石垣市
新庁舎ネットワーク等構築業務委託
仕様書

令和元年 11 月

石垣市

目次

１　背景・目的

本市では、令和 3 年 4 月供用予定の新庁舎において、電話回線、庁内 LAN 環境整備に加え、監視カメラや入室管理システム。その他

関連システムを含めた統合ネットワーク環境を新たに構築し、マイナンバー制度施行以降の高度化また複雑化するネットワーク要件に対応できる柔軟性及び耐障害性、強固なセキュリティと設定ミス及び設定エラー等のトラブルを防止する運用管理機構を兼ね備え、現庁舎より導入済みの、自治体クラウド基盤、セキュリティ強靭化関連システム基盤（二要素認証システム、仮想化基盤）を安定して稼働させることを前提に、新庁舎での業務遂行において最適な環境整備を目的とする。

２　プロジェクト概要

2.1. 件名

石垣市新庁舎ネットワーク等構築業務委託

2.2. 業務内容の概要

業務内容は、大きく以下の 5 項目に分類される。詳細は後述するが、ここでは概要について記載する。

2.2.1. 電話設備

① 電話交換機
② 多機能電話機
③ 電話回線の移設及び内線電話機の導入
（現状利用の加入者電話回線、ISDN 回線、光電話回線）

2.2.2. 庁内 LAN 機器設置

① ファイアウォール
② コアスイッチ
③ サーバスイッチ／フロアスイッチ
④ エッジスイッチ
⑤ 無線 LAN アクセスポイント
⑥ 端末認証サーバ（RADIUS サーバ）
⑦ ネットワーク監視システム（ログ管理基盤）

2.2.3. 監視カメラシステム

① 屋外カメラ
② 屋内カメラ（ドームカメラ／PTZ 型カメラ）
③ 映像レコーダ

2.2.4. 入室管理システム

① IC カードリーダー付き電気錠

2.2.5. その他

① 建物安全度判定サポートシステム

② 気象情報観測システム

2.3. 業務内容における重点事項

本業務における重点事項は、以下のとおりである。

2.3.1 操作性の向上による業務生産性の確保

現行ネットワーク上で稼働しているシステムにおいて、端末の利用環境においてストレスを生じさせないよう、アプリケーションの操作性と快適性を実現するため、ネットワーク基盤上において十分な性能を確保することとする。

2.3.2 運用期間中のネットワークの拡張性の確保

法制度改正、その他の施策による今後の ICT 利用環境の変化に柔軟に対応可能なシステムとし、ネットワーク構成変更や端末利用者数の増などに対して余裕を持った設計を行うこと。また、働き方改革を考慮し、運用期間中における職員の業務効率化に十分配慮した設計がなされていること。提案事業者は、本市が本業務を行う目的や期待する成果を十分理解した上でサービスを提供するとともに、期待する成果の達成に向け、本市のパートナーとして共に協力していくものとする。

2.3.3 運用管理上の負荷低減と業務継続性確保

ネットワーク上の各種システムの安定的稼働の実現と、少ないスタッフで効率的かつ確実な運用管理を行うため、ネットワーク機器の最適な監視システム環境を提供すること。

2.3.4 セキュリティ強化及びコスト負担の軽減の両立

平成 29 年 7 月総務省が示した「地方公共団体情報セキュリティ強靭化」対策、及び平成 30 年 9 月に総務省が提示した「地方公共団体における情報セキュリティポリシーに関するガイドライン」
に則り、事業者は、不正アクセス等のセキュリティ上における脅威に対し、十分な対策を実施すること。構築したネットワーク基盤は長期間利用することを想定しており、今後のＩＣＴ利用環境の変化に対して柔軟に対応可能なシステムとし、加えて運用管理コスト負担の軽減を図ること。

2.4. 履行場所

石垣市字真栄里地内(石垣市新庁舎)

2.5. 契約期間

構築期間：契約締結の翌日から開庁年度末まで（予定）

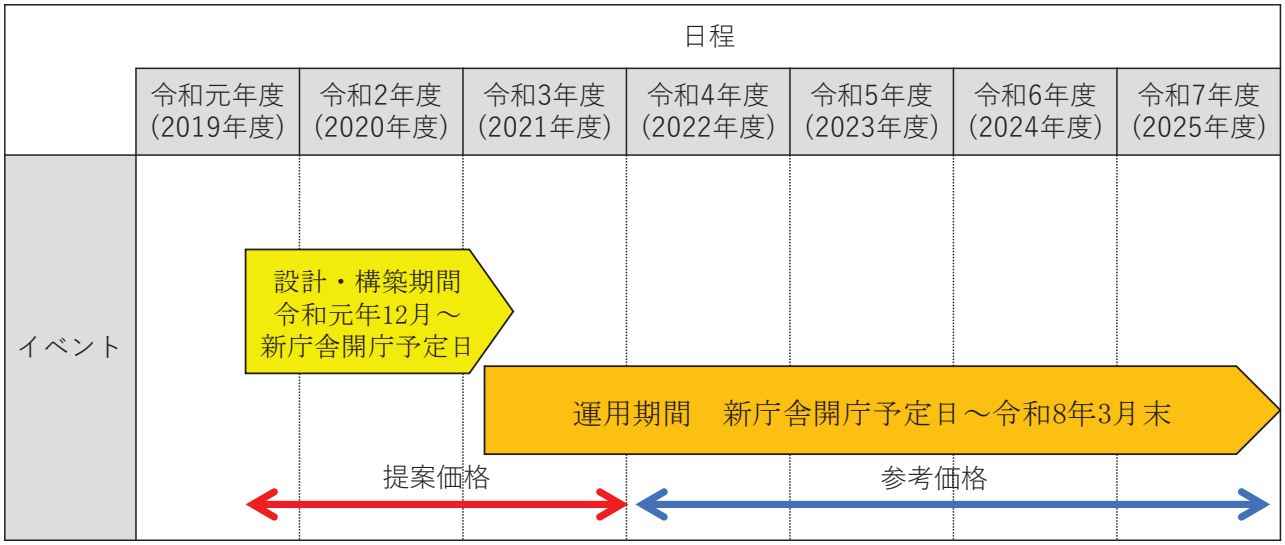
2.6. 提案上限額

212,570,000 円（消費税相当額含む）

開庁年度の初年度運用保守業務含む（令和３年度）
開庁２年目（令和４年度）以降の保守契約は別途締結するが、年度単位の見積もり費用についても提示すること。
提案内容に関わらず、この上限額を超える提案は受け付けない。

３　全体スケジュール

本業務及び関連業務のスケジュールを下記に示す。現在、令和 3 年度以降に予定されている新庁舎供用開始に向け、令和元年 12 月にプロポーザル方式により業者選定を行い、選定業者により本稼働開始時期に向けて各種設計、構築業務を行う。



4　基本情報

4.1. 電話設備（IP-PBX）について

新庁舎における電話設備（IP-PBX）は下表の通りとする。

下記に収容される以外の回線については別途協議の上、対応すること。

機器名称		現在の実装数	新庁舎における最大収容数	備考
内線	多機能標準 IP 電話	530	1024 以上	24 キー
	多機能 ISDN 用停電 IP 電話機	6		36 キー
	多機能カールコードレス電話機	30		24 キー
	オペレータ受付用中継台	2		全電話機の内線状況をモニタリングできること
	単体電話機	30		
外線	FAX	16		
	IP 電話回線	32		
	ISDN64 回線	6	512 以上	
	アナログ専用線(LD:2/OD:4)	6		LD/OD 接続
その他	通話録音機能	1		録音告知機能を有すること
	フルバックアップ電源（主電源）	1		3 時間以上
	オペレータ受付電話機用ヘッドセット	4(予備 2)		
	サンダーカット 7 個口	10		

4.2. ネットワーク環境について

4.2.1. ネットワーク系統

新庁舎ネットワークにおけるネットワーク系統は以下を想定している。

(1) インターネット接続系（沖縄県セキュリティクラウドに接続）
(2) LGWAN 接続系（内部情報系各種システムで利用）
(3) 基幹系（マイナンバー系）（個人番号利用事務で利用）
(4) 監視カメラ接続系
(5) 入室管理系
(6) ネットワーク監視系（ネットワーク関連機器の性能監視、死活監視で利用）

