

庁内ネットワーク更新業務実施事業 構築仕様書

令和 8 年 9 月

守口市企画財政部行財政改革・DX 推進課

目次

1. 総則	4
1-1 目的	4
1-2 関連文書・準拠基準	4
1-3 構築期間	5
1-4 現行構成	5
2. 基本要件	6
2-1 基本要件	6
3. 調達範囲と対象	6
3-1 調達範囲	6
3-2 対象拠点	7
3-3 対象機器	7
3-4 調達対象外	8
4. 統合運用監視基盤	8
4-1 提供形態・サイジング	8
4-2 可用性・保全	9
4-3 管理端末・UI	9
4-4 ネットワーク可視化に関する機能要件	9
4-5 無線 LAN コントローラ機能	10
4-6 マニュアル・教育	10
5. ネットワーク設計	11
5-1 VLAN・IP アドレス再設計	11
5-2 LGWAN 系無線利用端末の他拠点利用	12
5-3 マイナンバー系ネットワークにおける無線化	13
5-4 IP 電話導入に係る要件	15
6. ネットワーク機器の配線・設置要件	15
6-1 配線・設置に関する共通要件	15
6-2 本庁舎における要件	16
6-3 水道局における要件	18

6-4 保健センターにおける要件.....	19
6-5 WAN 用ルータ	19
7. ネットワーク機器の機器要件	20
7-1 機器に関する共通要件	20
7-2 サーバ室に設置するネットワーク機器	21
7-3 本庁舎における要件.....	24
7-4 水道局における要件.....	27
7-5 保健センターにおける要件.....	27
7-6 無線アクセスポイント	28
7-7 WAN 用ルータ	29
8. テスト・移行に係る要件.....	30
8-1 テストに係る要件.....	30
8-2 移行要件	30
9. セキュリティ要件	31
9-1 基本要件	31
9-2 ネットワーク管理におけるセキュリティ要件	33
10. プロジェクト要件.....	34
10-1 プロジェクト体制及び役割.....	34
10-2 プロジェクト体制及び役割に関する留意事項	35
10-3 プロジェクト計画書.....	35
10-4 WAN 回線更新を含む移行統括（PMO）要件.....	36
10-5 プロジェクト作業場所	36
10-6 プロジェクトに係る設備、備品、消耗品等	36
10-7 プロジェクトの会議体	37
10-8 レビュー・承認	38
10-9 課題管理	38
10-10 文書管理	38
11. 特記事項	38
12. その他仕様.....	40
13. 成果物.....	40

1. 総則

1-1 目的

本事業は、守口市（以下「本市」という。）における庁内ネットワークについて、運用管理の効率化、障害発生時の業務継続性の確保及情報セキュリティの向上を目的として、現行別契約としていた庁舎内ネットワーク、庁舎外 WAN 用ルータ管理、庁舎外施設の無線 AP を統合し、ネットワーク環境の更新を行うものである。

本事業では、現行構成を原則踏襲しつつ、以下を実施するものとする。

- ・ ネットワーク機器の更新及び新規敷設、配線引き直し
- ・ 統合運用監視基盤の導入
- ・ VLAN 構成及び IP アドレス体系の再設計
- ・ 本庁、水道局及び保健センターの 3 拠点における LGWAN 系無線利用端末の相互利用を可能とするためのネットワーク再設計及び必要な構築
- ・ マイナンバー利用事務系ネットワーク（以下、「マイナンバー系ネットワーク」と言う。）の無線化に係る実装可否の評価、並びに本市が実装を指示した場合の設計及び構築
- ・ 本庁舎における将来の IP 電話導入を見据えたネットワーク設計及び必要な機器選定
- ・ 将来の端末数、通信量、機能追加に柔軟に対応可能な拡張性を備えた構成の実現

また、安全かつ確実な移行のため、既存契約事業者、新規 WAN 提供事業者、その他関係事業者及び庁内関係部署との調整並びに移行統括を行うものとする。

1-2 関連文書・準拠基準

本事業の設計、構築、試験、移行及び運用設計にあたっては、以下の文書に準拠又は整合すること。

- ・ 守口市情報セキュリティポリシー
- ・ 総務省 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¹

また、必要に応じて以下の文書を参照し提案内容の妥当性を確保すること。

- ・ デジタル庁 国・地方ネットワーク関連文書²
- ・ 国家サイバー統括室 政府機関等のサイバーセキュリティ対策のための統一基準群³

なお、上記文書間で解釈の相違が生じる場合は、本市と協議の上、本市の判断に従うこと

1-3 構築期間

協議書締結日から令和 8 年 12 月 31 日までとする。

- ・ 本市外部施設間で通信するための WAN 回線用ルータの切替は、保守期限が到来する令和 8 年 12 月 28 日以前に完了すること。
- ・ 本調達で導入する機器の設置後から令和 8 年 12 月 31 日までの間は試用期間として機器使用に係る費用を求めないものとする。

1-4 現行構成

現行の構成等について、希望する事業者に対して以下の資料を別途貸与又は閲覧提供する。

- ・ 本庁舎 LAN 配線図
- ・ ネットワーク設計書
- ・ ネットワーク構成図
- ・ スイッチ設置・LAN 配線図（保健センター）
- ・ 電波サーベイ結果（水道局、保健センター）

また、必要に応じて現地確認の機会を設ける。実施方法、日程及び範囲は別途通知する。

¹ https://www.soumu.go.jp/denshijiti/index_00004.html

² <https://www.digital.go.jp/policies/national-and-local-networks>

³ <https://www.cyber.go.jp/policy/group/general/kijun.html>

2. 基本要件

2-1 基本要件

- ① 安定稼働：本システムは、24 時間 365 日の安定稼働を前提とし、重要機器については冗長化その他の手段により単一故障点を極小化すること。障害発生時には、業務継続性を確保できる構成及び運用とすること。
- ② 拡張性：端末数、通信量、拠点数、機能追加等の変化に対し、柔軟に拡張できること。
- ③ 情報セキュリティ：情報セキュリティ水準は現行水準以上を確保すること。
- ④ 監視・管理：すべての対象機器について、統合的な監視、状態管理、異常検知、通知及びログ収集に対応すること。障害発生時は、本市及び本市が別途契約する保守事業者と連携して対応すること。
- ⑤ 設計の整理：VLAN 構成および IP アドレス体系については、現状を見直し、管理性、拡張性及びセキュリティを考慮して再設計すること。
- ⑥ 調査対応：既存環境に不明点がある場合は、必要な調査を行った上で設計・構築を行うこと。なお、現行の個別システムが支障なく稼働できる適合性を確保すること。
- ⑦ 個別要件の詳細は各章に定めるとおりとする。

3. 調達範囲と対象

3-1 調達範囲

本事業の調達範囲は、次のとおりとする。

ネットワーク調査

ネットワーク設計

機器、ソフトウェア及び必要資材の調達

構築、設置、配線及び設定

試験及び移行

関係事業者との調整を含む移行統括業務

操作教育及び成果物作成

なお、対象機器、対象外機器、設計対象、設定変更対象、試験対象、保守対象及び他事業者調整の要否については、別紙 1「責任分界表」のとおりとする。

3-2 対象拠点

対象拠点は別紙 2「対象拠点一覧」のとおりとする。

なお、本庁舎、保健センター及び水道局については館内 LAN 及び無線 AP を含めた更新対象とし、それ以外の外部施設については、原則として WAN 用ルータ設置箇所までを対象とする。ただし、別紙 1 に個別記載がある場合はこの限りでない。

3-3 対象機器

- 以下の機器を調達対象とする。
 - ・ 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
 - ・ 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
 - ・ その他の提案内容を実現するために必要な機器、ケーブル類、UPS 等
- 提案機器は法人向けの新品とし、本仕様の要件を満たすとともに、現行の機器と同等以上の性能を有すること。また、現行以上の保守性、供給継続性及び管理性を確保すること。
- WAN 用ルータは本事業で調達・導入し、統合運用監視の対象に含めるこ

と。回線事業者側設定または責任分界点以降の作業が必要となる場合は、当該事業者と調整の上で実施すること。

3-4 調達対象外

以下の機器は調達対象外とする。

- 庁内で使用している業務システム関連サーバ（アプリケーション/DB 等）
- ドメインサーバ、ファイルサーバ、ウイルス対策管理サーバ、端末資産管理サーバ、KMS サーバ
- LGWAN 系 IEEE802.1X 認証サーバ、LGWAN 系 DHCP サーバ、LGWAN 接続用機器、セキュリティクラウド接続用機器
- WAN 回線役務、IP 電話関係機器（IP 電話機、PBX その他 IP 電話の運用基盤）。

ただし、これら調達対象外機器についても、本事業の設計、移行又は接続性確認のために設定影響調査、接続試験、調整又は情報提供が必要となる場合がある。その場合の責任分界及び実施主体は、別紙 1「責任分界表」によるものとする。

4. 統合運用監視基盤

統合運用監視基盤は、SNMP、Syslog その他必要な方式により監視対象機器の状態及びログを収集できること。

4-1 提供形態・サイジング

- 提供形態は、オンプレミス（物理/仮想アプライアンス/汎用 OS 上ソフトウェア）とし、本庁サーバ室に設置すること。
- クラウド又はハイブリッド構成を提案する場合は、次の事項を明記すること。
 - ・ データ保存場所
 - ・ 国内外のデータ取扱いの有無
 - ・ 契約終了時におけるデータ返却及び消去方法
 - ・ 障害時及び保守時の窓口体制
 - ・ 利用停止時の影響範囲

- ・ 本市の情報セキュリティポリシーとの適合性
- ・ 提案時に必要リソース（CPU/メモリ/ストレージ/IO 性能）、前提となる仮想基盤や OS、サポート期間、拡張上限（監視対象台数/ポート数/イベント数/ログ保持量・期間）、性能要件（代表監視頻度・同時監視台数時の応答）を明示すること。

4-2 可用性・保全

- ・ 統合運用監視基盤について、バックアップ対象、取得頻度、世代数、保管先及びリストア手順を整備すること。
- ・ 提案する可用性構成に応じて RTO（復旧時間目標）及び RPO（復旧時点目標）を明示し、その実現方法（迅速なリストア手順、予備機・イメージ展開、バックアップ頻度と保管先等）を具体的に示すこと。
- ・ 受入試験で代表障害時の復旧時間と復旧時点を確認すること。

4-3 管理端末・UI

- ・ 監視ソフト用の管理用 UI（主に Web ベース）は、日本語表示に対応し、専用クライアントを要さないことが望ましい。専用クライアントが必要な場合は、その導入・設定・ライセンスを本事業に含めること。
- ・ 常時監視・操作のための管理端末を 1 台は本事業で確保すること。端末 OS はベンダがサポートする LTS 版（例：Windows 10/11 Enterprise LTSC 相当等）とし、管理 UI が安定動作するブラウザ/解像度/メモリ等を満たすこと。
- ・ 管理端末に必要な OS ライセンス、管理 UI 利用に必要なソフトウェア、初期設定及び運用開始時点で必要な更新適用は、本事業の範囲に含むものとする。

4-4 ネットワーク可視化に関する機能要件

以下の機能を必須機能として有すること。下記に記載がなくとも有効と思われる追加の機能があれば積極的に追加提案を行うこと。

(1) ネットワーク可視化（トポロジ）。

- ・ サーバ、スイッチ、無線 AP、PC 等の接続関係並びに物理・論理構成を可

視化し、管理者が容易に把握できること。

- デバイス間の通信状況又は負荷状況について、管理者が確認できること。
- 構成情報は、自動取得又は手動登録その他適切な方法により作成及び更新できること。
- なお、可視化の実現方式、表示方法及び更新方法は問わないが、本市の運用管理上必要な構成把握及び障害時の影響確認が可能であること。

(2)監視（死活・状態・帯域・イベント）

- 統合運用監視基盤は、本事業対象機器及び本市が指定する既存機器を監視対象として登録可能であること
- 庁舎内ネットワークを構成する通信機器（FW、ルータ、スイッチ、無線AP、無線コントローラ等）および監視対象として指定した端末（サーバ等）について死活監視を行えること。
- 状態監視・異常検知 機器状態、ポート、帯域、パケット等を監視し、異常発生時に検知できること。
- SNMP Trap および Syslog の受信・相関に対応すること。

4-5 無線 LAN コントローラ機能

- 無線 AP の集中管理ができること。管理方式は、専用コントローラ方式、クラウド管理方式又は分散管理方式のいずれでも可とする。ただし、提案方式により、設定の一元管理、障害把握、ファームウェア管理、構成変更管理及び本仕様に定める運用性を満たすこと。
- クライアント分離、隣接無線 AP 検出、コントローラ断時の通信継続等が可能であれば合わせて提案すること。
- コントローラ機能を提案しない場合は、代替方式により同等以上の管理性を確保できる理由を具体的に示すこと。

4-6 マニュアル・教育

一般的なマニュアルに加え、日本語の簡易操作マニュアル（PDF）を提出すること。簡易操作マニュアルには少なくとも以下を含むこと。

- インストール、マップ作成、デバイス設定、デバイスレベル設定、アラート設定、グラフ作成・表示、レポート出力・利用に関する操作方法

- ・ インターフェイスの見方、アクションコマンド説明

5. ネットワーク設計

5-1 VLAN・IP アドレス再設計

VLAN 構成及び IP アドレス体系は、管理性、将来拡張性、障害影響範囲及びセキュリティ確保の観点から再設計すること。

なお、IP アドレス変更を伴う対象については、対象区分、影響範囲、暫定措置、切替条件及びロールバック条件を明記した移行計画を策定すること。

(1)VLAN 再設計

- ・ VLAN 構成を見直し、以下を満たす再設計を行うこと。
 - ・ 用途ごとのセグメント方針を定めること。
 - ・ VLAN-ID 割当として、予約領域・発番ルール・端末/無線端末等の増加を見込んだ将来拡張性を考慮すること。
 - ・ 管理/運用用 VLAN を定義すること。
 - ・ トランクポート及びアクセスポートの設計並びに許可 VLAN を明確化すること。
 - ・ L2 境界及び冗長制御方式を整理し、必要に応じて STP 等の採用方針を示すこと。
- ・ 要件に応じ、以下の技術の採用可否を評価し、採用する場合は具体的な構成案と運用方法を提示すること。
 - ・ ネットワークの論理分離（VRF）
 - ・ 大規模セグメント/マルチテナント対応（VXLAN/EVPN）
 - ・ 拠点間通信の最適化・一元管理（SD-WAN）

(2)IP アドレス再設計

IP アドレス体系を見直し、以下を満たす再設計を行うこと。

- ・ LGWAN 系、マイナンバー利用事務系、インターネット系ごとにアドレス体系を分離すること。
- ・ 予約領域及び発番ルールを含む管理標準化ルールを定義すること。
- ・ 将来拡張余地を確保すること。

- 既設 DHCP の継続利用を基本とし、必要に応じてスコープ追加・見直しを行うこと。なお、現行において DHCP を利用している系統は LGWAN 系のみである。既設 DHCP の拡張、設定変更その他必要な対応を行う場合は、現行保守事業者による作業又は調整が必要となるため、受託者は当該事業者と必要な調整を行うこと。これに要する費用は本事業に含めること。現行保守事業者の連絡先は別途提示する。
- マイナンバー系ネットワークにおいて DHCP サーバを新たに設ける場合は、安全性及び系統分離に十分配慮した構成とすること。この場合、DHCP サーバに係る機器、ソフトウェア、ライセンス、構築、設定、試験その他必要な費用は本事業に含めて見積もること。
- 固定 IP 機器・サーバ・複合機・業務機器の影響調査と、移行対象一覧及び対応方針を提示すること。
- IPv6 の採否及び方針（非対応/段階導入/デュアルスタック等）を明記すること。

(3)IP アドレスの移行方針

- IP アドレス移行については、業務影響を最小化する方式を基本とし、段階移行、並行稼働又は切替窓の設定を含む移行計画を策定すること。ロールバック手順は必須とする。
- 既存システムに関わる設定・IP アドレス等の移行は、業務影響と保守範囲を踏まえ、可能な範囲を各システムの更新時に実施し、更新時に実施が困難な対象は保守期間内に計画的に実施すること。全体計画には、対象区分（更新時／保守期間）、暫定対処、切替窓、ロールバックを含めること。

5-2 LGWAN 系無線利用端末の他拠点利用

- 現状、本庁の LGWAN 系端末は DHCP 管理し、庁外施設は固定 IP 設定であるため、他拠点に持ち出しした場合に通信できない。
- 本庁、水道局及び保健センターの 3 拠点において、LGWAN 系無線利用端末を拠点間で持ち運んだ場合であっても、端末側で個別の IP 設定変更を要することなく利用できる構成とすること。
- 受託者は、LGWAN 系無線利用端末の他拠点利用を可能とする構成について提案書に明記すること。

- 実現方式は、DHCP 化、認証連携、動的 VLAN その他適切な方法によるものとし、提案書には少なくとも以下を明記すること。
 - ・ 実現方式の概要
 - ・ 端末設定変更の可否
 - ・ 既存認証基盤及び DHCP サーバへの影響
 - ・ 切替時の業務影響
 - ・ 障害時の切り分け方法

5-3 マイナンバー系ネットワークにおける無線化

現状マイナンバー系ネットワークについては有線利用している。本事業においてはエッジスイッチ・無線 AP の配置を踏まえ、マイナンバー系ネットワークにおける端末利用方式について、無線化又は有線継続のいずれかを提案するものとする。

(1)評価及び提案

受託者は、マイナンバー系ネットワークにおける端末利用方式について、無線化又は有線継続のいずれかを提案書に明記すること。提案にあたっては、以下の観点から比較検討を行い、採用する方式及びその理由を具体的に示すこと。

- セキュリティ: 総務省「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」等の基準に準拠した上で、有線利用時と同等以上のセキュリティを確保できるか。具体的な脅威（盗聴、不正アクセス等）と、それに対する技術的・運用的対策を提示すること。
- 利便性・業務効率: 無線化による利便性の向上や業務効率化の効果を具体的に示すこと。
- 技術的実現性: 安定した通信を確保するための技術的要件（電波強度、干渉対策等）や、既存システム（認証基盤等）との連携について評価すること。
- コスト: 無線化に伴う初期導入コスト及び運用コストを算出すること。

(2)構築

受託者は、本市が採用した提案内容に基づき、必要な設計及び構築を行うこ

と。なお、無線化方式が採用された場合には、以下の要件をすべて満たすこと。

- 総務省「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」に適合すること。
- 認証は原則として 802.1X を用い、共用 ID を用いないこと。
- EAP 方式及び WPA2-Enterprise 又は WPA3-Enterprise の採用方針を明記すること。
- 利用者を適切に識別できる認証方式とし、認証された利用者のみがマイナンバー系ネットワークを利用できる構成とすること。
- マイナンバー系ネットワークの通信は、LGWAN 系やインターネット系等の他系統と SSID、VLAN、アクセス制御その他必要な方法により厳格に分離すること。他系統へ収容される設計は不可とする。
- 利用者識別、接続先ネットワーク、接続元無線 AP、接続時刻その他必要な接続ログを取得・保管し、保管期間、閲覧権限及び持出禁止等の運用を設計すること。
- 利用者識別、収容制御及びセグメント分離を実現する方式は、認証連携、SSID 分離、アクセス制御、必要に応じた動的 VLAN その他適切な方法によるものとし、その理由及び運用方法を明記すること。
- 既存端末の無線設定変更は、本事業の範囲で実施すること。なお、作業の実施にあたっては、現行の端末保守事業者と十分に調整を行うこと。
- 無線化方式を採用する場合であっても、マイナンバー端末については、現行資料及び別紙 3「マイナンバー端末および IP 電話の想定台数」に記載する台数以上を有線接続により利用可能な構成とすること。
- 無線化方式を採用する場合には、保健センターにおける無線化対応についても併せて検討すること。保健センターの既存スイッチを活用することを前提とし、LGWAN 系、マイナンバー系及びインターネット系のうち複数系統を無線化できる場合は、その構成及び実現方法を示すこと。なお、実現が困難な場合は、その理由を示すこと。

5-4 IP 電話導入に係る要件

(1) 適用範囲・前提

本庁舎における IP 電話導入は令和 9 年度を予定しており、本事業の範囲はエッジスイッチの設置までとし、IP 電話機、PBX その他の電話基盤自体は調達対象外とする。現状で想定している IP 電話数については、別紙 3「マイナンバー端末および IP 電話の想定台数」を確認すること。

受託者は、将来の IP 電話導入を見据え、少なくとも以下を満たす設計を行うこと。

- ・ IP 電話機用のエッジスイッチを用意すること。台数が少ない箇所については、フロアスイッチから直接配線することも可とする。
- ・ IP 電話機の有線接続を前提としたポート設計
- ・ PoE 給電を考慮した給電ポート数および PoE 予算設計
- ・ 音声 VLAN そのほかの論理分離設計（データ系トラフィックと干渉しないこと。）
- ・ QoS、優先制御、帯域設計その他音声品質確保のための設計

また、IP 電話の導入時には、受託者は庁舎内ネットワーク運用保守事業者としてネットワークにおける要件整理・接続試験・調整などを運用保守委託で実施すること。

6. ネットワーク機器の配線・設置要件

6-1 配線・設置に関する共通要件

(1)配線ケーブル

- ・ 配線は銅線および光ファイバーを対象とする。
- ・ 新規銅線はカテゴリ 6 以上とし、規格準拠、認証試験成績書提出、ラベリング必須とする
- ・ 光（幹線/アップリンク）は用途・距離に応じ OM3/OM4 または OS2 を採用すること。コネクタ種別は現行設備と整合。試験成績書提出、ラベリング必須とする。
- ・ エッジスイッチから端末等に接続するためのケーブルについては、エン

ドユーザの接続系統の誤接続を防止するため、ケーブル色分け、両端ラベリング、情報コンセント表示及び配線台帳整備を行うこと。識別方法は本市と協議の上決定すること。現状は、フロアスイッチとエッジスイッチ間の幹線（水色）、マイナンバー系ネットワーク（赤）、LGWAN系ネットワーク（黒）等、複数色で識別している。

- ・ 既存ケーブルの流用可否は調査で判定し、不足分は調達・施工、不要ケーブルは撤去・廃棄すること。

(2)設置

- ・ ラックに収容しないエッジスイッチ等機器は床置き以外で、保守交換容易な設置とすること。
- ・ 無線 AP は原則天井設置、困難箇所は協議の上高所壁面を可とする。旧設置箇所は原状回復すること。
- ・ 本庁舎本館、保健センター健康推進課執務室などフリーアクセスであるエリアは、床下を通線すること。フリーアクセスでない露出配線が必要な場合は、配線モール等により保護し、歩行・台車等の動線と交差しないよう安全性及び保守性に配慮して施工すること。
- ・ 強電系統との離隔・交差方法は関係法令・施設基準に従い、電磁干渉および安全に配慮すること。
- ・ 防火区画等の貫通部は建築・消防関連法令に従い適切な耐火措置（貫通部処理）を施すこと。また、美観と保守性を考慮し、点検口等からのアクセス性を確保すること。必要に応じ原状回復を行うこと。
- ・ 機器の梱包材などの廃棄物は受託者が処分すること。
- ・ 機器を搬入する際は、施設に損傷を与えないよう養生など必要な措置を実施すること。

6-2 本庁舎における要件

(1)配線・敷設

- ・ ディストリビューションスイッチからフロアスイッチを通り、各執務室へ無線 AP およびエッジスイッチを敷設すること。
- ・ 別館における配線方式、対象フロア及び設置条件については、現行レイアウト図面等及び現地調査結果に基づき、本館との整合を考慮して設計する

こと。

- 既存配線の取扱いについては、配線の敷設時期及び用途に応じて区分するものとし、5年前の更新時に更新又は新設したコアスイッチからディストリビューションスイッチまでの幹線、ディストリビューションスイッチからフロアスイッチまでの配線及びフロアスイッチからエッジスイッチまでの配線のうち当該更新時に新設したものについては、原則として流用するものとし個別調査は要しない。
- フロアスイッチからエッジスイッチまでの配線のうち、5年前の更新以前から継続使用しているものについては、原則として更新対象として見込むこと。
- エッジスイッチから端末、複合機、プリンタその他接続機器までの配線については、日常使用に伴う消耗及び摩耗を踏まえ調査を実施し、更新対象として見込むこと。
- ただし、上記の原則流用又は原則更新の区分により難しい事情がある場合は、本市と協議の上、必要な確認又は調整を行うこと。

(2)エッジスイッチ設置

エッジスイッチ設置に関する要件は以下のとおりとする。

- 原則として現行同様に各フロアの職員が在席する各拠点（島）に対し設置すること。
- 現状有線接続している端末・プリンタ数を満たす数のエッジスイッチを用意すること。ただし、5-3 マイナンバー系ネットワークにおける無線化にて無線化を提案する場合は、無線対象となる機器分については提案数から除いた適切な数を用意すること。
- 必要台数は現行レイアウト図面及び現地調査に基づき受託者が提案し、本事業開始後に協議の上決定すること。
- 本庁舎内の全会議室（地下1階～7階、9階～10階）はエッジスイッチを常設しないが、設置した場合に有線 LAN 接続が可能となるよう必要な配線経路、収容余地又は敷設方法を設計に含めること。
- 各フロアの有線 LAN では、当該ループ検知・抑止機能を有効化し、対象ポート、通知方法、復帰条件（自動/手動）を設計書に明記すること。

(3)無線 AP 設置

無線 AP 設置に関する要件は以下のとおりとする

- 地下 1 階～10 階（※7 階南フロアと 8 階を除く）及び別館 1, 2 階で常時安定接続できる環境を構築すること。
- 必要台数・設置場所は現行庁舎レイアウト図面及び現地調査に基づき受託者が提案し本事業開始後に協議の上決定すること。

