

# 庁内ネットワーク保守仕様書

令和 8 年 4 月

守口市企画財政部行財政改革・DX 推進課

# 目次

|                                |    |
|--------------------------------|----|
| 1. 基本方針.....                   | 4  |
| 1-1 基本方針 .....                 | 4  |
| 1-2 保守実施期間.....                | 4  |
| 1-3 システム稼働及び利用時間.....          | 4  |
| 2. 保守運用体制 .....                | 4  |
| 2-1 保守受付窓口 .....               | 4  |
| 2-2 受付窓口の対応時間.....             | 4  |
| 2-3 受付窓口の統一 .....              | 5  |
| 2-4 保守対象 .....                 | 5  |
| 2-5 運用方針 .....                 | 5  |
| 3. リモート保守 .....                | 11 |
| 4. セキュリティ要件.....               | 12 |
| 4-1 基本要件 .....                 | 12 |
| 4-2 ネットワーク管理におけるセキュリティ要件 ..... | 13 |
| 5. プロジェクト要件.....               | 14 |
| 5-1 プロジェクト体制及び役割.....          | 14 |
| 5-2 プロジェクト体制及び役割に関する留意事項 ..... | 15 |
| 5-3 プロジェクト計画書 .....            | 15 |
| 5-4 プロジェクト作業場所 .....           | 16 |
| 5-5 プロジェクトに係る設備、備品、消耗品等.....   | 16 |
| 5-6 プロジェクトの会議体 .....           | 16 |
| 5-7 レビュー・承認 .....              | 17 |
| 5-8 課題管理 .....                 | 17 |
| 5-9 文書管理 .....                 | 17 |
| 6. 特記事項.....                   | 18 |
| 6-1 事業終了時のデータ消去 .....          | 18 |
| 6-2 VLAN・IP アドレス再設計について .....  | 18 |
| 6-3 庁外施設の増減への対応について.....       | 18 |
| 7. その他仕様.....                  | 19 |

|                   |    |
|-------------------|----|
| 8. 成果物 .....      | 19 |
| 8-1 プロジェクト管理..... | 19 |
| 8-2 設計書 .....     | 19 |
| 8-3 運用設計 .....    | 19 |
| 8-4 その他 .....     | 19 |

## 1. 基本方針

### 1-1 基本方針

---

本仕様書は、守口市（以下「本市」という。）が実施する「市内ネットワーク更新業務実施事業」（以下「構築事業」という。）に係る保守運用業務の仕様を定めるものである。

受託者は、構築事業に係る構築仕様書に記載された目的及び基本要件を満たすよう、責任を持って安定した保守運用業務を遂行すること。また、本市のパートナーとして、保守運用に必要な知識的・技術的支援を行うこと。

