

嬉野市新庁舎ネットワーク構築業務機器・作業等  
特記仕様書

令和 7 年 12 月

嬉野市

## 1. ネットワーク要件

### 1.1. 概要

移転後庁舎におけるネットワークは三層分離におけるαモデルを基本とし、LGWAN 系、インターネット系は無線接続、番号利用系は有線接続を基本とする。それらの実現に必要な設計、調達、構築、移行作業、テスト、取付等を行うこと。

### 1.2. 現状の構成

- (1) 作業及び費用に関しては、作業内容を明確にしたうえで本市を通じて、既存ベンダーと調整を行うこと。

更新対象予定機器		
1	コアスイッチ	2 台
2	佐賀 IDC 設置センターL3 スイッチ	1 台
3	公共 NW 用ルータ	2 台
4	LGWAN 向けファイアウォール	1 台
5	フロアスイッチ	4 台
6	塩田庁舎フロアスイッチ（1F～3F）	3 台
7	塩田庁舎 1F（EPS）スイッチ	1 台
8	無停電電源装置	5 台
9	ネットワーク管理装置	1 台
継続利用予定		
1	図書館用フロアスイッチ	1 台
2	文化センター用フロアスイッチ	1 台
3	分散業務用分岐スイッチ	2 台
4	それらの先に接続されるネットワーク機器	一式

- (2) 端末

LGWAN 系		
1	物理端末	約 450 台
番号利用系		
1	物理端末	約 100 台
インターネット系		
1	物理端末	約 50 台
2	仮想ブラウザ	同時接続 75

- (3) ネットワーク全体の構成、現状のサーバ室内機器については「別紙\_ネットワーク構成図」に記載する。これらの書類は実施要領の方法に基づき資料請求を行ったものに提

供とする。

### 1.3. 基本要件

- (1) 業務の利便性、セキュリティ、安定性を可能な限り実現することを目的として、終日連続運転が可能な信頼性の高いシステム構成であること。
- (2) 令和7年11月時点で国内の同規模程度の地方自治体において個人番号利用事務系およびLGWAN系のコアスイッチとして稼働しているメーカーの製品で提案すること。なお、他自治体等で原因不明の障害やレスポンス低下等の事例が散見されていることから、問題が解決していないメーカー製品で提案した場合、失格もしくは技術や性能面の評価をしないこともあるため、メーカーや他市町の事例を確認して安定稼働するメーカーの製品で提案すること。
- (3) 本市全体として既存のネットワークに影響を与えないよう最適な設計を行い、現行ネットワークと比較してレスポンス低下等のないように機器の選定・設計を行うこと。
- (4) すべてのネットワーク機器が属する VLAN およびそれらのネットワーク機器の IP アドレスを設定し、管理 LAN として利用できる設計であること。
- (5) すべてのシステムは管理者のみがアクセスできる管理用のネットワークを VLAN 等で構築しアクセス制御を行うこと。
- (6) ネットワークの基本要件については、原則、既存のネットワークを継承することとするが、先進的な技術やセキュリティ向上に繋がる最新機能がある場合は、提案に含めること。
- (7) システムによっては固定 IP が必要なものも存在するため、現状のシステム利用環境を調査し、新環境に移行後もシステム利用に影響がでない構築を行うこと。
- (8) 既存の嬉野庁舎および塩田庁舎は並行稼働期間が存在するため、現行のネットワーク機器が当該期間中に収容できるよう設計を行うこと。

### 1.4. 既存環境の調査

- (1) 現行のネットワークについて既存ドキュメントの精査・実地調査を行い、移転計画立案、ネットワーク設計を行うこと。
- (2) 直接の更新対象ではない周辺ネットワークである小中学校、出先拠点ネットワーク等においても全体の構成を調査し、既存の運用に影響がでない設計をすること。
- (3) 以下のシステムおよびネットワークについて、新庁舎からこれまで同様に利用が可能となるように整備すること。これ以外にも現状調査の結果、引き続き接続が必要な既存ネットワークが見つかった場合はそれらについても同様に整備すること。