6-3 水道局における要件

(1)配線・敷設

- 水道局庁舎については現状 WAN 用ルータから、1～4 階の各フロアに設置したスイッチに配線し、当該スイッチから無線 AP および端末・プリンタへ配線している。なお、局内のケーブルについては老朽化しており使用から 30 年経過しているものもあるため、既存ケーブルの流用可否の調査の際留意すること。
- 水道局庁舎のスイッチの配置は現行配置を踏襲することとする。
- 既存 OA ボックスを流用する場合は、その寸法、耐荷重、放熱性及び保守性を確認すること。提案機器が既存 OA ボックスに収容できない場合は、本事業の範囲で必要な設置対応を行うこと。
- 高度浄水処理棟については、WAN 用ルータから直接無線 AP および端末・プリンタ等機器へ配線するものとする。

(2)無線 AP 設置

- 無線 AP の設置箇所は、別途提供する電波サーベイ結果および無線 AP 仕様想定範囲を示したレイアウト図面に基づき受託者が提案し事業開始後に協議の上決定することとする。
- 高度浄水処理棟については、WAN 用ルータから無線 AP へ配線する構成を想定しているため、無線 AP への電源供給が確実に行えるよう必要な措置を講じること。なお、WAN 用ルータに PoE 給電機能を必須とはせず、給電方法については、外付け PoE インジェクターの利用、電源コンセントからの給電その他適切な方法を含め、受託者の提案に基づき本市と協議の上、決定するものとする。

6-4 保健センターにおける要件

(1)配線・敷設

- 保健センターについては現状 WAN 用ルータから、1～4 階の各フロアに設置したスイッチに配線し、当該スイッチから無線 AP および端末・プリンタへ配線している。なお、センター内のスイッチおよびケーブルについては令和 6 年 9 月に敷設したケーブルと、それ以前から使用しているケーブルが混在しているため、既存ケーブルの流用可否の調査の際留意すること。
- 保健センターの既存スイッチは本事業における更新対象外とする。ただし、統合運用監視基盤における監視対象として取り込むことを原則とし、既存機器の仕様上取得可能な範囲で監視、通知及び状態把握を行うこと。なお、既存機器の仕様により監視対象化が困難な場合は、その理由及び代替案を提案書に明記すること。

(2)無線 AP 設置

- 無線 AP の設置箇所は、別途提供する電波サーベイ結果および無線 AP 仕様想定範囲を示したレイアウト図面に基づき受託者が提案し事業開始後に協議の上決定することとする。
- 保健センターにおける無線化については、庁内と同様の構成を基本とし、現行スイッチの構成を踏まえた上で、1 台の無線 AP による複数系統の収容が可能な場合は、その構成案及び必要条件を提案すること。本市の求める無線等の範囲は現行図面に記載しているためそちらを確認すること。なお、実現が困難な場合は、その理由を示すこと。

6-5 WAN 用ルータ

- WAN 用ルータは、各対象拠点に設置し、責任分界点である ONU 以降に接続すること。
- 現地調査結果に基づき、必要な配線、電源及び設置環境を整備すること。
- WAN 用ルータの設置にあたっては、回線種別、接続先機器、設置場所の条件及び将来拡張を考慮し、保守性及び運用性に配慮した構成とすること。
- WAN 用ルータは少なくとも以下を満たすこと。

- ・ 本市が指定する回線方式に対応できること
- ・ 遠隔から設定変更、状態確認及びログ確認が可能であること
- ・ 統合運用監視基盤の監視対象に含めること
- ・ 必要なルーティング、QoS 及びアクセス制御を設定可能であること。なお、ルーティング方式は提案内容に基づくものとし、詳細は 7-7 「WAN 用ルータ」の機器要件によること。
- ・ 回線切替時には、既存事業者及び新規回線事業者と調整の上、切替手順、試験手順及びロールバック手順を作成すること
- ・ 設置拠点、回線種別は別紙 2「拠点一覧」を参照すること。

7. ネットワーク機器の機器要件

7-1 機器に関する共通要件

本章に定める対象機器は、機器種別ごとの個別要件に加え、以下の共通要件を満たすこと。

- ・ 現行の利用状況及び本事業で見込まれる構成変更を踏まえ、安定運用が可能な性能、機能及び拡張性を有すること。
- ・ 将来の端末数、通信量、無線利用、機能追加及び構成変更に対応できること。
- ・ 機器の仕様上制約となる事項がある場合は、提案時に明示すること。
- ・ 省エネルギー性に配慮した機器を積極的に提案すること。
- ・ 機器の役割及び重要性に応じて、冗長化、冗長電源、冗長リンクその他適切な可用性対策を講じること。
- ・ 障害時に業務影響を最小化できる構成とし、交換、復旧及び切戻しが円滑に行えること。
- ・ 特定ベンダー独自技術に過度に依存せず、可能な限り IEEE 等の標準規格に準拠した機器であること。
- ・ 機器の状態確認、設定変更、障害切り分け及び保守対応に必要な管理手段を有すること。
- ・ 管理手段として、CLI 及び GUI による操作に対応すること。なお、GUI を有する場合は日本語表示に対応することが望ましい。

- 統合運用監視基盤との連携に必要な監視情報及びログ情報を取得可能であること。
- SNMPv3 による監視に対応すること。
- Syslog 等の標準的なプロトコルによりログ情報を取得可能であること。
- 時刻同期が必要な機器は、NTP により適切に時刻同期できること。
- 設定情報の保存、バックアップ及び復元が可能であること。
- 機器種別に応じて、アクセス制御、認証、ログ取得、設定保護、不正接続防止その他必要なセキュリティ機能を有すること。
- 管理通信は、SSH、HTTPS 等の暗号化された方式により実施できること。
- 不要なサービス、不要なポート及び不要な管理機能は停止又は無効化できること。
- 提案機器は、令和 13 年 12 月 31 日まで、メーカーによるハードウェア保守及びソフトウェアサポートが提供可能であること。
- 上記期間中、ファームウェア、セキュリティパッチその他必要なアップデートが提供されること。

ハードウェア保守の提供内容は、先出しセンドバック、オンサイト保守その他の対応区分を含め、提案時に明示すること。

- 将来の通信量増加やセキュリティ機能強化を見込み、十分な処理能力を有すること。提案時には、各ネットワーク機器について以下の項目について具体的な数値を明記すること。
 - ・ ファイアウォールスループット
 - ・ セキュリティ機能有効時のスループット
 - ・ VPN 利用時のスループット
 - ・ 最大同時セッション数
 - ・ 新規セッション処理性能

7-2 サーバ室に設置するネットワーク機器

本庁サーバ室に設置するネットワーク機器は、本市庁内ネットワーク全体の中核を担う機器として、高い可用性、処理性能、保守性及び拡張性を有すること。各機器は、7-1「機器に関する共通要件」に加え、以下の要件を満たすこ

と。

(1)ファイアウォール

ファイアウォールは、庁内ネットワークと外部接続系統との境界において、通信制御、脅威の検知及び防御並びに VPN 接続を担う機器として、以下の要件を満たすこと。

- 単一故障点を排除するため、2 台による冗長構成とすること。
- 冗長方式は、Active-Standby、Active-Active その他同等以上の可用性を確保できる方式とし、提案時にその構成及び切替動作を明示すること。
- 冗長切替時の通信影響を最小化できる構成とすること。
- 現行通信量、将来の通信量増加及び有効化するセキュリティ機能を考慮し、十分な処理性能を有すること。
- ステートフルパケットインスペクションに対応すること。
- 送信元/送信先 IP アドレス、ポート番号、プロトコル、アプリケーション識別その他必要な条件に基づく通信制御が可能であること。
- NAT/NAPT に対応すること。
- 静的ルーティングに対応すること。必要に応じて動的ルーティングにも対応可能であること。
- 不正侵入の検知又は防御機能を有すること。
- アプリケーション単位での識別及び制御が可能であること。
- URL フィルタリング、マルウェア対策その他の脅威対策機能を有することが望ましい。
- 必要に応じて、複数セグメントを論理的に収容できること。
- VPN 機能として IPsec-VPN に対応すること。必要に応じて、その他の安全な接続方式にも対応可能であること。
- 管理ログ、システムログ、通信ログ、セキュリティイベントログ及び VPN 接続ログを取得できること。
- 障害解析、監査及びインシデント対応に必要な情報を記録できること。
- コアスイッチ、外部接続回線、外部接続関連機器その他必要な接続先を考慮し、必要なインターフェース種別、速度及びポート数を備えること。受託者はネットワーク全体の設計に基づき、最適なポート構成を提案すること。

- 冗長接続、将来拡張及び保守作業を考慮し、必要な予備ポートを確保すること。
- なお、記載する性能要件は最低要件とし、各機能を有効化した状態で本市の利用条件を満たすこと。

(2)コアスイッチ（L3 スイッチ）

コアスイッチは、ファイアウォール、サーバ、本庁舎のディストリビューションスイッチ等を集約する基幹機器である。高速かつ安定した通信を常時提供するため、以下の要件を満たすこと。

- 単一故障点を排除するため、2 台による冗長構成とすること。
- 2 台を論理的に一体として運用できる構成又は同等以上の可用性及び保守性を確保できる構成であること。
- 片系障害時であっても通信継続に支障を生じない構成とすること。
- 庁内全体の通信を安定して処理できる十分なスイッチング容量及び転送性能を有すること。
- 将来の端末増加、無線利用拡大、IP 電話導入及び機能追加に対応可能な性能余力を有すること。
- 提案時には、主要な性能諸元を明記すること。
- L3 スイッチとして動作し、VLAN 間ルーティングが可能であること。
- 静的ルーティングに対応すること。必要に応じて動的ルーティングにも対応可能であること。
- IEEE 802.1Q 準拠の VLAN 機能を有すること。
- ACL による通信制御が可能であること。
- QoS 機能を有し、重要通信の優先制御に対応できること。
- LACP 等のリンクアグリゲーション機能に対応すること。
- 必要に応じて、論理分離機能に対応可能であること。
- ファイアウォール、サーバ室内スイッチ、ディストリビューションスイッチその他必要な接続先との接続を考慮し、必要なインターフェース種別、速度及びポート数を備えること。
- 将来の構成変更、機器増設及び保守作業に備え、必要な予備ポートを確保すること。

(3)サーバ室内スイッチ

サーバ室内スイッチは、本庁サーバ室内に設置する各種サーバ、統合運用監視基盤、管理端末その他必要な機器を収容するためのスイッチとして、以下の要件を満たすこと。

- 将来の構成変更、機器増設及び保守作業に備え、必要な予備ポートを確保すること。
- 接続対象機器の種別、台数及び通信要件を踏まえ、必要なポート数及び性能を有すること。
- コアスイッチと接続し、必要に応じて冗長アップリンク構成を採用できること。
- 接続対象の重要性を踏まえ、保守性及び将来拡張性に配慮した構成とすること。
- IEEE 802.1Q 準拠の VLAN 機能を有すること。
- 必要に応じて LACP 等のリンクアグリゲーションに対応すること。
- ループ防止、ポート制御その他必要な L2 機能を有すること。
- 接続対象に応じて必要なアクセス制御その他の設定が可能であること。
- 接続対象機器及びコアスイッチとの接続を考慮し、必要なインターフェース種別、速度及びポート数を備えること。
- 通信量、冗長性及び将来拡張を考慮した帯域を確保すること。

7-3 本庁舎における要件

本庁舎に設置するネットワーク機器は、執務室、会議室その他庁舎内の各エリアにおいて、安定した有線及び無線ネットワーク接続を提供するための機器として、7-1「機器に関する共通要件」に加え、以下の要件を満たすこと。

(1)ディストリビューションスイッチ

ディストリビューションスイッチは、本庁舎内の各フロアスイッチを集約し、コアスイッチとの接続を担う機器として、以下の要件を満たすこと。

- 接続対象となるフロアスイッチ及び上位接続を踏まえ、必要に応じて冗長構成又は冗長アップリンク構成を採用できること。
- 障害時に影響範囲を局所化できる構成とすること。
- 接続するフロアスイッチ及びその配下端末の通信を安定して処理できる十

分なスイッチング容量及び転送性能を有すること。

- 将来の端末増加、無線利用拡大及び機器増設に対応可能な性能余力を有すること。
- L2 スイッチ又は L3 スイッチとして必要な機能を有し、設計に応じて適切に運用できること。
- IEEE 802.1Q 準拠の VLAN 機能を有すること。
- 必要に応じて ACL による通信制御が可能であること。
- QoS 機能を有し、重要通信の優先制御に対応できること。
- LACP 等のリンクアグリゲーション機能に対応すること。
- ループ防止又はループ検知のために必要な機能を有すること。
- コアスイッチ及び各フロアスイッチとの接続を考慮し、必要なインターフェース種別、速度及びポート数を備えること。
- 上位及び下位接続について、冗長性、保守性及び将来拡張を考慮した構成とすること。

(2)フロアスイッチ

フロアスイッチは、本庁舎各階において執務用端末、プリンタ、無線アクセスポイント、IP 電話機その他必要な機器を収容するための機器として、以下の要件を満たすこと。

- 設置フロア（本館地下 1 階から 9 階各階南北 EPS）における接続対象機器の種別、台数及び通信要件を踏まえ、必要なポート数及び性能を有すること。
- ディストリビューションスイッチと接続し、必要に応じて冗長アップリンク構成を採用できること。
- 執務継続に支障を生じないように、保守性及び将来拡張性に配慮した構成とすること。
- フロアスイッチは、端末、プリンタ、無線アクセスポイントその他の情報系機器に加え、IP 電話機を同一機器に収容できること。なお、フロアスイッチについては、情報系機器用と IP 電話機用で物理的に機器を分離することは要しない。
- IEEE 802.1Q 準拠の VLAN 機能を有すること。
- ループ防止、ポート制御その他必要な L2 機能を有すること。

- DHCP スヌーピング、ARP スプーフィング対策、ポート単位のアクセス制御その他有効な L2 セキュリティ機能を有することが望ましい。
- 接続対象機器及び上位スイッチとの接続を考慮し、必要なインターフェース種別、速度及びポート数を備えること。
- IP 電話機を収容する場合は、情報系通信と論理的に分離できること。
- 無線アクセスポイントや IP 電話その他 PoE 受電機器を接続する箇所については、PoE (IEEE 802.af) 以上に対応し、想定台数のポート数を有し、想定接続台数に対して同時給電可能な装置全体の給電容量を有すること。
- IP 電話機を安定して利用できるよう、QoS による音声通信の優先制御に対応すること。

(3)エッジスイッチ

エッジスイッチは、会議室、窓口、共用部その他限られたエリアにおいて少数の端末、プリンタ、IP 電話又は無線アクセスポイントを収容するための機器として、以下の要件を満たすこと。

- 設置箇所における接続対象機器の種別、台数及び通信要件を踏まえ、必要なポート数及び性能を有すること。
- 設置箇所の用途に応じ、必要な静音性、設置性及び保守性に配慮した機器であること。
- 端末、プリンタその他の情報系機器を収容するためのエッジスイッチと、IP 電話を収容するためのエッジスイッチは、障害影響の分離、運用管理の明確化及び音声品質確保の観点から、同一筐体で共用せず、それぞれ別個の機器として構成すること。
- 執務空間、窓口又は会議室等への設置を考慮し、ファンレスであること。
- 設置性を考慮し、マグネットその他これと同等の方法により、机、什器その他適切な箇所へ固定できること。
- IEEE 802.1Q 準拠の VLAN 機能を有すること。
- ループ防止、ポート制御その他必要な L2 機能を有すること。
- ループ検知機能を有すること。ループを検知した場合には、ポートをリンクダウンさせる等、あらかじめ設定した動作を自動実行可能であること。
- ループ検知時には、LED 表示その他の方法により、異常を視覚的に確認できること。

- 接続対象に応じて必要なアクセス制御その他の設定が可能であること。
- 上位スイッチ及び接続対象機器との接続を考慮し、必要なインターフェース種別、速度及びポート数を備えること。
- 無線アクセスポイントその他 PoE 受電機器を収容する場合は、接続対象台数及び給電要件を踏まえ、必要な PoE 給電容量を確保すること。
- IP 電話を収容するエッジスイッチについては、音声通信を安定して利用できるよう、QoS による優先制御に対応すること。
- IP 電話用エッジスイッチについては、PoE+（IEEE 802.3at）に対応し、想定台数の IP 電話を接続可能なポート数を有し、同時給電可能な装置全体の給電容量を有すること。

7-4 水道局における要件

- 新たに調達する機器は、WAN 用ルータ 2 台（水道局庁舎、水道局高度浄水処理棟）、スイッチ 4 台、無線 AP8 台（うち 1 台を水道局高度浄水処理棟に設置）とする。
- 水道局庁舎の各フロアに設置するスイッチについては、4 台を想定すること。なお、提案に当たっては、現状使用しているポート数を満たすスイッチ（1G 対応、ファンレス、マネージド L2、8～20 ポート程度、ループ防止機能、Web GUI 管理機能）を選定すること。なお、無線アクセスポイントその他 PoE 受電機器を接続する箇所については、PoE（IEEE 802.af）以上に対応し、想定台数のポート数を有し、想定接続台数に対して同時給電可能な装置全体の給電容量を有すること。提案機器は、水道局庁舎内の各フロアにおいて、端末、プリンタ及び無線 AP の接続を収容し、安定した運用が可能な構成とすること。既存 OA ボックスその他設置環境へ収容する場合は、寸法、放熱性、保守性及び配線性を十分考慮すること。
- 無線 AP については 7-6 無線 AP、WAN 用ルータについては 7-7WAN 用ルータに記載の要件を満たすこと。

7-5 保健センターにおける要件

- 新たに調達する機器は、WAN 用ルータ、無線 AP とする。
- 無線 AP については 7-6 無線 AP、WAN 用ルータについては 7-7WAN 用ル

ータに記載の要件を満たすこと。

- 接続先スイッチが PoE 対応でない場合は、外付け PoE インジェクターの利用、または電源コンセントからの給電を含めて、受託者と協議の上で給電方法を決定すること。

7-6 無線アクセスポイント

無線アクセスポイントは、本庁舎、水道局、保健センターその他必要箇所において、業務利用に耐える安定した無線 LAN 環境を提供するための機器として、7-1「機器に関する共通要件」に加え、以下の要件を満たすこと。

(1)基本要件

- 設置箇所の利用形態、利用者数、端末数、電波状況及び想定トラフィックを踏まえ、安定した通信が可能な性能を有すること。
- 無線エリア設計に基づき、必要な設置台数、配置及び電波出力を適切に設定できること。
- 屋内設置を基本とし、設置場所の環境条件に適合すること。
- Wi-Fi 6 (IEEE 802.11ax) 以上に対応すること。
- 無線機能として以下を満たすこと。
 - ・ 2.4GHz 帯及び 5GHz 帯を同時に利用可能であること。6GHz 帯対応を提案可とする。
 - ・ 必要に応じて複数 SSID を提供できること。
 - ・ SSID ごとに認証方式、暗号化方式、VLAN その他必要な設定を分離できること。
 - ・ 利用状況及び周辺環境に応じて、チャンネル及び出力を適切に設定できること。
 - ・ 無線端末間通信を禁止する機能を有すること。
 - ・ インターネット系ネットワークについては、現行運用において 2.4GHz 帯の無線でステルス SSID を使用している。受託者は、特定の利用者以外による不用意な利用の抑止、LGWAN 系その他の系統との誤接続防止及び適切な系統分離を実現できる構成とすること。なお、これらの目的を同等以上に達成できる場合は、ステルス SSID 以外の方式による提案も可とする。WPA2-Enterprise 及び WPA3-

Enterprise に対応すること。

- 不正接続の抑止及び利用者の適切な認証を実施できること。
- 無線 LAN コントローラ又は同等の集中管理機能により、一元的に設定、監視及び保守が可能であること。
- 設定変更、障害確認、稼働状況確認その他運用管理に必要な情報を取得できること。
- 有線ネットワークとの接続に必要なインターフェースを有すること。
- PoE+ (IEEE 802.3at) 以上の受電に対応すること。
- 必要な給電条件は、接続先スイッチの PoE 設計と整合すること。

7-7 WAN 用ルータ

WAN 用ルータは、本庁舎と各拠点との間の広域通信を担い、安全かつ安定した拠点間接続を提供するための機器として、7-1「機器に関する共通要件」に加え、以下の要件を満たすこと。

- 接続する回線種別、帯域、拠点構成及び想定通信量を踏まえ、安定した広域通信を提供できる性能を有すること。
- 各拠点の業務継続に支障を生じないように、保守性及び将来拡張性に配慮した構成とすること。
- 契約回線帯域を十分に処理できるスループットを有すること。
- VPN 機能を利用する場合は、暗号化処理を含めて必要な性能を有すること。
- 提案時には、スループット、VPN 処理性能、搭載インターフェースその他主要な性能諸元を明記すること。主要な性能諸元を明記すること。
- ルーティング機能を有し、静的ルーティングに対応すること。なお、ルーティング方式は、静的ルーティング、動的ルーティングその他適切な方法によるものとし、採用方式、その理由、運用方法及び対応プロトコルを提案書に明記すること。
- 動的ルーティングを採用する場合は、対応可能なルーティングプロトコルを明記すること。
- IPsec-VPN に対応すること。
- QoS 機能を有し、重要通信の優先制御に対応できること。

- 必要に応じて回線障害時の切替又は迂回構成に対応可能であること。
- WAN 側及び LAN 側の接続を考慮し、必要なインターフェース種別、速度及びポート数を備えること。
- 接続先機器、回線終端装置及び将来拡張を考慮した構成とすること。
- 多拠点展開を考慮し、設定、展開及び保守が効率的に行えること。
- 必要に応じて、初期設定の自動展開その他運用負荷軽減に資する機能を有することが望ましい。

8. テスト・移行に係る要件

8-1 テストに係る要件

- 受託者は、単体試験、ネットワーク構成試験、統合運用監視基盤試験、無線 AP 試験、賦課試験を含む試験計画を作成し、本市の承認を得たうえで実施すること。
- 試験ごとに、目的、前提条件、手順、期待結果、合否判定基準、不具合発生時の取扱い及び再試験条件を明記すること。
- 試験項目は、機器の死活監視、設定確認、通信性能、冗長構成動作、セキュリティ設定及び運用管理機能を含むこと。
- 総合試験として、以下の動作確認を行うこと。
 - ・ 正常系・障害系（回線／機器切替）
 - ・ 情報セキュリティ関連機能
 - ・ ルーティング機能
 - ・ 外部接続機能
 - ・ 統合監視（可視化・監視・ログ収集・通知・バックアップなど）
 - ・ 外部施設間 WAN 疎通
- 試験結果は報告書としてとりまとめ、本市の承認を得ること。

8-2 移行要件

- 受託者は切替手順、ロールバック手順、業務影響の最小化策を含めた移行計画を策定し、本市の承認を得た上で実施すること。
- 移行にあたり、事前に必要な設定変更、試験及び関係者調整を完了させる

こと。

- 移行作業は受託者が統括し、本市及び関係事業者と調整しながら実施すること。
- 並行稼働期間の設定等により、業務継続性に影響を与えないこと。
- 切り替え時は、確実なサポート体制をとること。
- 切り替え後の障害に備え、ロールバック手順・発動条件・所要時間・確認手順を事前に整備し、可能な範囲でリハーサルすること。
- IP アドレスの変更を伴う場合は、影響調査・段階移行・復旧手順を含む計画を必須とする。
- 手戻りリスクが高い設定変更（コア切り替え、IP 一括変更、無線認証方式切り替え等）は、事前検証・レビュー・リハーサルを必須とする。
- WAN 回線更新に伴う切り替えについては、WAN 回線提供事業者と役割分担を明確化し、切替計画・試験計画・当日統括（指揮系統、エスカレーション）を含めて実施すること。
- 本番切替前には移行判定会を実施し、切替条件、実施体制、連絡体制、当日判断基準及びロールバック条件を確認すること。

9. セキュリティ要件

9-1 基本要件

- 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ぐこと、並びに、発生した場合に被害を最小限に抑えること。
- 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。
- 本事業において、発注者の意図しない変更や機密情報の窃取等が行われない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。
- 発注者の意図しない変更や機密情報の窃取等が行われないことを保証するための具体的な管理手順や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や各担当者がアクセス可能な範囲等を示した管理体制図）を発注者との協議の上、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。

- 本事業において発注者の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、発注者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や作業履歴等を記録し、発注元から要求された場合には提出させるようにする等）また、当該手順及び体制が妥当であることを証明するための書類を発注者との協議の上、必要と判断された場合は提出すること。
- 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。
- 本事業に従事する受託者の従業員すべてに対して、情報セキュリティに関することなどの教育を実施すること。
- 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に、脆弱性診断の実施、検出された脆弱性への対応を行うこと。
- また、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。
- 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を下表に示す。本事業における運用保守対象の範囲で該当するものは、各項目に対し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	・ 共用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 ・ 推測されやすい脆弱なパスワードが使用されている ・ 認証情報がファイル等に平文で書かれている
2	アクセス制御不備	・ 必要な強度の認証が行われていない ・ 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 ・ 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
3	暗号化不備	・ 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
4	資産管理、脆弱性管理不備	・ 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） ・ 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
5	Web アプリケーションの脆弱性	・ 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 ・ 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
6	ログ管理不備	・ 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） ・ 定期的なログの点検又は分析が実施されていない
7	外部委託の管理不備	・ 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 ・ 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

