資料３

動画配信プラットフォーム提供
提案仕様書

令和８年２月

福岡市総務企画局人事部研修企画課

目次

別添

- 別紙 1_機能要件一覧
- 別紙 2_システム利用規模
- 別紙 3_外部サービス利用要件確認票

1. 本業務の背景と目的

1.1. 背景

福岡市総務企画局人事部研修企画課では、動画を活用した職員研修を実施している。当課が行う各研修の動画配信は、それぞれ視聴期間を設定して（１、２ヵ月程度）開催しており、各研修の対象者はほぼ被らないため、１人に対し１年を通して視聴権限を渡す必要はない。

研修対象者１人が視聴する動画は３つ程度のため、動画配信のサイトに訪れる機会が少ないことから、初見でも分かりやすいユーザーインターフェースが求められている。

また、研修動画の作成は当課で行う必要があるため、動画作成補助機能（自動字幕作成機能など）があれば望ましい。

1.2. 目的

・配信動画を格納・視聴可能な容量を確保すること。
・庁内（業務用パソコン）、自宅（職員個人のスマートフォン等）など視聴環境に関わらないアクセスを確保すること。
・セキュリティ面で高い安全性を確保すること。
・研修受講者および研修管理者（研修企画課）にとって使いやすいユーザーインターフェースを確保すること。

2. 本業務の内容

2.1. 調達範囲

2.1.1. システムに係る調達範囲

本件における調達範囲は、以下のとおり。
・本市が要求する機能を満たすクラウド型サービスの提供及びサポート。
・本システム利用に当たって必要となるシステム資産や役務を含める。
・ソフトウェアについては、利用者が問題なく利用できるよう、必要となるソフトウェアライセンスや、その他の使用許諾を得ることとする。

2.2. スケジュール

2.2.1. 履行期間

履行期間は契約締結日から令和９年３月 31 日(水曜日)までとする。

利用開始までの現時点の想定スケジュールについては以下の通りだが、契約後、本市と協議のうえ決定するものとする。

図表－01　利用開始までのスケジュール

年	令和８年		
月	４月	５月	
作業内容	初期設定、テスト期間、導入サポート		導入後サポート

5 月中旬　利用開始

3. 資格

受託者は ISO/IEC27001（JIS27001）認証又はプライバシーマーク認証を取得していること。

4. 機能要件

本システムが備えるべき機能の要件は「別紙 1_機能要件一覧」にて提示する。

5. 非機能要件

5.1. 前提条件

・本業務において調達するシステムは、インターネット経由でアクセス可能なクラウドサービス（パブリッククラウド）として受託者が提供すること。
・十分な稼働実績を有するサービスであること。

5.1.1. 使いやすいユーザーインターフェース

「1. 本業務の背景と目的」に記載のとおり、本システムは受講者の利便性向上を目的としたものであることから、パソコン・タブレット・スマートフォンでの使用を想定した画面づくりや操作性が求められる。このため、研修受講者及び研修管理者（研修企画課）にとって使いやすいレスポンシブデザインを採用したユーザーインターフェースであること。

5.2. 利用環境

5.2.1. システム利用時間

システム利用時間は以下の通りである。
ただし、システムメンテナンス等の計画停止はこの限りではない。

図表－02 システム利用時間

	分類	通常時利用時間帯
オンライン	平日	0:00 ～ 24:00
	土日祝日	0:00 ～ 24:00

5.2.2. システム利用者

システム利用者は、以下の通り。
・本市職員

5.2.3. システム利用規模

システム利用者数、利用端末は以下の通りである。
多数の利用者（本市職員）が同時アクセスした場合でも、動作が極端に遅くなる等のトラブルなく、利用者が快適に利用できる容量と性能を確保するために、必要であれば動画の圧縮及び最適化を実施すること。ただし、動画の画質を著しく低下させて配信するなど、動画視聴に影響を及ぼさないこと。