・(1)～(3)は、職員が業務利用するネットワーク
・(4)～(5)は設備管理上独立したネットワーク
・(6)は、ネットワーク基盤業者が利用するネットワーク

4.2.2. システムとネットワークの接続関係

現庁舎のシステムはネットワーク接続[K1]拠点（新庁舎、基幹系（マイナンバー系）システムクラウドデータセンター、出張所、健康センター、学校、保育園等）を広域イーサネット（NTT 西日本の VPN ワイド)、その他、各担当課と契約したシステム提供業者が敷設した環境で接続している。具体的な接続関係は、　別途配布する「別紙１　移転対象システム一覧」「別紙２　移転対象ネットワーク」を参照のこと。

移転対象ネットワーク及び移転対象システムについて、石垣市、該当システム事業者、ネットワーク事業者と事前に協議の上、新庁舎のネットワーク設計及び構築に反映すること。

4.3.　端末及びプリンタ台数等について

端末台数及びプリンタ対数は以下の通りとする

4.3.1. 職員数

約 700 人（令和元年 10 月 1 日時点）　※臨時職員及び再任用職員を含む。

4.3.2. 端末台数

(1)　基幹系（マイナンバー系）（個人番号利用事務系）端末　200 台

(2)　LGWAN 接続系端末　700 台

(3)　その他端末

国保連端末、介護認定支援端末、防災関連（J アラート含む）端末

4.3.3. プリンタ台数

(1)　基幹系（マイナンバー系）プリンタ　25 台

(2)　複合機　10 台

4.3.4. 留意点

(1) LGWAN 接続系の端末は、モニターと接続し、内部情報系システム（職員ポータル、グループウェア財務会計システム)、VDI（インターネット接続系閲覧用）等を利用している（２画面または画面を複製する形)。

(2) 端末及びプリンタ台数は、およその数であり前後 10 台程度の差があることに留意すること。

4.4.　保有ライセンスについて

今回調達予定のサーバ機器類において、必要に応じて以下のライセンスについては当市の包括ライセンスを適用すること。

・ウイルスバスターコーポレートエディション

・SkySEA

4.5.　設備工事業者側との施工区分について

本提案事業者と設備工事業者等との施工区分は以下の通りとする。

作業において双方適宜調整の上、確実な構築を行うこと。

機器設置場所	本提案事業者	その他設備工事業者
交換機室 電話交換機室	・電話交換設備：主装置他、収納架の設備設定工事 ・IP 電話用光ケーブル主装置への接続 ・MDF 盤までの工事、光 PF 盤または PD 盤までの工事 ・メタルケーブル（各階 50 対 MDF から各 EPS＜IDF 盤＞、及び各部署への配線工事）	・内装設備：二重床、電話受付台から交換機室までの空配管工事（溝配管または床下転がし） ・電気設備：壁コンセント、電話交換設備用電源確保
サーバ室	・サーバラックへ、コアスイッチ、サーバスイッチ、ファイアウォール設置 ・光スプライスユニットの設置	・内装設備：二重床 ・電気設備：サーバ機器用電源コンセント、火報設備、その他設備 ・サーバラック：６架と２架は UPS 専用設置ラックへは光・UTP パネル設置、該当パネルからラック間を繋ぐ配線工事を想定 ・PT 盤：光複数回線集約用 E キャビネット設置用盤
EPS（各フロア）	・サーバ室～各 EPS 間の縦系／横系幹線は提案に応じた光ケーブルまたは任意の配線工事 ・各 EPS 内へのフロア SW の設置 ・各 EPS～各部署までの配線工事 ・各 EPS 内へネットワーク機器収容用 19 インチラックの設置 ・ラック内へ光スプライスユニットの設置パッチパネル設置 ・各種設備（システム利用 EPS 間への配線及び利用 EPS 内への SW/HUB の設置） ・各 EPS 内 IDF 盤（端子成端用盤）の設置と IDF 盤収容キャビネット（電話メタル用）	・電気設備：EPS 内各種機器電源工事（壁コンセント等） ・配管工事：EPS 縦系／横系幹線ルートの空配管工事とケーブルラックの設置及び各フロア内 EPS 間空配管工事とケーブルラックの設置（通線用のリード線の配線）
部署・課内フロア	・配線工事：フロア～部署までの提案に応じた任意の配線工事 ・HUB 設置：各課机 G と柱（壁面）の HUB 設	・内装設備：フロア床（溝配管）設置 ・電気設備：電源確保（壁コンセント等） ・天井吊りラック設置及び点検口設置

機器設置場所	本提案事業者	その他設備工事業者
	・電話機設置：各職員机上へ電話機設置・設定 ・部署・課内柱 SW 収納工事：HUB BOX 設置 ・無線 LAN アクセスポイント（AP）設置	
会議室	・配線工事：サーバ室 EPS～会議室までの配線 ・無線 LAN アクセスポイント（AP）設置 ・電話機設置工事	・会議室内装設備：二重床または溝配管 ・電気設備：電源確保（壁コンセント等） ・通信用空配管～情報ブランクコンセントプレート（終端部）までの工事 ・アクセスポイント設置壁または天井吊りラック設置
その他	・売店、食堂、カフェ、銀行、及びメタル用配線及び情報コンセントプレート設置	・売店、食堂、カフェ、銀行、議場内装設備：フロア床または溝配管 ・売店、食堂、カフェ、銀行内電気設備：床・壁コンセント、電源等の確保 ・上記通信用空配管需要報ブランクプレートまでの工事

4.6. その他

4.6.1. 公衆無線 LAN サービス

新庁舎に来庁した議員及び市民へのサービスとして、庁内及び議場を対象に公衆無線 WiFi 環境を新規に整備可能とするよう、下記の点に配慮すること。

本庁の無線 LAN アクセスポイント、無線 LAN ネットワークと分離すること。

① アクセスポイント設置場所については、本市と別途協議した場所に設定すること。

② 本庁のインターネット接続環境と分離すること。

5 機能要件、非機能要件

5.1. 電話設備

項目	機能
交換機等各種装置	・全デジタル電子式ボタン電話とすること。 ・交換機、電源装置、配線盤を整備すること。 ・通信キャリア回線を収容して電話交換設備として運用すること。 ・交換機は新庁舎２階の電話交換機室に設置すること。

項目	機能
	・交換機は、保守点検が容易な自立キャビネット型、壁掛け型、あるいはラックマウント方式で耐震性を考慮した構造とすること。 ・交換機の入力電源は AC100V（±10V）とすること。
基本機能	以下の機能に対応すること ・着信音識別機能を有し､内線からの着信呼と局線から内線への着信呼の呼出し信号を区別すること。 ・発信制御（ACR）機能を有すること。 ・内線番号の行数やその組合せを任意に設定できること。 ・システム（固定）短縮ダイヤル機能、可変短縮ダイヤル機能 ・フルコールバックトランスファ機能を有し、内線相互・局線発着信通話において､通話相手を一旦保留して他の通話相手を呼び出し保留中の通話相手をその通話相手に転送できること。 ・通話中の局線を一旦保留し､電話機のスピーカーにより離席者を呼び出し被呼者の応答操作により、局線の転送接続ができること。テナント毎にページングへの接続、規制ができること。 ・停電時に停電用電話機が使えること。 ・局線キャンプオン、内線キャンプオン機能を有し、内線呼出した相手が話中だった時に､相手の通話が終わり次第内線を呼び出せるように予約できること。 ・国際・市外・市内の発信規制ができること。 ・保留音送出機能を有すること。 ・交換機が呼び出しに応答して通話状態になった上で､最終的に呼び出したい内線電話を直接指定する簡易 DID 機能を有すること。 ・内線 1 回線単位に各種サービスクラスを付与することができること。 ・割り付けられた電話番号以外の電話番号を着信させるマルチライン設定を行えること。 ・グループ内内線着信時、同一グループ内内線にも着信表示を行い、応答できるマルチステーション機能を有すること。
収容等回線	・加入電話回線、ISDN 回線、IP 電話回線を収容すること。 ・リダイヤル機能を有し、局線発信時、相手が話中の場合や通話終了後に、再びその相手と通話したい時、特番ダイヤルだけで、前にダイヤルした番号を自動的に送出できること。 ・ピックアップグループ内の内線に着信があった時､同一グループ内の他の内線が特番により応答できる指定グループコールピックアップ機能を有すること。 ・１８４／１８６制御が可能なこと。
各種転送機能	・IP 電話機を収容すること。