9-2 ネットワーク管理におけるセキュリティ要件

- ・ 管理通信は、業務通信と分離した専用ネットワーク上で行うこと。
- ・ 管理者権限を分離し、共有 ID の使用は原則禁止とすること。やむを得ず使用する場合は、理由・代替策などを提案すること。
- ・ 管理操作ログが追跡できる仕組み（装置ログ、統合監視、台帳・変更管理等）を整備すること。
- ・ 各機器及び監視基盤において、ログを適切に取得・保管し、保管期間及び閲覧権限を設定できること。ログの保管期間、閲覧権限、バックアップ方針を運用設計に明記すること。
- ・ 機器ログ・監視ログの整合性確保のため、時刻同期（NTP 等）を設計に含めること。
- ・ 保守接続は暗号化された方式（例：SSH、HTTPS）で行い、不必要なポート及びサービスは無効化すること。

- 設定変更は事前承認制とし、変更履歴を記録すること。
- 機器間通信は暗号化されたプロトコル（例：IPsec、TLS）を使用すること。
- 管理端末及び設定情報は、適切な権限管理の下で保管し、持出を禁止すること。
- 受託者は、構築時点で推奨ファームウェアを適用し、以後の更入手順（影響評価、適用計画、ロールバック）を手順書に含めること。
- 重大な脆弱性が公表された場合の対応フロー（情報収集→影響評価→暫定/恒久対策→報告）を運用設計に含めること。

10. プロジェクト要件

10-1 プロジェクト体制及び役割

本事業を適切・効率的に履行するためのプロジェクト体制として、以下の役割を担うものを選任すること。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、それぞれ違う人物を選任すること。なお、(2)は、複数人選任することを妨げない。

(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。プロジェクト計画書を作成し、本事業を円滑に遂行するための各作業工程管理及び関連する業務や利害関係者との調整等を実施し、作業全体を統括して管理する。

本プロジェクトを管理するのに相応しいだけの知識や経験を有している者を採用すること。

(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プロジェクト計画書に基づき、現場で作業を実施する責任者。本市と現場レベルの打ち合わせを実施する者。本事業の各業務に精通し、知識や経験を有している者を採用すること。

(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セキュリティ管理を行う責任者を配置すること。

10-2 プロジェクト体制及び役割に関する留意事項

(1)プロジェクト体制の記載事項

受託者は、プロジェクト体制の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。

(2)プロジェクト体制の変更

原則としてプロジェクト体制の変更は原則認めないこととする。ただし、進捗に著しい遅れが発生した等の理由で要員の追加及び作業担当者の変更がやむを得ない場合は、速やかに改善策を書面で提示し、本市の承諾を得ること。

(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。

(4)プロジェクト停滞に伴う体制変更指示

プロジェクト計画書等で示した業務作業が適正に履行されていない、または、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、本市は、受託者に対して体制の変更を申し入れすることができるものとし、受託者はその申し入れに従い、適切に対応すること。

10-3 プロジェクト計画書

受託者は、契約締結から 10 日以内にプロジェクト計画書を提出すること。
また、プロジェクト計画書には、以下の内容を含めること。

- ・ プロジェクトの方針、目的
- ・ スケジュール
- ・ 体制図（体制と役割分担）
- ・ 対象範囲（スコープ）
- ・ 成果物

- ・ 制約条件
- ・ 品質管理目標
- ・ 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）
- ・ 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こと

10-4 WAN 回線更新を含む移行統括（PMO）要件

本庁舎と外部施設間で通信するための WAN 回線も同じく令和 8 年度に更新する予定である。安全かつ確実な移行を実施するため、受託者は、WAN 回線更新を含む全体移行の統括主体として、既存事業者、新規回線事業者、本市及び関係者との間で必要な調整を行うこと。

少なくとも以下を実施すること。

- ・ 本事業と WAN 回線更新を含む全体移行計画の策定
- ・ 関係者間の責任分解整理
- ・ 会議体（移行調整会議）の運営
- ・ 進捗管理
- ・ 課題管理及びリスク管理
- ・ 切替計画、切り替え判定基準およびロールバック計画の策定
- ・ 当日体制および連絡体制の整備
- ・ 移行結果報告書の作成
- ・ その他 PMO として必要な作業

10-5 プロジェクト作業場所

設計、設定等の準備は原則、受託者所内で実施すること。各作業の実施、各作業に関する打ち合わせ、報告、進捗会議については、原則として、本市の会議室またはオンラインで実施すること。

10-6 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。

10-7 プロジェクトの会議体

本事業の実施にあたっては、以下の会議体を開催し、議事内容について責任のある回答ができる要員を参加させること。会議の開催にあたっては、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すること。

(1)進捗確認会議

本業務の進捗状況確認、スケジュール管理、課題検討及び解決、品質管理等を実施するための会議を原則月1回の頻度で開催する。

(2)移行調整会議

既存庁舎内ネットワーク保守事業者、既存庁舎外ネットワーク事業者、次期庁舎外ネットワーク事業者など本市ネットワークに関与する契約事業者など関係者を招集し、移行に関する進捗状況確認、スケジュール管理、課題検討及び解決を実施するための調整会議を必要に応じて開催する。

(3)工程完了判定会議

各工程の完了時にレビューを行い、次の工程に進むための判定を行う会議を実施する。

(4)本番稼働判定会議

運用テスト（顧客受入テスト）を実施後に、本番稼働を実施してよいかの判定を行う会議を実施する。なお、本番稼働判定会議の際は、本番移行切替計画書を提示したうえで本番稼働の判定を行うものとする。

(5)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。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。

(6)責任者会議

緊急時、問題発生時、課題解消の進捗が芳しくない時等に、本市の求めに応じて、プロジェクトマネージャ（PM）が参加し、課題の解決を早急に図るための会議を実施すること。

10-8 レビュー・承認

手戻り・リスクを抑制するため、受託者は以下の承認ゲートを設定し、発注者の確認・承認を経て次工程へ進むこと。

- ・ 基本設計レビュー
- ・ 詳細設計レビュー
- ・ 本番切替判定
- ・ 検収前レビュー

10-9 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するため、課題管理を実施すること。

課題管理に当たり、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、解決日を課題一覧にまとめ、一元管理すること。また、その他必要と考えられる項目についても管理すること。

課題管理表の内容については、月次での状況確認及び整理を実施し、進捗確認会議で報告すること。また、課題の完了にあたっては、必ず受託者及び本市での合意を必須とすること。

10-10 文書管理

- ・ 必要に応じて、会議・打ち合わせにおける議事録等の作成、保管、管理を行うこと。
- ・ 受託者は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。

11.特記事項

(1)WAN 回線の更新について

- ・ WAN 回線の更新に当たっては、現行回線事業者が引き続き提供する場合は、原則として既設回線設備を活用し、新たな引込工事を要しない前提で移行計画を策定すること。

- ・ 新規回線事業者が参入する場合は、現行回線の運用を継続したまま別系統で新規回線を敷設することとし、少なくとも令和 8 年 12 月初旬までに敷設を完了の上、疎通確認及び切替作業に着手可能な状態とすること。
- ・ 受託者は、上記双方のケースを想定し、回線事業者、既存事業者、本市関係部署その他関係者との調整を含む移行計画を策定すること。移行計画には、事前確認事項、工程、試験項目、切替手順、切替条件、障害時対応、ロールバック手順及び役割分担を明記すること。

(2) 庁外施設の増減への対応について

- ・ 庁外施設については、今後の施設の統廃合、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ことを前提として設計及び構築を行うこと。
- ・ 受託者は、保守期間中に当該変動が生じた場合に、WAN 用ルータの再配置、流用、予備機活用その他必要な対応を円滑に実施できるよう、機器選定、設置条件、設定方針、監視方式、台帳整備及び成果物作成において十分配慮すること。
- ・ 拠点廃止等により不要となった WAN 用ルータについては、将来的に他拠点へ転用又は予備機として活用できるよう、設定初期化手順、再設定手順、移設時の確認事項及び管理方法を整理し、成果物に反映すること。
- ・ また、拠点新設又は機器故障時の迅速な対応を可能とするため、予備機の確保を前提とした機器構成及び管理方法を提案すること。

(3) 複合機無線化への対応について

- ・ 令和 7 年 3 月に一部複合機を LGWAN 系無線ネットワークへ追加したが、現状は接続先無線 AP に対応する VLAN に合わせた固定 IP アドレス設定による暫定運用を行っている。しかしながら、無線 AP の切替等の影響が疑われる通信不安定事象が発生しており、再起動により復旧する場合があるものの、安定運用に課題がある。
- ・ 受託者は、当該複合機の無線接続について、複合機の保守事業者と十分に調整の上、現行構成、VLAN 収容方式、IP アドレス付与方式、無線 AP との接続状況、ローミング時の影響その他必要事項を調査し、原因分析を行った上で、安定稼働に向けた見直し及び必要な設計・構築を実施するこ

と。

(4)停電対応

- ・ 本庁舎、保健センター及び水道局においては、電気設備点検等に伴う計画停電が今後実施される予定である。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月に停電作業が予定されており、保健センター及び水道局においても例年停電を伴う点検が実施されている。またそれ以外の庁外施設においても適宜点検等による計画停電が実施される。
- ・ 受託者は、これら計画停電を踏まえ、本事業で導入する機器が停電時及び復電時に安全かつ確実に停止及び復旧できるよう、必要な電源設計、起動停止手順、復旧確認手順及び障害時対応手順を整備すること。
- ・ また、保守期間中の計画停電対応を円滑に実施できるよう、構築時に停電対応手順、事前準備事項、当日対応事項、復電後確認項目、関係事業者との調整事項及び役割分担を整理し、成果物に反映すること。

(5)その他

- ・ 保守期間中に大阪版自治体情報セキュリティクラウドの更新（令和9年4月稼働開始予定）が予定されていることから、本事業の構築期間中においても、当該更新に関連して、本市庁舎内ネットワークの接続方式、設定内容、切替条件その他必要事項に関する照会、情報提供依頼、技術的協議又は調整が発生する可能性がある。受託者は、当該更新を見据え、構築期間中に必要となる情報提供、設定内容の確認、関係事業者との調整及び必要な設計上の配慮を本事業の範囲内で実施すること。
- ・ LBOの導入など将来的に拡張できる柔軟な構成となるよう設計すること。また、追加提案として将来的な拡張要素を必要に応じて提案すること。

12.その他仕様

本仕様書に定めのない事項は、本市と協議の上決定する。

13.成果物

最低限、以下の内容を含む成果物を提出すること。データ形式は、Microsoft Office で編集可能な形式とする。

- ・ 調査報告書
- ・ 基本設計書
- ・ 詳細設計書
- ・ 構成図（物理、論理、V L A N， I P アドレス、配線、W A N、監視）
- ・ パラメータシート（機器設定）
- ・ 試験計画書及び試験結果報告書
- ・ 移行計画書及び移行結果報告書
- ・ 運用設計書（監視/障害/変更/資産/アカウント/ログ）
- ・ 障害対応手順書
- ・ 設定バックアップ取得手順書
- ・ 管理者向け簡易操作マニュアル、教育資料、引継ぎ記録
- ・ 機器一覧、ライセンス一覧、配線台帳、 I P アドレス台帳

別紙 1 責任分界表

1. 目的

本表は、本事業における主な対象業務について、本市、受託者及び関係事業者の役割分担の基本的な考え方を示すものである。

受託者は、本表を踏まえ、本市、既存事業者、新規 WAN 回線事業者、対象外機器又は対象外システムの保守事業者その他関係者と必要な調整を行い、本事業を遂行すること。

なお、本表に記載のない事項又は詳細な役割分担については、契約締結後、本市と協議の上決定するものとする。

2. 凡例

記号	意味
◎	主担当
○	協力
△	情報提供、立会い、調整協力等
-	原則対象外

3. 関係者

略称	内容
本市	守口市
受託者	本事業の受託事業者
既存事業者等	既存 NW 保守事業者、既存 WAN 回線事業者、対象外機器又は対象外システムの保守事業者等
新規 WAN 回線事業者	本市が別途契約する WAN 回線事業者
施設管理者	各施設の施設管理者

4. 責任分界表

No	項目	主な作業内容	本市	受託者	既存事業者等	新規WAN回線事業者	施設管理者	備考
1	全体統括	全体方針決定、重要事項判断	◎	○	-	△	-	
2	PMO	スケジュール管理、会議運営、課題管理、関係者調整	△	◎	△	△	△	
3	調査	現地調査、既存資料確認、既設配線調査	△	◎	○	△	△	
4	設計	物理・論理構成、VLAN、IP、WAN、無線、監視、セキュリティ、移行設計	△	◎	△	△	△	
5	調達	機器、ソフトウェア、ラック、UPS、配線資材等の調達	-	◎	-	-	-	回線役務は対象外
6	構築	機器構築、設定、監視 基盤構築、管理端末構築	-	◎	△	△	-	
7	設置・施工	搬入、養生、設置、配線施工、試験、ラベリング、原状回復	△	◎	△	-	△	
8	既存機器連携	既存認証/DHCP、対象外機器、既存スイッチ等との調整、影響確認	△	◎	○	-	-	対象外機器側設定変更は原則当該保守主体
9	WAN 回線更新	回線切替計画、切替調整、ONU 以降接続、試験、切替統括	△	◎	△	○	-	回線提供は新規 WAN 回線事業者
10	LGWAN 端末拠点間利用	実現方式設計、設定変更、試験	△	◎	△	-	-	

11	マイナンバー 系無線化	実装可否評価、設計、 構築、試験	△	◎	△	-	-	実装有無は 本市判断に よる
12	将来 IP 電話 対応	PoE 余力、ポート余 力、音声 VLAN、QoS 設計	△	◎	△	-	-	IP 電話機 /PBX は対 象外
13	統合運用監視	監視項目設計、設定、 アラート、バックアッ プ、監視取込試験	△	◎	△	△	-	
14	試験	単体、結合、総合、障 害、冗長切替、接続試 験	△	◎	△	△	-	
15	移行	移行手順作成、本番切 替、移行統括	△	◎	△	△	△	
16	ロールバック	ロールバック実施	△	◎	△	△	-	判断は本 市、実施は 受託者
17	検収	検収確認、検収判定	◎	△	-	-	-	
18	教育・引継ぎ	操作教育、成果物提 出、運用引継ぎ	△	◎	△	△	-	

5. 補足

WAN 回線役務及び責任分界点までの提供責任は回線事業者が負うものと
し、受託者は責任分界点以降の接続、設定、試験及び切替調整を行う。

別紙2 対象拠点一覧

	基礎情報				利用端末数（PCのみ プリンタ等は除く）			WAN用ルータ			無線AP		
項番	拠点名	郵便番号	住所	施設管理者 （設置時調整先）	LGWAN系	マイナンバー系	インターネット系NW	設置数	回線種別	参考_現行ルータ機種	設置	参考_現行設置数	備考
1	守口市役所	570-8666	京阪本通2-5-5 守口市役所2階	総務課 行財政改革・DX推進課	1000	480	89	2	マイナンバー系／LGWAN系／インターネット系	Fortigate60E	要	68	
2	保健センター	570-0033	大宮通1-13-7	健康推進課	135	74	4	1	マイナンバー系／LGWAN系／インターネット系	Fortigate60E	要	7	
3	大日SC	570-0016	大日東町1-32 （イオンモール大日内）	総合窓口課	1	3	0	1	マイナンバー系／LGWAN系／インターネット系	Fortigate60E	対象外	-	
4	守口市水道局	570-0008	八雲北町3-37-31	水道局経営総務課	62	利用なし	5	1	LGWAN系／インターネット系	Fortigate60E	要	6	
5	高度浄水棟	570-0008	八雲北町3-38	水道局経営総務課	2	利用なし	0	1	LGWAN系／インターネット系	新規敷設のため、現行機なし	要	0	
6	守口小学校	570-0095	八島町13-40	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
7	庭窪小学校	570-0002	佐太中町1-6-10	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
8	八雲小学校	570-0006	八雲西町4-31-31	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	R10年度以降に閉校予定。閉校後、WAN用ルータは回収し予備として利用する。
9	錦小学校	570-0042	寺方錦通2-8-45	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
10	金田小学校	570-0011	金田町3-11-11	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
11	梶小学校	570-0015	梶町4-79-12	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
12	藤田小学校	570-0014	藤田町1-58-18	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
13	八雲東小学校	570-0021	八雲東町2-77-7	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
14	佐太小学校	570-0002	佐太中町6-11-51	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
15	よつば小学校	570-0012	大久保町2-17-26	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
16	さくら小学校	570-0035	東光町2-1-4	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
17	寺方南小学校	570-0047	寺方元町4-1-45	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
18	第一中学校	570-0086	竹町12-29	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
19	庭窪中学校	570-0002	佐太中町4-1-7	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
20	八雲中学校	570-0006	八雲西町3-5-21	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	R10年度以降に閉校予定。閉校後、WAN用ルータは回収し予備として利用する。
21	梶中学校	570-0015	梶町4-28-5	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
22	大久保中学校	570-0012	大久保町4-23-46	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
23	錦中学校	570-0043	南寺方東通4-1-31	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
24	樟風中学校	570-0034	西郷通3-14-60	教育委員会総務課	3	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
25	さつき学園	570-0055	春日町13-26	教育委員会総務課	7	利用なし	利用なし	1	LGWAN系	IX2106	対象外	-	
26	にじいろ 認定こども園	570-0014	藤田町1-57-19	こども施設課	17	利用なし	1	1	LGWAN系／インターネット系	Fortigate60E	対象外	-	令和9年度から民間に移管するため、WAN用ルータは令和9年度当初に回収予定。
27	あおぞら 認定こども園	570-0047	寺方元町4-1-8	こども施設課	13	利用なし	1	1	LGWAN系／インターネット系	Fortigate60E	対象外	-	
28	八雲学園	570-0007	下島町15-27	教育委員会総務課	6	利用なし	利用なし	0※	LGWAN系／インターネット系	新規敷設のため、現行機なし	対象外	-	R10年度以降に開校予定。 ※WAN用ルータはにじいろ認定こども園から回収した機器を利用予定。
29	もりぐち歴史館「旧中西家住宅」	570-0012	大久保町4-2-26	生涯学習・スポーツ振興課	2	利用なし	0	1	LGWAN系／インターネット系	新規敷設のため、現行機なし	対象外	-	
30	守口市門真市 消防組合本部	571-0045	門真市殿島町7-1	人事課	3	利用なし	利用なし	1	LGWAN系／インターネット系	Fortigate60E	対象外	-	
			合計		1305	557	100	30					

別紙3 マイナンバー端末およびIP電話の想定台数

(※) 会議室利用を除く

項番	基礎情報			マイナンバー系端末・プリンタ(※)			IP電話
	建物	フロア	課名		有線固定	無線	
1	別館	1F	情報管理室	23	8	15	1
2	本館	1F	総合窓口課(証明書発行コーナー)	20	11	9	7
3	本館	2F南	課税課、納税課、保険収納課、保険課	180	70	110	57
4	本館	2F北	会計室、総合窓口課	62	35	27	31
5	本館	3F南	障がい福祉課、生活福祉課	125	35	90	40
6	本館	3F北	地域福祉課、こども施設課、子育て支援政策課、高齢介護課	115	41	74	51
7	本館	3F西	リフレッシュルーム	3		3	2
8	本館	4F南	選挙管理委員会、監査委員会、危機管理室、法制文書課、契約課、人事課	39	15	24	46
9	本館	4F北	市長室、企画課、財政課、行財政改革・DX推進課、魅力創造発信課、まちづくり戦略課	1	0	1	38
10	本館	5F南	人権市民相談課、消費生活センター、コミュニティ推進課、生涯学習・スポーツ振興課、地域振興課、下水道課	0	0	0	56
11	本館	5F北	都市・交通計画課、住宅まちづくり課、道路公園課	3	0	3	39
12	本館	5F西	リフレッシュルーム	0	0	0	4
13	本館	6F南	教育センター	0	0	0	7
14	本館	6F北	環境対策課、保健給食課、学校教育課、教育総務課	1	0	1	55
15	本館	7F東	リフレッシュルーム	8	0	8	1
16	本館	9F東	会派控室	0	0	0	18
17	本館	9F北	議会事務局	0	0	0	8
18	保健センター	2F	市民健診等用	15	15	0	対象外
19	保健センター	3F	健康推進課、こども家庭センター	99	27	72	対象外
20	保健センター	4F	母子健診用	2	2	0	対象外
合計				696	259	437	461