LGWAN 系	
	LGWAN ネットワーク
	グループウェアシステム

	財務会計システム
	文書管理システム
	後期高齢者医療ネットワーク
	国保連合会ネットワーク
	水道料金・企業会計システム
	その他 LGWAN-ASP
番号利用系	
	住民基本台帳ネットワークシステム
	杵藤広域ネットワーク（基幹系システム）
	中間サーバネットワーク
インターネット系	
	図書館システム
	CMS
	WEB 会議用ネットワーク
	議員用 PC
	その他インターネットクラウドサービス
その他	
	小中学校ネットワーク
	出先機関ネットワーク
	電話環境
	複合機等
	防災システム
	議場配信システム
	デジタルサイネージ
	佐賀県公共ネットワーク

- (4) 各システムの物理および論理ネットワーク経路について整理の上、移転後庁舎での経路を資料化すること。
- (5) 各セグメント配下の端末の設定変更は原則発生しないように設計すること。必要となる場合は受注者が各システムの保守ベンダーと調整を主体的に行うこと。
- (6) 移行対象ではないサーバ、スイッチ、UPS についても調査を行い、必要な LAN 配線、電源容量、ラック構成などの設計、移転計画に含めること。
- (7) 各課で独自に敷設した回線およびシステムについて調査を行い、ネットワーク集約やラック構成などの設計、移転計画に含めること。
- (8) 各システムの物理および論理ネットワーク経路について整理の上、移転後庁舎での経路を資料化すること。

### 1.5. 物理ネットワーク

- (1) LGWAN 系、インターネット系は無線接続を基本とするが、一部共用端末等は有線接続で対応できる構成とすること
- (2) 番号利用系ネットワークは既存と同様に有線ネットワークとするが、将来の無線化も可能な構成とすること。
- (3) 複合機等のプリンタ、その他 LAN 接続を行う OA 機器は有線接続とする。
- (4) コアスイッチはフロアスイッチ、サーバスイッチを集約するだけでなく、LGWAN 接続用の機器や出先拠点とのイントラネット接続機器、新庁舎で継続利用する既設サーバやスイッチ、その他の機器なども収容する構成とすること。
- (5) フロアスイッチは、同一フロア内のアクセスポイント (AP)、島ハブ、情報コンセントを集約しつつ、フロアスイッチ障害が発生した場合に AP の耐障害性を高めるため、4.2. (5) に示す通り、フロアスイッチへの分散接続 (1 台のスイッチ故障で停止する AP が局所的になるよう) および、電波カバーエリアの冗長設計 (1 台の AP が故障しても、隣接する AP の電波で最低限の通信が維持できる設計) を行うこと。なお、フロアスイッチはスペースの関係上スタックによる冗長化ではなく予備機を利用したコールドスタンバイ構成で設置すること。
- (6) 島ハブ、AP について、機器自体の冗長化 (1 か所に 2 台設置等) は不要とするが必要な予備機等を準備し、緊急時に簡易的な作業と交換だけで対応できるようにすること。
- (7) サーバ室から EPS へ光ケーブルを敷設する場合は 10Gbps 対応させたスイッチに対してボトルネックとならない速度の光ケーブルとし、冗長構成にも対応できるように複数本の予備線を準備すること。ただし、公衆回線等のキャリア回線の引き込み回線については対象外とする。
- (8) 重要な基幹系データを優先的に通信できる機能を実装すること。
- (9) フロアスイッチの単一機器障害時において無線アクセスが停止しないように、複数スイッチに収容分散できる配線構成とする。また、スイッチは予備機構成とし、スイッチ故障時はケーブル差し替えだけで復旧できるように同一設定を投入すること。
- (10) 執務室側でループ接続が発生しても、ネットワーク全体に影響が出ない構成とすること。
- (11) 執務室側情報コンセント増設用にポート分のスイッチングハブを設計に含めること。
- (12) 旧嬉野庁舎と新庁舎の並行期間におけるネットワーク接続に必要な回線事業者との協議及び調整を行うこと。