項目	機能
	・市外発信規制機能を有すること。 ・夜間転送機能を有すること。 ・携帯電話発信時キャリア番号付加機能を有すること。 ・公専接続 / 専公接続を有すること
通話録音機能	・必要な部署に音声録音告知機能と音声録音機能を有すること。 ・録音方式には、自動録音と手動録音機能を有すること ・録音時間は 1,000 時間以上とすること。
多機能電話機	・押しボタンダイヤル式とすること。 ・機能キーは２４ボタン以上表示付とすること。サービス機能のキー割り付けが可能なこと。 ・機能キーによる保留が可能で、グループ内で同じ機能キーにより応答できること。 ・短縮ダイヤル／ワンタッチダイヤル機能を有すること。 ・音量調整機能を有すること。 ・表示モニタ（日時、ダイヤル通話時間等）は大型ディスプレイで漢字表示等により発着信履歴やナンバーディスプレイ表示が明確に確認することができること。 ・内線代表、代理応答、局線着信転送、局線着信表示が可能なこと。
その他、回線敷設等	・現状利用の加入者電話、ISDN、ひかり電話回線等を新庁舎へ現状のまま移転すること。 ・電話交換機に収容されない回線については別途配線を行うこと。 ・MDF から各階 EPS 内 IDF まで原則として 50 対ずつの配線を行うこと。 ・各階のフロア配線は、原則として、各階 EPS 内 IDF からフロア内 EPS 内 IDF 間まで 50 対の配線を行うこと。 ・オペレータ受付用中継台を設置し、全 IP 多機能電話機の内線状況をモニタリングできること。 ・その他、必要事項についてはその都度、発注者と協議の上実施すること。

5.2. 庁内 LAN

5.2.1. 基本事項

(1)建屋構成に配慮し、L3 スイッチ（コアスイッチ)、L2 スイッチ（サーバスイッチ、フロアスイッチ等)、端末接続用スイッチ（エッジスイッチ)、ファイアウォールを含めたネットワーク機器により、庁内ネットワークを整備すること。

(2)庁内の基幹系（マイナンバー系）端末、LGWAN 接続系端末を接続する無線 LAN 環境を整備すること。

(3)基幹系（マイナンバー系)、LGWAN 接続系セグメント毎に接続する各端末及びアクセスポイント等のネットワーク機器認証用の RADIUS サーバ環境を整備すること。

(4)ネットワークの監視を可能とするネットワーク監視システムを整備すること。
(5)IP 電話機が接続されることを考慮し、拡張性と可用性に配慮したネットワークとすること。
(6)提案機器とソフトウェア（ライセンス）の構成は、安定稼働を実現するために、メーカの推奨構成及び推奨値を遵守すること。

5.2.2. 機器設置場所

(1)ネットワーク機器は、以下の場所を原則として、提案事業者が最適とされる提案構成に従い、任意の場所に設置すること。
① サーバ室
② EPS 室
③ 執務室内 HUB ボックス
(2)端末接続用スイッチ（エッジスイッチ）はフロア内の各机の側面に接続することも可能とするが、業務に支障が生じないようにファンレス等静穏性に優れた機器とすること。
(3)外部拠点と接続する ONU（光回線終端装置）は各業務システムの収容ラックに設置すること。
(4)無線 LAN のアクセスポイント（AP）は執務室内、コミュニティースペース、会議室の柱壁面、壁面、天井に設置すること。
(5)停電時に非常用電源に切り替わるまでの 10 分程度の停止を踏まえて、可用性を確保した構成とすること。

5.2.3. 物理配線

(1)サーバ室（コアスイッチ）から各フロア EPS 間は、原則として光ファイバを敷設すること。光ファイバの心線数は、利用する心線数に加え、今後の拡張性を踏まえ予備の心線数を確保すること。
(2)各フロア EPS から、執務室、会議室、無線 LAN アクセスポイント等への配線は、光ファイバまたは UTP ケーブルによる、コスト面と可用性から最適とされる任意のケーブルを敷設すること。
(3)１本のケーブル切断で広範囲なネットワーク障害が発生しないよう、最適とされるケーブル本数を確保し、最適とされる配線経路によりケーブルを敷設すること。
(4)コミュニティールーム、会議室の情報コンセント（アウトレット）は、原則的に基幹系（マイナンバー系）（個人番号利用事務系）ネットワーク用回線、LGWAN 接続系（内部情報系）ネットワーク用として各１ポートずつ確保した配線とすること。
(5)原則として、コアスイッチ～フロアスイッチ間は 10GB 以上、フロアスイッチ～フロア内の各種主要スイッチ間は 1GB 以上を確保すること。
(6)情報コンセント（アウトレット）関連工事については、ケーブルラック、終端配管（PF 管）、ブランクプレート等までは建築（ゼネコン）側で工事を行う、アウトレット設置と各ケーブル配線作業は本提案事業者で行うこと。

5.2.4. 論理構成

(1)庁内 LAN は以下のセグメントに分離し、一部の特定通信を除いて、相互に通信ができないようにすること。

・　基幹系（マイナンバー系）（個人番号利用事務系）セグメント
・　LGWAN 接続系セグメント
・　インターネット接続系セグメント
・　その他（ネットワーク監視系セグメント、公衆無線 LAN サービス等）

(2)特定通信はファイアウォール等で制御し、送信元、宛先 IP アドレスおよび送信元、宛先ポート番号を指定して通信できるようにすること。

(3)基幹系（マイナンバー系）、LGWAN 接続系、インターネット接続系以外の、その他ネットワークセグメントに接続する機器構成及びセキュリティ面に配慮すること。

5.2.5. 新庁舎ネットワーク統合ファイアウォール仕様

運用管理の効率化及びセキュリティ強化の観点から、基幹系（マイナンバー系）、LGWAN 接続系、インターネット接続系セグメントの各論理接続を一元管理可能な機構を有することとする。

①　ファイアウォール/UTM 専用ハードウェアであること。
②　インターフェースは 10/100/1000 BASE-T（RJ-45）　×6 ポート以上を有すること。
③　ステートフルなファイアウォール機能を有し、送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポートを組み合わせたアクセス制御ポリシーが 10000 以上設定可能であること。
④　送信元 NAT、送信先 NAT、IP マスカレード機能を有すること。
⑤　ファイアウォールのスループットとして 8Gbps 以上、ファイアウォール同時セッションとして２M 以上を有すること。
⑥　アンチウイルス機能を有し、フローベースの処理で 1.2Gbps 以上のスループットを有すること。
⑦　シグネチャ型侵入検知・防御機能（IPS）を有し、2.2Gbps 以上のスループットを有すること。
⑧　ログ採取機能を有すること。
⑨　タグ VLAN 機能を有すること。
⑩　冗長化機能とすること。
⑪　Web ブラウザを利用した日本語表示での管理が可能なこと。
⑫　管理/運用機能として SNMP エージェント機能（Query 応答、Trap 送信）及び TELNET、SSH 機能を有すること。
⑬　EIA 規格準拠 19 インチラックに搭載可能なこと。
⑭　調達機器との接続に必要なケーブル類を含むこと。
⑮　仮想 UTM 機能を有すること。
⑯　IPS、アンチウイルス、スパム対策等の UTM の機能を運用期間中（令和 8 年 3 月まで）使用できる権利を含むこと。
⑰　運用期間中（令和 8 年 3 月末まで）のハードウェアのメーカ保守を含むこと。

5.2.6. 新庁舎コアスイッチ、サーバスイッチ、フロアスイッチ仕様

コアスイッチ及びサーバスイッチ、フロアスイッチは、エッジスイッチ及び無線 LAN アクセスポイントの接続を考慮して、レイヤ３スイッチとレイヤ２スイッチによる最適とされる構成とすること。調達機器との接続に必要なケーブル類を含むこと。