別紙4.仕様対応表

項番	項目	仕様内容	対応可否	対応内容
1	総則		－	－
1-1	目的	本事業は、守口市（以下「本市」という。）における庁内ネットワークについて、運用管理の効率化、障害発生時の業務継続性の確保及情報セキュリティの向上を目的として、現行別契約としていた庁舎内ネットワーク、庁舎外WAN用ルータ管理、庁舎外施設の無線APを統合し、ネットワーク環境の更新を行うものである。	－	－
1-1	目的	本事業では、現行構成を原則踏襲しつつ、以下を実施するものとする。 ・ネットワーク機器の更新及び新規敷設、配線引き直し ・統合運用監視基盤の導入 ・VLAN構成及びIPアドレス体系の再設計 ・本庁、水道局及び保健センターの3拠点におけるLGWAN系無線利用端末の相互利用を可能とするためのネットワーク再設計及び必要な構築 ・マイナンバー利用事務系ネットワーク（以下、「マイナンバー系ネットワーク」と言う。）の無線化に係る実装可否の評価、並びに本市が実装を指示した場合の設計及び構築 ・本庁舎における将来のIP電話導入を見据えたネットワーク設計及び必要な機器選定 ・将来の端末数、通信量、機能追加に柔軟に対応可能な拡張性を備えた構成の実現	－	－
1-1	目的	また、安全かつ確実な移行のため、既存契約事業者、新規WAN提供事業者、その他関係事業者及び庁内関係部署との調整並びに移行統括を行うものとする。	－	－
1-2	関連文書・準拠基準	本事業の設計、構築、試験、移行及び運用設計にあたっては、以下の文書に準拠又は整合すること。 ・守口市情報セキュリティポリシー ・総務省 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	○	本事業の設計、構築、試験、移行及び運用設計にあたっては、以下の文書に準拠又は整合いたします。 ・守口市情報セキュリティポリシー ・総務省 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
1-2	関連文書・準拠基準	また、必要に応じて以下の文書を参照し提案内容の妥当性を確保すること。 ・デジタル庁 国・地方ネットワーク関連文書 ・国家サイバー統括室 政府機関等のサイバーセキュリティ対策のための統一基準群	○	必要に応じて以下の文書を参照し提案内容の妥当性を確保いたします。 ・デジタル庁 国・地方ネットワーク関連文書 ・国家サイバー統括室 政府機関等のサイバーセキュリティ対策のための統一基準群
1-2	関連文書・準拠基準	なお、上記文書間で解釈の相違が生じる場合は、本市と協議の上、本市の判断に従うこと	○	上記文書間で解釈の相違が生じる場合は、貴市と協議の上、貴市の判断に従います。
1-3	構築期間	協議書締結日から令和8年12月31日までとする。	○	協議書締結日から令和8年12月31日の期間で構築を完了いたします。
1-3	構築期間	本市外部施設間で通信するためのWAN回線用ルータの切替は、保守期限が到来する令和8年12月28日以前に完了すること。	○	貴市外部施設間で通信するためのWAN回線用ルータの切替は、保守期限が到来する令和8年12月28日以前に完了いたします。
1-3	構築期間	本調達で導入する機器の設置後から令和8年12月31日までの間は試用期間として機器使用に係る費用を求めないものとする。	○	本調達で導入する機器の設置後から令和8年12月31日までの間は試用期間として機器使用に係る費用を求めません。
1-4	現行構成	現行の構成等について、希望する事業者に対して以下の資料を別途貸与又は閲覧提供する。 ・本庁舎LAN配線図 ・ネットワーク設計書 ・ネットワーク構成図 ・スイッチ設置 ・LAN配線図（保健センター） ・電波サーベイ結果（水道局、保健センター）	－	－
1-4	現行構成	また、必要に応じて現地確認の機会を設ける。実施方法、日程及び範囲は別途通知する。	－	－
2	基本要件			
2-1	基本要件	①安定稼働：本システムは、24時間365日の安定稼働を前提とし、重要機器については冗長化その他の手段により単一故障点を極小化すること。障害発生時には、業務継続性を確保できる構成及び運用とすること。	○	本庁舎の内部ファイアウォール、コアスイッチ、ディストリビューションスイッチ、サーバ室内スイッチは2台1組の冗長構成とします。またフロアスイッチはホットスタンバイ機を準備いたします。
2-1	基本要件	②拡張性：端末数、通信量、拠点数、機能追加等の変化に対し、柔軟に拡張できること。	○	各機器の性能は既存機器以上のもを導入し、またスイッチの台数・ポート数も十分に余裕をもった設計といたします。
2-1	基本要件	③情報セキュリティ：情報セキュリティ水準は現行水準以上を確保すること。	○	外部FWの設置やふるまい検知などにより現行水準以上のセキュリティを確保いたします。
2-1	基本要件	④監視・管理：すべての対象機器について、統合的な監視、状態管理、異常検知、通知及びログ収集に対応すること。障害発生時は、本市及び本市が別途契約する保守事業者と連携して対応すること。	○	Zabbix及びFortiAnalyzerにより、すべての対象機器について、統合的な監視、状態管理、異常検知、通知及びログ収集に対応いたします。障害発生時は、貴市及び貴市が別途契約する保守事業者と連携して対応いたします。
2-1	基本要件	⑤設計の整理：VLAN構成およびIPアドレス体系については、現状を見直し、管理性、拡張性及びセキュリティを考慮して再設計すること。	○	VLAN構成およびIPアドレス体系については、現状を見直し、管理性、拡張性及びセキュリティを考慮して再設計いたします。
2-1	基本要件	⑥調査対応：既存環境に不ポイントがある場合は、必要な調査を行った上で設計・構築を行うこと。なお、現行の個別システムが支障なく稼働できる適合性を確保すること。	○	既存環境に不ポイントがある場合は、必要な調査を行った上で設計・構築を行います。なお、現行の個別システムが支障なく稼働できる適合性を確保いたします。
2-1	基本要件	⑦個別要件の詳細は各章に定めたとおりとする。	－	－
3	調達範囲と対象			
3-1	調達範囲	本事業の調達範囲は、次のとおりとする。 ・ネットワーク調査 ・ネットワーク設計 ・機器、ソフトウェア及び必要資材の調達 ・構築、設置、配線及び設定 ・試験及び移行 ・関係事業者との調整を含む移行統括業務 ・操作教育及び成果物作成	○	本事業の調達範囲として、次のとおり実施いたします。 ・ネットワーク調査 ・ネットワーク設計 ・機器、ソフトウェア及び必要資材の調達 ・構築、設置、配線及び設定 ・試験及び移行 ・関係事業者との調整を含む移行統括業務 ・操作教育及び成果物作成
3-1	調達範囲	なお、対象機器、対象外機器、設計対象、設定変更対象、試験対象、保守対象及び他事業者調整の要否については、別紙1「責任分界表」のとおりとする。	○	対象機器、対象外機器、設計対象、設定変更対象、試験対象、保守対象及び他事業者調整の要否については、別紙1「責任分界表」に従います。
3-2	対象拠点	対象拠点は別紙2「対象拠点一覧」のとおりとする。	○	対象拠点は別紙2「対象拠点一覧」に従います。
3-2	対象拠点	なお、本庁舎、保健センター及び水道局については館内LAN及び無線APを含めた更新対象とし、それ以外の外部施設については、原則としてWAN用ルータ設置箇所までを対象とする。ただし、別紙1に個別記載がある場合はこの限り	○	本庁舎、保健センター及び水道局については館内LAN及び無線APを含めた更新対象とし、それ以外の外部施設については、原則としてWAN用ルータ設置箇所までを対象といたします。ただし、別紙1に個別記載がある場合は個別記載内容に
3-3	対象機器	以下の機器を調達対象とする。 ・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 ・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 ・その他の提案内容を実現するために必要な機器、ケーブル類、UPS等	○	以下の機器を調達対象といたします。 ・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 ・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 ・その他の提案内容を実現するために必要な機器、ケーブル類、UPS等
3-3	対象機器	提案機器は法人向けの新品とし、本仕様の要件を満たすとともに、現行の機器と同等以上の性能を有すること。また、現行以上の保守性、供給継続性及び管理性を確保すること。	○	提案機器は法人向けの新品であり、本仕様の要件を満たしております。現行の機器と同等以上の性能を有しております。また、セキュアSDプランチャや統合監視基盤により、現行以上の保守性、管理性を有しており、供給継続性も問題ございません
3-3	対象機器	WAN用ルータは本事業で調達・導入し、統合運用監視の対象に含めること。回線事業者側設定または責任分界点以降の作業が必要となる場合は、当該事業者と調整の上で実施すること。	○	WAN用ルータは本事業で調達・導入し、統合運用監視の対象に含めます。回線事業者側設定または責任分界点以降の作業が必要となる場合は、当該事業者と調整の上で実施いたします。
3-4	調達対象外	以下の機器は調達対象外とする。 ・庁内で使用している業務システム関連サーバ（アプリケーション/DB等） ・ドメインサーバ、ファイルサーバ、ウイルス対策管理サーバ、KMSサーバ ・LGWAN系IEEE802.1X認証サーバ、LGWAN系DHCPサーバ、LGWAN接続用機器、セキュリティクラウド接続用機器 ・WAN回線役務、IP電話関係機器（IP電話機、PBXその他IP電話の運用基盤）。	○	以下の機器は調達対象外といたします。 ・庁内で使用している業務システム関連サーバ（アプリケーション/DB等） ・ドメインサーバ、ファイルサーバ、ウイルス対策管理サーバ、KMSサーバ ・LGWAN系IEEE802.1X認証サーバ、LGWAN系DHCPサーバ、LGWAN接続用機器、セキュリティクラウド接続用機器 ・WAN回線役務、IP電話関係機器（IP電話機、PBXその他IP電話の運用基盤）。
3-4	調達対象外	ただし、これら調達対象外機器についても、本事業の設計、移行又は接続性確認のために設定影響調査、接続試験、調整又は情報提供が必要となる場合がある。その場合の責任分界及び実施主体は、別紙1「責任分界表」によ	○	これら調達対象外機器についても、本事業の設計、移行又は接続性確認のために設定影響調査、接続試験、調整又は情報提供が必要となる場合の責任分界及び実施主体は、別紙1「責任分界表」に従います
4	統合運用監視基盤	統合運用監視基盤は、SNMP、Syslogその他必要な方式により監視対象機器の状態及びログを収集できること。	○	統合運用監視基盤は、SNMP、Syslog等により監視対象機器の状態及びログを収集します。
4-1	提供形態・サイジング	提供形態は、オンプレミス（物理/仮想アプライアンス/汎用OS上ソフトウェア）とし、本庁サーバ室に設置すること。	○	提供形態は、オンプレミスとし、本庁サーバ室に設置いたします。
4-1	提供形態・サイジング	クラウド又はハイブリッド構成を提案する場合は、次の事項を明記すること。 データ保存場所 国内外のデータ取扱いの有無 契約終了時におけるデータ返却及び消去方法 障害時及び保守時の窓口体制 利用停止時の影響範囲 本市の情報セキュリティポリシーとの適合性 提案時に必要リソース（CPU/メモリ/ストレージ/IO性能）、前提となる仮想基盤やOS、サポート期間、拡張上限（監視対象台数/ポート数/イベント数/ログ保持量）	－	－
4-2	可用性・保全			
4-2	可用性・保全	統合運用監視基盤について、バックアップ対象、取得頻度、世代数、保管先及びリストア手順を整備すること。	○	統合運用監視基盤について、バックアップ対象、取得頻度、世代数、保管先及びリストア手順を整備いたします。

項番	項目	仕様内容	対応可否	対応内容
4-2	可用性・保全	提案する可用性構成に応じてRTO（復旧時間目標）及びRPO（復旧時点目標）を明示し、その実現方法（迅速なリストア手順、予備機・イメージ展開、バックアップ頻度と保管先等）を具体的に示すこと。	○	■ 構成概要 本システムは、以下の構成といたします。 ・監視サーバおよびログ収集サーバによる2台構成 ・ログの閲覧は管理端末にて実施 ・バックアップ保存先としてNAS(容量：16TB)を2台構成 ■ RTO/RPO ・RTO：障害判定後、概ね6時間以内の復旧を目標 ・RPO：障害発生直前の設定状態への復元を想定 ■ バックアップ対象および保存先 ■ バックアップ先 ・設定ファイル(監視サーバおよびログ収集サーバ) → NAS 1号機、2号機 ・ログ(SNMPトラップ)※監視サーバで受信 → NAS 1号機、2号機 ・ログ(syslog)※ログ収集サーバで受信 → NAS 1号機、2号機 ■ バックアップ方針 ・設定データは最新1世代を保持 ■ ログ保管期間 ・ログは1年間の保存を想定 ■ ウイルス対策について ・Windowsサーバ（ホストOS）：守口市様ご提供のウイルス対策ソフトを利用 ※ウイルス対策ソフトの導入作業および契約更新時の更新作業も実施いたします。 ・監視サーバ：仮想アプライアンス製品のため導入不可 ・ログ収集サーバ：アプライアンス製品のため導入不可 ※アプライアンス製品は専用OSのためウイルス対策ソフトの導入はできませんが、ベンダー提供のアップデート適用等により、一定のセキュリティ対策を実施しております。
4-2	可用性・保全	受入試験で代表障害時の復旧時間と復旧時点を確認すること。	○	受入試験で代表障害時の復旧時間と復旧時点を確認いたします。
4-3	管理端末・UI	監視ソフト用の管理用UI（主にWebベース）は、日本語表示に対応し、専用クライアントを要さないことが望ましい。専用クライアントが必要な場合は、その導入・設定・ライセンスを本事業に含めること。	○	監視ソフト用の管理用UI（主にWebベース）は、日本語表示に対応し、専用クライアントは不要です。
4-3	管理端末・UI	常時監視・操作のための管理端末を1台は本事業で確保すること。端末OSはベンダがサポートするLTS版（例：Windows 10/11 Enterprise LTSC相当等）とし、管理UIが安定動作するブラウザ/解像度/メモリ等を満たすこと。	○	・常時監視・操作のための管理端末を3台準備いたします。管理端末は LTSC相当を準備いたします。 ・管理端末のLTS版は、機能制限版なので、機器の管理ツールが利用できない可能性がある。その場合はLTS版ではなく通常版を利用する。 ・ウイルス対策ソフトは守口市様ご提供のウイルス対策ソフトを利用 ※ウイルス対策ソフトの導入作業および契約更新時の更新作業も実施いたします。
4-3	管理端末・UI	管理端末に必要なOSライセンス、管理UI利用に必要なソフトウェア、初期設定及び運用開始時点で必要な更新適用は、本事業の範囲に含むものとする。	○	管理端末に必要なOSライセンス、管理UI利用に必要なソフトウェア、初期設定及び運用開始時点で必要な更新適用を実施いたします。
4-4	ネットワーク可視化に関する機能要件	以下の機能を必須機能として有すること。下記に記載がなくとも有効と思われる追加の機能があれば積極的に追加提案を行うこと。	○	以下の機能を必須機能として有しております。
4-4	ネットワーク可視化に関する機能要件	(1)ネットワーク可視化（トポロジ）	○	(1)ネットワーク可視化（トポロジ）
4-4	ネットワーク可視化に関する機能要件	サーバ、スイッチ、無線AP、PC等の接続関係並びに物理・論理構成を可視化し、管理者が容易に把握できること。	○	サーバ、スイッチ、無線AP、PC等の接続関係並びに物理・論理構成を可視化し、管理者が容易に把握することが可能です。
4-4	ネットワーク可視化に関する機能要件	デバイス間の通信状況又は負荷状況について、管理者が確認できること。	○	デバイス間の通信状況又は負荷状況について、管理者が確認することが可能です。
4-4	ネットワーク可視化に関する機能要件	構成情報は、自動取得又は手動登録その他適切な方法により作成及び更新できること。	○	構成情報は、自動取得又は手動登録により作成及び更新が可能です。
4-4	ネットワーク可視化に関する機能要件	なお、可視化の実現方式、表示方法及び更新方法は問わないが、本市の運用管理上必要な構成把握及び障害時の影響確認が可能であること。	○	貴市の運用管理上必要な構成把握及び障害時の影響確認が可能です。
4-4	ネットワーク可視化に関する機能要件	ネットワーク可視化に関する機能要件	○	(2)監視（死活・状態・帯域・イベント）
4-4	ネットワーク可視化に関する機能要件	統合運用監視基盤は、本事業対象機器及び本市が指定する既存機器を監視対象として登録可能であること	○	統合運用監視基盤は、本事業対象機器及貴市が指定する既存機器を監視対象として登録可能です。
4-4	ネットワーク可視化に関する機能要件	庁舎内ネットワークを構成する通信機器（FW、ルータ、スイッチ、無線AP、無線コントローラ等）および監視対象として指定した端末（サーバ等）について死活監視を行えること。	○	庁舎内ネットワークを構成する通信機器（FW、ルータ、スイッチ、無線AP、無線コントローラ等）および監視対象として指定した端末（サーバ等）について死活監視を行うことが可能です。
4-4	ネットワーク可視化に関する機能要件	状態監視・異常検知 機器状態、ポート、帯域、パケット等を監視し、異常発生時に検知できること。	○	状態監視・異常検知 機器状態、ポート、帯域、パケット等を監視し、異常発生時に検知可能です。
4-4	ネットワーク可視化に関する機能要件	SNMP TrapおよびSyslogの受信・相関に対応すること。	○	SNMP TrapおよびSyslogの受信・相関に対応しております。
4-5	無線LANコントローラ機能	無線APの集中管理ができること。管理方式は、専用コントローラ方式、クラウド管理方式又は分散管理方式のいずれでも可とする。ただし、提案方式により、設定の一元管理、障害把握、ファームウェア管理、構成変更管理及び本仕様 に定める運用性を満たすこと。	○	無線APの集中管理が可能です。管理方式は、Fortinet社セキュアSDブランチ構成により内部ファイアウォールで一元管理を行います。設定の一元管理、障害把握、ファームウェア管理、構成変更管理が可能であり、本仕様に定める運用性を満たしております。
4-5	無線LANコントローラ機能	クライアント分離、隣接無線AP検出、コントローラ断時の通信継続等が可能であれば合わせて提案すること。	○	無線APでは、クライアント分離や隣接無線AP検出を提供可能です。コントローラ断時の通信継続はトンネルモードを利用するため、無線コントローラ（FortiGate）が完全に停止した場合、通信は停止します。ただし、無線コントローラ（FortiGate）を冗長構成とすることで、単一機器の故障であれば通信は維持されます。
4-5	無線LANコントローラ機能	コントローラ機能を提案しない場合は、代替方式により同等以上の管理性を確保できる理由を具体的に示すこと。	○	コントローラ機能をご提案いたします。
4-6	マニュアル・教育	一般的なマニュアルに加え、日本語の簡易操作マニュアル（PDF）を提出すること。簡易操作マニュアルには少なくとも以下を含むこと。 ・インストール、マップ作成、デバイス設定、デバイスレベル設定、アラート設定、グラフ作成・表示、レポート出力・利用に関する操作方法・インターフェイスの見方、アクションコマンド説明	○	一般的なマニュアルおよび日本語の簡易操作マニュアル（PDF）を提出いたします。簡易操作マニュアルには少なくとも以下を含めます。 ・インストール、マップ作成、デバイス設定、デバイスレベル設定、アラート設定、グラフ作成・表示、レポート出力・利用に関する操作方法・インターフェイスの見方、アクションコマンド説明
5	ネットワーク設計		○	
5-1	VLAN・IPアドレス再設計	VLAN構成及びIPアドレス体系は、管理性、将来拡張性、障害影響範囲及びセキュリティ確保の観点から再設計すること。	○	VLAN構成及びIPアドレス体系は、管理性、将来拡張性、障害影響範囲及びセキュリティ確保の観点から再設計いたします。
5-1	VLAN・IPアドレス再設計	なお、IPアドレス変更を伴う対象については、対象区分、影響範囲、暫定措置、切替条件及びロールバック条件を明記した移行計画を策定すること。	○	なお、IPアドレス変更を伴う対象については、対象区分、影響範囲、暫定措置、切替条件及びロールバック条件を明記した移行計画を策定いたします。
5-1	VLAN・IPアドレス再設計	(1)VLAN再設計	○	(1)VLAN再設計
5-1	VLAN・IPアドレス再設計	VLAN構成を見直し、以下を満たす再設計を行うこと。	○	VLAN構成を見直し、以下を満たす再設計を実施いたします。
5-1	VLAN・IPアドレス再設計	用途ごとのセグメント方針を定めること。	○	用途ごとのセグメント方針を定めます。
5-1	VLAN・IPアドレス再設計	VLAN-ID割当として、予約領域・発番ルール・端末/無線端末等の増加を見込んだ将来拡張性を考慮すること。	○	VLAN-ID割当として、予約領域・発番ルール・端末/無線端末等の増加を見込んだ将来拡張性を考慮いたします。
5-1	VLAN・IPアドレス再設計	管理/運用用VLANを定義すること。	○	管理/運用用VLANを定義いたします。
5-1	VLAN・IPアドレス再設計	トランクポート及びアクセスポートの設計並びに許可VLANを明確化すること。	○	トランクポート及びアクセスポートの設計並びに許可VLANを明確化いたします。
5-1	VLAN・IPアドレス再設計	L2境界及び冗長制御方式を整理し、必要に応じてSTP等の採用方針を示すこと。	○	L2境界及び冗長制御方式を整理し、必要に応じてSTP等の採用方針を示します。
5-1	VLAN・IPアドレス再設計	要件に応じ、以下の技術の採用可否を評価し、採用する場合は具体的な構成案と運用方法を提示すること。 ネットワークの論理分離（VRF） 大規模セグメント/マルチテナント対応（VXLAN/EVPN） 拠点間通信の最適化・一元管理（SD-WAN）	○	以下の技術の採用可否を評価した結果、既存を踏襲しVDOMを採用いたします。 ネットワークの論理分離（VRF） 大規模セグメント/マルチテナント対応（VXLAN/EVPN） 拠点間通信の最適化・一元管理（SD-WAN）
5-1	VLAN・IPアドレス再設計	(2)IPアドレス再設計	○	(2)IPアドレス再設計
5-1	VLAN・IPアドレス再設計	IPアドレス体系を見直し、以下を満たす再設計を行うこと。	○	IPアドレス体系を見直し、以下を満たす再設計を実施いたします。
5-1	VLAN・IPアドレス再設計	LGWAN系、マイナンバ－利用事務系、インターネット系ごとにアドレス体系を分離すること。	○	LGWAN系、マイナンバ－利用事務系、インターネット系ごとにアドレス体系を分離いたします。
5-1	VLAN・IPアドレス再設計	予約領域及び発番ルールを含む管理標準化ルールを定義すること。	○	予約領域及び発番ルールを含む管理標準化ルールを定義いたします。
5-1	VLAN・IPアドレス再設計	将来拡張余地を確保すること。	○	将来拡張余地を確保いたします。
5-1	VLAN・IPアドレス再設計	既設DHCPの継続利用を基本とし、必要に応じてスコープ追加・見直しを行うこと。なお、現行においてDHCPを利用している系統はLGWAN系のみである。既設DHCPの拡張、設定変更その他必要な対応を行う場合は、現行保守事業者による作業又は調整が必要となるため、受託者は当該事業者と必要な調整を行うこと。これに要する費用は本事業に含めること。現行保守事業者の連絡先は別途提示する。	○	既設DHCPの継続利用し、必要に応じてスコープ追加・見直しを行います。DHCPの利用はLGWAN系のみとします。既設DHCPの拡張、設定変更その他必要な対応を行う場合は、現行保守事業者と必要な調整を行います。これに要する費用は提案金額に含めております。
5-1	VLAN・IPアドレス再設計	マイナンバ－系ネットワークにおいてDHCPサーバを新たに設ける場合は、安全性及び系統分離に十分配慮した構成とすること。この場合、DHCPサーバに係る機器、ソフトウェア、ライセンス、構築、設定、試験その他必要な費用は本事業に含めて見積もること。	○	マイナンバ－系ネットワークでDHCPサーバは導入いたしません。
5-1	VLAN・IPアドレス再設計	固定IP機器・サーバ・複合機・業務機器の影響調査と、移行対象一覧及び対応方針を提示すること。	○	固定IP機器・サーバ・複合機・業務機器の影響調査と、移行対象一覧及び対応方針を提示いたします。
5-1	VLAN・IPアドレス再設計	IPv6の採否及び方針（非対応/段階導入/デュアルスタック等）を明記すること。	○	WAN回線は既設ISPおよび回線サービスに合わせます。WAN回線以外はIPv6は非対応です
5-1	VLAN・IPアドレス再設計	(3)IPアドレスの移行方針	○	(3)IPアドレスの移行方針
5-1	VLAN・IPアドレス再設計	IPアドレス移行については、業務影響を最小化する方式を基本とし、段階移行、並行稼働又は切替窓の設定を含む移行計画を策定すること。ロールバック手順は必須とする。	○	IPアドレス移行については、業務影響を最小化する方式を基本とし、段階移行、並行稼働又は切替窓の設定を含む移行計画を策定いたします。またロールバック手順も作成いたします。

項番	項目	仕様内容	対応可否	対応内容
5-1	VLAN・IPアドレス再設計	既存システムに関わる設定・IPアドレス等の移行は、業務影響と保守範囲を踏まえ、可能な範囲を各システムの更新時に実施し、更新時に実施が困難な対象は保守期間内に計画的に実施すること。全体計画には、対象区分（更新時／保守期間）、暫定対処、切替窓、ロールバックを含めること。	○	既存システムに関わる設定・IPアドレス等の移行は、業務影響と保守範囲を踏まえ、可能な範囲を各システムの更新時に実施し、更新時に実施が困難な対象は保守期間内に計画的に実施いたします。全体計画には、対象区分（更新時／保守期間）、暫定対処、切替窓、ロールバックを含めます。
5-2	LGWAN系無線利用端末の他拠点利用	現状、本庁のLGWAN系端末はDHCP管理し、庁外施設は固定IP設定であるため、他拠点に持ち出した場合に通信できない。	－	－
5-2	LGWAN系無線利用端末の他拠点利用	本庁、水道局及び保健センターの3拠点において、LGWAN系無線利用端末を拠点間で持ち運んだ場合であっても、端末側で個別のIP設定変更を要することなく利用できる構成とすること。	○	水道局・保健センターの拠点用WANルータにDHCP機能を持たせることで、本庁、水道局及び保健センターの3拠点において、LGWAN系無線利用端末を拠点間で持ち運んだ場合であっても、端末側で個別のIP設定変更を要することなく利用できるようにいたします。
5-2	LGWAN系無線利用端末の他拠点利用	受託者は、LGWAN系無線利用端末の他拠点利用を可能とする構成について提案書に明記すること。	○	水道局・保健センターの拠点用WANルータにDHCP機能を持たせる構成といたします。
5-2	LGWAN系無線利用端末の他拠点利用	実現方式は、DHCP化、認証連携、動的VLANその他適切な方法によるものとし、提案書には少なくとも以下を明記すること。 ・実現方式の概要 ・端末設定変更の要否 ・既存認証基盤及びDHCPサーバへの影響 ・切替時の業務影響 ・障害時の切り分け方法	○	実現方式は以下の通りです。 ・実現方式の概要：出先の拠点用WANルータにDHCP機能を持たせる構成といたします。 ・端末設定変更の要否：端末の設定変更は必要です。 ・既存認証基盤及びDHCPサーバの影響：無線APのアドレスが変更となる場合は認証基盤にRADIUSクライアント登録が必要。