### 1.6. 論理ネットワーク

- (1) 仮想ネットワーク間が安全に通信できるようにファイアウォールにて制御すること。
- (2) 原則としてスタティックルーティングを使用すること。

- (3) 執務室におけるフレキシブルな端末利用を実現するために、ネットワーク認証により接続する端末等の通信を行うセグメントを自動で判別する仕組み（ダイナミック VLAN）を導入すること。
- (4) 各ネットワーク間は物理的または論理的に遮断すること。ネットワーク間で特別に通信を許可しているものは現状の設定を調査し、特定通信として整理の上、本市との協議の上、必要と判断したものは同様に許可すること。また、LGWAN 系ネットワーク及び番号利用系ネットワークについては、コアスイッチ上で VRF 等により論理的に分離し、相互の通信は原則禁止とすること。やむを得ず相互通信が必要な場合は、本市と協議の上、特定通信としてファイアウォールにより制御すること。
- (5) 原則として新設する VLAN 以外は、既存 VLAN 構成を踏襲すること。ただし不要な VLAN や効率的な管理が可能な場合は統廃合を提案すること。
- (6) 既存の通信ルールを調査し整理した上で、必要なものは新環境でも同等の設定を行うこと。
- (7) LGWAN 系への DHCP サービス導入にあたり、DHCP サーバや既存通信機器の具体的な構成（冗長化構成、払い出しリリース期間）を提案すること。
- (8) 新ネットワーク全体の IP アドレス体系を再設計し、将来の拡張性を考慮した『IP アドレス管理計画書』を提案すること。また、IP アドレスの使用状況等の管理方法なども提案すること。

#### 1.7. 無線 LAN 設計

- (1) 新庁舎・塩田庁舎のすべての執務室、会議室、会議スペース議会および業務上端末を利用する可能性のある部屋をカバーする無線環境を構築するために必要な無線アクセスポイントを設置すること。
- (2) 想定される用途は LGWAN 系、インターネット系、議員用となり、それぞれでネットワークおよび SSID を分離し最適なネットワーク、認証方法・暗号化方式を設定すること。
- (3) LGWAN 系の SSID は職員の業務用端末が接続する SSID である。端末認証には重要資産を取り扱うことから端末証明書で認証すること。
- (4) インターネット系 SSID はセキュリティクラウドを介さないインターネット接続用の SSID であり、主に窓口で利用するタブレットや WEB 会議利用の端末など本市ドメインに参加しない職員用端末が利用する想定である。
- (5) 無線 LAN は Wi-Fi6 以上に対応したの機器で構築を行うこと。詳細は「3.3 機能要件」を参照すること。
- (6) 5GHz 帯利用時は物理的な干渉や気象レーダーなどの干渉時にも通信に影響が出ない設計をすること。
- (7) 多数の端末が接続することでトラフィックが増大することがないように最適な設置およびチャネル等の無線 LAN 機器設定を行うこと。