### 1-2 保守実施期間

---

保守実施期間は、令和 9 年 1 月 1 日から令和 13 年 12 月 31 日までとする。

### 1-3 システム稼働及び利用時間

---

本システムは、24 時間 365 日の稼働及び運用を可能とすること。

## 2. 保守運用体制

### 2-1 保守受付窓口

---

受託者は、本運用保守業務に関する受付窓口を設置すること。

受付窓口は、日本語で円滑に対応でき、かつ情報機器に関する専門的知識を有する担当者が対応すること。

また、受付窓口の連絡手段として、少なくとも電話及び電子メールを提供すること。

### 2-2 受付窓口の対応時間

---

受付窓口の対応時間は、次のとおりとする。

#### (1) 通常運用時（問合せ、設定変更依頼等）

対応時間: 平日 9 時 00 分から 17 時 30 分まで

#### (2) 緊急対応時（夜間休日開庁時、障害発生時、セキュリティインシデント発生時又はその疑いがある場合等）

対応時間: 24 時間 365 日

## 2-3 受付窓口の統一

---

構築事業で調達した全てのハードウェア、ソフトウェア、ライセンス及び関連資材について、受託者が一元的な窓口として対応すること。

## 2-4 保守対象

---

保守対象は、本事業において受託者が調達・導入する全てのハードウェア、ソフトウェア、ライセンス及び関連資材とする。

主な対象は以下のとおりであるが、これらに限定されない。

- ・ ファイアウォール
- ・ コアスイッチ
- ・ サーバ室内スイッチ
- ・ ディストリビューションスイッチ
- ・ フロアスイッチ
- ・ エッジスイッチ
- ・ 無線アクセスポイント（以下「無線 AP」という。）
- ・ 統合運用監視基盤（アプライアンス、ソフトウェア、ライセンスを含む。）
- ・ 無線コントローラ又はこれに相当する管理機能
- ・ 監視用管理端末
- ・ WAN 回線用ルータ
- ・ その他提案内容を実現するために導入した機器

なお、保守対象の詳細は、契約締結後に提出する保守対象一覧において確定するものとする。

また、保健センターの既存スイッチ等、本事業の構築対象外であるが、統合運用監視基盤の監視対象となる機器については、障害発生時の一次切り分け支援までを保守範囲に含むものとする。

## 2-5 運用方針

---

受託者は、本事業で導入する全ての機器、ソフトウェア及びライセンス等

(以下「本システム」という。)について、以下の運用及び保守体制を確立し、安定的かつ効率的な運用を維持すること。

### 2-5-1 運用体制の確立

- (1) 本システムの安定稼働を維持するため、必要な運用及び保守を実施すること。
- (2) 運用に必要な各種手順書及びマニュアル類を整備し、常に最新の状態に更新すること。
- (3) 障害発生時等の緊急連絡先として、24時間365日対応可能な窓口を設置し、専門知識を有する担当者が直接対応する体制を確立すること。
- (4) 保守拠点には、常時保守要員（SE及びCE）が待機しており、修理、点検、保守その他のアフターサービスについて迅速に対応できること。
- (5) 障害発生時は、本市からの連絡又は統合運用監視基盤による障害検知後、以下の時間以内に対応を開始すること。

リモート着手：1時間以内

現地着手：2時間以内

### 2-5-2 障害対応

- (1) ネットワーク障害又は情報セキュリティインシデント（その疑いを含む。）の発生に備え、通常連絡先、緊急連絡先及び対応フローを明記した緊急時対応体制図を本市に提出すること。また、年末年始等の長期閉庁期間に際しては、専用の連絡体制を提示すること。
- (2) 障害発生時は、統合運用監視基盤によるアラート検知又は本市からの連絡により、障害又はその予兆を覚知した場合、直ちに原因調査に着手すること。業務に支障を来すおそれのある重要障害の場合は、平日・休日を問わず、本市の指示の下、迅速に復旧対応を行うこと。
- (3) 本市からの連絡のみでは障害の一次切り分けが困難な場合は、受託者の判断で速やかに現地に保守作業員（SE及びCE）を派遣し、障害の切り分け作業を実施すること。
- (4) 他システム（サーバ及びネットワーク）で通信異常等の障害が発生した場合は、本システムの観点から切り分け支援を保守業務の範囲内で実施するこ

と。本システム側に設定変更等の対応が必要な場合は、関係事業者と詳細な調整を行った上で、迅速に対応すること。

### **2-5-3 SOC 連携・セキュリティインシデント対応**

(1) 受託者は、本市の庁内ネットワークに関するセキュリティ監視及び初動対応の一次窓口として、本システムに係るアラート、異常又は情報セキュリティインシデントの疑いを検知した場合は、速やかに確認、切り分け及び必要な応急対応を行うこと。

(2) 大阪版自治体情報セキュリティクラウド事業者その他の関係事業者から、本システムに関連するアラート又は調査依頼を受けた場合は、本市と連携の上、必要な確認、技術調整及び対応を行うこと。

