

水俣市自治体ネットワーク強靱化更新事業  
委託業務に関する要件仕様書

令和7年1月

水俣市

## 第1編 調達概要

### 1 件名

水俣市自治体ネットワーク強靱化更新事業委託業務（以下「本業務」という）

### 2 背景と目的

本市では、現行電算システムの機器の摩耗と老朽化に伴い、住民サービスの安定かつ持続可能な運営の観点から、令和7年度に対象機器の更新を実施する。また、平成27年に総務省によって示された「自治体情報システム強靱性向上モデル」に対し、その効果や課題、新たな時代の要請を踏まえ、令和2年に「自治体情報セキュリティ対策の見直しについて」として提言された新しいガイドラインに基づいて、新電算システムの調達、構築を本業務にて実施する。

電算システムの更新にあたり、以下を基本方針とする。

- (1) 住民サービスが低下することなく構築コストを低減すること。(①コスト低減)
- (2) 業務が中断することなく住民サービスを継続できること。(②耐災害性)
- (3) 総務省の「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」に準拠すること。(③セキュリティ強化)

### 3 契約期間

本業務は、次の2項目に分けて契約を締結する。

- (1) 水俣市自治体ネットワーク強靱化更新事業  
令和7年3月から令和8年3月31日まで（2年間の債務負担行為）
- (2) 水俣市基幹系及びインターネット接続系環境整備事業 運用保守業務  
令和8年1月1日から令和12年12月31日まで  
運用期間は5年間。ただし、運用期間の延長も想定する。

### 4 納入期限

前項3契約期間（1）の納入期限は、令和7年11月30日とし、令和7年12月1日から12月31日までの仮稼働期間後、令和8年1月1日から本稼働とする。

### 5 構築場所

水俣市役所  
受託者設備設置拠点

## 6 提案限度額

(1) 水俣市自治体ネットワーク強靱化更新事業 更新業務 100,000,000 円

(2) 水俣市自治体ネットワーク強靱化事業 運用保守業務 (5年間) 35,101,000 円

更新業務・運用保守業務の合計 135,101,000 円 (消費税及び地方消費税額を含む。)

なお、更新業務においては前記(1)に定める費用(消費税及び地方消費税額を含む。以下に同じ)の範囲内で令和7年12月1日から仮稼働、令和8年1月1日から本稼働とし、運用保守業務に係る費用(以下「保守料」という。)は本稼働日から発生するものとする。

保守料は、令和8年1月1日から令和12年12月31日までにおける60月分のサポート費用、機器保守料、通信運搬費等の維持管理費用とし、前記(2)に定める費用の範囲内とする。