図表－03　システム利用規模

項目	規模
システム 利用 ID	最低利用 ID：動画視聴者、管理者含め　1,000ID ※ID は研修期間が終了する毎に別人に付け替えをする。（共用利用）
利用端末	・本市の情報系端末パソコン（本市庁内で使用しているパソコン） ・研修受講者が各自で所有するパソコン、タブレット又はスマートフォン
配信動画数等	「別紙 2_システム利用規模」　のとおり

5.3. システム利用環境

5.3.1. 端末

【本市職員利用端末】
端末の状況は、利用している OS が異なる等、複数の利用環境があることに注意すること。クライアント環境の一例を以下に示す。

図表－04 職員利用端末の仕様（例）

情報系端末パソコン

区分	項目	仕様・導入ソフトウェア名等
ハードウェア	CPU	Intel Core i5 以上（第 13 世代以降） 又は Core ultra 5 以上 もしくは AMD Ryzen 5 以上（第 4 世代以降）
	メモリ容量	16GB 以上
	ディスク容量	内蔵 SSD 250GB 以上
	解像度	1,920×1,080 ドット以上
ソフトウェア	OS	Windows 11 Pro 64 ビット
	ブラウザ	Microsoft Edge

なお、本システムは端末に搭載された Web ブラウザ（Microsoft Edge 等）から利用可能であり、かつシステムの利用にあたりアプリケーション等の追加インストールを必要としないこと。

※本市のインターネットまでの接続については、「5.3.2.ネットワーク」を参照

【自宅からの利用端末】

自宅からの利用端末については、パソコンのほか、スマートフォンやタブレットなど可能な限り多様な端末、OS、ブラウザからのアクセスに対応していること。

OS やブラウザについては、サポート期限内のバージョンに対応していること。

※自宅からの利用については、アプリのインストールを可とする。

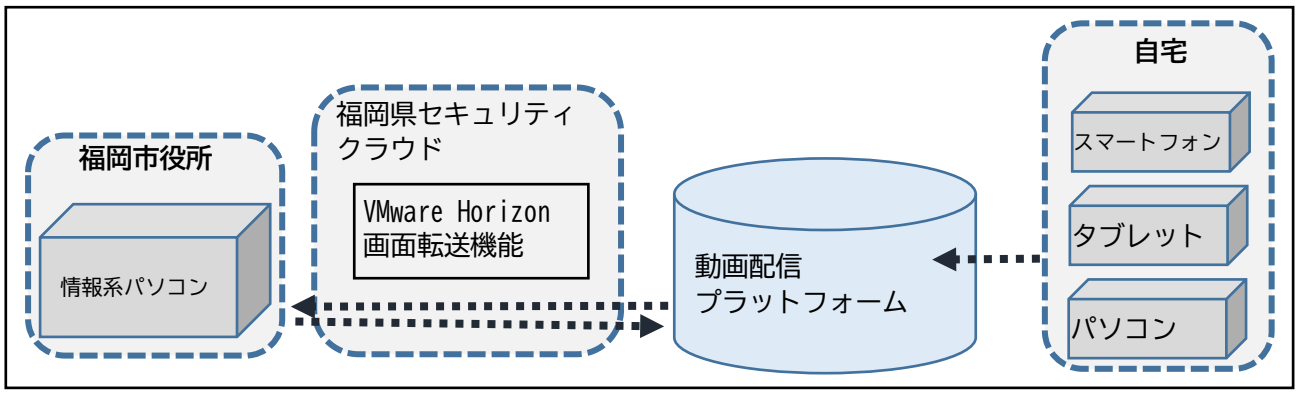
5.3.2.ネットワーク

本システムはインターネット環境に接続して使用する。

なお、本市庁舎内から利用する場合は、VMware Horizon の画面転送機能を用いてインターネットへ接続する。

ネットワーク構成に関しては、以下のネットワーク構成図を参照すること。

図表－05 ネットワーク構成図



5.4.クラウド要件

本システムは、インターネット経由でアクセス可能なクラウド環境（パブリッククラウド）において、所謂「ソフトウェア等提供サービス（SaaS）」として受託者が調達するものであることを前提に、以下の要件を満たしたものとすること。