### **2-5-4 保守部品・予備機の管理**

(1) 機器故障に備え、常時保守部品（代替機、付属品及びソフトウェア等を含む。）を国内の保守拠点に保有し、迅速な交換及び復旧が可能であること。特に重要機器については、本庁舎内に予備機を配備するなど、より迅速な復旧策を講じること。

(2) 機器の部品交換は、可能な限りホットスワップ（活線挿抜）で対応できる構成とすること。ホットスワップが不可能な機器については、業務への影響を最小限に抑える手順及び構成をあらかじめ本市に提示すること。

### **2-5-5 構成変更・技術支援**

(1) 構築時に再設計された VLAN 及び IP アドレスの構成情報を台帳で正確に管理すること。本市の依頼に基づき VLAN 又は IP アドレスの追加、変更又は削除を行った際は、速やかに台帳を更新し、最新版を本市に提供すること。

(2) 本市が新たに契約する他システムの導入、既存システムの更新その他本市の業務都合により、本システムの各種設定変更（ファイアウォール、スイッチ、無線 AP、監視設定等）が必要となった場合は、保守業務の範囲内で対応すること。その際は、本市に代わり、システム導入事業者等と詳細な技術調整を主体的に行い、安全かつ円滑に設定変更を実施すること。

(3) 本市の人事異動、組織改編、執務室レイアウト変更、課室の移転等に伴い、ネットワーク機器、端末、プリンタ、複合機その他接続機器の移設、接続先変更又は設定変更（VLAN 割り当て、アクセス制御等を含む。）が必要となった場合は、保守業務の範囲内で対応すること。この場合において、受託者は、必要に応じて軽微な配線変更、疎通確認及び台帳更新を実施すること。なお、フロアスイッチからエッジスイッチへの新規配線敷設・配線ルート変更その他これに類する工事は本項の対象外とする。また、当該対応は保守期間5年間で10回程度の実施を見込むものとする。

#### 2-5-6 定期点検・改善提案

(1) 受託者は、年1回以上の定期保守点検を実施すること。点検に当たっては、ログ分析、性能評価及び機器又は配線の物理的状态確認を行い、その結果並びに必要な対応事項を報告書として取りまとめ、本市に提出すること。

(2) 受託者は、保守期間を通じて、本システムのパフォーマンス（通信速度、遅延、リソース使用率等）又はセキュリティに関する課題若しくは問題点が判明した場合は、ネットワークの専門的知見に基づき、具体的な解決策又は改善策を積極的に提案すること。また、保守期間中に導入機器又はソフトウェアについてメーカーサポート終了（EOL/EOS）が公表された場合は、速やかに本市へ報告すること。報告に当たっては、少なくとも次の事項を含めること。

ア 対象機器又はソフトウェアの名称

イ メーカーサポート終了日

ウ サポート終了による影響範囲

エ 代替措置の提案

なお、具体的な対応については、本市と受託者が協議の上、決定するものとする。

(3) 受託者は、年間保守スケジュールを作成し、月1回以上の定例会を開催すること。定例会においては、稼働状況、障害対応実績、インシデント発生状況、定期保守点検結果、改善提案の内容及び対応状況並びにメーカーサポート終了（EOL/EOS）に係る影響又は対応方針がある場合はその内容を報告すること。

### 2-5-7 緊急時対応

(1) 計画停電が実施される際は、関連する調整、事前準備、当日の立会い及び事後確認まで、必要な対応を行うこと。なお、本庁舎においては少なくとも令和9年3月及び令和12年3月に計画停電が見込まれ、保健センター及び水道局においても例年、電気設備点検等に伴う計画停電が実施される見込みがあることを踏まえ、受託者は必要な作業体制、連絡体制、対応手順及び復旧確認項目をあらかじめ整備すること。

(2) 障害対応作業を実施する際は、緊急時を除き、事前に作業計画書（作業内容、手順、影響範囲及び切り戻し手順を明記したもの）を提出し、本市職員に説明を行うこと。また、作業終了後は、速やかに作業完了報告書を提出し、説明を行うこと。