## 7 契約方法

公募型プロポーザル方式による随意契約

## 第2編 調達範囲

### 1 実施する業務

本業務では図1 電算システムの現行構成に示すサーバ等の更新を実施するものとする。

※サーバ論理構成については図2に示す。

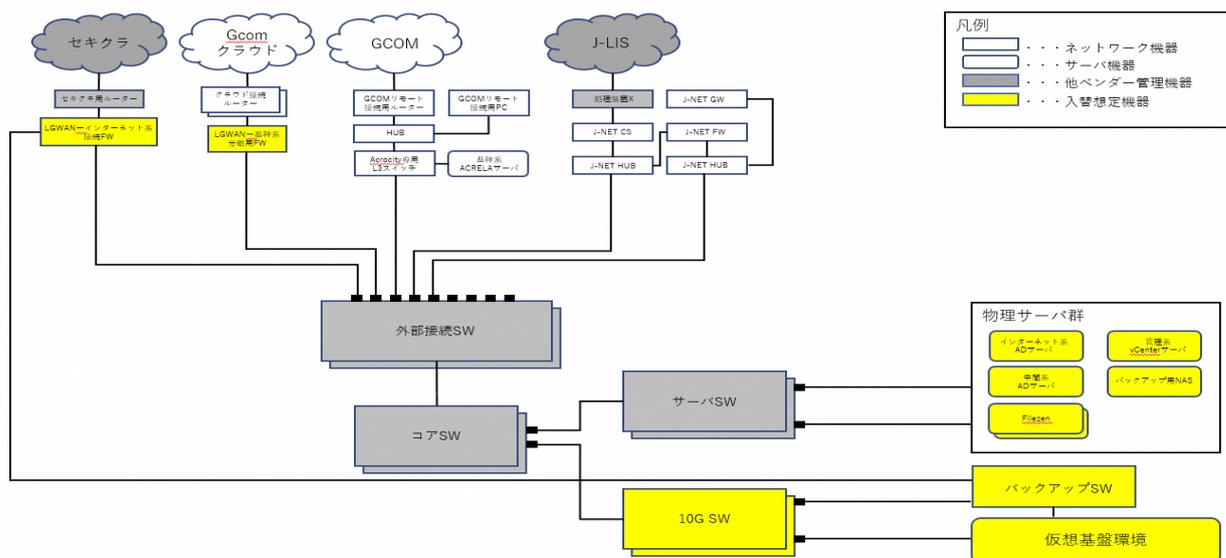


図1 電算システムの現構成と本業務対象範囲

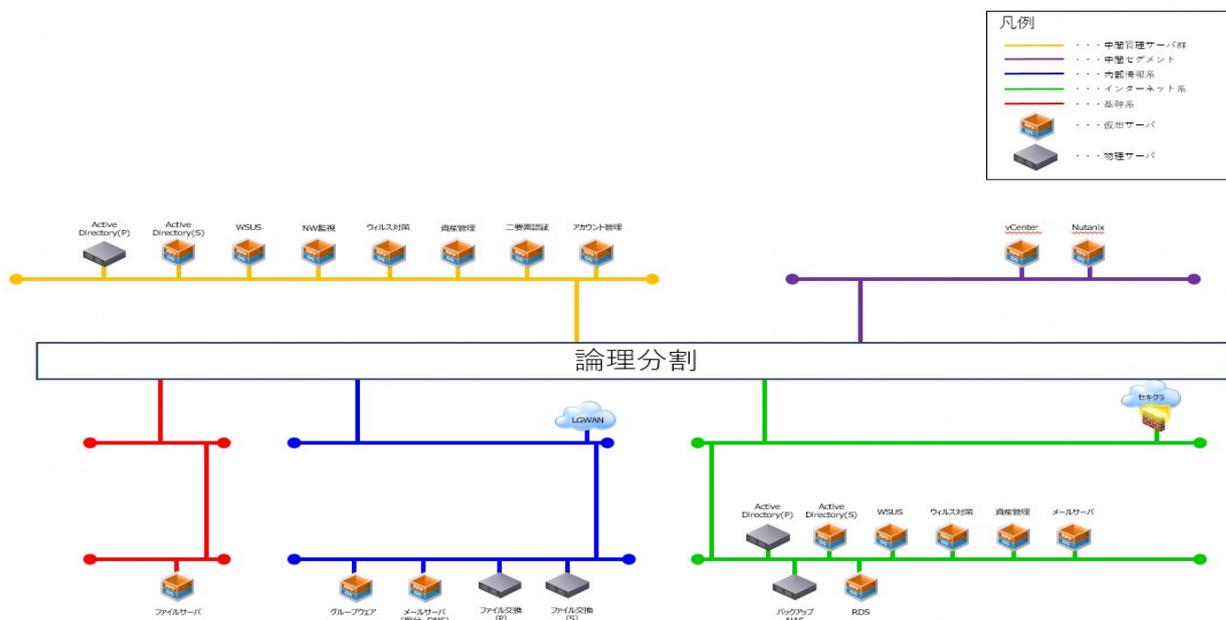


図2 サーバ論理構成

## 2 調達・構築範囲

本業務において更新・廃止・追加するシステム並びに、必要となるソフトウェア等の調達・構築範囲を表1のとおりとする。

表1 本業務における調達・構築範囲一覧表

項	対象の名称	種別	数量	備考
1	仮想環境基盤	調達・再構築	1 式	基幹系、インターネット接続系ネットワーク
2	中間系 ActiveDirectory	調達・再構築	2 台	1 台は物理サーバにて構築 もう一台は1の仮想環境上に構築 (冗長化想定)
3	中間系 WSUS	再構築	1 台	1の仮想環境上に構築
4	中間系 NW 監視	廃止		
5	中間系ウイルス対策 ライセンスは1年分	調達・再構築	1 台	1の仮想環境上に構築。必要に応じてライセンスを含めること 基幹系端末用 (120 台分) 2年目以降のクライアントライセンスは本市が別途調達する。
6	中間系資産管理 ライセンスは1年分	調達・再構築	1 台	1の仮想環境上に構築。必要に応じてライセンスを含めること 基幹系端末用 (120 台分) 2年目以降のクライアントライセンスは本市が別途調達する。
7	中間系二要素認証	調達・再構築	1 台	1の仮想環境上に構築。必要に応じてライセンスを含めること 基幹系端末用 (120 台分)
8	中間系アカウント管理	廃止		
9	基幹系ファイルサーバ	再構築	1 台	1の仮想環境上に構築
10	内部情報系グループウェア	調達・再構築	1 台	1の仮想環境上に構築。必要に応じてライセンスを含めること 外部デバイス (スマホ等) から利用可能なシステムであること。
11	内部情報系メールサーバ	調達・再構築	1 台	1の仮想環境上に構築。必要に応じてライセンスを含めること

1 2	内部情報系ファイル交換	調達・再構築	1 台	1 の仮想環境上に構築。再構築後は中間系に属し、無害化機能を付与
1 3	インターネット系 ActiveDirectory	廃止		
1 4	インターネット系 WSUS	廃止		
1 5	インターネット系ウイルス 対策	廃止		
1 6	インターネット系資産管理	廃止		