①受託者が調達するサービスが、基盤層（IaaS や PaaS）とソフトウェア層（SaaS）を通して同一の事業者から提供される構成の場合

・受託者が調達するサービスが、「別紙 3_外部サービス利用要件確認票」のサービス提供者ワークシートの各要件を満たすことが、契約書、約款、公開資料その他サービス提供事業者からの提供資料により確認できること。

②受託者が提供するサービスの基盤層（IaaS や PaaS）とソフトウェア層（SaaS）が、複数の事業者から提供される構成の場合（例：AWS、AZURE、GCP 等を IaaS/PaaS として利用し、その上に動画配信プラットフォームが構築される構成の場合）

・IaaS、PaaS、SaaS 等のサービス提供者単位で、「別紙 3_外部サービス利用要件確認票」の各要件を満たすことが、契約書、約款、公開資料その他サービス提供事業者からの提供資料により確認できること。

③受託者が実施するサポート業務が、「別紙 3_外部サービス利用要件確認票」のサービス利用者ワークシートの各要件を満たすことが、契約書、約款、公開資料その他受託者からの提供資料により確認できること。

5.5. 可用性要件

5.5.1. 継続性

システム構成の冗長化により、特定箇所に故障が発生した場合に業務への影響を局所化すること。

図表－06 継続性要件

対象	内容
RPO（目標復旧地点）（平常業務停止時）	業務停止を伴う障害が発生した際には、障害発生時点（日次バックアップ+アーカイブからの復旧）までのデータ復旧を目標とすること。
RTO（目標復旧時間）（平常業務停止時）	業務停止を伴う障害が発生した際には、２日以内でのシステム復旧を目標とすること。
RLO（目標復旧レベル）（平常業務停止時）	業務停止を伴う障害が発生した際には、全システム機能の復旧を実施すること。
システム再開目標（大規模災害時）	情報システムに甚大な被害が生じた場合、情報システムは、1 カ月以内に再開することを目標とすること。
稼働率	年間のシステム稼働率は、計画停止時間を除外したうえで 99%を目標とすること。

5.5.2. 耐障害性

同一構成の仮想環境を複数用意し、アプリケーションレベルの冗長化を図ること。なお、本システムで冗長化構成を実現するに当たり負荷分散装置等が必要な場合においては、仮想アプライアンス等のソフトウェア製品で負荷分散環境を実現すること（当該ソフトウェアは本利用契約範囲に含む）。

5.5.3. 災害対策

地震、水害、テロ、火災などの大規模災害時や、ハードウェアの大規模障害の対策として、遠隔保管を実施すること。

5.6. 性能・拡張性要件

性能・拡張性については、「5.2.3. システム利用規模」を踏まえ、多数の利用者（本市職員）が同時アクセスした場合でも、動作が極端に遅くなる等のトラブルなく、利用者が快適に利用できる容量と性能を確保すること。

5.7. システム監視要件

本市が求める監視要件は以下のとおり。

図表－07　主な監視要件

対象	内容
各種ハードウェア（サーバ、ネットワーク、ストレージ）のハードウェア監視	SNMP Trap/Get 等
仮想サーバの死活監視	ノード監視（Ping 監視等）、OS プロセス監視 等
仮想サーバ上の OS レベルでのリソース監視	CPU 使用率、ディスク空き容量 等
仮想サーバ上のログ監視	OS のシステムログ 等