### 2-5-8 特定の更新・導入への対応

下記各事業への対応は、ネットワーク側の設定変更及び技術支援を保守業務の範囲内で実施すること。ただし、ネットワーク構成の大幅な再設計を伴う等、当初想定を著しく超える作業が必要となる場合は、本市と受託者が協議の上、対応を決定するものとする

(1) 構築仕様書 5-4 に定める IP 電話導入（令和9年度予定）の際は、ネットワーク側の要件整理、接続設計、他事業者との調整、接続試験、トラブルシューティング等、導入に必要な技術支援を保守業務の範囲内で実施すること。

(2) 保守期間中に更新を予定している大阪版自治体情報セキュリティクラウド（令和9年4月稼働開始予定）、強靱化対応によるマイナンバー系管理サーバの更新（令和10年1月稼働予定）、庁内情報機器更新（令和12年2月に現行契約終了）に伴い、本市の庁舎内ネットワークの設定変更が必要となる場合には、当該作業についても保守業務の範囲内で対応すること。

### 2-5-9 技術支援・情報提供

(1) 本市からの技術的な質問又は相談に対し、随時速やかに回答すること。

(2) 機器の正常稼働に必要な OS 又はソフトウェア等の操作方法、設定確認等に関する技術支援（Q&A 対応）について、本市からの依頼に基づき確実に対応すること。

(3) 機器の故障、ソフトウェアの不具合、セキュリティ脆弱性、パッチ適用又はバージョンアップ等に関する情報を能動的に収集及び分析し、本システムへの影響を評価の上、対策の必要性を速やかに本市へ報告すること。対策を実施する場合は、本市と協議の上、計画的に実施すること。

(27) 本市が必要と判断した場合又は保守作業により設定情報の変更等が生じた場合は、以下の支援を保守業務の範囲内で提供すること。

- ・ マニュアル改訂版の提供
- ・ 保守及び技術情報等の提供
- ・ 各種技術支援及び勉強会の開催

## 2-5-10 品質管理目標 (SLA)

受託者は、本システムの安定運用を確保するため、本章に定める品質管理目標 (SLA) を遵守すること。

なお、具体的な測定方法、対象範囲及び算定条件の詳細については、契約締結後、本市と協議の上、プロジェクト計画書又は運用保守計画書において定めるものとする。

最低限設定すべき SLA 項目は、以下のとおりとし、SLA の達成状況は、月次報告書において報告すること。また、正当な理由なく SLA を達成できなかった場合は、受託者は原因を分析し、再発防止策を含む改善報告を本市へ提出すること。

天災、計画停電その他受託者の責に帰さない事由による障害については、復旧目標時間の適用について本市と受託者が協議の上、決定するものとする。

### SLA の評価項目と基準

| 業務   | 項目   | サービスレベル                    |
|------|--|----------------------------|
| 可用性  | 稼働時間   | 24 時間 365 日                |
|      | 稼働率  | 99.9%以上/月                  |
| 障害対応 | 障害報告時間<br>(ハードウェア、ソフトウェア障害<br>検知から監視ツールの発報機能等<br>による報告までの時間) | 30 分以内                     |
|      | 着手時間   | リモート着手：1時間以内<br>現地着手：2時間以内 |

|        |  |                |
|--------|--|----------------|
|        | 復旧時間<br>(ハードウェア、ソフトウェア障害<br>検知から復旧までの時間) | 6 時間以内         |
| 月次報告   | 報告内容                                     | 発生したアラート及び対応結果 |
|        | 実施頻度                                     | 1 回/月          |
| 業務品質改善 | サービスレベル遵守と対応                             | 監視運用上の課題と改善    |
|        | 改善提案頻度                                   | 年 1 回          |
| レスポンス  | 画面遷移                                     | 3 秒以内          |