項番	項目	仕様内容	対応可否	対応内容
6-2	本庁舎における要件	既存配線の取扱いについては、配線の敷設時期及び用途に応じて区分するものとし、5年前の更新時に更新又は新設したコアスイッチからディストリビューションスイッチまでの幹線、ディストリビューションスイッチからフロアスイッチまでの配線及びフロアスイッチからエッジスイッチまでの配線のうち当該更新時に新設したものについては、原則として流用するものとし、個別調査は要しない。	○	既設配線については全配線を調査の上、劣化・損傷しているものについてはコネクタ交換や再配線を実施いたします。
6-2	本庁舎における要件	フロアスイッチからエッジスイッチまでの配線のうち、5年前の更新以前から継続使用しているものについては、原則として更新対象として見込むこと。	○	既設配線については全配線を調査の上、劣化・損傷しているものについてはコネクタ交換や再配線を実施いたします。
6-2	本庁舎における要件	エッジスイッチから端末、複合機、プリンタその他接続機器までの配線については、日常使用に伴う消耗及び摩耗を踏まえ調査を実施し、更新対象として見込むこと。	○	既設配線については全配線を調査の上、劣化・損傷しているものについてはコネクタ交換や再配線を実施いたします。
6-2	本庁舎における要件	ただし、上記の原則流用又は原則更新の区分により難しい事情がある場合は、本市と協議の上、必要な確認又は調整を行うこと。	○	上記の原則流用又は原則更新の区分により難しい事情がある場合は、貴市と協議の上、必要な確認又は調整を実施いたします。
6-2	本庁舎における要件	(2)エッジスイッチ設置		(2)エッジスイッチ設置
6-2	本庁舎における要件	エッジスイッチ設置に関する要件は以下のとおりとする。	○	エッジスイッチ設置に関する要件は以下のとおりといたします。
6-2	本庁舎における要件	原則として現行同様に各フロアの職員が在席する各拠点（島）に対し設置すること。	○	原則として現行同様に各フロアの職員が在席する各拠点（島）に対し設置いたします。
6-2	本庁舎における要件	現状有線接続している端末・プリンタ数を満たす数のエッジスイッチを用意すること。ただし、5-3マイナンバー系ネットワークにおける無線化にて無線化を提案する場合は、無線対象となる機器分については提案数から除いた適切な数を用意すること。	○	現状有線接続している端末・プリンタ数を満たす数のエッジスイッチを用意いたします。
6-2	本庁舎における要件	必要台数は現行レイアウト図面及び現地調査に基づき受託者が提案し、本事業開始後に協議の上決定すること。	○	必要台数は現行レイアウト図面及び現地調査に基づき弊社からご提案し、本事業開始後に協議の上決定いたします。
6-2	本庁舎における要件	本庁舎内の全会議室（地下1階～7階、9階～10階）はエッジスイッチを常設しないが、設置した場合に有線LAN接続が可能となるよう必要な配線経路、収容余地又は敷設方法を設計に含めると。	○	本庁舎内の全会議室（地下1階～7階、9階～10階）はエッジスイッチを常設しないが、設置した場合に有線LAN接続が可能となるよう必要な配線経路、収容余地又は敷設方法を設計に含めます。
6-2	本庁舎における要件	各フロアの有線LANでは、当該ループ検知・抑止機能を有効化し、対象ポート、通知方法、復帰条件（自動/手動）を設計書に明記すること。	○	各フロアの有線LANでは、当該ループ検知・抑止機能を有効化し、対象ポート、通知方法、復帰条件（自動/手動）を設計書に明記いたします。
6-2	本庁舎における要件	(3)無線AP設置		(3)無線AP設置
6-2	本庁舎における要件	無線AP設置に関する要件は以下のとおりとする	○	無線AP設置に関する要件は以下のとおりといたします。
6-2	本庁舎における要件	地下1階～10階（※7階南フロアと8階を除く）及び別館1，2階で常時安定接続できる環境を構築すること。	○	地下1階～10階（※7階南フロアと8階を除く）及び別館1，2階で常時安定接続できる環境を構築いたします。
6-2	本庁舎における要件	必要台数・設置場所は現行庁舎レイアウト図面及び現地調査に基づき受託者が提案し本事業開始後に協議の上決定すること。	○	必要台数・設置場所は現行庁舎レイアウト図面及び現地調査に基づき弊社から提案し本事業開始後に協議の上決定いたします。
6-3	水道局における要件	(1)配線・敷設		(1)配線・敷設
6-3	水道局における要件	水道局庁舎については現状WAN用ルータから、1～4階の各フロアに設置したスイッチに配線し、当該スイッチから無線APおよび端末、プリンタへ配線している。なお、局内のケーブルについては老朽化しており使用から30年経過しているものもあるため、既存ケーブルの流用可否の調査の際留意すること。	○	水道局内のケーブルについては全配線張り替えを行います。
6-3	水道局における要件	水道局庁舎のスイッチの配置は現行配置を踏襲することとする。	○	水道局庁舎のスイッチの配置は現行配置を踏襲いたします。
6-3	水道局における要件	既存OAボックスを流用する場合は、その寸法、耐荷重、放熱性及び保守性を確認すること。提案機器が既存OAボックスに収容できない場合は、本事業の範囲に必要な設置対応を行うこと。	○	既存OAボックスを流用する予定です。その際はその寸法、耐荷重、放熱性及び保守性が問題無いことを確認の上流用いたします。問題がある場合は必要な設置対応を行います。
6-3	水道局における要件	高度浄水処理棟については、WAN用ルータから直接無線APおよび端末・プリンタ等機器へ配線するものとする。	○	高度浄水処理棟については、WAN用ルータから直接無線APおよび端末・プリンタ等機器へ配線いたします。
6-3	水道局における要件	(2)無線AP設置		(2)無線AP設置
6-3	水道局における要件	無線APの設置箇所は、別途提供する電波サーベイ結果および無線AP仕様想定範囲を示したレイアウト図面に基づき受託者が提案し事業開始後に協議の上決定することとする。	○	無線APの設置箇所は、電波サーベイ結果および無線AP仕様想定範囲を示したレイアウト図面にに基づき弊社から提案し事業開始後に協議の上決定いたします。
6-3	水道局における要件	高度浄水処理棟については、WAN用ルータから無線APへ配線する構成を想定しているため、無線APへの電源供給が確実に行えるよう必要な措置を講じること。なお、WAN用ルータにPoE給電機能を必須とせず、給電方法については、外付けPoEインジェクターの利用、電源コンセントからの給電その他適切な方法を含め、受託者の提案に基づき本市と協議の上、決定するものとする。	○	高度浄水処理棟については、無線APへの電源供給用に確実に行えるようPoEインジェクタを準備いたします。
6-4	保健センターにおける要件	(1)配線・敷設		(1)配線・敷設
6-4	保健センターにおける要件	保健センターについては現状WAN用ルータから、1～4階の各フロアに設置したスイッチに配線し、当該スイッチから無線APおよび端末、プリンタへ配線している。なお、センター内のスイッチおよびケーブルについては令和6年9月に敷設したケーブルと、それ以前から使用しているケーブルが混在しているため、既存ケーブルの流用可否の調査の際留意すること。	○	既設配線については全配線を調査の上、劣化・損傷しているものについてはコネクタ交換や再配線を実施いたします。
6-4	保健センターにおける要件	保健センターの既存スイッチは本事業における更新対象外とする。ただし、統合運用監視基盤における監視対象として取り込むことを原則とし、既存機器の仕様上取得可能な範囲で監視、通知及び状態把握を行うこと。なお、既存機器の仕様により監視対象化が困難な場合は、その理由及び代替案を提案書に明記すること。	○	保健センターの既存スイッチは本事業における更新対象外といたしますが、統合運用監視基盤における監視対象といたします。
6-4	保健センターにおける要件	(2)無線AP設置		(2)無線AP設置
6-4	保健センターにおける要件	無線APの設置箇所は、別途提供する電波サーベイ結果および無線AP仕様想定範囲を示したレイアウト図面に基づき受託者が提案し事業開始後に協議の上決定することとする。	○	無線APの設置箇所は、別途提供する電波サーベイ結果および無線AP仕様想定範囲を示したレイアウト図面にに基づき弊社が提案し事業開始後に協議の上決定いたします。
6-4	保健センターにおける要件	保健センターにおける無線化については、庁内と同様の構成を基本とし、現行スイッチの構成を踏まえた上で、1台の無線APによる複数系統の収容が可能な場合は、その構成案及び必要条件を提案すること。本市の求める無線等の範囲は現行図面に記載しているためそちらを確認すること。なお、実現が困難な場合は、その理由を示すこと。	○	現行構成では、保健センターのフロアスイッチが内部系（LGWAN）とインターネット系で物理的に分離されており、かつフロアスイッチはVLANタグ設定に非対応であると想定されるため、無線APで利用可能な無線ネットワークは単一系統に限定されています。 一方で、新規導入するエッジスイッチを用いて内部系（LGWAN系）のフロアスイッチを取り替えることで、無線APから内部系およびインターネット系の双方のネットワークを利用可能とする構成といたします。
6-5	WAN用ルータ			
6-5	WAN用ルータ	WAN用ルータは、各対象拠点に設置し、責任分界点であるONU以降に接続すること。	○	WAN用ルータは、各対象拠点に設置し、責任分界点であるONU以降に接続いたします。
6-5	WAN用ルータ	現地調査結果に基づき、必要な配線、電源及び設置環境を整備すること。	○	現地調査結果に基づき、必要な配線、電源及び設置環境を整備いたします。
6-5	WAN用ルータ	WAN用ルータの設置にあたっては、回線種別、接続先機器、設置場所の条件及び将来拡張を考慮し、保守性及び運用性に配慮した構成とすること。	○	WAN用ルータの設置にあたっては、回線種別、接続先機器、設置場所の条件及び将来拡張を考慮し、保守性及び運用性に配慮した構成といたします。
6-5	WAN用ルータ	WAN用ルータは少なくとも以下を満たすこと。	○	WAN用ルータは少なくとも以下を満たします。
6-5	WAN用ルータ	本市が指定する回線方式に対応できること	○	貴市が指定する回線方式に対応いたします。
6-5	WAN用ルータ	遠隔から設定変更、状態確認及びログ確認が可能であること	○	遠隔から設定変更、状態確認及びログ確認が可能です。
6-5	WAN用ルータ	統合運用監視基盤の監視対象に含めること	○	統合運用監視基盤の監視対象に含めることが可能です。
6-5	WAN用ルータ	必要なルーティング、QoS及びアクセス制御を設定可能であること。なお、ルーティング方式は提案内容に基づくものとし、詳細は7-7「WAN用ルータ」の機器要件によること。	○	必要なルーティング、QoS及びアクセス制御を設定可能です。なお、ルーティング方式はOSPFとし、詳細は7-7「WAN用ルータ」の機器要件を満たします。
6-5	WAN用ルータ	回線切替時には、既存事業者及び新規回線事業者と調整の上、切替手順、試験手順及びロールバック手順を作成	○	回線切替時には、既存事業者及び新規回線事業者と調整の上、切替手順、試験手順及びロールバック手順を作成いたします。
6-5	WAN用ルータ	設置拠点、回線種別は別紙2「拠点一覧」を参照すること。	○	設置拠点、回線種別は別紙2「拠点一覧」を参照いたします。
7	ネットワーク機器の機器要件			
7-1	機器に関する共通要件			
7-1	機器に関する共通要件	本章に定める対象機器は、機器種別ごとの個別要件に加え、以下の共通要件を満たすこと。	○	対象機器は、機器種別ごとの個別要件に加え、以下の共通要件を満たします。
7-1	機器に関する共通要件	現行の利用状況及び本事業で見込まれる構成変更を踏まえ、安定運用が可能な性能、機能及び拡張性を有すること。	○	構成機器は現行以上の性能を有しており、現行の利用状況及び本事業で見込まれる構成変更を踏まえ、安定運用が可能な性能、機能及び拡張性を有しています。
7-1	機器に関する共通要件	将来の端末数、通信量、無線利用、機能追加及び構成変更に対応できること。	○	構成機器は現行以上の性能を有しており、将来の端末数、通信量、無線利用、機能追加及び構成変更に対応可能です。
7-1	機器に関する共通要件	機器の仕様上制約となる事項がある場合は、提案時に明示すること。	○	機器の仕様上制約となる事項は特ありません。
7-1	機器に関する共通要件	省エネルギー性に配慮した機器を積極的に提案すること。	○	フロアスイッチハブブランナー基準に準拠した製品を導入するなど、省エネルギー性に配慮した機器を採用しております。
7-1	機器に関する共通要件	機器の役割及び重要性に応じて、冗長化、冗長電源、冗長リンクその他適切な可用性対策を講じること。	○	本庁舎の内部ファイアウォール、コアスイッチ、ディストリビューションスイッチ、サーバ室内スイッチは2台1組の冗長構成とします。またフロアスイッチはホットスタンバイ機を準備いたします。
7-1	機器に関する共通要件	障害時に業務影響を最小化できる構成とし、交換、復旧及び切戻しが円滑に行えること。	○	本庁舎の内部ファイアウォール、コアスイッチ、ディストリビューションスイッチ、サーバ室内スイッチは2台1組の冗長構成とします。またフロアスイッチはホットスタンバイ機を準備いたします。
7-1	機器に関する共通要件	特定ベンダー独自技術に過度に依存せず、可能な限りIEEE等の標準規格に準拠した機器であること。	○	導入機器はIEEE等の標準規格に準拠しております。
7-1	機器に関する共通要件	機器の状態確認、設定変更、障害切り分け及び保守対応に必要な管理手段を有すること。	○	機器の状態確認、設定変更、障害切り分け及び保守対応に必要な管理手段であるセキュアSDプランチによる一元管理、Zabbixによる監視、FortiAnalyzerによるログ収集に対応しております。
7-1	機器に関する共通要件	管理手段として、CLI及びGUIによる操作に対応すること。なお、GUIを有する場合は日本語表示に対応することが望	○	管理手段として、CLI及びGUIによる操作に対応しております。なお、GUIは日本語表示に対応しております。
7-1	機器に関する共通要件	統合運用監視基盤との連携に必要な監視情報及びログ情報を取得可能であること。	○	統合運用監視基盤との連携に必要な監視情報及びログ情報を取得可能です。
7-1	機器に関する共通要件	SNMPv3による監視に対応すること。	○	SNMPv3による監視に対応しております。
7-1	機器に関する共通要件	Syslog等の標準的なプロトコルによりログ情報を取得可能であること。	○	Syslog等の標準的なプロトコルによりログ情報を取得可能です。
7-1	機器に関する共通要件	時刻同期が必要な機器は、NTPにより適切に時刻同期できること。	○	時刻同期が必要な機器は、NTPにより適切に時刻同期可能です。
7-1	機器に関する共通要件	設定情報の保存、バックアップ及び復元が可能であること。	○	設定情報の保存、バックアップ及び復元が可能です。
7-1	機器に関する共通要件	機器種別に応じて、アクセス制御、認証、ログ取得、設定保護、不正接続防止その他必要なセキュリティ機能を有す	○	機器種別に応じて、アクセス制御、認証、ログ取得、設定保護、不正接続防止その他必要なセキュリティ機能を有しており
7-1	機器に関する共通要件	管理通信は、SSH、HTTPS等の暗号化された方式により実施できること。	○	管理通信は、SSH、HTTPSによる暗号化された方式により実施可能です。
7-1	機器に関する共通要件	不要なサービス、不要なポート及び不要な管理機能は停止又は無効化できること。	○	不要なサービス、不要なポート及び不要な管理機能は停止又は無効化可能です。
7-1	機器に関する共通要件	提案機器は、令和13年12月31日まで、メーカーによるハードウェア保守及びソフトウェアサポートが提供可能であるこ	○	提案機器は、令和13年12月31日まで、メーカーによるハードウェア保守及びソフトウェアサポートが提供可能です。
7-1	機器に関する共通要件	上記期間中、ファームウェア、セキュリティパッチその他必要なアップデートが提供されること。	○	上記期間中、ファームウェア、セキュリティパッチその他必要なアップデートが提供されます。
7-1	機器に関する共通要件	ハードウェア保守の提供内容は、先出しセンドバック、オンサイト保守その他の対応区分を含め、提案時に明示すること。	○	メカ保守は以下のとおりです。 ファイアウォール、コアスイッチ、ディストリビューションスイッチ、サーバ室内スイッチ、WANルータについては、冗長化構成の機器は平日オンサイト保守、単一構成の機器は24時間365日オンサイト保守となります。またフロアスイッチ、エッジスイッチ、無線AP、SFPモジュールは先出しセンドバック保守となります。

項番	項目	仕様内容	対応可否	対応内容
7-1	機器に関する共通要件	将来の通信量増加やセキュリティ機能強化を見込み、十分な処理能力を有すること。提案時には、各ネットワーク機器について以下の項目について具体的な数値を明記すること。 ・ファイアウォールスループット ・セキュリティ機能有効時のスループット ・VPN利用時のスループット ・最大同時セッション数 ・新規セッション処理性能	○	構成機器は現行以上の性能を有しており、将来の通信量増加やセキュリティ機能強化を見込み、十分な処理能力を有しています。各ネットワーク機器について以下の項目について具体的な数値については提案書を参照願います。 ・ファイアウォールスループット ・セキュリティ機能有効時のスループット ・VPN利用時のスループット ・最大同時セッション数 ・新規セッション処理性能
7-2	サーバ室に設置するネットワーク機器	本庁サーバ室に設置するネットワーク機器は、本市庁内ネットワーク全体の中核を担う機器として、高い可用性、処理性能、保守性及び拡張性を有すること。各機器は、7-1「機器に関する共通要件」に加え、以下の要件を満たすこと。	○	本庁サーバ室に設置するネットワーク機器は、貴市庁内ネットワーク全体の中核を担う機器として、高い可用性、処理性能、保守性及び拡張性を有しております。各機器は、7-1「機器に関する共通要件」に加え、以下の要件を満たしております。
7-2	サーバ室に設置するネットワーク機器	(1)ファイアウォール		(1)ファイアウォール
7-2	サーバ室に設置するネットワーク機器	ファイアウォールは、庁内ネットワークと外部接続系統との境界において、通信制御、脅威の検知及び防御並びにVPN接続を担う機器として、以下の要件を満たすこと。	○	ファイアウォールは、庁内ネットワークと外部接続系統との境界において、通信制御、脅威の検知及び防御並びにVPN接続を担う機器として、以下の要件を満たしております。
7-2	サーバ室に設置するネットワーク機器	単一故障点を排除するため、2台による冗長構成とすること。	○	単一故障点を排除するため、2台による冗長構成といたします。
7-2	サーバ室に設置するネットワーク機器	冗長方式は、Active-Standby、Active-Activeその他同等以上の可用性を確保できる方式とし、提案時にその構成及び切替動作を明示すること。	○	ファイアウォールの冗長方式は、Active-Standby、Active-Activeの両方が可能で、故障時は自動的に切替ます。
7-2	サーバ室に設置するネットワーク機器	冗長切替時の通信影響を最小化できる構成とすること。	○	自動的に切り替わるため、冗長切替時の通信影響を最小化できる構成となっております。
7-2	サーバ室に設置するネットワーク機器	現行通信量、将来の通信量増加及び有効化するセキュリティ機能を考慮し、十分な処理性能を有すること。	○	構成機器は現行以上の性能を有しており、現行通信量、将来の通信量増加及び有効化するセキュリティ機能を考慮し、十分な処理性能を有しております。
7-2	サーバ室に設置するネットワーク機器	ステートフルパケットインスペクションに対応すること。	○	ステートフルパケットインスペクションに対応しております。
7-2	サーバ室に設置するネットワーク機器	送信元/送信先IPアドレス、ポート番号、プロトコル、アプリケーション識別その他必要な条件に基づく通信制御が可能であること。	○	送信元/送信先IPアドレス、ポート番号、プロトコル、アプリケーション識別に基づく通信制御が可能です。
7-2	サーバ室に設置するネットワーク機器	NAT/NAPTに対応すること。	○	NAT/NAPTに対応しております。
7-2	サーバ室に設置するネットワーク機器	静的ルーティングに対応すること。必要に応じて動的ルーティングにも対応可能であること。	○	静的ルーティングに対応しております。必要に応じて動的ルーティングにも対応可能です。
7-2	サーバ室に設置するネットワーク機器	不正侵入の検知又は防御機能を有すること。	○	不正侵入の検知又は防御機能を有しております。
7-2	サーバ室に設置するネットワーク機器	アプリケーション単位での識別及び制御が可能であること。	○	アプリケーション単位での識別及び制御が可能です。
7-2	サーバ室に設置するネットワーク機器	URLフィルタリング、マルウェア対策その他の脅威対策機能を有することが望ましい。	○	外部ファイアウォールはURLフィルタリング、マルウェア対策その他の脅威対策機能を有しております。
7-2	サーバ室に設置するネットワーク機器	必要に応じて、複数セグメントを論理的に収容できること。	○	複数セグメントを論理的に収容可能です。
7-2	サーバ室に設置するネットワーク機器	VPN機能としてIPsec-VPNに対応すること。必要に応じて、その他の安全な接続方式にも対応可能であること。	○	ファイアウォールはVPN機能としてIPsec-VPNに対応しています。
7-2	サーバ室に設置するネットワーク機器	管理ログ、システムログ、通信ログ、セキュリティイベントログ及びVPN接続ログを取得できること。	○	管理ログ、システムログ、通信ログ、セキュリティイベントログ及びVPN接続ログを取得可能です。
7-2	サーバ室に設置するネットワーク機器	障害解析、監査及びインシデント対応に必要な情報を記録できること。	○	障害解析、監査及びインシデント対応に必要な情報を記録可能です。
7-2	サーバ室に設置するネットワーク機器	コアスイッチ、外部接続回線、外部接続関連機器その他必要な接続先を考慮し、必要なインターフェース種別、速度及びポート数を備えること。受託者はネットワーク全体の設計に基づき、最適なポート構成を提案すること。	○	コアスイッチ、外部接続回線、外部接続関連機器その他必要な接続先を考慮し、必要なインターフェース種別、速度及びポート数を備えております。
7-2	サーバ室に設置するネットワーク機器	冗長接続、将来拡張及び保守作業を考慮し、必要な予備ポートを確保すること。	○	ファイアウォールは冗長接続、将来拡張及び保守作業を考慮し、必要な予備ポートを確保しております。
7-2	サーバ室に設置するネットワーク機器	なお、記載する性能要件は最低要件とし、各機能を有効化した状態で本市の利用条件を満たすこと。	○	なお、記載する性能要件は最低要件とし、各機能を有効化した状態で貴市の利用条件を満たします。
7-2	サーバ室に設置するネットワーク機器	(2)コアスイッチ（L3スイッチ）		(2)コアスイッチ（L3スイッチ）
7-2	サーバ室に設置するネットワーク機器	コアスイッチは、ファイアウォール、サーバ、本庁舎のディストリビューションスイッチ等を集約する基幹機器である。高速かつ安定した通信を常時提供するため、以下の要件を満たすこと。	○	コアスイッチは、ファイアウォール、サーバ、本庁舎のディストリビューションスイッチ等を集約する基幹機器である。高速かつ安定した通信を常時提供するため、以下の要件を満たします。
7-2	サーバ室に設置するネットワーク機器	単一故障点を排除するため、2台による冗長構成とすること。	○	単一故障点を排除するため、2台による冗長構成としております。
7-2	サーバ室に設置するネットワーク機器	2台を論理的に一体として運用できる構成又は同等以上の可用性及び保守性を確保できる構成であること。	○	コアSWは2台によるMC-LAG機能により、冗長構成を可用性、保守性を確保できる構成としております。
7-2	サーバ室に設置するネットワーク機器	片系障害時であっても通信継続に支障を生じない構成とすること。	○	片系障害時であっても通信継続に支障を生じない構成としております。
7-2	サーバ室に設置するネットワーク機器	庁内全体の通信を安定して処理できる十分なスイッチング容量及び転送性能を有すること。	○	構成機器は現行以上の性能を有しており、庁内全体の通信を安定して処理できる十分なスイッチング容量及び転送性能を有しております。
7-2	サーバ室に設置するネットワーク機器	将来の端末増加、無線利用拡大、IP電話導入及び機能追加に対応可能な性能余力を有すること。	○	将来の端末増加、無線利用拡大、IP電話導入及び機能追加に対応可能な性能余力を有しております。
7-2	サーバ室に設置するネットワーク機器	提案時には、主要な性能諸元を明記すること。	○	提案書をご参照願います。
7-2	サーバ室に設置するネットワーク機器	L3スイッチとして動作し、VLAN間ルーティングが可能であること。	○	L3スイッチとして動作し、VLAN間ルーティングが可能です。
7-2	サーバ室に設置するネットワーク機器	静的ルーティングに対応すること。必要に応じて動的ルーティングにも対応可能であること。	○	静的ルーティングに対応しております。必要に応じて動的ルーティングにも対応可能です。
7-2	サーバ室に設置するネットワーク機器	IEEE 802.1Q準拠のVLAN機能を有すること。	○	IEEE 802.1Q準拠のVLAN機能を有しております。
7-2	サーバ室に設置するネットワーク機器	ACLによる通信制御が可能であること。	○	ACLによる通信制御が可能です。
7-2	サーバ室に設置するネットワーク機器	QoS機能を有し、重要通信の優先制御に対応できること。	○	QoS機能を有し、重要通信の優先制御に対応可能です。
7-2	サーバ室に設置するネットワーク機器	LACP等のリンクアグリゲーション機能に対応すること。	○	LACP等のリンクアグリゲーション機能に対応しております。
7-2	サーバ室に設置するネットワーク機器	必要に応じて、論理分離機能に対応可能であること。	○	必要に応じて、論理分離機能に対応可能です。
7-2	サーバ室に設置するネットワーク機器	ファイアウォール、サーバ室内スイッチ、ディストリビューションスイッチその他必要な接続先との接続を考慮し、必要なインターフェース種別、速度及びポート数を備えること。	○	ファイアウォール、サーバ室内スイッチ、ディストリビューションスイッチその他必要な接続先との接続を考慮し、必要なインターフェース種別、速度及びポート数を備えております。
7-2	サーバ室に設置するネットワーク機器	将来の構成変更、機器増設及び保守作業に備え、必要な予備ポートを確保すること。	○	将来の構成変更、機器増設及び保守作業に備え、必要な予備ポートを確保しております。
7-2	サーバ室に設置するネットワーク機器	(3)サーバ室内スイッチ		(3)サーバ室内スイッチ
7-2	サーバ室に設置するネットワーク機器	サーバ室内スイッチは、本庁サーバ室内に設置する各種サーバ、統合運用監視基盤、管理端末その他必要な機器を収容するためのスイッチとして、以下の要件を満たすこと。	○	サーバ室内スイッチは、本庁サーバ室内に設置する各種サーバ、統合運用監視基盤、管理端末その他必要な機器を収容するためのスイッチとして、以下の要件を満たしております。
7-2	サーバ室に設置するネットワーク機器	将来の構成変更、機器増設及び保守作業に備え、必要な予備ポートを確保すること。	○	将来の構成変更、機器増設及び保守作業に備え、必要な予備ポートを確保しております。
7-2	サーバ室に設置するネットワーク機器	接続対象機器の種別、台数及び通信要件を踏まえ、必要なポート数及び性能を有すること。	○	接続対象機器の種別、台数及び通信要件を踏まえ、必要なポート数及び性能を有しております。
7-2	サーバ室に設置するネットワーク機器	コアスイッチと接続し、必要に応じて冗長アップリンク構成を採用できること。	○	コアスイッチと接続し、必要に応じて冗長アップリンク構成を採用可能です。
7-2	サーバ室に設置するネットワーク機器	接続対象の重要性を踏まえ、保守性及び将来拡張性に配慮した構成とすること。	○	接続対象の重要性を踏まえ、保守性及び将来拡張性に配慮した構成としております。
7-2	サーバ室に設置するネットワーク機器	IEEE 802.1Q準拠のVLAN機能を有すること。	○	IEEE 802.1Q準拠のVLAN機能を有しております。
7-2	サーバ室に設置するネットワーク機器	必要に応じてLACP等のリンクアグリゲーションに対応すること。	○	必要に応じてLACP等のリンクアグリゲーションに対応しております。
7-2	サーバ室に設置するネットワーク機器	ループ防止、ポート制御その他必要なL2機能を有すること。	○	ループ防止、ポート制御その他必要なL2機能を有しております。
7-2	サーバ室に設置するネットワーク機器	接続対象に応じて必要なアクセス制御その他の設定が可能であること。	○	接続対象に応じて必要なアクセス制御その他の設定が可能です。
7-2	サーバ室に設置するネットワーク機器	接続対象機器及びコアスイッチとの接続を考慮し、必要なインターフェース種別、速度及びポート数を備えること。	○	接続対象機器及びコアスイッチとの接続を考慮し、必要なインターフェース種別、速度及びポート数を備えております。
7-2	サーバ室に設置するネットワーク機器	通信量、冗長性及び将来拡張を考慮した帯域を確保すること。	○	通信量、冗長性及び将来拡張を考慮した帯域を確保しております。
7-3	本庁舎における要件	本庁舎に設置するネットワーク機器は、執務室、会議室その他庁舎内の各エリアにおいて、安定した有線及び無線ネットワーク接続を提供するための機器として、7-1「機器に関する共通要件」に加え、以下の要件を満たすこと。	○	本庁舎に設置するネットワーク機器は、執務室、会議室その他庁舎内の各エリアにおいて、安定した有線及び無線ネットワーク接続を提供するための機器として、7-1「機器に関する共通要件」に加え、以下の要件を満たしております。
7-3	本庁舎における要件	(1)ディストリビューションスイッチ		(1)ディストリビューションスイッチ
7-3	本庁舎における要件	ディストリビューションスイッチは、本庁舎内の各フロアスイッチを集約し、コアスイッチとの接続を担う機器として、以下の要件を満たすこと。	○	ディストリビューションスイッチは、本庁舎内の各フロアスイッチを集約し、コアスイッチとの接続を担う機器として、以下の要件を満たしております。
7-3	本庁舎における要件	接続対象となるフロアスイッチ及び上位接続を踏まえ、必要に応じて冗長構成又は冗長アップリンク構成を採用できること。	○	接続対象となるフロアスイッチ及び上位接続を踏まえ、必要に応じて冗長構成又は冗長アップリンク構成を採用可能です。
7-3	本庁舎における要件	障害時に影響範囲を局所化できる構成とすること。	○	2台による冗長構成といたします。