① EIA 規格準拠 19 インチラックに搭載可能なこと。
② 電源冗長化構成が可能であること。また、活性交換が可能なこと。
③ 提案構成あわせて、1Gbps/10Gbps イーサネットまたは FCoE を適宜サポートすること。
④ １筐体あたり、提案構成にあわせて 24 ポート及び 48 ポート以上の 10/100/1000BASE-T インターフェースを有すること。
⑤ １筐体あたり、提案構成にあわせた SFP+インターフェースを有すること。
⑥ IEEE802.1q VLAN Tagging に準拠していること。
⑦ IEEE802.1d に準拠したスパニングツリー機能、IEEE802.1w に準拠した高速スパニングツリー機能、及び IEEE802.1s に準拠した多重スパニングツリー機能を有すること。
⑧ IEEE802.3ad Link Aggregation 機能を有すること。
⑨ IEEE802.1p の優先制御機能を有すること。
⑩ ループ検知機能、ストーム制御機能を有すること。
⑪ スイッチの追加等によりルートブリッジが変更されてしまう事態を防止する機能を有すること。
⑫ MAC アドレスと IP アドレスのマップをスイッチ上で管理することによって偽造 ARP(Address Resolution Protocol)による不正な通信盗聴を防止できること。
⑬ 特定のポートの DHCP スヌーピングを介して取得した IP アドレスのみを許可することで、不正な接続（IP なりすまし）を防止できること。
⑭ 将来、要求によって、IPv6 環境への移行が可能なこと。
⑮ トラフィック解析のためポートのミラーリング機能を有すること
⑯ NTP クライアント機能を有し、一貫したタイムスタンプを刻むことが可能なこと。
⑰ Syslog サーバにメッセージを送信可能なこと。
⑱ SNMPv1/v2/v3 による管理機能を有すること。
⑲ 自治体や公的機関への導入実績を有するメーカ・ベンダーの機種とすること。
⑳ 運用期間中（令和８年３月末まで）のハードウェアのメーカ保守を含むこと。

5.2.7. 新庁舎エッジスイッチ仕様

必要に応じて、調達機器との接続に必要なケーブル類を含むこと。

① インテリジェントレイヤ２スイッチ機能を有すること。
② インターフェースは 10/100/1000 BASE-T（RJ-45）×8 ポート以上有すること。
③ 10/100/1000 Mbps 自動認識機能を有すること。
④ ループ検知機能を有すること。
⑤ 同一ポートで 802.1x 認証、MAC アドレス認証、Web 認証および、それらを組み合わせたト

リプル認証機能をサポートしていること。また、認証されたユーザ及び MAC アドレスに対して VLAN をダイナミックに割り当てが可能なこと。

⑥ RADIUS 認証に対応もしくは EAP フレーム透過機能を有すること。EAP フレーム透過機能を有すること。

⑦ マグネット等で側面への設置が可能であること。または、調達にはマグネットを含むこと。

⑧ 静音性が考慮された機器であること。

⑨ 雷サージ対策が取られていること。

⑩ エッジスイッチから各端末まではカテゴリ 5e 以上の規格 UTP ケーブルを配線し各端末へ接続すること。なお、UTP ケーブルの配色については、本市と協議し決定していくこととする。

⑪ 運用期間中（令和 8 年 3 月末まで）のハードウェアのメーカ保守を含むこと。

5.2.8. 無線 LAN 仕様

必要に応じて、調達機器との接続に必要なケーブル類を含むこと。

サイトサーベイ作業を行い、コミュニティースペース、会議室等の配置構成及び各執務エリアに設置された端末台数を考慮し最適な設置場所と台数を決定すること。

(1) 無線 LAN のアクセスポイント仕様

① Wi-Fi 認定を取得し IEEE802.11a/b/g/n/ac の規格に準拠していること。

② ESS-ID ステルス機能を有していること。

③ IEEE802.3af 規格の PoE 受電に対応していること。

④ 動検知式の 10/100/1000BASE-T（RJ-45）イーサネットを 1 ポート以上有すること。

⑤ 無線 LAN のアンテナは内蔵していること。

⑥ 壁面や天井に設置された状態でも LED で稼働状態が識別できること。

⑦ PoE スイッチによる給電以外の方法にも対応していること。(例:PoE 給電アダプタ、AC アダプタ)

⑧ 動作時湿度は 10～90%の範囲内で、且つ結露しないこと。

⑨ RADIUS 認証に対応すること。

⑩ EAP フレーム透過機能を有すること。

⑪ 静音性が考慮された機器であること。

⑫ 雷サージ対策が取られていること。

(2) 無線 LAN コントローラの仕様

① 動的なチャンネル割り当て機能を有し、チャンネル干渉等の問題に自動的に対応し、解消する機能を有すること。

② 電波強度の自動調整機能を有し、問題が発生した場合も自動的に発見、対応し、解消する機能を有すること。

③ アクセスポイント間で自動的に負荷分散する機能を有すること。アクセスポイントの故障があった場合、電波が届いていないエリアを自動検出し、カバレッジホールを自動的に解

消する機能を有すること。

④ 上記 ①～③の機能に関し、常に監視を行い、最適な無線環境を自動的に維持できる機能を有すること。

⑤ 無線ネットワークへのアクセス制限機能を有し、ユーザ単位での設定が可能なこと。

⑥ IEEE 802.1X 無線 LAN 認証に対応すること。以下の EAP タイプに対応すること。

- EAP-TLS、
- PEAPv1/GTC、
- PEAPv0/MSCHAPv2

⑦ 認証サーバ（RADIUS サーバ）及び認証システムと連携できること。認証サーバ（RADIUS サーバ）と連携することにより、下位スイッチを IEEE802.1X を用いて認証する機能を有すること。かつ、サプリカントとして上位スイッチにて IEEE802.1X を用いて認証される機能を有すること。

⑧ IEEE 802.1X 認証に任意の複数回連続で認証失敗したクライアントの接続を拒否できること。接続拒否後、一定時間経過後、再度接続ができること。また、本機能は、SSID 毎に異なるポリシーを適用できること。

⑨ IEEE 802.1X 無線 LAN クライアント認証において、認証システムの片系統が障害等で利用できなくなった場合でも、正常に利用できる手段を提供すること。

⑩ クライアント側で意識せず、アクセスポイントを跨るローミングができること。

⑪ 無線 LAN クライアント間の通信をブロックすることが可能であること。

⑫ 1 台のコントローラで 10 台以上のアクセスポイントに対応できること。

⑬ 電波環境について、管理者が以下の情報を任意に参照できること。

- 通信負荷
- 電波干渉状況
- 電波雑音の影響度
- 接続しているクライアントの受信信号強度、信号対雑音比
- アクセスポイント間の影響度合い、影響範囲にあるアクセスポイントの列挙
- 許可されていない無線機器の列挙、無線環境に影響を与える要因の列挙

⑭ アクセスポイントの障害交換時及び新規増設時に初期設定を必要とせずに使用するための機能を有すること。

⑮ オフピークを含む無線非稼動時に電力消費を削減する機能を有すること。デバイスの消費電力を測定し、所定のルールに基づいてアクションを実行し、消費電力の調整機能を有すること。

⑯ IEEE802.1X 未対応端末に接続するため、VLAN 等の対応により安全性と利便性を確保できる機能を有すること。

⑰ 雷サージ対策が取られていること。

また、無線 LAN の管理として以下の機能を有すること。

① 無線 LAN システムの通信品質を評価してレポートする機能を有すること。

② 無線 LAN システムに接続しているユーザ情報を表示する機能を有すること。無線 LAN コ

ントローラで検知した不正 AP の情報を一元的に表示や分類する機能を有すること。
③ 無線 LAN システムにおけるゲストユーザアカウントや管理専用ゲストアカウントを作成する機能を有すること。
④ 無線 LAN システムへ接続するクライアント端末の認証ログ/アクセスログを収集し、出力する機能を有すること。
⑤ 無線 LAN システムの管理者アカウントに関するセキュリティ機能を有すること(管理者や接続端末の限定、利用者用ネットワークと管理用ネットワークの分離機能、複数の管理者登録機能、管理者パスワード変更機能等)。
⑥ 管理者アカウントの認証ログ及び操作ログを蓄積し、出力する機能も有すること。

5.2.9. 認証サーバ（RADIUS サーバ）仕様

① ネットワークログオン認証として、ネットワークサービス利用者のユーザ名・パスワード等を保持し、庁内ネットワークに接続する庁舎内及び外部拠点の端末、各フロアスイッチ及び無線 LAN アクセスポイント等のネットワーク機器へのアクセス認証可能な機能を有すること。
② ネットワークを介した端末への不正端アクセスを防止するため、接続可能な MAC アドレスの一元管理を行い、MAC アドレス認証を実現する機能を有すること。
③ IEEE802.1X 認証に必要な証明書の実装が困難な端末、プリンタ等も対象とすること。
④ CSV 形式のファイル等から RADIUS 管理情報（ユーザ ID、IP アドレス、パスワード、MAC アドレスなど）の一括登録が可能な機能を有すること。
⑤ エンタープライズ中間 CA は、耐障害性を考慮し、2 台構成とすること。
⑥ 無線 LAN コントローラの IEEE802.1X 認証(EAP-TLS 認証)の認証サーバ(RADIUS サーバ)として動作すること。なお、IEEE802.1X 認証（EAP-TLS 認証）対応したフロアスイッチ、エッジスイッチとも連携が可能であること。
⑦ 700 アカウント以上のユーザ情報の登録・管理が可能であること。
⑧ IEEE802.1X 認証に対応した証明書発行機能を有すること。また、証明書の発行は、Web ブラウザ経由で行うことが可能であること。
⑨ EAP-TLS、PEAP 等本業務で採用する規格は、WindowsOS・Active Directory との連携、無線 LAN 接続対象端末との親和性を考慮し、採用する証明書及び CA は、庁内ネットワークポリシー、セキュリティ、運用の容易性を総合的に俯瞰した上で、最適な方式とすること。
⑩ クライアント証明書の一括発行、失効、ダウンロードが可能であること。
⑪ 認証サーバとして、クライアント証明書の有効性を確認することができること。
⑫ 認証局(CA)として、クライアント証明書の失効リストを提供できること。
⑬ ActiveDirectory/LDAP サーバにあるアカウント情報を参照し、認証情報として利用することができること。