1 7	インターネット系メールサ ーバ	廃止	1 台	
1 8	バックアップサーバー	調達・再構築	1 台	1 の仮想環境上に構築。 再構築後は中間系に移動 バックアップソフトを含めること
1 9	RDS (リモートデスクトッ プ)	調達・再構築	1 台	1 の仮想環境上に構築。 内部情報系に構築し、出先拠点端 末からの接続用として 30 セッシ ョン Word, Excel, PowerPoint, Access を導入すること (30 ライセン ス)
2 0	インターネット系仮想ブラ ウザ	新規調達	1 台	1 の仮想環境上に構築。内部情報 系端末からのインターネット閲覧 用
2 1	監視サーバ	調達・構築	1 台	1 の仮想環境とは別のサーバまた はアプライアンスとして構築
2 2	Windows Server クライアントアクセス ライセンス	調達	1 式	基幹系端末 120 台 情報系端末 410 台 上記端末に対応したライセンスを 必要に応じ用意すること
2 3	LGWAN-インターネット系接 続 FW	調達・再構築	1 台	既存踏襲設計にて入替想定
2 4	LGWAN-基幹系分離用 FW	調達・再構築	1 台	既存踏襲設計にて入替想定

上記以外で提案するシステムに必要なソフトウェア、ライセンス等があれば調達範囲に含めること。

### 3 対象外システム

システムのうち、内部情報系ネットワークの各種システムは本業務の対象外とする。  
※ただし、グループウェア及びメールサーバは除く。

## 第3編 要求仕様

### 1 システムの要求仕様

システムの要求仕様として以下の項目について記載する。

※詳細な要件仕様については「【別紙3】機能要件書」を参照。

- (1) 仮想基盤の基本要件
- (2) 仮想基盤のハードウェアに関する基本要件
  - 1) 仮想基盤（ハイパーバイザー含む）
  - 2) バックアップストレージ
  - 3) 無停電電源装置
  - 4) KVM スイッチおよびコンソール
- (3) 各種サーバに関する基本要件
  - 1) Active Directory サーバ
  - 2) WSUS サーバ
  - 3) ウィルス対策サーバ
  - 4) 資産管理サーバ
  - 5) 2要素認証サーバ
  - 6) ファイルサーバ
  - 7) グループウェアサーバ
  - 8) メールサーバ
  - 9) ファイル交換・無害化サーバ
  - 10) RDS（リモートデスクトップ）
  - 11) 仮想ブラウザサーバ
  - 12) バックアップサーバー
- (4) 分離用FWに関する基本要件

