４） 納品されるすべての機器、サービス、機能、ソフトウェア等について、その構成、設定、利用方法、保守等に関するマニュアル、ドキュメントを作成し、電子媒体で納品すること。

（５） 事務基盤導入時に、利用方法等について当財団職員が適切に利用できるように研修教育を実施すること。

６．　スケジュール

No	項目	日程・期限等	備考
1	契約締結	令和 8 (2026)年 1 月下旬	
2	基盤構築	契約後～令和 8 年 7 月 31 日	
3	運用保守	令和 8(2026)年 8 月 1 日～3 年間	

７．　契約期間

契約は、以下の期間に係る業務についてそれぞれ締結するものとする。

基盤構築業務　：　契約締結日の翌日から令和 8(2026)年 7 月 31 日まで

運用保守業務　：　令和 8(2026)年 8 月 1 日から 3 年間

８．　納入検査

本システムの納入時には、当財団にて納入検査を実施するものとする。

納入検査の結果、本仕様書との不一致が確認された場合は、当財団と協議の上、受託者は無償で是正措置を実施すること。

９．　支払条件

（１） 導入期間の作業等に係る基盤構築費用については、納入検査に合格した場合に、契約書に基づき一括で支払うものとする。

（２） システム利用期間に係る利用料等及び運用・保守に係る費用については、月払とし、受託者の請求に基づき支払うものとする。

１０．利用期間における制約条件

（１） 稼働から３年間利用できること

（２） 購入する機器及びソフトウェア４年間の保守・サポート費用を基盤構築費用に含めること。

１１．特記事項

（１） 知的財産権等

① 本業務に関し作成・変更・更新されるドキュメント類の著作権（著作権法第 21 条から第 28 条に定める全ての権利を含む）は、受託者が本業務の従前より権利を保有していた等の明確な理由により、応札時にあらかじめ権利譲渡不可能と示されたもの以外、当財団に帰属するものとする。本業務に係り発生した権利については、受託者は著作者人格権を行使しないものとすること。

② 本業務によって発生した権利については、今後、二次的著作物が作成された場合等であっても、受託者は原著作物の著作権者としての権利を行使しないものとすること。

③ 本業務によって作成、変更及び修正されるドキュメント類、プログラム等に第三者が権利を有する著作物が含まれる場合、受託者は当該著作物の使用に必要な費用負担や使用許諾契約に係る一切の手続きを行うこと。この場合は、事前に当財団へ報告し、承認を得ること。

④ 受託者は、当財団の事前の書面による承諾を得た場合を除き、この契約によって生ずる権利又は義務の全部若しくは一部を第三者に譲渡、承継させてはならない。

⑤ 本業務によって第三者が有する著作物をめぐる紛争については、受託者の責任、負担において一切を処理すること。

（２）　守秘義務

① 受託者は、本業務に関して何人に対しても、受託期間中又は受託期間終了後を問わず、業務上知り得た内容に関する守秘義務を遵守すること。

② 受託者は、本業務に関して当財団から提供を受けた資料等について、守秘義務を遵守するとともに業務終了後速やかに返却又は確実に破棄すること。

③ 受託者は、本業務に関して当財団から提供を受けた資料等について、当財団の許可なく複写又は複製してはならない。なお、提供された資料のうち、個人情報に係わるもの及び当財団の情報セキュリティに係わるものは、施錠可能な保管庫に収納する等、適正に管理すること。