5.2.10. ネットワーク監視システム

ネットワーク監視システムは、新庁舎ネットワーク基盤を構成するネットワーク及びネットワーク機器の稼働状況監視、障害状況監視等を行う環境を提供する。ネットワーク監視システムの要求仕様は以下のとおりとする。

① 監視対象は以下とすること。
- 新庁舎移転後の新規ネットワーク関連機器（FW、スイッチ類、無線 LAN アクセスポイント等）

② 本業務で導入し監視対象とする機器に対し、ネットワークの死活監視、各種状態監視、障害や不正アクセス等の予兆監視を行うこと（監視対象それぞれの管理ソフト等を使用して監視を行う場合は、それらの管理ソフト等からの通知を本ネットワーク監視サービスで統合管理できること。

③ 以下の要件に従い、稼働状況監視ができること
- 監視対象の接続構成について担当職員でも容易に把握できる画面インターフェースであること。
- ネットワーク機器の死活監視（サーバ、装置のハードウェア監視も含む）ができること。

④ 以下の要件に従い、障害状況監視ができること。
- ネットワーク機器のイベントログのエラーメッセージ監視ができることが可能なこと。
- ネットワーク機器等を SNMP TRAP により監視できること。
- 障害発生時の検知から原因特定、影響範囲等を把握できるネットワーク管理を行うことが可能であること。

⑤ マップ表示機能として監視対象機器のインターフェース、サービス、リンク等の状態変化があった場合は、色や形状の変化等で確認できること。

⑥ 監視対象機器の使用率データをオンライン（管理サーバ上、閲覧可能）2 週間以上、オフライン（バックアップサーバ上）で１カ月以上保持すること。

⑦ 主要機器（ファイヤーウォール等）アクセスログについては、オンライン（管理サーバ上、閲覧可能）で 3 カ月以上、オフライン（外部媒体）で１年以上保持すること。また、本市の求めに応じてログの分析が可能であること。

⑧ 障害等発生時に、メールの他、ブザーまたはパトライト等による発報手段を有すること。

⑨ 各種パフォーマンスレポート出力できること。レポートを利用して情報システム係職員への月次報告を行うこと。レポートが全て英文である等分かりづらい場合は、事業者にて分かりやすい形への加工あるいは解説を行うこと。

⑩ ログ管理機能として、インシデントの早期発見、分析、対策立案を行うため、ファイアウォール、各種スイッチ、無線 LAN 機器の各種ログ情報を取得できること。

5.3. 監視カメラシステム

屋外カメラ、屋内カメラも設備工事業者側であらかじめ敷設された配管に必要な通信ケーブルの配線を

行うこと。

5.3.1. 屋外カメラ

① 屋外の監視カメラとして、駐車場に２台設置し、駐車場の安全な運用管理を可能とする超低照度カメラとすること。

① 最低被写体照度としてカラー：0.015 lux 以下に対応すること。 ② 屋外カメラとして以下の機能を有すること。 ・ 逆光、教法補正機能、霧補正機能を有すること。 ・ 6.5～143mm、光学ズーム２２倍のレンズを有すること ・ 撥水タイプとすること。 ③ パン範囲は 360°（エンドレス)とし、パン速度は 0.1°/s～240°/s （プリセットスピード：300°/s)とすること。 ④ チルト範囲は-15°～+90°（オートリバース)とし、チルト速度は 0.1°/s～160°/s （プリセットスピード：240°/s)とすること。 ⑤ 消費電力：47W 以下とすること. ⑥ 動作環境として、動作温度：-40℃～+70℃、動作湿度は 10%～95%（結露しない）とすること。

5.3.2. 屋内カメラ

屋内カメラとして、庁舎１階へ１１台、２階へ４台、３階へ２台設置すること。

うち、屋内 PTZ カメラを１階総合受付窓口近くに１台設置し、その他は屋内ドームカメラを設置すること。

① 屋内ドームカメラの仕様は以下とする。 ・ 最低被写体照度：0.012 lux(カラー)、0.006 lux（黒）以下 ・ ダイナミックレンジ：144 dB 以上 ・ 画角：【水平】30°（TELE）～110°（WIDE)【垂直】17°（TELE）～59°（WIDE）程度 ② PTZ カメラの仕様は以下とする。 ・ 最低被写体照度：0.015 lux(カラー)、0.006 lux（黒）以下 ・ ダイナミックレンジ：144dB 以上 ・ 画角：【水平】3.5°（TELE）～74°（WIDE)【垂直】2.0°（TELE）～42°（WIDE）程度 ・ 回転範囲：【水平】0°～350°【垂直】-3.0°～90° ③ 移動する人の識別性が向上する識別向上機能を有すること。

5.3.3. ネットワークビデオレコーダ

監視カメラの映像を記録するネットワークビデオレコーダの仕様は以下の通りとする。カメラ操作や映像再生機器等の設置管理は警備室で行えるようにすること。

① 標準８台のカメラ接続が可能なこと。 ② 録画・再生機能として、録画圧縮方式は H.265 以上を有し、PC を使用せずにカメラ操作、録

画映像の再生を可能とすること。
③ 最大１６画面の分割表示を可能とし、全画面表示切り替え時には最大 32 画面分割表示ができること。
④ 最適な画質により、２～３週間程度の映像保存が可能なこと。

5.4. 入
室管理システム

職員証 IC カードを利用できる入室管理システムを整備すること。
設備工事業者側であらかじめ敷設された配管に必要な通信ケーブルの配線を行うこと。
対象ゲートは１階（８扉）、２階（１１扉※サーバ室含む）、３階（４扉）とし、ゲートに設置されたブランクボックスに設置すること。

① IC カードは ISO/IEC 14443 TypeB または TypeC の方式に対応すること。
② 入室のみカードによる認証を行うが、緊急時及び非常時にカードを用いない入室方式についても明記すること。
③ 入室履歴をログデータとして保存可能なこと。
④ 電気錠は設備建築工事側の範囲となるが、カードリーダーとの動作連動について建築事業者と別途協議すること。

5.5. その他

5.5.1. 建物安全度判定サポートシステム

① 地震時に建物の揺れを計測し、建物の安全度を判定するための情報（建物安全度判定情報）を提供すること。
② 建物の揺れを計測するセンサーは加速度計（上下１成分、水平２成分）を用いること。
③ 地震の収束後速やかに建物安全度判定情報の提供が可能なこと。
④ 地震計測ごとに計測開始時刻（年月日含む）を収録装置に保存できること。（クラウド利用を含む）
⑤ 建物安全度判定情報をメール等により通知可能なこと。
⑥ 災害発生時でも、建物安全度判定情報の提供が可能なこと。

5.5.2. 気象情報観測システム

① 建物における風向･風速および雨量を気象情報として提供すること。
② 災害発生時でも、気象情報の提供が可能なこと。

5.6. 各種非機能要件

新庁舎ネットワーク基盤における各種非機能要件・前提条件を以下に示す。

5.6.1. 各非機能要件定義の前提条件

5.6.2. 稼働時間

業務にて新庁舎ネットワーク基盤を利用する時間（以下「オンライン稼働時間」という。）は以下のとお

りとする。ただし、計画停止時間を除く。

稼働時間

		通常時利用時間帯
稼働時間	平日	24 時間（計画停止を除く）
	土日、祝祭日	

5.7. システム運用管理要求仕様

5.7.1. 前提条件

新庁舎ネットワーク基盤を安定して提供するため、原則全てのネットワーク関連機器について、各ハードウェアの挙動を監視すると共に、障害発生時の検知から原因特定等を速やかに把握できるネットワーク運用管理を行うこと。