#### (1) 仮想基盤の基本要件

- ・構成方式（HCI方式または3Tier方式）は問わないが、可用性・負荷分散・拡張性を考慮した設計でかつ耐障害性に優れたものを提案すること。構成

「【別紙 4】 参考 VM 配置図」を参照し十分なリソースを確保した仮想基盤を構築すること。その際、不足等があれば適宜リソースを追加し、安定稼働に向けて過不足が無いように提案を行うこと。

- ・耐障害性を考慮し、冗長構成を実現させること。
- ・仮想基盤内接続は 10G ネットワークにて構成し、冗長化を図ること。
- ・市内ネットワークの既存 L3 スイッチ（コアスイッチ）と冗長化構成で接続すること。接続は 10GBASE-SR とすること。  
 ※既存 L3 スイッチ（コアスイッチ）の品名・型番は Aruba8320 JL479A#ACF
- ・既存 L3 スイッチの SFP モジュール等を調達し設定すること。仮想基盤環境⇔既存 L3 スイッチ間のケーブル長は 5m 必要。
- ・市内ネットワークへ接続する場合には、三層分離（または総務省ガイドラインの新しいモデル）を維持する必要があるため、要件定義を入念に行い、本市の承認を得た上で、構成設計を行うこと。
- ・仮想化ハイパーバイザーの OS はサポート契約を有し、脆弱性等が発見された場合に必要に応じ、速やかにバージョンアップ等の措置が行える構成とすること。
- ・仮想基盤を構成する全ての機器が接続可能な無停電電源装置を導入すること。
- ・仮想基盤の保守について、リモート接続で、監視、保守等の操作が行えるようにすること。

## (2) 仮想基盤のハードウェアに関する基本要件

### 1) 仮想基盤（ハイパーバイザー含む）

仮想基盤のハードウェアは下記要件を最低限満たすこと。

項目	仕様	数量
CPU	インテル Xeon Gold 5415 以上で動作クロック 3.0GHz 以上	適宜
メモリ	適宜	
ハードディスク	ハイパーバイザーOS のインストール領域とし、RAID により冗長化すること。 15000 回転 SAS12Gbps 以上の転送速度であること。 ディスクは、活性化交換に対応していること。	
インターフェース	ネットワーク接続のため 10GBASE-SR を合計 4 ポート備えること。 ネットワークインターフェイスカードは冗長構成とすること。 3Ter 方式の場合は共有ストレージ接続用として、16Gbps ファイバーチャネルを 4 ポート以上備えること。	2 枚以上
電源	冗長電源であり、冷却ファンを有すること。 電源、冷却ファンは活性化交換に対応していること。 電源は無停電電源装置から取得すること。	2 本以上

ハイパーバイザ	VMware vSphere および vCenter
ー	ライブマイグレーション、ハイアベイラビリティ機能が利用可能なライセンスであること。
OS	仮想マシンの必要数分の WindowsServer2022 ライセンスを準備すること。
その他	以上の仕様に基づく物理サーバを複数台により仮想環境を構成し、仮想環境管理サーバはどちらかの物理サーバ上で稼働させること。 19 インチラックマウントタイプ 2U 以下であること。

## 2) バックアップストレージ

仮想サーバのバックアップを取得するストレージで、各仮想サーバのストレージとは異なる筐体とすること。ハードウェア要件は、下記を満たすこと

項目	仕様
ストレージ構成	SMB/CIFS、FTP、SFTP、NFS、HTTP/HTTPS のプロトコルによる NAS 機能を有すること。
ディスク構成、容量	RAID による冗長構成が可能なこと。 実効容量として RAID-5 で 30TB 以上であること。
インターフェース	1000BASE-T 以上を 1 ポート備えること。
電源	無停電電源装置から取得すること。