- (8) 無線 LAN 機器は集中管理方式を取ること。
- (9) 無線 AP は冗長化や通信範囲で補完しあう等、故障時に最小限の影響になるように設計すること。
- (10) 住民向け Wi-Fi は別途「Ureshino City Wi-Fi」として別公衆回線を引き込んで提供しているため、それらの機器の取付も想定した設置、ネットワーク設計およびチャネル設計を行うこと。
- (11) 本稼働後に無線の速度低下、接続トラブルが発生する場合は調査を行い、改善するために必要な機器のチューニング等を行うこと。
- (12) 将来的に出先拠点でも同様に無線化を行う可能性があるため、必要なネットワークの延伸が可能な構成とするとともに端末台数が増えても収容および集中管理が可能な設計とすること。
- (13) 職員用公用スマートフォンを接続して、スマートフォンの OS アップデート等を行う可能性があるため、スマートフォンの接続も想定した設計とすること。なお、スマートフォンの最大想定数は職員数とする。
- (14) 定期的に無線アクセスポイント機器のファームウェアアップデートを行うこと。ただしファームウェアの不具合で業務が一斉に停止しないよう配慮したうえで更新対応を行うこと。
- (15) 住民向け Wi-Fi は大規模災害発生時に認証なしで接続できる公衆接続用の SSID に切り替えることができること。対象となる範囲は本市と協議の上決定する。
- (16) 無線 LAN 環境下で Web 会議システム（Microsoft Teams, Zoom 等を想定）を安定的に利用できるよう、帯域制御および QoS（IEEE 802.11e/WMM 等）設計を行うこと。特に、音声・映像パケットが他の通信（大容量ファイル転送等）の影響で途切れることがないよう、マーキング（DSCP 値）等に基づいた優先制御を行う構成を提案すること。
- (17) 特殊天井における電波設計への配慮について、調達仕様書「3.3. 設備設計（5）」に示す特殊天井（特にルーバー天井）への無線 AP 設置にあたっては、天井の材質（特に金属製の場合）が電波に与える減衰（アッテネーション）や反射を考慮すること。

## 2. サーバ室要件

### 2.1. 無停電電源装置

- (1) 今回導入する機器について必要となる無停電電源装置を導入すること。

### 2.2. 配線、電源

- (1) 電源設計は提案機器以外の既存機器も含むすべての機器を計算して提案すること。必要な電源容量については建築設計側へ要望を出すこと。
- (2) 導入機器および既存の移転機器の接続に必要な LAN ケーブルおよび電源は本業務で設

置すること。

- (3) サーバ室内に設置する無停電電源装置に対する給電は、分電盤側の系統は無停電電源装置 1 台それぞれが独立した系統となるよう設計すること。
- (4) 今回導入した機器類は、新規で導入する無停電装置と OA タップ等を利用して接続をすること。また、今後の拡張性を見越して OA タップ等の口数の設計を行うこと。
- (5) 配線は導入後もメンテナンスが容易になるよう建築側の設計に合わせて提案を行うこと。

### 2.3. 既存機器の収容について

- (1) 本件で導入する以外の既存のサーバ、ネットワーク機器等についても収容できるよう事前調査の上、ラック搭載設計を行うこと。
- (2) 配線の取り回しや電源容量を考えた上で各ラック内に配置する機器を既存機器含めて設計すること。その際、今後の機器更新タイミングを考慮して、同一時期に更新するものはなるべく同一ラックへ収容する搭載設計とすること。
- (3) 本業務ではサーバーラックの調達の対象外とし、サーバーラックは本市が別途調達するものとする。受注者は別途調達されるラックの仕様（寸法・搭載重量・電源形状等）を踏まえ、機器搭載設計・配線計画・電源容量設計を行うこと。

## 3. 機器要件

機器要件については現状の構成を元に想定されるスペックを記載している。これらの要件を満たすことが原則ではあるが新庁舎での新しいネットワーク環境構築にあたって同等以上の性能を発揮でき、よりコストパフォーマンスに優れ効率的な構成を提案できる場合はその旨を明記して提案すること。

### 3.1. コアスイッチ

庁内ネットワーク全体の中心となるスイッチであり、高い性能、信頼性、拡張性を有すること。

#### 3.1.1. 性能要件

- (1) 十分なスイッチング容量（バックプレーン容量）およびパケット転送能力（pps）を有し、将来的なトラフィック増大にも対応可能なこと。コアスイッチのスイッチング容量およびパケット転送能力は、全職員業務を遂行する中で将来的なトラフィック増（例：5 年後に現状の 1.5 倍）にも耐えうる設計とし、その性能の算出根拠を明示すること。