5.8. 信頼性要求仕様

5.8.1. 稼働率

新庁舎ネットワーク基盤として、可用性の高い冗長構成とすること。主要サービスの稼働率は定期保守による停止、自然災害による停電、回線事業者に起因するネットワーク停止等の事態を除き、以下表記載の数値を目安とすること。冗長化構成でサービス継続している場合の１系故障等は稼働と見なす。

サービス	目安となる稼働率
ファイアウォール コアスイッチ サーバスイッチ フロアスイッチ RADIUS サーバ 監視カメラシステム 入室管理システム	99.9%以上
その他のシステム	99.5%以上

5.8.2. 障害時対応手順の策定要件

障害時対応手順の策定についての要件は以下のとおりとする。

障害対応手順の策定要件

要素	要件
障害時運用手順	障害時の連絡体制・対応フロー等を定めて、運用作業手順書に記述すること。運用作業手順書は、運用設計段階において作成し、総合テスト及び運用テストを通じて手順の検証を行うこと。
被災を想定した手順	本市が指定する想定災害に対して、復旧手順を策定すること。復旧手順は本市担当職員が理解、作業が可能なものとすること。

5.9. 性能要求仕様

新庁舎ネットワーク基盤に係る性能要件は以下のとおりとする。

性能要件

要素	要件
拡張性	使用期間中に見込まれる、利用拠点の拡大、利用者及び端末数の拡大に伴うデータ量、ネットワーク接続機器の増減に対して、システムパフォーマンスが劣化しないように、十分と考えられる性能を確保した機器とすること。

5.10. 使用性・効率性要求仕様

新庁舎ネットワーク基盤に係る使用性・効率性要件は以下のとおりとする。

(1) 使用性・効率性要件

要素	要件
ユーザインターフェース等	・ 運用管理画面において、各システムの画面構成、画面遷移及び入出力操作方法に一貫性があること。 ・ 日本語に対応した画面や直感的に操作しやすい画面により、管理の負荷が軽減できること。

5.11. セキュリティ要求仕様

5.11.1. セキュリティ要件全般

新庁舎ネットワーク基盤は、機密性、秘匿性の高い情報を管理する。よって、情報資産の「機密性」、「完全性」及び「可用性」を維持するため、設計から構築、運用における各工程における「技術的脅威」、「人的脅威」及び「物理的脅威」に対して安全管理措置等の対策を講じること。新庁舎ネットワーク基盤におけるセキュリティ要件は以下のとおりとする。

セキュリティ要件一覧

要素		要件
機密性	認証	・ アクセスを許可されたユーザに対しての権限管理を行う機能を設けること。なお、権限管理の最小単位は利用者 ID 単位とし、本庁及び事業者の職員、所属部課等によって権限を設定すること。 ・ 権限管理については、Active Directory 等によって設定されたユーザ権限と連携すること。
	ログ	・ システムログの参照や消去等にあたっては、システム管理権限等により閲覧者を限定できること。
完全	対策基準・実施手順の策定	・ 本市の規定類を遵守し、各システムにおける各工程のセキュリティ対策基準、セキュリティ実施手順を策定すること。

要素		要件
	セキュリティ運用	・継続的にセキュリティが確保されるよう、PDCA サイクルで管理運用を行い、セキュリティレベルが低減することのないように取組むこと。
	ログ	・システムログ及びアプリケーションログを取得し、取得したログの漏えい、改ざん、破壊等を防止できる機能を設けること。
	不正侵入・不正利用の防止	・庁外からの不正な接続及び侵入、市民情報を含む行政情報資産の漏えい、改ざん、消去、破壊、不正利用等を防止するための対策を講じること。
	ウイルス対策	・サーバ環境は、アンチウィルスソフトウェア等を活用して、不正プログラム対策を実施できること。
可用性	監視	・セキュリティ機能の稼働状況を監視し、必要に応じて警告等を発する機能を設けること。

5.12. ハードウェア構成仕様

本業務で構築する新庁舎ネットワーク基盤で調達するネットワーク機器、その他安定稼働に必要となるハードウェア等について、ハードウェア及びシステム構成を明示すること。

6　構築関連要件

新庁舎ネットワーク基盤を遅滞なく構築するために必要となる本業務の要件を以下に示す。

6.1. プロジェクト管理要求仕様

事業者は「計画」「遂行」「リスク管理」を適切に行い、スコープやスケジュールに基づいて的確に各業務を実施し、本業務全体をプロジェクトとして成立・成功させること。また、本業務の推進にあたり、プロジェクト計画書を策定し、プロジェクト計画書に規定するプロジェクト管理方針に基づいたプロジェクト管理を実施すること。

なお、本業務の確実かつ円滑な遂行にあたって、必要なスキル及び経験を有するメンバーを配したプロジェクト体制を整えること。

6.1.1. プロジェクト計画書の策定

事業者は、本書記載事項に基づき、システムの構築における具体的な体制、スケジュール、プロジェクト管理方針、品質管理方針、プロジェクト管理方法等を含んだプロジェクト計画書を作成の上、その内容について本市の承認を得ること。

6.1.2. プロジェクト管理

事業者は、作成し承認されたプロジェクト計画書に基づき、プロジェクト管理を行うこと。プロジェクト管理を行うための様式、報告項目について、事前に本市に提示の上、承諾を得ること。また、会議体を設置して、定期的な報告を実施すること。事業者は、本市と事業者に係るメンバー間のコミュニケー

ションツールを用いて、本業務に携わる全てのメンバーに対して情報・データ共有や会議開催周知等が迅速且つ効率的に行えるようにすること。プロジェクト管理項目は以下のとおりとする。

(1) プロジェクト管理要件一覧

管理項目	管理内容
進捗管理	・プロジェクト計画策定時に定義したスケジュールに基づく進捗管理を実施すること。 ・事業者は、実施スケジュールと状況の差を把握し、進捗の自己評価を実施し、定例報告会において本市に報告すること。 ・進捗及び進捗管理に是正の必要がある場合は、その原因及び対応策を明らかにし、速やかに是正の計画を策定すること。
品質管理	・プロジェクト計画策定時に定義した品質管理方針に基づく品質管理を実施すること。事業者は、品質基準と状況の差の把握、品質の自己評価を実施し、各工程完 ・了報告会において本市に報告すること。 ・品質及び品質管理に是正の必要がある場合は、その原因と対応策を明らかにし、速やかに是正の計画を策定すること。
変更管理	・仕様確定後に仕様変更の必要が生じた場合に、事業者はその影響範囲及び対応に必要な工数等を識別した上で、変更管理ミーティングを開催し、本市と協議の上対応方針を確定すること。

また、事業者は、定期報告の会議体として市が定める「定例報告会」「工程完了報告会」「作業部会」等の定例会に必要に応じ参加することとし、市の要請に応じて、必要な報告書類を会議開催の前日までに作成、本市担当職員へ送付の上、会議終了後、会議内容（議事録等）を書面で本市へ報告し、その了承を得ること。

なお、規定した以外の会議が必要な場合、適宜必要な会議を開催すること。

6.1.3. プロジェクト体制

本業務の遂行にあたっては、必要なスキル及び経験を有するメンバーを配したプロジェクト体制を整えること。また、プロジェクト責任者並びに本システムの設計・構築業務、テスト業務、システム切り替え業務、研修業務及び保守業務等の各領域別に責任者を定めること。（業務に支障を与えない限り、責任者の兼任は可能とする）上記に加えて、プロジェクトを推進する上で必要なセキュリティの管理体制を整え、情報セキュリティ対策状況を管理する責任者を定めること。

6.1.4. メンバースキル

本書に定める全作業内容を理解し、実施するために必要な知識、能力を有すること（知識及び能力に応じた作業者の定義は下記スキル要件一覧のとおりとする）。

なお、本プロジェクト全体の統括責任者及び各業務領域の責任者を必ず配置し、必要に応じて作業者を指示するリーダーを配置すること。

(1) スキル要件一覧

メンバー	スキルの詳細
プロジェクト管理能力を有する者（プロジェクト責任者）	・プロジェクト実施計画を策定し、システムの設計・構築、テスト、システムの評価及びプロジェクト間の調整を行い、生産性及び品質の向上に資する管理能力を有すること。 ・人口 5 万人以上の地方公共団体、職員 700 人以上の法人格を有する組織等におけるネットワーク基盤のプロジェクト経験を有すること。
品質管理能力を有する者	・事業者の品質管理規準に従い、プロジェクトを離れて第三者的かつ客観的に、プロジェクト全般の品質状況を監査し、評価・改善する能力を有すること（事業者内の品質管理組織でも構わない）。
新庁舎ネットワーク基盤に関する知識を有する者	・運用管理についての専門知識と評価、改善技術を理解した上で、新庁舎ネットワーク基盤を実現するために最適なネットワーク構成の設計・構築・運用技術及び技術コンサルティング能力を有すること。