## 3) 無停電電源装置

無停電電源装置は、今回導入するすべての物理機器への電源供給を行うとともに、停電が発生した場合の対策を担う機器として導入する。

項目	仕様
無停電電源装置	仮想基盤、バックアップストレージに安定して電源供給が可能な容量を有すること。 既設の 100V30A 電源回路を使用すること。
停電対策	一定時間を超える停電が発生した場合に、収容する機器を緩やかにシャットダウンするよう構成し、構築を行うこと。
その他	19 インチラックマウントタイプであること。 運用保守期間中のバッテリーの劣化によるアラート発生時は、無償でバッテリー交換が可能なこと。

## 4) KVM スイッチおよびコンソール

KVM スイッチおよびコンソールは仮想基盤を構成する物理機器にコンソール接続

する目的で導入する。

項目	仕様
KVM スイッチ	19 インチラックにマウントして設置可能であること。コンソール側のモニタ上で操作画面を呼び出し、接続先の切替等が可能であること。
コンソール	19 インチラックにマウントして設置可能であること。モニタを折りたたんで収納することができ、折りたたんだ時のサイズが 1U に収まること。17 インチ以上の LCD モニタ、キーボード、タッチパッドを搭載すること。調達する KVM スイッチのコンソール側で接続が可能であること。

### (3) 各種サーバに関する基本要件

#### 1) Active Directory サーバ

中間管理系ネットワークに配置し、現行環境を既存踏襲し再構築を行うこと。また、それぞれの系統に構築するサーバは冗長構成にて構築を行い、プライマリーを物理サーバで構築し、セカンダリーは仮想基盤上に構築すること。

※既存踏襲範囲・・・ユーザ/グループ、GPO、ファイルコピー等

#### 2) WSUS サーバ

中間管理系ネットワークに配置し、基幹系端末の更新プログラム制御を行う。現行環境を踏襲し再構築を行うこと。最新更新プログラムについては、最適な取得方法を提案し、常に最新更新プログラムを適用すること。

#### 3) ウィルス対策サーバ

中間管理系ネットワークに配置し、基幹系端末及び各系統サーバに対し、エンドポイントセキュリティ対策を行う。現行環境を踏襲し再構築を行うこと。最新パターンファイル取得については、最適な取得方法を提案し、常に最新更新プログラムを適用すること。

※参考 トレンドマイクロ株式会社の Trend Micro Apex One を利用中

※機能要件は【別紙 3】「機能確認書」参照

#### 4) 資産管理サーバ

中間管理系ネットワークに配置し、現行の資産管理運用を踏襲し、再構築を行うこと。現行運用中の機能は資産管理、ログ管理、USB 制御。基幹系端末 100 台

※参考 エムオーテックス株式会社の LanScope Cat を利用中

※機能要件は【別紙 3】「機能確認書」参照

5) 2要素認証サーバ

中間管理系ネットワークに配置し、現行静脈認証に IC カード認証を追加し再構築を行うこと。IC カード認証に必要な認証装置についても今回の調達に含めること。IC カード認証装置 (Felica、NFC 対応) は 50 台を導入すること。静脈認証装置は既存のものを利用する。