### 3. リモート保守

障害発生時の原因調査及び復旧作業等を迅速に行うため、リモート保守を導入する。リモート保守については、以下の要件を全て満たすこと。

- (1) リモート接続は、専用線又は IP-VPN により接続すること。なお、インターネット VPN は認めない。また、IP-VPN を使用する場合は、通信を暗号化すること。
- (2) リモート保守を行う環境は、受託者の社内汎用ネットワークから物理的又は論理的に分離された、専用のセキュアなネットワーク環境であること。
- (3) リモート保守を行う作業室は、入退室管理システム等を備え、許可された作業者以外は立ち入ることができないこと。
- (4) リモート接続を行う端末は、常に最新のウイルス定義ファイル並びに OS 及びソフトウェアのセキュリティパッチが適用されていること。
- (5) リモート接続及び操作に関するログ（接続日時、作業者、操作内容等）を記録し、本市の求めに応じて提出できること。
- (6) リモート保守に必要な回線等の費用は、全て受託者の負担とすること。

## 4. セキュリティ要件

### 4-1 基本要件

- (1) 本事業において、情報セキュリティに関する事故及び障害等の発生を未然に防止するとともに、発生した場合には被害を最小限に抑えること。
- (2) 情報セキュリティに関する事故及び障害等が発生した場合には、速やかに本市に報告し、対応策について協議すること。
- (3) 本事業において、本市の意図しない変更又は機密情報の窃取等が行われないうことを保証する管理が、一貫した品質保証体制の下でなされていること。
- (4) 本市の意図しない変更又は機密情報の窃取等が行われないうことを保証するための具体的な管理手順及び品質保証体制を証明する書類（例えば、品質保証体制の責任者及び各担当者がアクセス可能な範囲等を示した管理体制図）を、本市との協議の上、必要と判断された場合は提出すること。また、第三者機関による品質保証体制を証明する書類等が提出可能な場合は、提出すること。
- (5) 本事業において、本市の意図しない変更が行われるなどの不正が見つかった場合には、追跡調査又は立入検査等、本市と連携して原因を調査し、排除するための手順及び体制を整備していること。例えば、運用保守業務におけるシステムの操作ログ又は作業履歴等を記録し、本市から要求された場合には提出できるようにすること。また、当該手順及び体制が妥当であることを証明する書類を、本市との協議の上、必要と判断された場合は提出すること。
- (6) 本事業の各工程において、情報セキュリティに係るサプライチェーン・リスクを低減する対策が行われていること。
- (7) 本事業に従事する受託者の従業員全てに対して、情報セキュリティに関する教育を実施すること。
- (8) セキュリティ関連のテストの実施結果が確認できること。情報システムに対する脆弱性検査を実施する場合については、「デジタル庁 政府情報システムにおける脆弱性診断ガイドライン」の実施基準を満たすよう、脆弱性診断の実施及び検出された脆弱性への対応を行うこと。
- (9) 脆弱性検査の終了時には、実施内容及び結果を脆弱性検査結果報告書に取りまとめること。
- (10) 行政情報システムにおいて含有されやすいセキュリティ上の問題点とし