項番	項目	仕様内容	対応可否	対応内容
7-3	本庁舎における要件	接続するフロアスイッチ及びその配下端末の通信を安定して処理できる十分なスイッチング容量及び転送性能を有すること。	○	接続するフロアスイッチ及びその配下端末の通信を安定して処理できる十分なスイッチング容量及び転送性能を有しております。
7-3	本庁舎における要件	将来の端末増加、無線利用拡大及び機器増設に対応可能な性能余力を有すること。	○	将来の端末増加、無線利用拡大及び機器増設に対応可能な性能余力を有しております。
7-3	本庁舎における要件	L2スイッチ又はL3スイッチとして必要な機能を有し、設計に応じて適切に運用できること。	○	L2スイッチ又はL3スイッチとして必要な機能を有し、設計に応じて適切に運用です。
7-3	本庁舎における要件	IEEE 802.1Q準拠のVLAN機能を有すること。	○	IEEE 802.1Q準拠のVLAN機能を有しております。
7-3	本庁舎における要件	必要に応じてACLによる通信制御が可能であること。	○	必要に応じてACLによる通信制御が可能です。
7-3	本庁舎における要件	QoS機能を有し、重要通信の優先制御に対応できること。	○	QoS機能を有し、重要通信の優先制御に対応可能です。
7-3	本庁舎における要件	LACP等のリンクアグリゲーション機能に対応すること。	○	LACP等のリンクアグリゲーション機能に対応可能です。
7-3	本庁舎における要件	ループ防止又はループ検知のために必要な機能を有すること。	○	ループ防止又はループ検知のために必要な機能を有しております。
7-3	本庁舎における要件	コアスイッチ及び各フロアスイッチとの接続を考慮し、必要なインターフェース種別、速度及びポート数を備えること。	○	コアスイッチ及び各フロアスイッチとの接続を考慮し、必要なインターフェース種別、速度及びポート数を備えております。
7-3	本庁舎における要件	上位及び下位接続について、冗長性、保守性及び将来拡張を考慮した構成とすること。	○	上位及び下位接続について、冗長性、保守性及び将来拡張を考慮した構成としております。
7-3	本庁舎における要件	(2)フロアスイッチ		(2)フロアスイッチ
7-3	本庁舎における要件	フロアスイッチは、本庁舎各階において執務用端末、プリンタ、無線アクセスポイント、IP電話機その他必要な機器を収容するための機器として、以下の要件を満たすこと。	○	フロアスイッチは、本庁舎各階において執務用端末、プリンタ、無線アクセスポイント、IP電話機その他必要な機器を収容するための機器として、以下の要件を満たしております。
7-3	本庁舎における要件	設置フロア（本館地下1階から9階各階南北EPS）における接続対象機器の種別、台数及び通信要件を踏まえ、必要なポート数及び性能を有すること。	○	設置フロア（本館地下1階から9階各階南北EPS）における接続対象機器の種別、台数及び通信要件を踏まえ、必要なポート数及び性能を有しております。
7-3	本庁舎における要件	ディストリビューションスイッチと接続し、必要に応じて冗長アップリンク構成を採用できること。	○	ディストリビューションスイッチと接続し、必要に応じて冗長アップリンク構成を採用可能です。
7-3	本庁舎における要件	執務継続に支障を生じないよう、保守性及び将来拡張性に配慮した構成とすること。	○	執務継続に支障を生じないよう、ホットスタンバイ構成としております。
7-3	本庁舎における要件	フロアスイッチは、端末、プリンタ、無線アクセスポイントその他の情報系機器に加え、IP電話機を同一機器に収容できること。なお、フロアスイッチについては、情報系機器用とIP電話機用で物理的に機器を分離することは要しない。	○	フロアスイッチは、端末、プリンタ、無線アクセスポイントその他の情報系機器に加え、IP電話機を同一機器に収容可能です。
7-3	本庁舎における要件	IEEE 802.1Q準拠のVLAN機能を有すること。	○	IEEE 802.1Q準拠のVLAN機能を有しております。
7-3	本庁舎における要件	ループ防止、ポート制御その他必要なL2機能を有すること。	○	ループ防止、ポート制御その他必要なL2機能を有しております。
7-3	本庁舎における要件	DHCPスヌーピング、ARPスプーフィング対策、ポート単位のアクセス制御その他有効なL2セキュリティ機能を有することが望ましい。	○	フロアSWはDHCPスヌーピング、ARPスプーフィング対策、ポート単位のアクセス制御機能を有しております。
7-3	本庁舎における要件	接続対象機器及び上位スイッチとの接続を考慮し、必要なインターフェース種別、速度及びポート数を備えること。	○	接続対象機器及び上位スイッチとの接続を考慮し、必要なインターフェース種別、速度及びポート数を備えております。
7-3	本庁舎における要件	IP電話機を収容する場合は、情報系通信と論理的に分離できること。	○	IP電話機を収容する場合は、情報系通信と論理的に分離可能です。
7-3	本庁舎における要件	無線アクセスポイントやIP電話その他PoE受電機器を接続する箇所については、PoE（IEEE 802.af）以上に対応し、想定台数のポート数を有し、想定接続台数に対して同時給電可能な装置全体の給電容量を有すること。	○	無線アクセスポイントやIP電話その他PoE受電機器を接続する箇所については、PoE（IEEE 802.af）以上に対応しております。想定台数のポート数を有し、想定接続台数に対して同時給電可能な装置全体の給電容量を有しております。
7-3	本庁舎における要件	IP電話機を安定して利用できるよう、QoSによる音声通信の優先制御に対応すること。	○	IP電話機を安定して利用できるよう、QoSによる音声通信の優先制御に対応しております。
7-3	本庁舎における要件	(3)エッジスイッチ		(3)エッジスイッチ
7-3	本庁舎における要件	エッジスイッチは、会議室、窓口、共用部その他限られたエリアにおいて少数の端末、プリンタ、IP電話又は無線アクセスポイントを収容するための機器として、以下の要件を満たすこと。	○	エッジスイッチは、会議室、窓口、共用部その他限られたエリアにおいて少数の端末、プリンタ、IP電話又は無線アクセスポイントを収容するための機器として、以下の要件を満たしております。
7-3	本庁舎における要件	設置箇所における接続対象機器の種別、台数及び通信要件を踏まえ、必要なポート数及び性能を有すること。	○	設置箇所における接続対象機器の種別、台数及び通信要件を踏まえ、必要なポート数及び性能を有しております。
7-3	本庁舎における要件	設置箇所の用途に応じ、必要な静音性、設置性及び保守性に配慮した機器であること。	○	設置箇所の用途に応じ、必要な静音性、設置性及び保守性に配慮した機器を採用しております。
7-3	本庁舎における要件	端末、プリンタその他の情報系機器を収容するためのエッジスイッチと、IP電話を収容するためのエッジスイッチは、障害影響の分離、運用管理の明確化及び音声品質確保の観点から、同一筐体で共用せず、それぞれ別個の機器として構成すること。	○	端末、プリンタその他の情報系機器を収容するためのエッジスイッチと、IP電話を収容するためのエッジスイッチは、障害影響の分離、運用管理の明確化及び音声品質確保の観点から、同一筐体で共用せず、それぞれ別個の機器として構成いたします。
7-3	本庁舎における要件	執務空間、窓口又は会議室等への設置を考慮し、ファンレスであること。	○	執務空間、窓口又は会議室等への設置を考慮し、ファンレスとなっております。
7-3	本庁舎における要件	設置性を考慮し、マグネットその他これと同等の方法により、机、什器その他適切な箇所へ固定できること。	○	設置性を考慮し、マグネットその他これと同等の方法により、机、什器その他適切な箇所へ固定可能です。
7-3	本庁舎における要件	IEEE 802.1Q準拠のVLAN機能を有すること。	○	IEEE 802.1Q準拠のVLAN機能を有しております。
7-3	本庁舎における要件	ループ防止、ポート制御その他必要なL2機能を有すること。	○	ループ防止、ポート制御機能を有しております。
7-3	本庁舎における要件	ループ検知機能を有すること。ループを検知した場合には、ポートをリンクダウンさせる等、あらかじめ設定した動作を自動実行可能であること。	○	ループ検知機能を有しております。ループを検知した場合には、ポートをリンクダウンさせる等、あらかじめ設定した動作を自動実行可能です。
7-3	本庁舎における要件	ループ検知時には、LED表示その他の方法により、異常を視覚的に確認できること。	○	エッジSWはループ検知時には、LED表示により、異常を視覚的に確認可能です。
7-3	本庁舎における要件	接続対象に応じて必要なアクセス制御その他の設定が可能であること。	○	エッジSWは接続対象に応じて802.1xによるアクセス制御設定が可能です。
7-3	本庁舎における要件	上位スイッチ及び接続対象機器との接続を考慮し、必要なインターフェース種別、速度及びポート数を備えること。	○	上位スイッチ及び接続対象機器との接続を考慮し、必要なインターフェース種別、速度及びポート数を備えております。
7-3	本庁舎における要件	無線アクセスポイントその他PoE受電機器を収容する場合は、接続対象台数及び給電要件を踏まえ、必要なPoE給電容量を確保すること。	○	無線アクセスポイントその他PoE受電機器を収容する場合は、接続対象台数及び給電要件を踏まえ、必要なPoE給電容量を確保しております。
7-3	本庁舎における要件	IP電話を収容するエッジスイッチについては、音声通信を安定して利用できるよう、QoSによる優先制御に対応すること。	○	IP電話を収容するエッジスイッチについては、音声通信を安定して利用できるよう、QoSによる優先制御に対応しております。
7-3	本庁舎における要件	IP電話用エッジスイッチについては、PoE+（IEEE 802.3at）に対応し、想定台数のIP電話を接続可能なポート数を有し、同時給電可能な装置全体の給電容量を有すること。	○	IP電話用エッジスイッチについては、PoE+（IEEE 802.3at）に対応しております。想定台数のIP電話を接続可能なポート数を有し、同時給電可能な装置全体の給電容量を有しております。
7-4	水道局における要件	新たに調達する機器は、WAN用ルータ2台（水道局庁舎、水道局高度浄水処理棟）、スイッチ4台、無線AP8台（うち1台を水道局高度浄水処理棟に設置）とする。	○	新たに調達する機器は、WAN用ルータ2台（水道局庁舎、水道局高度浄水処理棟）、スイッチ4台、無線AP9台（うち1台を水道局高度浄水処理棟に設置）といたします。
7-4	水道局における要件	水道局庁舎の各フロアに設置するスイッチについては、4台を想定すること。なお、提案に当たっては、現状使用しているポート数を満たすスイッチ（1G対応、ファンレス、マネージドL2、8～20ポート程度、ループ防止機能、Web GUI管理機能）を選定すること。なお、無線アクセスポイントその他PoE受電機器を接続する箇所については、PoE（IEEE 802.af）以上に対応し、想定台数のポート数を有し、想定接続台数に対して同時給電可能な装置全体の給電容量を有すること。提案機器は、水道局庁舎内の各フロアにおいて、端末、プリンタ及び無線APの接続を収容し、安定した運用が可能な構成とすること。既存OAボックスその他設置環境へ収容する場合は、寸法、放熱性、保守性及び配線性を十分考慮すること。	○	水道局庁舎の各フロアに設置するスイッチについては、4台といたします。なお、現状使用しているポート数を満たすスイッチ（1G対応、ファンレス、マネージドL2、8～20ポート程度、ループ防止機能、Web GUI管理機能）を選定しております。なお、無線アクセスポイントその他PoE受電機器を接続する箇所については、PoE（IEEE 802.af）以上に対応し、想定台数のポート数を有し、想定接続台数に対して同時給電可能な装置全体の給電容量を有しております。提案機器は、水道局庁舎内の各フロアにおいて、端末、プリンタ及び無線APの接続を収容し、安定した運用が可能な構成としております。既存OAボックスその他設置環境へ収容する場合は、寸法、放熱性、保守性及び配線性を十分考慮いたします。
7-4	水道局における要件	無線APについては7-6無線AP、WAN用ルータについては7-7WAN用ルータに記載の要件を満たすこと。	○	無線APについては7-6無線AP、WAN用ルータについては7-7WAN用ルータに記載の要件を満たしております。
7-5	保健センターにおける要件	新たに調達する機器は、WAN用ルータ、無線APとする。	○	新たに調達する機器は、WAN用ルータ、無線AP、コールドスタンバイ用エッジスイッチといたします。
7-5	保健センターにおける要件	無線APについては7-6無線AP、WAN用ルータについては7-7WAN用ルータに記載の要件を満たすこと。	○	無線APについては7-6無線AP、WAN用ルータについては7-7WAN用ルータに記載の要件を満たしております。
7-5	保健センターにおける要件	接続先スイッチがPoE対応でない場合は、外付けPoEインジェクターの利用、または電源コンセントからの給電を含めて、受託者と協議の上で給電方法を決定すること。	○	外付けPoEインジェクターを導入いたします。
7-6	無線アクセスポイント	無線アクセスポイントは、本庁舎、水道局、保健センターその他必要箇所において、業務利用に耐える安定した無線LAN環境を提供するための機器として、7-1「機器に関する共通要件」に加え、以下の要件を満たすこと。	○	無線アクセスポイントは、本庁舎、水道局、保健センターその他必要箇所において、業務利用に耐える安定した無線LAN環境を提供するための機器として、7-1「機器に関する共通要件」に加え、以下の要件を満たします。
7-6	無線アクセスポイント	(1)基本要件		(1)基本要件
7-6	無線アクセスポイント	設置箇所の利用形態、利用者数、端末数、電波状況及び想定トラフィックを踏まえ、安定した通信が可能な性能を有すること。	○	設置箇所の利用形態、利用者数、端末数、電波状況及び想定トラフィックを踏まえ、安定した通信が可能な性能を有しております。
7-6	無線アクセスポイント	無線エリア設計に基づき、必要な設置台数、配置及び電波出力を適切に設定できること。	○	無線エリア設計に基づき、必要な設置台数、配置及び電波出力を適切に設定可能です。
7-6	無線アクセスポイント	屋内設置を基本とし、設置場所の環境条件に適合すること。	○	屋内設置を基本とし、設置場所の環境条件に適合しております。
7-6	無線アクセスポイント	Wi-Fi 6（IEEE 802.11ax）以上に対応すること。	○	Wi-Fi 6（IEEE 802.11ax）以上に対応しております。
7-6	無線アクセスポイント	無線機能として以下を満たすこと。	○	無線機能として以下を満たしております。
7-6	無線アクセスポイント	2.4GHz帯及び5GHz帯を同時に利用可能であること。6GHz帯対応を提案可とする。	○	2.4GHz帯及び5GHz帯を同時に利用可能です。6GHz帯にも対応可能です。
7-6	無線アクセスポイント	必要に応じて複数SSIDを提供できること。	○	必要に応じて複数SSIDを提供可能です。
7-6	無線アクセスポイント	SSIDごとに認証方式、暗号化方式、VLANその他必要な設定を分離できること。	○	SSIDごとに認証方式、暗号化方式、VLANその他必要な設定を分離可能です。
7-6	無線アクセスポイント	利用状況及び周辺環境に応じて、チャネル及び出力を適切に設定できること。	○	利用状況及び周辺環境に応じて、チャネル及び出力を適切に設定可能です。
7-6	無線アクセスポイント	無線端末間通信を禁止する機能を有すること。	○	無線端末間通信を禁止する機能を有しております。
7-6	無線アクセスポイント	インターネット系ネットワークについては、現行運用において2.4GHz帯の無線でステルスSSIDを使用している。受託者は、特定の利用者以外による不意な利用の抑止、LGWAN系その他の系統との誤接続防止及び適切な系統分離を実現できる構成とすること。なお、これらの目的を同等以上に達成できる場合は、ステルスSSID以外の方式による提案も可とする。WPA2-Enterprise及びWPA3-Enterpriseに対応すること。	○	インターネット系ネットワークについては、ステルスSSIDを使用いたします。WPA2-Enterprise及びWPA3-Enterpriseに対応しております。
7-6	無線アクセスポイント	不正接続の抑止及び利用者の適切な認証を実施できること。	○	不正接続の抑止及び利用者の適切な認証を実施可能です。
7-6	無線アクセスポイント	無線LANコントロール又は同等の集中管理機能により、一元的に設定、監視及び保守が可能であること。	○	無線LANコントロール又は同等の集中管理機能により、一元的に設定、監視及び保守が可能です。
7-6	無線アクセスポイント	設定変更、障害確認、稼働状況確認その他運用管理に必要な情報を取得できること。	○	設定変更、障害確認、稼働状況確認その他運用管理に必要な情報を取得可能です。
7-6	無線アクセスポイント	有線ネットワークとの接続に必要なインターフェースを有すること。	○	有線ネットワークとの接続に必要なインターフェースを有しております。
7-6	無線アクセスポイント	PoE+（IEEE 802.3at）以上の受電に対応すること。	○	PoE+（IEEE 802.3at）以上の受電に対応可能です。
7-6	無線アクセスポイント	必要な給電条件は、接続先スイッチのPoE設計と整合すること。	○	必要な給電条件は、接続先スイッチのPoE設計と整合いたします。
7-7	WAN用ルータ	WAN用ルータは、本庁舎と各拠点との間の広域通信を担い、安全かつ安定した拠点間接続を提供するための機器として、7-1「機器に関する共通要件」に加え、以下の要件を満たすこと。	○	WAN用ルータは、本庁舎と各拠点との間の広域通信を担い、安全かつ安定した拠点間接続を提供するための機器として、7-1「機器に関する共通要件」に加え、以下の要件を満たします。
7-7	WAN用ルータ	接続する回線種別、帯域、拠点構成及び想定通信量を踏まえ、安定した広域通信を提供できる性能を有すること。	○	接続する回線種別、帯域、拠点構成及び想定通信量を踏まえ、安定した広域通信を提供できる性能を有しております。
7-7	WAN用ルータ	各拠点の業務継続に支障を生じないよう、保守性及び将来拡張性に配慮した構成とすること。	○	1台構成としますが、障害発生時には業務継続に支障がでないよう、24時間365日のオンサイト保守にて対応いたします。
7-7	WAN用ルータ	契約回線帯域を十分に処理できるスループットを有すること。	○	契約回線帯域を十分に処理できるスループットを有しております。
7-7	WAN用ルータ	VPN機能を利用する場合は、暗号化処理を含めて必要な性能を有すること。	○	VPN機能を利用する場合は、暗号化処理を含めて必要な性能を有しております。
7-7	WAN用ルータ	提案時には、スループット、VPN処理性能、搭載インターフェースその他主要な性能諸元を明記すること。主要な性能諸元を明記すること。	○	提案書をご参照願います。
7-7	WAN用ルータ	ルーティング機能を有し、静的ルーティングに対応すること。なお、ルーティング方式は、静的ルーティング、動的ルーティングその他適切な方法によるものとし、採用方式、その理由、運用方法及び対応プロトコルを提案書に明記すること。	○	ルーティング機能を有し、静的、動的ルーティングに対応しております。なお、既存のルーティング方式はOSPFであるため、対応プロトコルはOSPFといたします。
7-7	WAN用ルータ	動的ルーティングを採用する場合は、対応可能なルーティングプロトコルを明記すること。	○	拠点間通信は既存踏襲でOSPFを採用予定となります
7-7	WAN用ルータ	IPsec-VPNに対応すること。	○	IPsec-VPNに対応可能です。