5.8. セキュリティ要件

以下に示す要件に留意し、セキュリティを担保すること。

図表－08　セキュリティ要件

要件	内容	
アクセス・利用制限	本システムは、利用者ごとのアクセス管理が行われ、割り当てられた権限の範囲で操作可能な仕組みであること。なお、管理者画面は本市の IP アドレスによる通信のみを許可し、外部からのアクセスを制限すること。 利用者の個人情報等の機密性の高い情報を格納・保存するデータベースサーバは非公開セグメントに設置し、公開セグメントとの間にはゲートウェイ機器（ファイアーウォール機能を含む）を設置すること。又は、サービス構成者によって適切に構築し、同等のセキュリティを担保すること。 なお、ゲートウェイ機器のファームウェアを適時に更新し、脆弱性が存在しない状態を維持すること。	
データの秘匿	伝送データの暗号化の有無	伝送データについては、SSL／TSL（1.2 以上）等の暗号化通信により第三者からの盗聴や改ざん等をされること無く安全に通信できること。
	蓄積データの暗号化の有無	蓄積データについては、認証情報（ID・パスワード・メールアドレス）を暗号化し管理すること。
ウイルス対策	本システムは、ウイルスやマルウェア等を検知/防御するための WAF や IPS 等のセキュリティ対策を実施していること。 （未知のマルウェアへの対策や振る舞い検知を含む。） なお、ファームウェア・シグネチャを適時に更新し、情報セキュリティ上の脅威に対応できる状態を維持すること。	
ログ対応	サーバログの取得	取得したログについて、漏洩、改ざん、消去等を防止できる機能を設けること。また、取得したログについて、可能な限り容易に確認ができること。なお、ログは１年以上保存できること。
	取得対象ログ	システムログ： サーバ単位で発生した事象（起動/終了、ハードウェア故障等の障害、プログラム等の動作状況）の記録。
		アプリケーションログ： サーバ上のアプリケーションやソフトウェアで発生した事象の記録。
		セキュリティログ： アプリケーションログのうち、情報セキュリティに関連するログを想定している。システムへのログイン履歴及び成否等を記録した監査ログを含む記録。
バックアップ・リストア	外部データの利用可否	障害時等に新システム内部のデータのみでシステムを復旧できるようなバックアップ・リストア方式とすること。
	データ復旧の対応範囲	障害発生時のデータ損失防止策を講じること。 ※障害によりデータの損失が生じた場合、「RPO（目標復旧地点）」で定めた時点までデータを復旧すること。
	バックアップ自動化の範囲	フルバックアップ、差分バックアップを組み合わせたバックアップのスケジューリングができること。またこのスケジュールに従い自動でバックアップ処理を実行できること。
		バックアップの実施状況をシステム管理者が確認できること。バックアップが正常に終了しなかった場合、対応方針について本市と協議すること。
	バックアップ取得間隔	システム全体（OS、ミドルウェア、業務アプリケーション等）： 初期設定時、及びシステム更新時（改修、設定変更等実施時）に取得。
		データベース：1 日 1 回程度
		ログ：1 日 1 回

要件	内容
データ消去	サービス期間終了後にデータの消去完了を明記した証明書を提出すること。 データ消去及び証明書の具体的手段については、ISMAP 管理基準マニュアル」で示されている「論理的消去」（データを暗号化した後、暗号鍵を消去し、元のデータの復号を不可能とする方法）も含め、本市と協議のうえ決定する。
ウェブアプリケーションのセキュリティ実装	SQL インジェクション 、OS コマンド・インジェクション やクロスサイト・スクリプティング等の脆弱性で発生しうる脅威や特に注意が必要なウェブサイトの特徴等に対し、脆弱性の原因そのものをなくす根本的な解決策、攻撃による影響の低減を図られていること。また、脆弱性診断を稼動前に実施し、検出された脆弱性を解消すること。
サプライチェーン・リスクへの対応	システムの構成に他の事業者のクラウドサービスを含む場合は、サプライチェーン・リスクを低減する対策が行なわれていること。

また、上記のほか、本市セキュリティポリシー、「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）」、独立行政法人情報処理推進機構「安全なウェブサイトの作り方（第７版）」に準拠するものとする。