※参考 株式会社ディー・ディー・エスの EVEMA を利用中

※既存静脈認証装置：mofiria 製 FVA-U3SX

※機能要件は【別紙 3】「機能確認書」参照

6) 基幹系ファイルサーバ

基幹系ネットワークに配置し、現行環境を踏襲し再構築を行うこと。

※既存踏襲範囲・・・ユーザ/グループ、GPO、ファイルコピー等

7) グループウェアサーバ

内部情報系ネットワークに配置し、現行環境を踏襲し再構築を行うこと。

また既存のグループウェアからのデータ移行は必須とする。

※参考 株式会社ネオジャパンの Desknet's を利用中

※機能要件は【別紙 3】「機能確認書」参照

8) メールサーバ

内部情報系ネットワークに配置し、現行環境を踏襲し再構築を行うこと。

既存環境からはユーザ、パスワード、クォータ設定等について移行想定。

※参考 Postfix、Dovecot、Bind を利用中

9) ファイル交換・無害化サーバ

中間管理系ネットワークに新規配置し、インターネット系-内部情報系間の安全なファイル交換 (無害化機能も含む) を行うための環境を構築すること。

別途構築する仮想ブラウザとの親和性を重視し、シームレスな連携も実現できること。

※シームレスな連携とは職員の負荷軽減を考慮し、複数回のシステムログインを減らすなどの考慮を指す。

10) RDS (リモートデスクトップ)

中間管理系ネットワークに配置し、出先拠点に設置されている内部情報系端末からの閲覧用として、新規構築を行うこと。同時接続は 30 台を想定する。

Word, Excel, PowerPoint, Access30 ライセンスを導入すること。

1 1) 仮想ブラウザサーバ

中間管理系ネットワークに配置し、内部情報系端末からのインターネット閲覧用として、新規構築を行うこと。CAL 等の付帯するライセンス等を省くことが可能なシステムであること。

※機能要件は【別紙 3】「機能確認書」参照

1 2) バックアップサーバ

- ・本業務にて構築する仮想サーバのバックアップ、ファイルサーバのバックアップを取得することを目的として新規に構築すること。
- ・仮想環境に対応し、仮想マシン単位でイメージバックアップを取得する機能を有するバックアップソフトウェアを導入すること。
- ・バックアップソフトウェアは上記に加え、仮想マシン単位のイメージバックアップ、ファイル単位でのバックアップ、ストレージ等のバックアップにも対応していること

(4)分離用 FW に関する要件

- ・現行同様に系統間の通信について制御を行える環境を構築すること。
- ・設計方針、設定内容等については現行踏襲とし、新たな設計が発生しないように考慮すること。

※参考機種：FortiGate 100F

上記と同等以上の機能を有する機器を選定すること。

## 監視・運用保守環境の要求仕様

本業務で調達・構築するシステムの監視、運用保守環境の要求仕様として、以下の項目について記載する。

- (1) 監視・運用保守環境の基本要件
- (2) 監視・運用保守環境のハードウェア、ネットワークに関する要件
  1. 監視サーバ
  2. リモート保守端末およびネットワーク

(1) 監視・運用保守環境の基本要件

- ・監視サーバを構築して、本業務で導入する仮想基盤、仮想サーバの監視を行う。

日頃の監視業務は本市にて実施する。

- バックアップ取得状態監視およびシステムで障害が発生した場合の保守対応は本市の申告をもとに本業務の受注事業者による対応範疇とする。
- バックアップサーバー以外の Active Directory、WSUS 等に関する運用業務は、本市にて実施する。
- 前述の障害対応を迅速に行うため、本業務の受注事業者の拠点から、リモートで保守業務が実施できるネットワーク環境、保守端末を整備すること。
- 保守用のリモート接続回線は閉域網とすること。
- 複数のハードウェアの安定した運用保守業務のため、コンソール接続用 KVM を導入する。

(2) 監視・運用保守環境のハードウェア、ネットワークに関する要件

(2) - 1 監視サーバ

- 監視サーバは、独立したハードウェアとして調達、構築すること。

• 監視サーバの要求仕様

項目	仕様
監視システム	Zabbix-6.0 以上 本業務で導入する仮想基盤、仮想サーバ全体を監視可能であること。
ログの保存	冗長構成のディスクに保存可能なこと。 監視グラフのデータとして1年間保存可能であること。
構成	仮想基盤（ストレージ含む）、仮想サーバの CPU、メモリ、ディスク、ネットワーク使用率を監視し、グラフとして推移データを保存可能であること。 閾値を設け、異常時にアラートを発報すること。