なお、本業務における事業者におけるメンバー選定においては現時点において人事異動や他プロジェクトへの引抜きのリスクが無く、システム構築完了まで本業務に従事できるメンバーを選定すること。やむを得ずプロジェクト発足時からの要員変更を実施するにあたっては、変更後の要員のスキルが前任者と同等以上であることを証する書面を本市に提出の上、必ず事前に本市の了承を得ること。

6.2. システム設計等要求仕様

本書に記載された各種要件に基づき、各種設計、運用・保守設計等を実施すること。また、本システムの稼働に適したネットワーク及びシステムの仕様を確定し、必要な設定を行うこと。
なお、設計・構築に係る成果物の作成や本市への各種報告においては、設計・構築手法及びその結果について本市が容易に理解できるようにすること。

6.2.1. 設計・構築手法

設計・構築手法の要件は、設計・構築手法要件一覧のとおりとする。

(1) 設計・構築手法要件一覧

要件	内容
設計（構築）方針	構築するサービスは長期間運用することを前提として、機能拡張性及び保守性の高いシステムとすること。 本業務で導入するネットワーク、及びシステムに加え、既設の業務システムが確実に動作する環境を構築すること。

要件	内容
設計（構築）手法	本業務の各工程を網羅し、品質の確保とスケジュールの短縮を図ることが可能な設計（構築）手法であること。 本業務に適用する設計（構築）手法について、他案件での適用実績を有すること。 本業務に参画するメンバー全員が、適用する設計（構築）手法に精通していること。 本市の業務を中断することなく、新庁舎へのシステム移行について実現可能な構築手法を用いること。
ハードウェア・ソフトウェア仕様策定	ハードウェア及びソフトウェアについては、本業務の要件を満たす最適なハードウェア及びソフトウェアの仕様を策定すること。 (ｱ) 仕様策定したハードウェア等のスペック等が妥当である根拠が明確であること。 (ｲ) 仕様策定における性能的な根拠を付すること。 (ｳ) 本書の各要件（特に非機能要件）を十分理解した構成とすること。 (ｴ) ソフトウェアライセンス数が過大又は過小にならないよう、本書の各要件を十分理解して仕様策定すること。
構築に必要となるソフトウェア、及びラインセス	本システムの構築を遂行するために必要となるソフトウェア。及びライセンス等に関しては必ず有し事業者において準備すること。

.

6.3. テスト要求仕様

各種テストの実施にあたっては、適時適切なタイミングで、テスト実施体制と役割、作業及びスケジュール、テスト環境、テスト方法、テストデータ等についての検討を実施した上で、工程別に必要なテスト計画書、仕様書等を作成し、当該成果物に基づき適切に実施すること。テストの結果は、本市がテスト結果を判断可能な形で報告すること。

6.3.1. テスト方法

事業者は、事前に各関係者の役割分担をテスト計画書にて明確化した上で、各種テスト計画書等に基づいて、各種テストを主体的に実施すること。テストにおいて、エラー及び障害発生を確認した場合は、必要に応じて本市へ報告を行った後、復旧作業を行うこと。また、性能面での問題が発生した場合には、必要なチューニング措置を施すこと。

6.3.2. 品質判定基準

システムテスト工程における品質判定は、定性的基準、端末動作確認結果等、各テスト結果から総合的に判断する。品質判定基準表は品質判定基準表のとおり。

(1) 品質判定基準表

品質判定項目	内容
定性的基準	・システム機能、システム連携等の各テストが完了しており、不具合及び障害については全て解消し、正しくテストが実施されたことが実証されていること。 ・課題／問題管理表の対応が完了していること（やむを得ず完了しない課題は、影響範囲、期限等を明確に示し、本市の承認を得ること)。 ・システムテスト時の指摘事項、対応内容に対する外部仕様書、操作マニュアルへの反映が完了していること（設計品質の確保)。
負荷テスト	・負荷試験では､運用上の性能が十分業務に支障のない性能であることを実証すること。 ・

6.4. システム移行支援仕様

新庁舎引き渡し後の各種システム及び端末の移行に際して、本市との協議の上、適時適切なタイミングで、既存システムを提供する各社の移行範囲、移行実施体制と役割、作業及びスケジュール、移行環境、移行対象、移行方法及び検証方法等について、必要に応じて支援すること。

(1)移行準備

ネットワーク体系への影響が想定される移行が必要なデータ（アカウント情報、利用者のプロファイル情報、各部課の共有フォルダに保存された電子データ等）を選別・分析し、作業に必要となる設計資料等の作成を行う場合、必要に応じて支援を行うこと。

(2)移行時期

令和 3 年度以降に実施し、ネットワーク体系への影響が想定される各社が実施するデータ移行の整合性確認、動作確認等の作業について、本市と協議の上、必要に応じて支援すること。

7　保守運用要件

新庁舎ネットワーク基盤に係る開庁初年度の運用保守業務（以下「運用保守業務」という。）は以下に示すとおりとする。また詳細な実現方式・仕様については本書内の該当章を参照すること。
なお、運用保守業務は本市業務の根幹を担うものである。よってこれらの特性によりシステム的・運用的に問題が生じないよう各保守運用業務で適切な措置を取ること。

7.1. 保守作業要求仕様

7.1.1. 保守作業一覧

開庁初年度における、新庁舎ネットワーク基盤に係る保守作業の要件は下記保守作業一覧のとおりとする。

保守作業一覧

作業名	作業内容
ハードウェア設定の変更・追加・削除、ハードウェアの交換	定期点検、障害対応、その他原因に基づくネットワークおよび本調達システムの設定変更・追加・削除及びハードウェアの交換作業の実施。
ファームウェア、ソフトウェア設定の変更・追加・削除、ファームウェア、ソフトウェア再インストール等	定期点検、障害対応、その他原因に基づくファームウェア、ソフトウェアの設定変更・追加・削除及び再インストール作業の実施。
ファームウェア、ソフトウェアバージョンアップ	ファームウェア、ソフトウェアのバージョンアップに係る関係者（本市、本システム構築範囲内のシステム・メーカ及び構築範囲外のシステム・メーカとの調整、仕様検討及び決定、本市担当職員への説明、適用作業及びテストの実施。
ソフトウェアバグの対応	ファームウェア、ソフトウェアバグに起因する修正プログラムの検証及び適用作業の実施。
各保守作業に伴うドキュメントの更新作業	各保守業務に伴い変更が発生した場合のドキュメントの更新作業及び運用変更を行った際のドキュメントの更新作業の実施。

7.1.2. 運用保守時間と作業概要、作業実施者の内訳

運用保守時間及び作業実施者等を運用保守時間と作業概要、作業実施者の内訳を提案書に示すこと。

運用保守時間と作業概要、作業実施者の内訳

項目	対応時間	運用保守概要	作業実施者
ハードウェア、保守業務	平日 8:30～17:30 （部品交換、代替機対応等について、原則午前中受付分は当日オンサイトとする。対応にあたりオンライン業務に影響を与える場合は、オンライン稼働時間外に対応すること。）	調達するハードウェアメーカの保守サービス対応 事業者による部品交換、代替機対応等保守作業	本業務事業者
ソフトウェア保守業務	平日 8:30～17:30 （構成変更について、対応にあたりオンライン業務に影響を与える場合は、オンライン稼働時間外に対応すること。）	調達するソフトウェアメーカの保守サービス対応 事業者による設定変更、再インストール等対応等保守作業	本業務事業者

項目	対応時間	運用保守概要	作業実施者
システム運用業務	平日 8:30～17:30	システムの正常稼働を維持するための運用作業及び主管課依頼事項等の対応を行う	本市情報システム係
ヘルプデスク業務	平日 8:30～17:30	本市情報システム係からの問い合わせ対応	本業務事業者
障害対応時間	24 時間 365 日	新庁舎ネットワーク基盤に障害が発生した場合の復旧対応	本業務事業者