#### 3.1.2. 信頼性・冗長性

- (1) スタック（仮想シャーシ技術）をし、機器障害時にも通信断が無い冗長構成とする



こと。

#### 3.1.3. 機能要件

- (1) 高度な L3 ルーティング機能（スタティック、ダイナミック）を有すること。また、複数のネットワークセグメントを論理的に分離・ルーティングするための VRF (Virtual Routing and Forwarding)等の機能をサポートすること。
- (2) VLAN (Virtual LAN) 機能、QoS (Quality of Service) 機能、ACL (Access Control List) による詳細なパケットフィルタリング機能を有すること。

#### 3.1.4. 管理要件

- (1) SNMP、Syslog、CLI (Command Line Interface)、Web GUI による管理・監視が可能であること。なお、高度な機能（VRF、BGP 等）の利用に追加ライセンスが必要な場合は、その体系を明示すること。

### 3.2. フロアスイッチ

各フロアの EPS（機器設置スペース）に設置し、職員が使用する PC、プリンタ、および無線 AP 等の末端機器を集約するスイッチであること。

#### 3.2.1. 性能要件

- (1) エンドユーザー向けポートとして、1Gbps（1000BASE-T）ポートを必要数備えること。
- (2) 10Gbps ポートを最低 2 ポート以上備え、10Gbps でコアスイッチと接続すること。

#### 3.2.2. 給電機能

- (1) 無線アクセスポイント等への給電のため、PoE（IEEE 802.3at: PoE+）に対応し、スイッチ全体で十分な給電容量を持つこと。また、将来的な高出力機器（Wi-Fi 6E AP 等）を見据え、IEEE 802.3bt（PoE++）への対応も考慮することが望ましい。

#### 3.2.3. 信頼性・冗長性

- (1) コアスイッチとのアップリンクポートは、リンクアグリゲーション（LACP）等により冗長化・帯域増強等が可能な構成とすること。なお、障害ポイントを増加させないようにするため、フロアスイッチ同士の接続は認めない。
- (2) EPS 室等に設置するフロアスイッチは場所や配線の都合上冗長化しないが、予備機対応構成とするため同一設定を維持した予備機を必要数同一場所に保管すること。

#### 3.2.4. セキュリティ機能

- (1) VLAN 機能、QoS 機能を有すること。
- (2) 後述するネットワーク認証装置と連携し、IEEE 802.1X 認証（ポートベース認証）に対応可能であること。
- (3) ループ検知・防止機能、ポートセキュリティ（MAC アドレスフィルタリング等）を有すること。

#### 3.2.5. 管理要件

- (1) コアスイッチ同様、SNMP、Syslog、CLI、Web GUI による管理・監視が可能な機器であること。

### 3.3. 無線アクセスポイント

庁舎内の執務室、会議室、共用スペース等において、Wi-Fi 環境を提供するため、安定した高速通信が可能なエンタープライズ向け機器であること。

#### 3.3.1. 規格要件

- (1) 最新の Wi-Fi 規格である Wi-Fi 6(IEEE 802.11ax)に準拠していること。6GHz 帯を利用する Wi-Fi 6E への対応も、将来性或電波干渉の観点から積極的に評価する。Wi-Fi 6E 対応機器を提案する場合は、Wi-Fi 64 機器を提案する場合との差額（機器費用、PoE スイッチ費用、ライセンス費用）を明示すること。また、6GHz 帯を利用するメリット（想定される利用シーン、電波干渉の回避効果）と、現時点での対応端末の普及状況を踏まえた費用対効果について説明すること。
- (2) WPA3 (WPA3-Enterprise, WPA3-Personal) による強固な暗号化に対応していること。

#### 3.3.2. 機能要件

- (1) 複数の SSID を運用可能であり、VLAN と連携して職員用のネットワークを論理的に分離できること。
- (2) ゲストネットワークにおいては、端末間通信を禁止する「クライアントアイソレーション（AP アイソレーション等）」機能を有すること。
- (3) PoE(PoE+以上) による受電に対応し、フロアスイッチとは PoE による電源供給とするが、個別の電源供給にも対応できること。
- (4) 電波強度やチャネルを自動調整して通信を円滑に行う機能を有すること。
- (5) 不正なアクセスポイントを検知・通知し、可能な限りその影響を低減（遮断）する機能（WIDS/WIPS）を有すること。