（３）　再委託

① 受託者は、本業務の全部又は主要部分を第三者に再委託することはできない。

② 受託者は、本業務の一部を再委託する場合は、事前に再委託する業務、再委託先等を当財団に書面で提出し、承認を受けること。

③ 受託者は、機密保持、知的財産権等に関して本仕様書が定める受託者の責務を再委託先業者も負うよう、必要な処置を実施し、当財団に書面で提出し、承認を得ること。

④ 受託者は、第三者に再委託する場合は、その最終的な責任を負うこと。

（４）　遵守事項

① 民法、刑法、著作権法、不正アクセス行為の禁止等に関する法律等の関連法規を遵守すること。

１２．その他

（１） 本提案及び基盤構築に必要となる機器、媒体、通信等にかかる費用は受託者が負担すること。

（２） その他本業務を実施する上で新たに発生した事項、提案等については当財団と協議の上で対応するものとする。

以上

(参考資料)　現行の事務基盤の概要

１．現行事務基盤の構築状況

現行の事務基盤は、令和３年（2021 年）３月に構築されたものであり、以下の通り運用されている。

（１） 構成概要

・データセンターにおいて、VMware を用いた仮想環境上に構築。

・閉域 VPN により、事務所と安全に接続。

（２） ネットワーク分離

・通常系（インターネット接続可能）と暗号系（インターネット非接続）に分離。

（３） 端末構成

・当財団事務室にはシンクライアント端末を設置。

・通常系・暗号系の双方に VDI 接続し、仮想デスクトップを利用。

（４） 通常系の接続状況

・インターネットに接続している。

・業務システム（t－マネージャ）への接続は行えない。

（５） 暗号系の接続状況

・インターネット非接続。

・内部 LAN により、業務システム（t－マネージャ）及び Dr.Sum サーバに接続。

（６） 業務システムの構成

・業務システム（t－マネージャ）は、同一データセンター内の別仮想環境上で稼働する Web システム。

（７） ファイルサーバのセキュリティ

・暗号系ファイルサーバには「秘文」を導入。

・共有フォルダ単位でファイルを暗号化。

（８） バックアップ体制

・日次でバックアップを取得。

・名古屋 BCP サイトへバックアップデータを伝送。

（９） 利用者数

・通常系：12 名

・暗号系：10 名

（１０）ファイル移動（通常系→暗号系）

・特定フォルダを介してファイル移動を実施。

（１１）ファイル移動（暗号系→通常系）

・特定フォルダを介し、有権限者のみファイル移動可能。

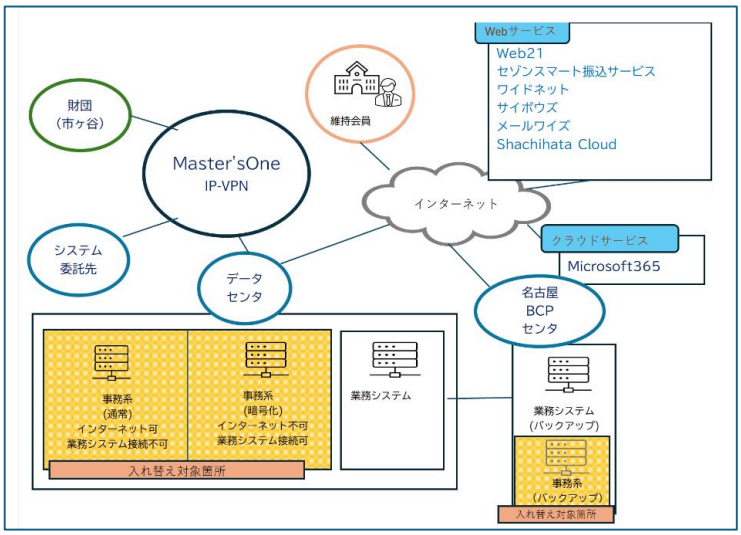
（１２）利用可能アプリケーション

以下のアプリケーションを利用可能している。

No.	アプリケーション名	備考
1	Microsoft Office365	通常系・暗号系共通
2	Microsoft Edge	
3	7-Zip	
4	TeraPad	
5	Just PDF 5 Pro	
6	Symantec Endpoint Protection	
7	Microsoft Teams	通常系のみ
8	Datalizer for Excel（Dr.Sum Excel アドイン）	暗号系のみ
9	秘文(Device Control, Data Encryption)	

※文書作成が主な作業で負荷が大きいアプリケーション等は利用していない。

２．構成イメージ



３．暗号系サーバ機の構成

機　　能	CPU	メモリ	ディスク
AD サーバ(プライマリ、セカンダリ)	2 コア	8GB	300GB
ファイルサーバ※	2 コア	16GB	2000GB
アンチウイルスサーバ	2 コア	8GB	300GB
vCenter サーバ	4 コア	16GB	435GB
VDI 14 台	2 コア	8GB	100GB
バックアップサーバ	8 コア	32GB	10,000GB

※暗号化ファイルの現在の保存データ容量：650GB

４．通常系の構成及び運用状況

通常系は、従来のシンクライアント環境から FAT PC を使用した環境へ移行済みであり、以下の通り構成・運用されている。

1. 端末構成
   - ・使用端末 ： Microsoft Surface Pro（第 11 世代）Copilot+ PC
   - ・CPU　　： Snapdragon® X Plus
   - ・メモリ　： 16 GB
   - ・台数　　： 12 台
2. ファイルサーバの構成変更
   通常系ファイルサーバのデータは、Microsoft 365 の SharePoint へ移行済み。
3. 認証方式の変更
   FAT PC の認証は、Entra ID による多要素認証（Windows Hello for Business）を採用。
4. アンチウイルス対策の変更
   従来使用していた Symantec Endpoint Protection から、Microsoft Defender for Business へ移行。
5. エンドポイント管理
   クラウドベースのエンドポイント管理ソリューションとして、Microsoft Intune を採用している。
6. クラウドバックアップ体制
   Onedrive 及び Microsoft 365 の SharePoint については、クラウドサービスを利用してバックアップを取得。