(2) - 2 リモート保守端末およびネットワーク

- リモート保守用として事業者拠点と本市庁舎を接続する回線サービスは閉域網とすること。
- リモート保守回線のネットワークは、本市の業務ネットワークを経由することなく、保守対象に接続可能な構成とすること。
- リモート保守用端末は、専用端末として、保守用ネットワークのみに接続可能な構成とすること。

## 導入作業

- (1) 構築する仮想基盤は、今回導入する仮想サーバを集約する前提で提案すること。この際、各ネットワーク間、システム間で障害が発生した場合には、仮想基盤とネットワークとの障害切り分けを行い、既存保守ベンダーと連携して迅速に障害対応できるようにすること。特に、セキュリティ事故が発生しないように留意すること。また、移行スケジュールの取り纏め及び移行作業時の既存業務システムベンダー支援をオンサイト、Web 会議で実施する事を前提とし、集約完了までの工程を責任もって実施すること。
- (2) 基幹系端末は、本市側で調達し構築する。ただし、必要な助言等を行うこと。
- (3) 本業務で調達する資産管理ソフト・ウィルス対策ソフトの端末へのインストール作業は本市で行う。ただし、必要な助言等を行うこと。
- (4) 各作業項目の状況が把握できる詳細スケジュールをもって進捗を管理し、定期的に本市に報告すること。
- (5) 試験を実施する際は、事前に本市と協議し、承認された内容に従い実施すること。
- (6) 本市の既存システムに影響を与えないように、細心の注意と試験計画をもって作業すること。
- (7) 現状、ネットワークやサーバシステムが全庁に影響しているため、切替作業を計画する際は必要に応じリハーサルも考慮するなど、短期間で業務運用に支障を与えないように実施すること。
- (8) 導入中に既存保守ベンダーや関連業者と調整が必要な場合は、必ず本市を窓口として業者間の直接のやり取りは実施しないこと。また、その際の記録を必ず残すこと。
- (9) 本市の業務を考慮した安全な導入を実施すること。
- (10) 導入中に既存環境に障害が発生した場合は、導入業者が責任をもって正常な状態に戻すこと。
- (11) 既存ネットワーク接続などのため、既存環境の機器・システムに変更が必要な場合の作業費も含めて見積もること。  
また既存保守ベンダーに作業依頼が必要な場合は、既存保守ベンダーへ作業委託する費用を包括したうえで、導入作業費として見積ること。作業内容、費用が不明確な場合は、そのリスクを考慮したうえで、積算すること。
- (12) 熊本県セキュリティクラウドの利用方針変更、熊本県・市町村電子自治体共同運営協議会セキュリティポリシーの変更などに伴い、作業内容、構築業務に変更のリスクがあることを考慮したうえで、設計すること。

## 移行作業

- (1) 本業務において構築する仮想サーバのデータおよび環境設定の移行等について、仮想サーバの要求仕様に記載の内容に沿って、作業を計画すること。

- (2) クライアントのデータ移行作業は、本業務範囲外とする。
- (3) 現行システムは令和8年3月31日までは稼働予定である。
- (4) 既存で稼働している個人番号系ネットワーク、LGWAN系ネットワーク、インターネット系ネットワーク、管理系ネットワークのネットワーク・システムに支障をきたさない移行計画を立案すること。
- (5) 試験を実施する際は、事前に本市と協議し、承認された内容に従い実施すること。
- (6) 本市の既存システムに影響を与えないように、十分な検討と細心の注意をもって作業すること。

## 運用保守

新電算システムにかかわる運用保守業務は、下記要件を満たすこと。

### (1) 体制・役割

正常稼働時、障害発生時、セキュリティインシデント検知時、組織的に状況に応じた対応ができるよう、業務ごとの責任者を明確にしたうえで、然るべき組織体制及び連絡・報告体制が構築されること。