6. サポート要件

6.1. サポート要員

受託者は、サポート要員として、以下のスキルを有する要員を配置すること。

図表－09 要員スキル要件

要求するスキル	スキルの詳細
導入ソフトウェアに関する専門知識	・導入するソフトウェア（OS・ミドルウェア含む）に関する専門知識と、本調達の要求事項を理解したうえで、最適なシステム構成の設計・構築・運用に係る技術及び技術コンサルティング能力を有すること。 ・本業務で利用するクラウドサービスに係る認定資格等を有すること。 ・国、地方公共団体又は特別法により設立された公共法人若しくはこれと同等とみなすことができる団体において、本業務と同等のシステム導入及び運用業務の経験を有すること。

6.2. 導入サポート

6.2.1. ヒアリング

受託者は、導入に向けて必要な事項をヒアリングすること。ヒアリングに当たっては、「1.1 背景と目的」を踏まえて、受講者の負担軽減、事務処理の効率化及びリスク回避を図るために、本システムの導入効果を最大限発揮できるよう支援すること。

6.2.2. 初期設定

受託者は、ヒアリングした事項をもとに、本市が円滑に利用開始できるよう、初期設定を行うこと。

ここでいう初期設定とは、本市（管理者 ID）が「別紙 1_機能要件一覧」に示す機能を利用できる状態を指す。

6.3. 導入後の活用支援

6.3.1. ヘルプデスク

以下の利用時間帯及び業務内容での対応を基本とする。ただし、翌日のオンライン運用に影響を与えると思われる場合は、本市と協議のうえ対応を決定する。

図表－10 ヘルプデスク対応時間

分類	通常時対応時間帯
平日	10:00～17:00
土日祝日	－

図表－11 ヘルプデスク業務内容

業務	作業	内容
ヘルプデスク（管理者からの問合せ対応）	受付	本市からのメール等による問合せについて、受付・回答を行うこと。
	調査／回答	調査結果が既存事象であった場合には、速やかに回答すること。

※システム利用者（研修受講者）からの問合わせ対応は含まないものとする。

6.3.2.障害時対応等

その他、システム導入後に係る業務について、以下に示す。

図表－12 業務内容

業務	作業	内容
セキュリティ管理	システムの安定運用	ソフトウェア、設備・機器、セキュリティに関して定期的な保守を行うこと
	システム監視	各システム・サービスの運用継続に係る以下の監視を行うこと。監視は、２４時間３６５日対応すること。 ・死活監視、プロセス監視、性能監視 ・計画外のアプリケーション又はプロセスの停止
	ウイルス対策	ウイルス対策ソフトのパターンファイル（定義ファイル）等のソフトウェアについて、原則として最新版に更新すること。ただし、最新版に更新することにより安定稼働が保証されない場合は、この限りではない。
障害対応	システム障害の早期発見・予防に努め、ソフトウェアやコンテンツ等に関する攻撃及び脆弱性に関連する早期警戒警報、勧告及びパッチを受理した場合は、直ちにセキュリティ対策を行うこと。	
	障害対応状況は、障害収束から速やかに報告すること。また、運用上の課題がある場合は、速やかに報告すること。	
	計画的なシステム停止以外の要因によりシステムの不具合やサービス停止が発生した場合、受託者は直ちにサービスの復旧又は代替手段を用意し、サービスの安定運用に努めること。	
	情報漏えいや不正アクセス等の情報セキュリティインシデントを検知した場合、受託者は情報インシデントの発生（疑いの段階を含む）を認知してから 24 時間以内に本市へ第一報を報告すること。その後、原因、影響範囲、対応状況、再発防止策について、本市と協議の上、速やかに詳細報告を行うこと。	

7.その他留意事項

・本市及び第三者機関などによる監査・検査等が実施される場合やその他本市からの求めがあった場合は、本市の指示に従い資料作成・実地調査・質疑応答など速やかに対応すること。
・すべての作業において、本市の業務等に影響を及ぼすおそれがある場合は、事前に明らかにし、本市の指示に従い作業を実施すること。
・本仕様書に定める事項に疑義が生じた場合、又は本仕様書に定めのない事項で協議の必要がある場合は、受託者は本市と協議を行うこと。
・実施の詳細については、本市と密に連絡を取り合い、業務を遂行すること。

以上