項番	項目	仕様内容	対応可否	対応内容
7-7	WAN用ルータ	QoS機能を有し、重要通信の優先制御に対応できること。	○	QoS機能を有し、重要通信の優先制御に対応可能です。
7-7	WAN用ルータ	必要に応じて回線障害時の切替又は迂回構成に対応可能であること。	○	必要に応じて回線障害時の切替又は迂回構成に対応可能です。
7-7	WAN用ルータ	WAN側及びLAN側の接続を考慮し、必要なインターフェース種別、速度及びポート数を備えること。	○	WAN側及びLAN側の接続を考慮し、必要なインターフェース種別、速度及びポート数を備えております。
7-7	WAN用ルータ	接続先機器、回線終端装置及び将来拡張を考慮した構成とすること。	○	接続先機器、回線終端装置及び将来拡張を考慮した構成としております。
7-7	WAN用ルータ	多拠点展開を考慮し、設定、展開及び保守が効率的に行えること。	○	多拠点展開を考慮し、セキュアSDブランチ構成により、設定、展開及び保守が効率的に実施可能です。
7-7	WAN用ルータ	必要に応じて、初期設定の自動展開その他運用負荷軽減に資する機能を有することが望ましい。	○	必要に応じて、初期設定の自動展開が可能です。
8	テスト・移行に係る要件			
8-1	テストに係る要件			
8-1	テストに係る要件	受託者は、単体試験、ネットワーク構成試験、統合運用監視基盤試験、無線AP試験、賦課試験を含む試験計画を作成し、本市の承認を得たうえで実施すること。	○	受託者は、単体試験、ネットワーク構成試験、統合運用監視基盤試験、無線AP試験、賦課試験を含む試験計画を作成し、貴市の承認を得たうえで実施いたします。
8-1	テストに係る要件	試験ごとに、目的、前提条件、手順、期待結果、合否判定基準、不具合発生時の取扱い及び再試験条件を明記すること。	○	試験ごとに、目的、前提条件、手順、期待結果、合否判定基準、不具合発生時の取扱い及び再試験条件を明記いたします。
8-1	テストに係る要件	試験項目は、機器の死活監視、設定確認、通信性能、冗長構成動作、セキュリティ設定及び運用管理機能を含む	○	試験項目は、機器の死活監視、設定確認、通信性能、冗長構成動作、セキュリティ設定及び運用管理機能を含めます。
8-1	テストに係る要件	総合試験として、以下の動作確認を行うこと。 ・正常系・障害系（回線／機器切替） ・情報セキュリティ関連機能 ・ルーティング機能 ・外部接続機能 ・統合監視（可視化・監視・ログ収集・通知・バックアップなど） ・外部施設間WAN疎通	○	総合試験として、以下の動作確認を行います。 ・正常系・障害系（回線／機器切替） ・情報セキュリティ関連機能 ・ルーティング機能 ・外部接続機能 ・統合監視（可視化・監視・ログ収集・通知・バックアップなど） ・外部施設間WAN疎通
8-1	テストに係る要件	試験結果は報告書としてとりまとめ、本市の承認を得ること。	○	試験結果は報告書としてとりまとめ、貴市の承認を得ます。
8-2	移行要件	受託者は切替手順、ロールバック手順、業務影響の最小化策を含めた移行計画を策定し、本市の承認を得た上で実施すること。	○	切替手順、ロールバック手順、業務影響の最小化策を含めた移行計画を策定し、貴市の承認を得た上で実施いたします。
8-2	移行要件	移行にあたり、事前に必要な設定変更、試験及び関係者調整を完了させること。	○	移行にあたり、事前に必要な設定変更、試験及び関係者調整を完了いたします。
8-2	移行要件	移行作業は受託者が統括し、本市及び関係事業者と調整しながら実施すること。	○	移行作業は弊社が統括し、貴市及び関係事業者と調整しながら実施いたします。
8-2	移行要件	並行稼働期間の設定等により、業務継続性に影響を与えないこと。	○	並行稼働期間の設定等により、業務継続性に影響を与えないよう実施いたします。
8-2	移行要件	切り替え時は、確実なサポート体制をとること。	○	切り替え時は、確実なサポート体制をとります。
8-2	移行要件	切り替え後の障害に備え、ロールバック手順・発動条件・所要時間・確認手順を事前に整備し、可能な範囲でリハーサルすること。	○	切り替え後の障害に備え、ロールバック手順・発動条件・所要時間・確認手順を事前に整備し、可能な範囲でリハーサルを実施します。
8-2	移行要件	IPアドレスの変更を伴う場合は、影響調査・段階移行・復旧手順を含む計画を必須とする。	○	IPアドレスの変更を伴う場合は、影響調査・段階移行・復旧手順を含む計画を策定いたします。
8-2	移行要件	手戻リスクが高い設定変更（コア切り替え、IP一括変更、無線認証方式切り替え等）は、事前検証・レビュー・リハーサルを必須とする。	○	手戻リスクが高い設定変更（コア切り替え、IP一括変更、無線認証方式切り替え等）は、事前検証・レビュー・リハーサルを必須いたします。
8-2	移行要件	WAN回線更新に伴う切り替えについては、WAN回線提供事業者と役割分担を明確化し、切替計画・試験計画・当日統括（指揮系統、エスカレーション）を含めて実施すること。	○	WAN回線更新に伴う切り替えについては、WAN回線提供事業者と役割分担を明確化し、切替計画・試験計画・当日統括（指揮系統、エスカレーション）を含めて実施いたします。
8-2	移行要件	本番切替前には移行判定会を実施し、切替条件、実施体制、連絡体制、当日判断基準及びロールバック条件を確認すること。	○	本番切替前には移行判定会を実施し、切替条件、実施体制、連絡体制、当日判断基準及びロールバック条件を確認いたします。
9	セキュリティ要件		○	
9-1	基本要件	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ぐこと、並びに、発生した場合に被害を最小限に抑えること。	○	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ぐこと、並びに、発生した場合に被害を最小限に抑えます。
9-1	基本要件	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。	○	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、速やかに貴市に報告し、対応策について協議いたします。
9-1	基本要件	本事業において、発注者の意図しない変更や機密情報の窃取等が行われない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。	○	貴市の意図しない変更や機密情報の窃取等が行われないことを保証する管理を、一貫した品質保証体制の下で実施いたします。
9-1	基本要件	発注者の意図しない変更や機密情報の窃取等が行われないことを保証するための具体的な管理手順や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や各担当者がアクセス可能な範囲等を示した管理体制図）を発注者との協議の上、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。	○	貴市の意図しない変更や機密情報の窃取等が行われないことを保証するための具体的な管理手順や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や各担当者がアクセス可能な範囲等を示した管理体制図）を貴市との協議の上、必要と判断された場合は提出いたします。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、提出いたします。
9-1	基本要件	本事業において発注者の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、発注者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や作業履歴等を記録し、発注元から要求された場合には提出させるようにする等）また、当該手順及び体制が妥当であることを証明するための書類を発注者との協議の上、必要と判断された場合は提出すること。	○	貴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ときに、追跡調査や立入検査等、貴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いたします。（例えば、運用・保守業務におけるシステムの操作ログや作業履歴等を記録し、発注元から要求された場合には提出させるようにする等）また、当該手順及び体制が妥当であることを証明するための書類を貴市との協議の上、必要と判断された場合は提出いたします。
9-1	基本要件	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。	○	本事業の各工程においては、情報セキュリティに係るサプライチェーン・リスクを低減するための対策を講じております。取引先に対する信用調査の実施に加え、お客様情報保護に関する覚書の締結、および定期的なお客様情報保護体制の確認を行っております。
9-1	基本要件	本事業に従事する受託者の従業員すべてに対して、情報セキュリティに関することなどの教育を実施すること。	○	本事業に従事する弊社の従業員すべてに対して、情報セキュリティに関することなどの教育を実施いたします。
9-1	基本要件	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に、脆弱性診断の実施、検出された脆弱性への対応を行うこと。	○	セキュリティ関連のテストの実施結果をご報告いたします。 情報システムに対して脆弱性診断を実施する場合は、「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」に定める実施基準を満たすよう、脆弱性診断の実施および検出された脆弱性への適切な対応を行います。 また、プラットフォーム診断においては、Nmapに準拠したツールを使用する予定です。
9-1	基本要件	また、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。	○	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ます。
9-1	基本要件	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を下表に示す。本事業における運用保守対象の範囲で該当するものは、各項目に対して漏れなく対応すること。	○	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を下表に示す。本事業における運用保守対象の範囲で該当するものは、各項目に対して漏れなく対応します。
9-2	ネットワーク管理におけるセキュリティ要件	管理通信は、業務通信と分離した専用ネットワーク上で行うこと。	○	管理通信は、業務通信と分離した専用ネットワーク上で行います。
9-2	ネットワーク管理におけるセキュリティ要件	管理者権限を分離し、共有IDの使用は原則禁止とすること。やむを得ず使用する場合は、理由・代替策などを提案すること。	○	管理者権限を分離し、共有IDの使用は原則禁止いたします。 エッジSW、UPSは単一のアカウントでの運用となりますので、作業日時、作業者、作業内容を台帳管理するなど運用対応を行います。
9-2	ネットワーク管理におけるセキュリティ要件	管理操作ログが追跡できる仕組み（装置ログ、統合監視、台帳・変更管理等）を整備すること。	○	管理操作ログが追跡できる仕組み（装置ログ、統合監視、台帳・変更管理等）を整備いたします。
9-2	ネットワーク管理におけるセキュリティ要件	各機器及び監視基盤において、ログを適切に取得・保管し、保管期間及び閲覧権限を設定できること。ログの保管期間、閲覧権限、バックアップ方針を運用設計に明記すること。	○	各機器及び監視基盤において、ログを適切に取得・保管し、保管期間及び閲覧権限を設定可能です。ログの保管期間、閲覧権限、バックアップ方針を運用設計に明記いたします。
9-2	ネットワーク管理におけるセキュリティ要件	機器ログ・監視ログの整合性確保のため、時刻同期（NTP等）を設計に含めること。	○	機器ログ・監視ログの整合性確保のため、時刻同期（NTP等）を設計に含めます。
9-2	ネットワーク管理におけるセキュリティ要件	保守接続は暗号化された方式（例：SSH、HTTPS）で行い、不必要なポート及びサービスは無効化すること。	○	保守接続は暗号化された方式（例：SSH、HTTPS）で行い、不必要なポート及びサービスは無効化いたします。
9-2	ネットワーク管理におけるセキュリティ要件	設定変更は事前承認制とし、変更履歴を記録すること。	○	設定変更は事前承認制とし、変更履歴を記録いたします。
9-2	ネットワーク管理におけるセキュリティ要件	機器間通信は暗号化されたプロトコル（例：IPsec、TLS）を使用すること。	○	管理通信はSSH,https(TLS)を使用いたします
9-2	ネットワーク管理におけるセキュリティ要件	管理端末及び設定情報は、適切な権限管理の下で保管し、持出を禁止すること。	○	管理端末及び設定情報は、適切な権限管理の下で保管し、持出を禁止いたします。
9-2	ネットワーク管理におけるセキュリティ要件	受託者は、構築時点で推奨ファームウェアを適用し、以後の更新手順（影響評価、適用計画、ロールバック）を手順書に含めること。	○	構築時点で推奨ファームウェアを適用し、以後の更新手順（影響評価、適用計画、ロールバック）を手順書に含めます。
9-2	ネットワーク管理におけるセキュリティ要件	重大な脆弱性が公表された場合の対応フロー（情報収集→影響評価→暫定/恒久対策→報告）を運用設計に含めること。	○	重大な脆弱性が公表された場合の対応フロー（情報収集→影響評価→暫定/恒久対策→報告）を運用設計に含めます。
10	プロジェクト要件		○	
10-1	プロジェクト体制及び役割	本事業を適切・効率的に履行するためのプロジェクト体制として、以下の役割を担うものを選任すること。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、それぞれ違う人物を選任すること。なお、(2)は、複数人選任することを妨げない。	○	本事業を適切・効率的に履行するためのプロジェクト体制として、以下の役割を担うものを選任するいたします。以下の(1)は、(2)から(4)の役割は兼務いたしません。
10-1	プロジェクト体制及び役割	(1)プロジェクトマネージャ（PM）		(1)プロジェクトマネージャ（PM）
10-1	プロジェクト体制及び役割	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。プロジェクト計画書を作成し、本事業を円滑に遂行するための各作業工程管理及び関連する業務や利害関係者との調整等を実施し、作業全体を統括して管理する。	—	—
10-1	プロジェクト体制及び役割	本プロジェクトを管理するのに相応しいだけの知識や経験を有している者を採用すること。	○	本プロジェクトを管理するのに相応しいだけの知識や経験を有している者を採用しております。
10-1	プロジェクト体制及び役割	(2)プロジェクトリーダー（PL）		(2)プロジェクトリーダー（PL）
10-1	プロジェクト体制及び役割	プロジェクトマネージャが作成したプロジェクト計画書に基づき、現場で作業を実施する責任者。本市と現場レベルの打ち合わせを実施する者。本事業の各業務に精通し、知識や経験を有している者を採用すること。	○	本事業の各業務に精通し、知識や経験を有している者を採用しております。
10-1	プロジェクト体制及び役割	(3)プロジェクト品質管理者		(3)プロジェクト品質管理者
10-1	プロジェクト体制及び役割	プロジェクトの品質管理を行う責任者を配置すること。	—	—
10-1	プロジェクト体制及び役割	(4)セキュリティ管理者		(4)セキュリティ管理者
10-1	プロジェクト体制及び役割	本プロジェクトを通じてセキュリティ管理を行う責任者を配置すること。	—	—
10-2	プロジェクト体制及び役割に関する留意事項	(1)プロジェクト体制の記載事項		(1)プロジェクト体制の記載事項
10-2	プロジェクト体制及び役割に関する留意事項	受託者は、プロジェクト体制の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。	○	プロジェクト体制の役割分担を明確にし、貴市の指示に基づき適切に対応いたします。

項番	項目	仕様内容	対応可否	対応内容
10-2	プロジェクト体制及び役割に関する留意事項	(2)プロジェクト体制の変更		(2)プロジェクト体制の変更
10-2	プロジェクト体制及び役割に関する留意事項	原則としてプロジェクト体制の変更は原則認めないこととする。ただし、進捗に著しい遅れが発生した等の理由で要員の追加及び作業担当者の変更がやむを得ない場合は、速やかに改善策を書面で提示し、本市の承諾を得ること。	○	やむを得ずプロジェクト体制の変更を要する場合は、速やかに改善策を書面で提示し、貴市の承諾を得ることいたします。
10-2	プロジェクト体制及び役割に関する留意事項	(3)情報セキュリティ確保の体制整備		(3)情報セキュリティ確保の体制整備
10-2	プロジェクト体制及び役割に関する留意事項	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。	○	事業者組織全体のセキュリティを確保するとともに、貴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いたします。
10-2	プロジェクト体制及び役割に関する留意事項	(4)プロジェクト停滞に伴う体制変更指示		(4)プロジェクト停滞に伴う体制変更指示
10-2	プロジェクト体制及び役割に関する留意事項	プロジェクト計画書等で示した業務作業が適正に履行されていない、または、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、本市は、受託者に対して体制の変更を申し入れすることができるものとし、受託者はその申し入れに従い、適切に対応すること。	○	プロジェクト計画書等で示した業務作業が適正に履行されていない、または、本仕様書において定義する各要件を満たしていないと貴市が判断し、貴市から体制の変更を申し入れがあった場合は、その申し入れに従い、適切に対応いたします。
10-3	プロジェクト計画書	受託者は、契約締結から10日以内にプロジェクト計画書を提出すること。また、プロジェクト計画書には、以下の内容を含めること。 ・プロジェクトの方針、目的 ・スケジュール ・体制図（体制と役割分担） ・対象範囲（スコープ） ・成果物 ・制約条件 ・品質管理目標 ・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） ・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こと	○	契約締結から10日以内にプロジェクト計画書を提出いたします。プロジェクト計画書には、以下の内容を含めます。 ・プロジェクトの方針、目的 ・スケジュール ・体制図（体制と役割分担） ・対象範囲（スコープ） ・成果物 ・制約条件 ・品質管理目標 ・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） ・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こと
10-4	WAN回線更新を含む移行統括（PMO）要件	本庁舎と外部施設間で通信するためのWAN回線も同じく令和8年度に更新する予定である。安全かつ確実な移行を実施するため、受託者は、WAN回線更新を含む全体移行の統括主体として、既存事業者、新規回線事業者、本市及び関係者との間で必要な調整を行うこと。	○	WAN回線更新を含む全体移行の統括主体として、既存事業者、新規回線事業者、貴市及び関係者との間で必要な調整を行います。
10-4	WAN回線更新を含む移行統括（PMO）要件	少なくとも以下を実施すること。 ・本事業とWAN回線更新を含む全体移行計画の策定 ・関係者間の責任分解整理 ・会議体（移行調整会議）の運営 ・進捗管理 ・課題管理及びリスク管理 ・切替計画、切り替え判定基準およびロールバック計画の策定 ・当日体制および連絡体制の整備 ・移行結果報告書の作成 ・その他PMOとして必要な作業	○	少なくとも以下を実施いたします。 ・本事業とWAN回線更新を含む全体移行計画の策定 ・関係者間の責任分解整理 ・会議体（移行調整会議）の運営 ・進捗管理 ・課題管理及びリスク管理 ・切替計画、切り替え判定基準およびロールバック計画の策定 ・当日体制および連絡体制の整備 ・移行結果報告書の作成 ・その他PMOとして必要な作業
10-5	プロジェクト作業場所	設計、設定等の準備は原則、受託者所内で実施すること。各作業の実施、各作業に関する打ち合わせ、報告、進捗会議については、原則として、本市の会議室またはオンラインで実施すること。	○	設計、設定等の準備は原則、弊社所内で実施いたします。各作業の実施、各作業に関する打ち合わせ、報告、進捗会議については、原則として、貴市の会議室またはオンラインで実施いたします。
10-6	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。	○	本事業に使用する設備及び消耗品等については弊社が負担いたします。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貴市にご負担いただきます。
10-7	プロジェクトの会議体	本事業の実施にあたっては、以下の会議体を開催し、議事内容について責任のある回答ができる要員を参加させること。会議の開催にあたっては、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すること。	○	本事業の実施にあたっては、以下の会議体を開催し、議事内容について責任のある回答ができる要員を参加させます。会議の開催にあたっては、弊社で必要な討議資料を用意いたします。また、各会議体について、必要に応じて、弊社で議事録を作成いたします。
10-7	プロジェクトの会議体	(1)進捗確認会議		(1)進捗確認会議
10-7	プロジェクトの会議体	本業務の進捗状況確認、スケジュール管理、課題検討及び解決、品質管理等を実施するための会議を原則月1回の頻度で開催する。	○	本業務の進捗状況確認、スケジュール管理、課題検討及び解決、品質管理等を実施するための会議を原則月1回の頻度で開催いたします。
10-7	プロジェクトの会議体	(2)移行調整会議		(2)移行調整会議
10-7	プロジェクトの会議体	既存庁舎内ネットワーク保守事業者、既存庁舎外ネットワーク事業者、次期庁舎外ネットワーク事業者など本市ネットワークに關与する契約事業者など関係者を招集し、移行に関する進捗状況確認、スケジュール管理、課題検討及び解決を実施するための調整会議を必要に応じて開催する。	○	既存庁舎内ネットワーク保守事業者、既存庁舎外ネットワーク事業者、次期庁舎外ネットワーク事業者など貴市ネットワークに關与する契約事業者など関係者を招集し、移行に関する進捗状況確認、スケジュール管理、課題検討及び解決を実施するための調整会議を必要に応じて開催いたします。
10-7	プロジェクトの会議体	(3)工程完了判定会議		(3)工程完了判定会議
10-7	プロジェクトの会議体	各工程の完了時にレビューを行い、次の工程に進むための判定を行う会議を実施する。	○	各工程の完了時にレビューを行い、次の工程に進むための判定を行う会議を実施いたします。
10-7	プロジェクトの会議体	(4)本番稼働判定会議		(4)本番稼働判定会議
10-7	プロジェクトの会議体	運用テスト（顧客受入テスト）を実施後に、本番稼働を実施してよいかの判定を行う会議を実施する。なお、本番稼働判定会議の際は、本番移行切替計画書を提示したうえで本番稼働の判定を行うものとする。	○	運用テスト（顧客受入テスト）を実施後に、本番稼働を実施してよいかの判定を行う会議を実施いたします。なお、本番稼働判定会議の際は、本番移行切替計画書を提示したうえで本番稼働の判定を行います。
10-7	プロジェクトの会議体	(5)緊急対応会議		(5)緊急対応会議
10-7	プロジェクトの会議体	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。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。	○	緊急時（障害発生時等）の対応を検討するため、貴市の求めに応じて会議を開催いたします。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）が参加いたします。
10-7	プロジェクトの会議体	(6)責任者会議		(6)責任者会議
10-7	プロジェクトの会議体	緊急時、問題発生時、課題解消の進捗が芳しくない時等に、本市の求めに応じて、プロジェクトマネージャ（PM）が参加し、課題の解決を早急に図るための会議を実施すること。	○	緊急時、問題発生時、課題解消の進捗が芳しくない時等に、貴市の求めに応じて、プロジェクトマネージャ（PM）が参加し、課題の解決を早急に図るための会議を実施いたします。
10-8	レビュー・承認	手戻り/リスクを抑制するため、受託者は以下の承認ゲートを設定し、発注者の確認・承認を経て次工程へ進むこと。 ・基本設計レビュー ・詳細設計レビュー ・本番切替判定 ・検収前レビュー	○	手戻り/リスクを抑制するため、以下の承認ゲートを設定し、貴市の確認・承認を経て次工程へ進みます。 ・基本設計レビュー ・詳細設計レビュー ・本番切替判定 ・検収前レビュー
10-9	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するため、課題管理を実施すること。	○	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するため、課題管理を実施いたします。
10-9	課題管理	課題管理に当たり、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、解決日を課題一覧にまとめ、一元管理すること。また、その他必要と考えられる項目についても管理すること。	○	課題管理に当たり、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、解決日を課題一覧にまとめ、一元管理いたします。また、その他必要と考えられる項目についても管理いたします。
10-9	課題管理	課題管理表の内容については、月次での状況確認及び整理を実施し、進捗確認会議で報告すること。また、課題の完了にあたっては、必ず受託者及び本市での合意を必須とすること。	○	課題管理表の内容については、月次での状況確認及び整理を実施し、進捗確認会議で報告いたします。また、課題の完了にあたっては、必ず弊社及び貴市での合意を必須といたします。
10-10	文書管理	必要に応じて、会議・打ち合わせにおける議事録等の作成、保管、管理を行うこと。	○	必要に応じて、会議・打ち合わせにおける議事録等の作成、保管、管理を行います。
10-10	文書管理	受託者は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。	○	受託者はプロジェクト内で作成する文書を一元管理し、貴市の求めに応じて提示できるようにいたします。
11	特記事項	(1)WAN回線の更新について		(1)WAN回線の更新について
11	特記事項	WAN回線の更新に当たっては、現行回線事業者が引き続き提供する場合、原則として既設回線設備を活用し、新たな引込工事を要しない前提で移行計画を策定すること。	○	WAN回線の更新に当たっては、現行回線事業者が引き続き提供する場合、原則として既設回線設備を活用し、新たな引込工事を要しない前提で移行計画を策定いたします。
11	特記事項	新規回線事業者が参入する場合は、現行回線の運用を継続したま別系統で新規回線を敷設することとし、少なくとも令和8年12月初旬までに敷設を完了の上、疎通確認及び切替作業に着手可能な状態とすること。	○	新規回線事業者が参入する場合は、現行回線の運用を継続したま別系統で新規回線を敷設することとし、少なくとも令和8年12月初旬までに敷設を完了の上、疎通確認及び切替作業に着手可能な状態とするよう調整を図ります。
11	特記事項	受託者は、上記双方のケースを想定し、回線事業者、既存事業者、本市関係部署その他関係者との調整を含む移行計画を策定すること。移行計画には、事前確認事項、工程、試験項目、切替手順、切替条件、障害時対応、ロールバック手順及び役割分担を明記すること。	○	上記双方のケースを想定し、回線事業者、既存事業者、貴市関係部署その他関係者との調整を含む移行計画を策定いたします。移行計画には、事前確認事項、工程、試験項目、切替手順、切替条件、障害時対応、ロールバック手順及び役割分担を明記いたします。
11	特記事項	(2)庁外施設の増減への対応について		(2)庁外施設の増減への対応について
11	特記事項	庁外施設については、今後の施設の統廃合、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ことを前提として設計及び構築を行うこと。	○	庁外施設については、今後の施設の統廃合、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ことを前提として設計及び構築を行います。
11	特記事項	受託者は、保守期間中に当該変動が生じた場合に、WAN用ルータの再配置、流用、予備機活用その他必要な対応を円滑に実施できるよう、機器選定、設置条件、設定方針、監視方式、台帳整備及び成果物作成において十分配慮すること。	○	保守期間中に当該変動が生じた場合に、WAN用ルータの再配置、流用、予備機活用その他必要な対応を円滑に実施できるよう、機器選定、設置条件、設定方針、監視方式、台帳整備及び成果物作成において十分配慮いたします。
11	特記事項	拠点廃止等により不要となったWAN用ルータについては、将来的に他拠点へ転用又は予備機として活用できるよう、設定初期化手順、再設定手順、移設時の確認事項及び管理方法を整理し、成果物に反映すること。	○	拠点廃止等により不要となったWAN用ルータについては、将来的に他拠点へ転用又は予備機として活用できるよう、設定初期化手順、再設定手順、移設時の確認事項及び管理方法を整理し、成果物に反映いたします。
11	特記事項	また、拠点新設又は機器故障時の迅速な対応を可能とするため、予備機の確保を前提とした機器構成及び管理方法を提案すること。	○	拠点新設又は機器故障時の迅速な対応を可能とするため、予備機の確保を前提とした機器構成及び管理方法を提案いたします。
11	特記事項	(3)複合機無線化への対応について		(3)複合機無線化への対応について
11	特記事項	令和7年3月に一部複合機をLGWAN系無線ネットワークへ追加したが、現状は接続先無線APIに対応するVLANに合わせた固定IPアドレス設定による暫定運用を行っている。しかしながら、無線APの切替等の影響が疑われる通信不安定事象が発生しており、再起動により復旧する場合があるものの、安定運用に課題がある。	—	
11	特記事項	受託者は、当該複合機の無線接続について、複合機の保守事業者と十分に調整の上、現行構成、VLAN収容方式、IPアドレス付与方式、無線APとの接続状況、ローミング時の影響その他必要事項を調査し、原因分析を行った上で、安定稼働に向けた見直し及び必要な設計・構築を実施すること。	○	当該複合機の無線接続について、複合機の保守事業者と十分に調整の上、現行構成、VLAN収容方式、IPアドレス付与方式、無線APとの接続状況、ローミング時の影響その他必要事項を調査し、原因分析を行った上で、安定稼働に向けた見直し及び必要な設計・構築を実施いたします。

項番	項目	仕様内容	対応可否	対応内容
11	特記事項	(4)停電対応		(4)停電対応
11	特記事項	本庁舎、保健センター及び水道局においては、電気設備点検等に伴う計画停電が今後実施される予定である。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月に停電作業が予定されており、保健センター及び水道局においても例年停電を伴う点検が実施されている。またそれ以外の庁外施設においても適宜点検等による計画停電が実施される。		－
11	特記事項	受託者は、これら計画停電を踏まえ、本事業で導入する機器が停電時及び復電時に安全かつ確実に停止及び復旧できるよう、必要な電源設計、起動停止手順、復旧確認手順及び障害時対応手順を整備すること。	○	これら計画停電を踏まえ、本事業で導入する機器が停電時及び復電時に安全かつ確実に停止及び復旧できるよう、必要な電源設計、起動停止手順、復旧確認手順及び障害時対応手順を整備いたします。
11	特記事項	また、保守期間中の計画停電対応を円滑に実施できるよう、構築時に停電対応手順、事前準備事項、当日対応事項、復電後確認項目、関係事業者との調整事項及び役割分担を整理し、成果物に反映すること。	○	保守期間中の計画停電対応を円滑に実施できるよう、構築時に停電対応手順、事前準備事項、当日対応事項、復電後確認項目、関係事業者との調整事項及び役割分担を整理し、成果物に反映いたします。
11	特記事項	(5)その他		(5)その他
11	特記事項	保守期間中に大阪版自治体情報セキュリティクラウドの更新（令和9年4月稼働開始予定）が予定されていることから、本事業の構築期間中においても、当該更新に関連して、本市庁舎内ネットワークの接続方式、設定内容、切替条件その他必要事項に関する照会、情報提供依頼、技術的協議又は調整が発生する可能性がある。受託者は、当該更新を見据え、構築期間中に必要となる情報提供、設定内容の確認、関係事業者との調整及び必要な設計上の配慮を本事業の範囲内で実施すること。	○	大阪版自治体情報セキュリティクラウドの更新を見据え、構築期間中に必要となる情報提供、設定内容の確認、関係事業者との調整及び必要な設計上の配慮を本事業の範囲内で実施いたします。
11	特記事項	LBOの導入など将来的に拡張できる柔軟な構成となるよう設計すること。また、追加提案として将来的な拡張要素を必要に応じて提案すること。	○	LBOの導入など将来的に拡張できる柔軟な構成となるよう設計します。
12	その他仕様	本仕様書に定めのない事項は、本市と協議の上決定する。	○	本仕様書に定めのない事項は、貴市と協議の上決定いたします。
13	成果物	最低限、以下の内容を含む成果物を提出すること。データ形式は、Microsoft Officeで編集可能な形式とする。 調査報告書 基本設計書 詳細設計書 構成図（物理、論理、V L A N、I P アドレス、配線、W A N、監視） パラメータシート（機器設定） 試験計画書及び試験結果報告書 移行計画書及び移行結果報告書 運用設計書（監視/障害/変更/資産/アカウント/ログ） 障害対応手順書 設定バックアップ取得手順書 管理者向け簡易操作マニュアル、教育資料、引継ぎ記録 機器一覧、ライセンス一覧、配線台帳、I P アドレス台帳	○	以下の内容を含む成果物を提出いたします。データ形式は、Microsoft Officeで編集可能な形式とします。 調査報告書 基本設計書 詳細設計書 構成図（物理、論理、V L A N、I P アドレス、配線、W A N、監視） パラメータシート（機器設定） 試験計画書及び試験結果報告書 移行計画書及び移行結果報告書 運用設計書（監視/障害/変更/資産/アカウント/ログ） 障害対応手順書 設定バックアップ取得手順書 管理者向け簡易操作マニュアル、教育資料、引継ぎ記録 機器一覧、ライセンス一覧、配線台帳、I P アドレス台帳