### (2) 障害対応

- ① 24時間、365日、機器・ネットワーク・サービスで発生する障害の本市による申告を有人による故障・障害受付体制が構築されること。  
障害申告を受け付けたあと、復旧措置（応急措置、恒久措置、予防措置）等を実施する対応時間および体制を提案すること。
- ② 障害対応にあたり、決められた運用手順に従い、然るべき本市の担当者・責任者に連絡・報告し、実施すべき対策について協議すること。
- ③ 障害対応の状況は、定期的（月次）にレポートで報告すること。  
既存保守会社と協力し、然るべき復旧措置を実施すること。

### (3) メンテナンス

- ① 本業務で導入された機器やサービスが、運用保守契約期間中において正常に稼働できるよう、必要に応じて定期点検と部品交換を行うこと。
- ② 本業務で導入された機器やサービスが、運用保守契約期間中において正常に稼働できるよう、インストールされたOSやソフトウェアが最新状態に維持するためのバージョンアップ、パッチ適用、ファイル更新などを本市と調整のうえ実施すること。端末のソフトウェアは対象外とし、対応については年に2回など、頻度を提案すること。  
緊急の機器部品の不具合やソフトウェアのバグ・セキュリティホールなどに対応する交換部品やパッチファイルが発表された場合、提案する頻度に限らず、該当機器に対して遅

延なく部品交換やパッチ適用を実施すること。

### (3) 運用支援

- ① 本業務で導入された機器やサービスに対して、利用者から設定変更などの要求があった場合、変更対応可能な範囲を提案すること。
- ② 本業務で導入された機器やサービスに関して、利用者から問い合わせがあった場合、可能な限りの情報提供やアドバイスを行うこと。

### (4) バックアップ

本業務で導入された機器及びサービスにおけるユーザデータ及びシステムデータのバックアップを定期的に取り得し、必要な場合に指定したバックアップしたデータを指定した機器やサービスに復元（リストア）できること。

### (5) 定例会と報告

- ① 四半期に1回、定例会を開催し、本業務で導入された機器及びサービスにかかわる運用状況の報告と、改善措置の協議などを行うこと。
- ② 毎月、本業務で導入された機器及びサービスにおける障害対応状況を報告書にまとめ報告すること。毎月、本業務で導入された機器及びサービスにかかわる作業計画を報告書にまとめ、定例会で報告を行うこと。
- ③ 本業務で導入された機器及びサービスに関連する情報は、都度定例会で情報共有を行う。定例会の開催サイクルは、責任者間協議のうえ、変更することができる。

## 納品物

本業務の遂行にあたり、各段階において納品するドキュメント類は表2に示す通りで、納品は紙または電子媒体のいずれかの形式とすること。

表 2 納品物リスト

ドキュメント名	内 容	納品時期
①業務実施計画書	本業務の実施体制、実施内容、スケジュール、進捗管理方法、連絡体制など	本業務開始前
②基本設計書	新電算システムとして実装すべき機能とセキュリティ対策、移行方法、運用ルールなど	構築作業開始前
③詳細設計書	基本設計書で定められた事項を実現するための具体的な方法、設定パラメータとその設定根拠など	構築作業開始前

④テスト計画書	構築したシステムの性能や、可用性、正常性を確認するテストの実施計画	テスト開始前
⑤テスト報告書	実施した確認テストの結果	稼働開始前
⑥移行計画書	新電算システムに移行する手順とスケジュール	移行作業開始前
⑦各種パラメータ設定表	導入した機器や、仮想環境、ネットワークなどの設定パラメータ	稼働開始時
⑧各種操作マニュアル	業務端末や仮想サーバなどの操作マニュアル	稼働開始時
⑨運用保守手順書	新電算システムにかかわる運用保守の役割分担、体制、連絡方法、作業手順など	稼働開始時
⑩定例会議事録（一式）	本業務の期間中に開催した定例会の議事録一式	本業務終了時

#### 操作研修・講習会

本業務において、構築完了した新環境の操作教育等を情報システム担当者向けに実施すること。実施場所は本市とすること。

#### その他要件

本業務において、「背景と目的」で挙げた4つの目的（①コスト低減、②耐災害性、③セキュリティ強化）に資するような提案があれば、独自提案として提案すること。