て、少なくとも以下の各項目に対し、本事業における運用保守対象の範囲で該当するものについて漏れなく対応すること。

| 項番 | 要因               | セキュリティ上の問題点   |
|----|------------------|---|
| 1  | 認証管理不備           | <ul style="list-style-type: none"> <li>・ 共有アカウントが使用される際に、利用者特定の仕組みや取扱いに関するルールが整備されていない</li> <li>・ 推測されやすい脆弱なパスワードが使用されている</li> <li>・ 認証情報がファイル等に平文で書かれている</li> </ul>  |
| 2  | アクセス制御不備         | <ul style="list-style-type: none"> <li>・ 必要な強度の認証が行われていない</li> <li>・ ネットワーク、システムへのアクセス制限が実施されていない</li> <li>・ アクセス権が必要最小限のアクセス権付与が守られておらず、過剰である</li> </ul>             |
| 3  | 暗号化不備            | <ul style="list-style-type: none"> <li>・ 重要情報が流れる各機器間の通信経路において、必要な暗号化が実施されていない</li> </ul>   |
| 4  | 資産管理、脆弱性管理不備     | <ul style="list-style-type: none"> <li>・ 利用しているソフトウェアや機器の状態を把握していない（最新状態を維持できていない）</li> <li>・ OS やミドルウェア、ファームウェア等の脆弱性対策が適切に実施されていない</li> </ul>                        |
| 5  | Web アプリケーションの脆弱性 | <ul style="list-style-type: none"> <li>・ SQL インジェクション、クロスサイトスクリプティング等の初歩的な Web アプリケーションの脆弱性が存在している</li> <li>・ パラメータ改ざんにより、本来アクセスできないデータを操作できるなどの脆弱性が存在している</li> </ul> |
| 6  | ログ管理不備           | <ul style="list-style-type: none"> <li>・ ログ取得の範囲が目的に応じて定められていない（必要なログが取得されていない）</li> <li>・ 定期的なログの点検又は分析が実施されていない</li> </ul>  |
| 7  | 外部委託の管理不備        | <ul style="list-style-type: none"> <li>・ 外部委託に係る契約に、遵守事項で定める委託先の情報セキュリティ対策が含まれていない</li> <li>・ 外部委託に係る契約に基づき、委託先における情報セキュリティ対策の履行状況を確認していない</li> </ul>                 |

## 4-2 ネットワーク管理におけるセキュリティ要件

- (1) 管理者 ID 及び特権 ID は適切に管理し、アクセス権は必要最小限とすること。
- (2) 管理用通信は、暗号化された安全な方式により実施すること。
- (3) 設定変更、管理者操作、障害対応等に関するログを取得し、必要に応じて追跡可能な状態を維持すること。
- (4) 構成情報、設定情報及び台帳情報を適切に管理し、変更時には速やかに更新すること。
- (5) ソフトウェア、ファームウェア及び各種セキュリティパッチの適用状況を

管理し、必要な対策を講じること。

(6) 保守に使用する端末及び管理端末については、利用者、利用場所及び用途を明確にし、適切なアクセス制御を実施すること。

## 5. プロジェクト要件

### 5-1 プロジェクト体制及び役割

本事業を適切かつ効率的に履行するため、受託者は以下の役割を担う者を選任すること。以下の(1)は、(2)から(4)の役割は兼務することはできないものとし、それぞれ異なる者を選任すること。ただし、(2)について複数人を選任することを妨げない。

また、保守体制は、原則として構築時の PM 及び PL が参加する体制とすること。やむを得ず要員が交代する場合であっても、保守運用が安定したと本市が判断するまでは、必要に応じて構築時要員を保守作業、定例会等に参加させること。

#### (1) プロジェクトマネージャ (PM)

本事業における業務責任者として、本プロジェクトにおける決定権を有し、業務を確実かつ円滑に進めることができる者であること。業務実施計画書を作成し、本事業を円滑に遂行するため、各作業工程の管理及び関連業務や利害関係者との調整等を実施し、作業全体を統括管理すること。なお、本プロジェクトの管理に相応しい知識及び経験を有する者を配置すること。

#### (2) プロジェクトリーダー (PL)

プロジェクトマネージャが作成した業務実施計画書に基づき、現場で作業を実施する責任者であること。本市との現場レベルの打合せを実施する者であり、本事業の各業務に精通し、必要な知識及び経験を有する者を配置すること。