別紙5.提案明細書（守口市）

製品名	型番	製品名	スペック等	数量	単位	備考
▼ファイアウォール（内部）						
FortiGate 400F	FG-400F	Fortinet	ポート仕様：16ポート GE RJ45,8ポート GE SFP,8ポート 10GE SFP+ スループット（転送速度）：105Mbps TCPセッション数（新規/最大）：500,000/7,800,000 冗長構成：Active-Active/Active-Passive ルーティング機能：PBR/static/dynamic、ルーティングプロトコル：RIP/OSPF/BGP NAT/NAPT、ICMP/SNMP/Syslog監視、時刻同期（NTP）：対応 VPN方式、接続可能数（拠点間/ポート接続）：IPsec VPN（2,000/50,000）	2	台	
FortiGate 400F	FC-10-0400F-247-02-60	Fortinet	FortiGate-400F 5Y、FortiCare Premium Support	2	式	
FortiGate 400F	FC-10-0400F-247-02-01	Fortinet	FortiGate-400F 1M、FortiCare Premium Support	12	式	
▼ファイアウォール（外部）						
FortiGate 200G	FG-200G	Fortinet	ポート仕様：16ポート GE RJ45,4ポート GE SFP,8ポート 10GE SFP+ スループット（転送速度）：39.7Mbps TCPセッション数（新規/最大）：400,000/1,100,000 冗長構成：Active-Active/Active-Passive ルーティング機能：PBR/static/dynamic、ルーティングプロトコル：RIP/OSPF/BGP NAT/NAPT、ICMP/SNMP/Syslog監視、時刻同期（NTP）：対応 VPN方式、接続可能数（拠点間/ポート接続）：IPsec VPN（2,000/16,000）	1	台	
FortiGate 200G	FC-10-FG2HG-950-02-60	Fortinet	Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL/DNS & Video Filtering, Antispam Service, and FortiCare Premium)	1	式	
FortiGate 200G	FC-10-FG2HG-950-02-01	Fortinet	FortiGate-200G 1M、Unified Threat Protection (UTP)	6	台	
▼コアスイッチ						
FortiSwitch 1024E	FS-1024E	Fortinet	ポート仕様：24ポート 1G/10G SFP+、4ポート 40G/100G QSFP+ スループット（転送速度）：1309Mbps 冗長構成：Active-Active ルーティング機能：static ICMP/SNMP/Syslog監視、時刻同期（NTP）：対応 電力：デュアル冗長	2	台	
FortiSwitch 1024E	FC-10-S1E24-247-02-60	Fortinet	FortiCare Premium Support(60カ月)	2	式	
FortiSwitch 1024E	FC-10-S1E24-247-02-01	Fortinet	FortiCare Premium Support(12カ月単位)	12	式	
▼サーバ室内スイッチ（1G）						
FortiSwitch 424E	FS-424E	Fortinet	ポート仕様：24ポート 1GE RJ45,4ポート 10GE SFP+ スループット（転送速度）：190Mbps 冗長構成：Active-Active ルーティング機能：static ICMP/SNMP/Syslog監視、時刻同期（NTP）：対応	8	台	
FortiSwitch 424E	FC-10-S424E-247-02-60	Fortinet	FortiSwitch-424E 5Y、24x7 FortiCare Contract	8	式	
FortiSwitch 424E	FC-10-S424E-247-02-01	Fortinet	FortiSwitch-424E 1M、24x7 FortiCare Contract	48	式	
▼サーバ室内スイッチ（10G）						
FortiSwitch T1024E	FS-T1024E	Fortinet	ポート仕様：24ポート 1G/10GE RJ45,4ポート 40G/100G QSFP+ スループット（転送速度）：1309Mbps 冗長構成：Active-Active ルーティング機能：static ICMP/SNMP/Syslog監視、時刻同期（NTP）：対応	2	台	
FortiSwitch T1024E	FC-10-T1E24-247-02-60	Fortinet	FortiCare Premium Support(60カ月)	2	式	
FortiSwitch T1024E	FC-10-T1E24-247-02-01	Fortinet	FortiCare Premium Support(12カ月単位)	12	式	
▼データセンター用スイッチ						
FortiSwitch 1048G	FS-1048G	Fortinet	ポート仕様：48ポート GE/10GE SFP/SFP+、8ポート 100GE QSFP28 スループット（転送速度）：2000Mbps VLAN機能：IEEE 802.1Q VLAN対応 ポート制御機能：対応（ループ検知時遮断） ループ検知：STP-RSTP-MSTP ACL/QoS機能、ICMP/SNMP/Syslog監視、時刻同期（NTP）：対応	2	台	
FortiSwitch 1048G	FC-10-FSG48-247-02-60	Fortinet	FortiCare Premium Support(60カ月)	2	式	
FortiSwitch 1048G	FC-10-FSG48-247-02-01	Fortinet	FortiCare Premium Support(12カ月単位)	12	式	
▼ポアスイッチ（24port）						
FortiSwitch 124F-FPOE	FS-124F-FPOE	Fortinet	ポート仕様：24ポート GE RJ45,4ポート 10GE SFP+ スループット（転送速度）：190Mbps VLAN機能：IEEE 802.1Q VLAN対応 ポート制御機能：対応（ループ検知時遮断） ループ検知：STP-RSTP-MSTP ACL/QoS機能、ICMP/SNMP/Syslog監視、時刻同期（NTP）：対応 PoE給電機能：24ポート PoE+ PoE+（IEEE 802.3at対応）：対応(最大30W/ポート) PoE給電容量：370W	19	台	予備機1台含む 数量を23→19へ変更
FortiSwitch 124F-FPOE	FC-10-S124F-247-02-60	Fortinet	FortiSwitch-124F-FPOE 5Y、24x7 FortiCare Contract	19	式	予備機1台含む 数量を23→19へ変更
FortiSwitch 124F-FPOE	FC-10-S124F-247-02-01	Fortinet	FortiSwitch-124F-FPOE 1M、24x7 FortiCare Contract	114	式	予備機1台含む 数量を138→114へ変更
▼ポアスイッチ（48port）						
FortiSwitch 148F-FPOE	FS-148F-POE	Fortinet	ポート仕様：48ポート GE RJ45,4ポート 10GE SFP+ スループット（転送速度）：190Mbps VLAN機能：IEEE 802.1Q VLAN対応 ポート制御機能：対応（ループ検知時遮断） ループ検知：STP-RSTP-MSTP ACL/QoS機能、ICMP/SNMP/Syslog監視、時刻同期（NTP）：対応 PoE給電機能：24ポート PoE+ PoE+（IEEE 802.3at対応）：対応(最大30W/ポート) PoE給電容量：370W	19	台	予備機1台含む 数量を15→19へ変更
FortiSwitch 148F-FPOE	FC-10-148FP-247-02	Fortinet	FortiSwitch-148F-POE 5Y、24x7 FortiCare Contract	19	式	予備機1台含む 数量を15→19へ変更
FortiSwitch 148F-FPOE	FC-10-148FP-247-02-01	Fortinet	FortiSwitch-148F-POE 1M、24x7 FortiCare Contract	114	式	予備機1台含む 数量を90→114へ変更
▼エッジスイッチ（標準用）						
WEBスマート L2スイッチ	DGS-1210-20/F2	D-Link	ポート仕様：20ポート GE RJ45,4ポート SFPコンポ スループット（転送速度）：148.8Mbps VLAN機能：IEEE 802.1Q VLAN対応 ポート制御機能：対応（ループ検知時遮断） ループ検知：STP-RSTP-MSTP ACL/QoS機能、ICMP/SNMP/Syslog監視、時刻同期（NTP）：対応	165	台	予備機4台含む 数量を164→165へ変更
WEBスマート L2スイッチ	DMG-SH1	D-Link	メタル筐体スイッチ用マグネットシート	165	枚	予備機4台含む 数量を164→165へ変更
▼エッジスイッチ（IP電話機用）						
ギガビットL2スマートスイッチ	DGS-1210-10MP/F3	D-Link	ポート仕様：8ポートRJ45,2ポート 1G SFP2Dytr スループット（転送速度）：148.8Mbps VLAN機能：IEEE 802.1Q VLAN対応 ポート制御機能：対応（ループ検知時遮断） ループ検知：STP-RSTP-MSTP ACL/QoS機能、ICMP/SNMP/Syslog監視、時刻同期（NTP）：対応 PoE給電機能：8ポート PoE+ PoE+（IEEE 802.3at対応）：対応(最大30W/ポート) PoE給電容量：130W	124	台	予備機4台含む 数量を134→124へ変更
ギガビットL2スマートスイッチ	DMG-SH1	D-Link	メタル筐体スイッチ用マグネットシート	124	枚	予備機4台含む 数量を134→124へ変更
▼エッジスイッチ（拠点間用）						
WEBスマート L2スイッチ	DGS-1210-20/F2	D-Link	ポート仕様：20ポート GE RJ45,4ポート SFPコンポ スループット（転送速度）：29.8Mbps VLAN機能：IEEE 802.1Q VLAN対応 ポート制御機能：対応（ループ検知時遮断） ループ検知：STP-RSTP-MSTP ACL/QoS機能、ICMP/SNMP/Syslog監視、時刻同期（NTP）：対応	5	台	
WEBスマート L2スイッチ	DMG-SH1	D-Link	メタル筐体スイッチ用マグネットシート	5	枚	

▼無線アクセスポイント						
FortiAP 231K	FAP-231K-J	Fortinet	入力電源: PoE受電 IEEE 802.3at対応 ポート仕様: 1ポートGE (PoE有) 以下の機能に対応: 電源出力設定: Wi-Fi 6(IEEE 802.11ax), 2.4GHz帯/5GHz帯同時利用, 6GHz帯対応, 複数SSID提供, チャネル/出力 設定, 無線端末間通信禁止機能, スタビリティSSID使用, WPA2(3)-Enterprise, 集中管理機能, PoE+以上受電対応 SSIDごとの認証方式, 暗号化方式, VLANごとの設定: WPA2/WPA3 Enterprise対応, VLAN分離設定対応 設定変更, 障害検出, 接続状況情報取得: 対応(SNMP, CL1/GUI) FortiAP 231K 5Y FortiCare Premium Support FortiAP 231K 1M FortiCare Premium Support	76	台	予備機1台含む
FortiAP 231K	FC-10-P231K-247-02-60	Fortinet		76	式	予備機1台含む
FortiAP 231K	FC-10-P231K-247-02-01	Fortinet		456	式	予備機1台含む
▼統合運用監視基盤 (運用管理サーバ)						
PowerEdge R360	PowerEdge R360	Dell Technologies	Trusted Platform Module : Trusted Platform Module 2.0 V6 シャーシ構成: 2.5インチ シャーシ 最大 8 ホットプラグ ハードドライブ 搭載可能, アダプター PERC 11 プロセッサ: インテル® Xeon® 6 プロセッサ 6315P 2.8G, 4C/4T, 12M キャッシュ, ターボ, (55W) DDR5-4800 プロセッサ-メモリ構成: エリートシナ メモリ-構成タイプ: パフォーマンス 最適化 メモリ- DIMM タイプ/スピード: 5600MT/s UDIMM メモリ-容量: 32GB UDIMM, 5600MT/s ECC RAID 構成: C3, 2 HDDs または SSDs RAID1 1 (適合 タイプ/スピード/容量) RAID コントローラ: PERC H755 アダプター カード ハードドライブ: 1.2TB ハードドライブ ISE SAS 12Gbps 10k 512n 2.5インチ ホットプラグ ファン: スタンダード ファン 電源コネクタ: デュアル, (1+1) 冗長, ホットプラグ 電源 コネクタ, 600W MM (100-240Vac) 電源ケーブル: 電源コネクタ - C13, 2M, 125V, 15A (日本) マザーボード: PowerEdge R360 マザーボード Broadcom 5720 デュアルポート 1Gb オンボードポート LOM 付, MLX 追加ネットワークカード: Broadcom 57416 デュアルポート 10GbE BASE-T アダプター, PCIe100- プロファイル オペレーティングシステム: Windows Server 2025 スタート, 1637 FL, x64/なし, CALなし, 多言語 ラグレール: ReadyRails スライドレール ケーブル マネジスト プラシダック (A12) PCIeライザー: ライザー 構成 2, Butterfly Gen4 ライザー (x8/x8) 製品保証: ベンシック 営業曜日 12 ヶ月, 12 ヶ月 保守サービス (延長・アップグレード): ProSupport Plus 24時間 コーシナ クリイナル, 66 ヶ月 Dell サービス/オンサイト診断サービス: Dell サービス/オンサイト診断サービス	1	台	
▼統合運用監視基盤 (ログ収集サーバ)						
Fortianalyzer 810G	FAZ-810G	Fortinet	ログ処理: 200GB/日 分析処理レート: 4,000ログ/秒 コンプライアンスレート: 6,000ログ/秒 管理デバイス数/VDOM数 (最大): 800 最新分析日数: 50 インターフェース: 4xGbE RJ45, 2SFP ストレージ容量: 16TB (4x4TB) 3.5インチSAS HDD RAIDストレージ管理: 対応 (0,1,5,5,5e,10) RAIDタイプ: ハードウェア (ソフトウェア対応) FortiAnalyzer-810G FortiCare Premium Support FortiAnalyzer-810G FortiCare Premium Support	1	式	
Fortianalyzer 810G	FC-10-AZ81G-247-02-60	Fortinet		1	式	
Fortianalyzer 810G	FC-10-AZ81G-247-02-01	Fortinet		6	式	
Fortianalyzer 810G	FC-10-AZ81G-661-02-60	Fortinet		1	式	
Fortianalyzer 810G	FC-10-AZ81G-661-02-01	Fortinet		6	式	
▼NAS						
WS5220DN16W5	WS5220DN16W5	Buffalo	容量: 16TB (8TB×2) ベイ: 2ベイ (RAID1/0対応) CPU: Intel Atom C3338 メモリ: 8GB ネットワーク: 10GbE ×1, 1GbE ×2 デラステーション用 オンサイト保守HDD渡部不零 データ復旧1回無償パック保守5年	2	台	物品追加
WS5220DN16W5	OP-TSON-SY/DNRD	Buffalo		2	式	物品追加
▼監視用管理端末						
Dell Pro 15 Essential	NBLA155-012N1	Dell Technologies	Dell Pro 15 Essential(Core i5-1334U/16GB/512GB/光学ドライブなし/Win11Pro/Officeなし/15.6型/FHD/非タッチ/1年保守)	3	式	
Dell Pro 15 Essential	PEL-W1P5PN-1	Dell Technologies	(90日以内客数増)Dell Pro Essential Lapto 1 台psシリーズ 保守アップグレード 1年プロサポートから5年プロサポート オンサイト 翌営業日対応	3	式	
Windows 11 Enterprise LTSC ライセンス	DG7GMGF0P460002	マイクロソフト (CSP)	Windows 11 Enterprise LTSC 2024 Upgrade	3	式	物品追加
▼WAN回線用ルータ (70G)						
FortiGate 70G	FG-70G	Fortinet	ポート仕様: 1ポート GE WAN, 5ポート GE LAN スループット (転送速度): 15Mpps TCPセッション数 (新規/最大): 100,000/1,400,000 冗長構成: Active-Active/Active-Passive ルーティング機能: PBR/static/dynamic, ルーティングプロトコル: RIP/OSPF/BGP NAT/NAPT, ICMP/SNMP/Syslog監視, 時刻同期 (NTP): 対応 VPN方式, 接続可能数 (拠点間/ポート接続): IPsec VPN (200/500)	8	台	
FortiGate 70G	FC-10-GT70G-247-02-60	Fortinet	FortiGate-70G SY FortiCare Premium Support	8	式	
FortiGate 70G	FC-10-GT70G-247-02-01	Fortinet	FortiGate-70G 1M FortiCare Premium Support	48	式	
▼WAN回線用ルータ (50G)						
FortiGate 50G	FG-50G	Fortinet	ポート仕様: 1ポート GE WAN, 3ポート GE RJ45 スループット (転送速度): 50Gbps TCPセッション数 (新規/最大): 85,000/720,000 冗長構成: Active-Active/Active-Passive ルーティング機能: PBR/static/dynamic, ルーティングプロトコル: RIP/OSPF/BGP NAT/NAPT, ICMP/SNMP/Syslog監視, 時刻同期 (NTP): 対応 VPN方式, 接続可能数 (拠点間/ポート接続): IPsec VPN (200/250)	21	台	
FortiGate 50G	FC-10-GT50G-247-02-60	Fortinet	FortiGate-50G SY FortiCare Premium Support	21	式	
FortiGate 50G	FC-10-GT50G-247-02-01	Fortinet	FortiGate-50G 1M FortiCare Premium Support	126	式	
▼1ポート保守用ルータ						
FortiGate 50G	FG-50G	Fortinet	ポート仕様: 1ポート GE WAN, 3ポート GE RJ45 スループット (転送速度): 50Gbps TCPセッション数 (新規/最大): 85,000/720,000 冗長構成: Active-Active/Active-Passive ルーティング機能: PBR/static/dynamic, ルーティングプロトコル: RIP/OSPF/BGP NAT/NAPT, ICMP/SNMP/Syslog監視, 時刻同期 (NTP): 対応 VPN方式, 接続可能数 (拠点間/ポート接続): IPsec VPN (200/250)	3	台	
FortiGate 50G	FC-10-GT50G-247-02-60	Fortinet	FortiGate-50G SY FortiCare Premium Support	3	式	
FortiGate 50G	FC-10-GT50G-247-02-01	Fortinet	FortiGate-50G 1M FortiCare Premium Support	18	式	
▼SFPEジャーナル						
FN-TRAN-SFP+SRモジュール	FN-TRAN-SFP+SR	Fortinet	10GE SFP+ transceiver module, short range 10GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots	238	個	予備2式含む
▼UPS (サーバ/EP5用)						
BN150RA	BN150RAG6	オムロン・シリアル・ソリューションズ	無停電電源装置 BN150RA本体・無償保証6年分 運転方式: ラインインタラクティブ方式 冷却方式: 強制空冷 (ファンあり) 定格入力電圧: AC100V/120V 入力周波数: 50/60Hz±4Hz 最大電流 (定格入力電圧時/最小入力電圧時): 13.6A/15A 入力保護容量: 45A 定格出力電圧: AC100V/120V 定格出力電流: 100V mode: 12.4A/120V mode: 12.5A 出力容量: 100Vmode: 1240VA/1240W/120Vmode: 1500VA/1440W バックアップ時間 (最大負荷時): 100V mode: 5.5分 (1240W) /120V mode: 4.5分 (1440W)	24	台	予備機1台含む
BN150RA	SC22G6	オムロン・シリアル・ソリューションズ	1GB対応ネットワークカード SC22+無償保証6年分	24	台	予備機1台含む
▼UPS (拠点用)						
BN50T	BN50TG6	オムロン・シリアル・ソリューションズ	無停電電源装置 BN50T本体・無償保証6年分 無停電電源装置 BN150RA本体・無償保証6年分 運転方式: ラインインタラクティブ方式 冷却方式: 自然空冷 (ファンなし) 定格入力電圧: AC100V 入力周波数: 50/60Hz±4Hz 最大電流 (定格入力電圧時/最小入力電圧時): 6A/7.5A 入力保護容量: 10A 定格出力電圧: AC100V 定格出力電流: 5A 出力容量: 500VA/450W バックアップ時間 (最大負荷時): 8.5分 (450W)	28	台	予備機1台含む
BN50T	SC22G6	オムロン・シリアル・ソリューションズ	1GB対応ネットワークカード SC22+無償保証6年分	28	台	予備機1台含む
▼ラック						
ラック	FSS100-720EKN	日華工業	PSシリーズ サーバ収納タイプ 19型/W700	1	台	物品追加
ラック	-TKSL	日華工業	19型標準用 天吊タイプ 樹脂製ラック 3個付	1	台	物品追加
ラック	-TC	日華工業	天吊ケーブル引き込みタイプ 天吊樹脂製仕様	1	台	物品追加
ラック	RD72-6H	日華工業	キャスター/スリッパ無 (2個入)	1	個	物品追加
ラック	RD72-6HS	日華工業	キャスター/スリッパ付 (2個入)	1	個	物品追加
ラック	RD73-9	日華工業	レベルフット (2個入)	2	個	物品追加
ラック	RD732-16	日華工業	レベルフット・取付金具	1	個	物品追加
▼その他						
ギガビットPoE(パシ)クター	GPI-130	Fortinet	1-Port Gigabit PoE Power Injector, 802.3at up to 30W for GPI-130 Gigabit PoE Injector	7	台	物品追加 (保証センター用)

別紙6.提案明細書（水道局）

製品名		型番	製品名	スペック等	数量	単位	備考
▼WAN回線用ルータ（70G）（水道局向け）							
FortiGate 70G		FG-70G	Fortinet	ポート仕様：1ポート GE WAN, 5ポート GE LAN スループット（転送速度）：15Mpps TCPセッション数（新規/最大）：100,000/1,400,000 冗長構成：Active-Active/Active-Passive ルーティング機能：PBR/static/dynamic、ルーティングプロトコル：RIP/OSPF/BGP NAT/NAPT、ICMP/SNMP/Syslog監視、時刻同期（NTP）：対応 VPN方式、接続可能数（拠点間/リモート接続）：IPsec VPN（200/500）	1	台	
FortiGate 70G		FC-10-GT70G-247-02-60	Fortinet	FortiGate-70G 5Y FortiCare Premium Support	1	式	
FortiGate 70G		FC-10-GT70G-247-02-01	Fortinet	FortiGate-70G 1M FortiCare Premium Support	6	式	
▼WAN回線用ルータ（50G）（水道局向け）							
FortiGate 50G		FG-50G	Fortinet	ポート仕様：1ポート GE WAN, 3ポート GE RJ45 スループット（転送速度）：5Gbps TCPセッション数（新規/最大）：85,000/720,000 冗長構成：Active-Active/Active-Passive ルーティング機能：PBR/static/dynamic、ルーティングプロトコル：RIP/OSPF/BGP NAT/NAPT、ICMP/SNMP/Syslog監視、時刻同期（NTP）：対応 VPN方式、接続可能数（拠点間/リモート接続）：IPsec VPN（200/250）	1	台	
FortiGate 50G		FC-10-GT50G-247-02-60	Fortinet	FortiGate-50G 5Y FortiCare Premium Support	1	式	
FortiGate 50G		FC-10-GT50G-247-02-01	Fortinet	FortiGate-50G 1M FortiCare Premium Support	6	式	
▼フロアスイッチ（水道局向け）							
WEBスマート L2スイッチ		DGS-1210-20/F2	D-Link	ポート仕様：20ポート GE RJ45, 4ポート SFPコンボ スループット（転送速度）：29.8Mpps VLAN機能：IEEE 802.1Q VLAN対応 ポート制御機能：対応（ループ検知時遮断） ループ検知：STP-RSTP-MSTP ACL/QoS機能、ICMP/SNMP/Syslog監視、時刻同期（NTP）：対応	4	台	
WEBスマート L2スイッチ		DMG-SH1	D-Link	メタル筐体スイッチ用マグネットシート	4	枚	
▼無線アクセスポイント（水道局向け）							
FortiAP 231K		FAP-231K-J	Fortinet	入力電源：PoE受電 IEEE 802.3at対応 ポート仕様：1ポート GE（PoE有） 以下の機能に対応： 電波出力設定、Wi-Fi 6(IEEE 802.11ax)、2.4GHz帯/5GHz帯同時利用、6GHz帯対応、複数SSID提供、チャネル/出力設定、無線端末間通信禁止機能、ステルスSSID使用、WPA2(3)-Enterprise、集中管理機能、PoE+以上受電対応 SSIDごとの認証方式、暗号化方式、VLAN分離設定：WPA2/WPA3 Enterprise対応、VLAN分離設定対応 設定変更、障害確認、機動状況情報取得：対応(SNMP, CLI/GUI)	9	台	
FortiAP 231K		FC-10-P231K-247-02-60	Fortinet	FortiAP 231K 5Y FortiCare Premium Support	9	式	
FortiAP 231K		FC-10-P231K-247-02-01	Fortinet	FortiAP 231K 1M FortiCare Premium Support	54	式	
▼UPS（脱点用）（水道局向け）							
BN50T		BN50TG6	オムロンソーシアルソリューション	無停電電源装置 BN50T本体+無償保証6年分 無停電電源装置 BN150RA本体+無償保証6年分 運転方式：ラインインタラクティブ方式 冷却方式：自然空冷（ファンレス） 定格入力電圧：AC100V 入力周波数：50/60Hz±4Hz 最大電流（定格入力電圧時/最小入力電圧時）：6A/7.5A 入力保護容量：10A 定格出力電圧：AC100V 定格出力電流：5A 出力容量：500VA/450W バックアップ時間（最大負荷時）：8.5分（450W）	2	台	
BN50T		SC22G6	オムロンソーシアルソリューション	1G対応ネットワークカード SC22+無償保証6年分	2	台	
▼その他（水道局向け）							
AC Power Adapter		SP-FAP200-PA-US	Fortinet	AC電源アダプター	8	台	予備機1台含む 数量を7→8に変更
ギガビットPoEインジェクター		GPI-130	Fortinet	1-Port Gigabit PoE Power Injector, 802.3at up to 30W for GPI-130 Gigabit PoE Injector	3	台	予備機1台含む 数量を2→3へ変更