7.1.3. 作業実施計画書に基づく管理

本業務の事業者が、運用保守計画書に予め決められた作業の他に、新庁舎ネットワーク基盤の運用保守作業又は本市からの依頼作業を実施する場合は、作業内容や作業実施日時を記載した作業実施計画書を事前に提出すること。また、作業完了後は、作業結果報告及び成果物を本市へ引き渡すこととする。システムに対して計画外の作業を行う場合も、作業実施計画書により本市へ報告を行い、承認を得るものとする。これら作業実施に関するフロー及び定型様式は、本業務における運用保守設計において定義すること。運用保守業務は、運用保守設計に基づき日々の運用保守作業を実施するものとし、作業内容は必ず手順化すること。作業前には作業手順を本市へ明示し、承認を得ること。

7.2. 運用作業要求仕様

7.2.1. 運用作業要件

新庁舎ネットワーク基盤における開庁初年度における運用作業の要件は運用作業一覧（該当部分に〇がある作業は本業務事業者にて実施）のとおりとする。

なお、該当部分に〇がない作業についても、適宜、最適な改善提案等を行うとともに、作業に関連してシステム障害等が発生した場合には、業務に支障をきたすことのないよう対応支援を行うこと。

運用作業一覧

作業名	作業内容	該当
運用報告会の開催	保守実績、運用実績、障害報告、問い合わせ対応等運用保守に係る報告書の作成と報告会議を開催すること。	〇
改善提案	日常運用保守業務から導き出される改善提案があれば実施すること。	〇
セキュリティ対応支援	セキュリティインシデント発生時に本市と協議の上対応支援を行うこと。	〇
他システムリプレ	構築範囲内のネットワークへの影響について情報提供を行う。	〇

ース、新規システム導入支援等	構築範囲内のネットワークについて設定変更を実施する。	○
	他システムリプレース､新規導入に関わる障害対応を支援する。	○
監視	機器の停止や異常の早期発見のため、ネットワーク監視システムによる、ネットワーク機器の死活監視、サービス監視、SNMPトラップ監視を行う。	
	異常を検知した場合は､各システムの運用手順書や簡易手順書、一時切り分け書等に従い対応を行う。	
	機器の入れ替え等が行われた場合、ネットワーク監視システムに登録を実施する。	○
構成管理	ネットワーク関連機器（スイッチ類、ファイアウォール、ルータ、無線 LAN アクセスポイント）の構成管理（設定状況やインストールされているソフトウェアの記録管理）を行う。	○
アカウント管理	システム及びネットワーク運用保守用のアカウント管理(参照、登録、変更、削除）について最適な管理手法について提案を行うこと（グループポリシー含む。）	○
	システム及びネットワーク運用保守用のアカウント管理(参照、登録、変更、削除）作業の実施及び年度更新作業の実施（グループポリシー含む。）。	
運用管理方式の変更対応	運用保守設計の見直し、変更の承認依頼及び変更作業の手順化の実施。	○
その他	法定停電対応、作業後の正常性確認 ※サービス稼働後、初回の法定停電及び作業後の正常性確認対応については、本市への引き継ぎを兼ねて対応を行い、作業手順書を作成すること。	○

7.3. 障害対応要求仕様

開庁初年度における新庁舎ネットワーク基盤の運用における障害対応作業、各種コンティンジェンシープランについて提示すること。要件については以下障害対応要件一覧のとおりとする。

(1) 障害対応要件一覧

作業名	作業内容
障害要因特定作業	障害一次切り分け作業の結果に基づく障害要因特定作業の実施。
障害復旧管理	障害復旧までの体制、作業に係る一連の管理業務の実施。(報告、連絡、相談等)。

作業名	作業内容
障害復旧作業	障害復旧作業の実施。
エスカレーション対応	各メーカ等へのエスカレーション対応。
その他障害復旧に必要な作業	障害連絡、報告等、その他各種障害要因に応じた障害復旧に必要な作業。（コンティンジェンシープラン作成含む）

7.4. 業務継続に係る要件

開庁初年度において、本業務の事業者はシステムの業務継続性確保のために、業務継続対応要件一覧に示す各項目に定めた内容を遵守すること。

(1) 業務継続対応要件一覧

要素	要件
参集	本市において震度 5 弱以上が計測された場合、新庁舎ネットワーク基盤の動作状況、1 次切り分け、簡易復旧（リブート等）程度が実施可能な者を、1 名以上で本市庁舎内へ参集させること。
情報資産台帳の作成	新庁舎ネットワーク基盤構築時は、本市が提示するフォーマットに基づき情報資産台帳を作成し、資源の追加、変更、削除等にあたって常に最新の状態として管理できるようにすること。
訓練への参加	外的脅威によりシステム停止した場合の復旧訓練等に参加し、各種復旧作業を本業務の範囲内で実施すること。

８　成果物一覧

下記表以外の成果物（完成図書）について、必要に応じて本市と協議の上、提出すること。

想定成果物一覧

No.	成果物	内容
全般		
1	設計概要・導入方針	構築後の庁内ネットワーク全体の概要、再構築により実現される通信環境の機能改善、品質の向上などを記載すること。
物理設計		
1	機器一覧	導入する機器に関して、機器種別や設置場所等を一覧化し記載すること。
2	機器仕様	本仕様書の内容に対応していることを示す機器仕様を製品カタログ等から抜粋、要約し、記載する。
3	機能仕様	機能仕様を製品カタログ等から抜粋、要約し、記載すること。
4	ネットワーク構成	庁内全体のネットワーク構成図を記載する。 物理ネットワーク構成図を記載すること。
5	収納 BOX 内・ラック配線	導入機器を設置する、マシン室のラック、各フロアの HUB BOX 内の LAN・電源配線・スイッチポート収容等を記載すること。
論理設計		
1	IP アドレス設計	IP アドレス設計や、各機能に設定するネットワーク情報（設計仕様）を記載する。 論理ネットワーク構成図を記載すること。
2	ルーティング設計	ルーティング設計や、各機種に設定するルーティング情報（設計仕様）を記載すること。
3	ネットワーク認証設計	ネットワーク認証設計や、各機種に設定するネットワーク認証情報（設計仕様）を記載すること。
4	監視ネットワーク設計	ネットワーク機器の監視ネットワーク設計仕様や、各機器に設定する設計仕様を記載すること。
5	セキュリティ設計	ネットワーク機器のセキュリティ設計仕様や、各機器に設定する設計仕様を記載すること。
信頼性・品質保証設計		
1	機器冗長設計	各機器障害に対応する冗長設計等の信頼性設計情報を記載すること。
2	経路冗長構成	各機器の経路障害に対応する冗長設計等の信頼性情報を記載し、障害時の迂回経路等を記載すること。
3	電源冗長設計	各機器の電源障害に対応する冗長設計等の信頼性設計情報を記載する。
4	帯域保証設計	各機器の帯域制御（IP 電話等一定量以上の通信品質確保に対する制御設定など）に対応する設計情報を記載すること。

No.	成果物	内容
移行設計		
1	機器移行方針	各機器の移行方針及び導入スケジュールを移行計画として記載すること。
2	作業工程	機器毎、拠点毎等に応じた、移行作業工程（手順書）を記載すること。
3	リスク対応	上記作業工程中で発生し得るリスク（想定される影響など）及び、本市が対応するべき内容等を網羅的に記載すること。
構築、保守運用関連		
1	作業実施計画書	構築及び運用時において、作業内容や作業実施日時について記載すること。
2	運用保守計画書	保守実績、運用実績、障害報告、問い合わせ対応等運用保守について記載すること。
3	運用管理手順	日々の運用管理や障害等発生時に必要な手順を記載すること。
その他事項		
1	機器選定理由	納品する機器やソフトウェアとの選定理由を記載すること。
2	各種規則・ポリシー仕様	物理・論理設計に問わず、市の合意し実施する各種規則、ポリシー仕様を記載する。 （例）機器貼付けテプラシール記載ルール
3	研修資料	システム、ネットワーク管理者となる職員に対し、本市のネットワーク及び導入するシステムが理解できる資料
4	試験成績	構築完了を証する各システムや各機器等の試験を実施し、その成績結果の承認を受けた書面（試験成績・検査合格通知書）を完成図書にファイルし提出すること。
5	保守代行登録	メーカ５年間の保守登録を実施し、保証書または登録番号とその 登録機器名（シリアルNOも含む）を記載の一覧表を作成のうえ完成図書にファイリングし提出すること。