#### (3) プロジェクト品質管理者

プロジェクトの品質管理を行う責任者を配置すること。

#### (4) セキュリティ管理者

本プロジェクトを通じて情報セキュリティ管理を行う責任者を配置すること。

## 5-2 プロジェクト体制及び役割に関する留意事項

---

### 5-2-1 プロジェクト体制の記載事項

受託者は、プロジェクト体制における役割分担を明確にし、本市の指示に基づき適切に対応すること。

### 5-2-2 プロジェクト体制の変更

受託者は、契約時に提示したプロジェクト体制を原則維持すること。やむを得ず要員の追加又は担当者の変更が必要となる場合は、変更理由、後任者の経歴、引継計画及び業務への影響を記載した書面を速やかに提出し、本市の承認を得ること。

### 5-2-3 情報セキュリティ確保の体制整備

本事業に係る業務を行う事業者は、事業者組織全体のセキュリティを確保するとともに、本市から求められた当該業務の実施において情報セキュリティを確保するための体制を整備すること。

### 5-2-4 プロジェクト停滞に伴う体制変更指示

業務実施計画書等で示した作業が適正に履行されていない場合又は本仕様書において定義する各要件を満たしていないと本市が判断した場合は、本市は受託者に対して体制変更を申し入れることができるものとし、受託者はこれに適切に対応すること。

## 5-3 プロジェクト計画書

---

受託者は、契約締結後 10 日以内にプロジェクト計画書を提出すること。なお、プロジェクト計画書には、少なくとも以下の内容を含めること。

- ・ プロジェクトの方針及び目的
- ・ スケジュール
- ・ 体制図（体制及び役割分担）
- ・ 対象範囲（スコープ）
- ・ 保守対象一覧（ハードウェア、ソフトウェア、ライセンス等）
- ・ 運用監視計画（監視対象、検知方法、調査・分析、報告）

- ・ 品質管理目標 (SLA)
- ・ 課題管理計画
- ・ コミュニケーションマネジメント (会議体、合意形成プロセス、作業計画書、運用業務フロー)
- ・ 情報の適正な取扱いのための情報セキュリティ対策
- ・ その他プロジェクト管理に必要な事項

#### 5-4 プロジェクト作業場所

---

運用保守作業に係る設計、設定等の準備は、原則として受託者の事業所内で実施すること。

また、機器の設置及び設定、各作業に関する打合せ、報告、レビュー並びに進捗会議等については、原則として本市の会議室等で実施すること。なお、会議についてはオンラインでの実施も可とする。

#### 5-5 プロジェクトに係る設備、備品、消耗品等

---

本事業に使用する設備、備品及び消耗品等については、受託者が負担すること。ただし、庁内で使用する電気料金等の光熱水費については、本市の負担とする。

#### 5-6 プロジェクトの会議体

---

本事業の実施に当たっては、以下の会議体を開催し、議事内容について責任ある回答ができる要員を参加させること。会議の開催に当たっては、受託者側で必要な討議資料を用意すること。また、各会議体について、必要に応じて受託者側で議事録を作成し、本市に提出すること。

##### 5-6-1 定例報告会議

運用保守業務の作業状況について定期的に確認を行うため、月1回の頻度で会議(定例会)を開催すること。

受託者は、定例会において、以下の内容について報告を行うものとする。

- ・ スケジュール管理状況
- ・ 課題管理状況(課題管理表)
- ・ 保守運用業務の実施状況

- ・ インシデント報告
- ・ ライセンス及びセキュリティパッチの状況
- ・ 品質管理目標（SLA）の遵守状況

#### 5-6-2 緊急対応会議

緊急時（障害発生時等）の対応を検討するため、本市の求めに応じて会議を開催すること。緊急対応会議には、原則としてプロジェクトマネージャ（PM）及びプロジェクトリーダー（PL）が参加するものとする。

#### 5-7 レビュー・承認

---

受託者は、本仕様書に基づき提出する各種計画書、設計書、報告書、作業計画書等について、本市のレビューを受け、必要に応じて修正の上、承認を得ること。ただし、緊急対応時はこの限りでなく、事後速やかに報告し、本市の確認を受けること。

#### 5-8 課題管理

---

プロジェクトの中で発生する各種課題について、課題の認識、対応案の検討、解決及び報告のプロセスを明確にすることを目的として、課題管理を実施すること。

課題管理に当たっては、課題内容、影響、優先度、発生日、担当者、対応状況、対応策、対応結果及び解決日を課題一覧に取りまとめ、一元管理すること。なお、その他必要と考えられる項目についても適切に管理すること。

#### 5-9 文書管理

---

受託者は、必要に応じて会議又は打合せにおける議事録等を作成し、保管及び管理を行うこと。

また、プロジェクト内で作成する文書を一元管理し、本市の求めに応じて提示できるようにすること。

## 6. 特記事項

### 6-1 事業終了時のデータ消去

---

(1) 本契約が満了し、又は受託者の都合により本契約を解除し、機器を搬出する場合は、受託者がそれらに要する費用を負担すること。また、機器搬出時に機器内にデータが残存する場合は、物理的破壊の手法を用いて完全にデータを消去すること。

(2) 撤去対象の既存機器の記憶媒体装置等については、再度データを取得できないよう必要な措置を講じること。

(3) 機器内データを物理破壊により完全に消去する際は、必ず作業時の写真を撮影し、破壊前及び破壊後の写真を含む資料を本市に提出すること。

なお、必要に応じて、リース会社に対し事前調整を行うこと。

### 6-2 VLAN・IP アドレス再設計について

---

構築仕様書に定める VLAN 構成及び IP アドレス体系の再設計に係る実装は、原則として構築期間内に実施するものとする。

ただし、やむを得ない事情により構築期間内の実施が困難であると本市と受託者が合意した場合は、保守運用期間中に実施できるものとする。

この場合、受託者は、対象範囲、実施時期、影響範囲、暫定措置及びロールバック手順を記載した計画書を作成し、本市の承認を得た上で実施すること。なお、当該対応は、本契約に基づく保守運用の範囲内で実施するものとする。

### 6-3 庁外施設の増減への対応について

---

本市の出先機関については、保守期間中に施設の統廃合、移転、新設その他の事情により対象拠点数が増減する可能性がある。受託者は、当該変動に伴う WAN 用ルータの再配置、流用、予備機管理その他必要な設定変更に対応すること。

拠点廃止等により不要となった WAN 用ルータは、本市と協議の上、他拠点への転用又は予備機として活用するものとする。この場合に必要となる設定変更、設置変更、監視設定変更、WAN 回線事業者その他関係事業者との調整及び台帳更新は、保守業務の範囲内で実施すること。

また、拠点の新設又は機器故障に備え、受託者は本市と協議の上、必要数の予備機を確保すること。

## 7. その他仕様

本仕様書に定めのない事項については、本市と受託者が協議の上、決定する。

## 8. 成果物

受託者は、最低限、以下の内容を含む成果物を作成し、提出すること。

なお、データ形式は Microsoft Office で編集可能な形式とすること。

### 8-1 プロジェクト管理

---

- ・ 運用保守計画書
- ・ 年間運用保守スケジュール
- ・ 課題管理表

### 8-2 設計書

---

構築時に納品した設計書について、修正又は更新が発生した場合に限り、更新版を提出すること。

### 8-3 運用設計

---

- ・ 管理者マニュアル
- ・ 障害対応マニュアル
- ・ 運用保守業務フロー

### 8-4 その他

---

- ・ 月次報告書
- ・ 運用保守作業実施時の作業計画書、作業実施スケジュール及びコンテンツエンジニアリングプラン
- ・ 作業完了報告書
- ・ 議事録（本市が求めた場合）

- ・ 定期保守点検報告書
- ・ 脆弱性検査結果報告書（実施した場合）

なお、運用保守作業を実施する際は、事前に作業計画書、作業実施スケジュール及びコンティンジェンシープランを提出し、本市の承認を得た上で実施すること。