#### 3.3.5. 管理要件

- (1) 複数のアクセスポイントを一元管理するための「無線 LAN コントローラ」（物理ア

プライアンス、仮想アプライアンス、クラウド型等、構成は問わない) によって集中管理できること。なお、三層分離を意識したセキュリティ対策を十分に考慮した管理方法で提案すること。

### **3.4. ネットワーク認証装置**

庁内ネットワーク（有線・無線）に接続する端末の正当性を検証し、不正な端末の接続を防止・排除するための認証基盤であること。

#### **3.4.1. 認証機能**

- (1) IEEE 802.1X 認証（証明書認証：EAP-TLS、ID/パスワード認証：PEAP 等）に対応していること。
- (2) MAC アドレス認証（プリンタや複合機など 802.1X 非対応機器向け）に対応していること。

#### **3.4.2. 連携機能**

- (1) 認証情報基盤として、Active Directory 等と連携可能であること。
- (2) 認証結果（成功/失敗）に基づき、スイッチや無線 AP と連携して動的に VLAN を割り当てる機能を有すること。

#### **3.4.3. 信頼性・管理要件**

- (1) 認証サービスを停止させないため、アプライアンスの冗長構成（Active/Standby または Active/Active）が可能であること。
- (2) 認証ログ（成功・失敗履歴）、アクセスログ等を収集・管理できること。
- (3) 導入する機能（検疫機能等）に応じたライセンス体系、および将来的な端末数増加に伴うライセンス追加の考え方を明示すること。

### **3.5. 無停電電源装置**

落雷や商用電源の瞬断・停電発生時に、コアスイッチ、ネットワーク認証装置、無線 LAN コントローラなど、ネットワークの中核を担う重要な機器に対して電力を供給し、システムのダウンを防ぐ装置であること。

#### **3.5.1. 方式・容量**

- (1) サーバーおよびネットワーク機器の保護に適した「常時インバータ給電方式（オンライン方式）」または「ラインインタラクティブ方式」であること。
- (2) 接続する全機器の総消費電力をカバーし、かつ安全マージン（例：30%以上）を見込んだ十分な出力容量を有すること。

#### 3.5.2. バッテリー要件

- (1) 商用電源断から、システムを安全にシャットダウンするまで、または非常用発電機が起動するまでの間の電力を供給可能なバッテリー容量を有すること。
- (2) バッテリーは運用中の交換（ホットスワップ対応が望ましい）が可能であり、期待寿命や交換推奨時期を管理機能にて確認できること。

#### 3.5.3. 管理機能

- (1) バッテリーや負荷状況等の状態確認が可能であること。
- (2) 電源障害発生時に、シャットダウン信号をサーバー等へ送信するソフトウェア（またはネットワークカード）と連携可能であること。
- (3) 設置場所に適した形状（ラックマウント型またはタワー型）であること。

### 3.6. 島ハブ

執務室内のデスク配置（島）において、情報コンセントの不足を補い、複数の端末（PC、IP 電話等）をフロアスイッチに効率的に接続するための小型スイッチであること。

#### 3.6.1. 性能要件

- (1) 全ポートが 1Gbps（1000BASE-T）に対応していること。（最低 5 ポート以上）
- (2) アップリンクポート（フロアスイッチ接続用）を 1 ポート以上有すること。

#### 3.6.2. 機能要件

- (1) 単なるリピータハブではなく、インテリジェントスイッチであること。
- (2) フロアスイッチと連携し、VLAN（タグ VLAN）を透過または処理できること。
- (3) 意図しないループ接続を防止するための「ループ検知・防止機能」を有すること。

#### 3.6.3. 給電・設置

- (1) AC アダプタによる電源供給、またはフロアスイッチからの PoE 受電で動作するモデル（PoE パススルー機能も可）を、設置環境に応じて適切に選定すること。PoE パススルー機能を利用する場合は、当該機器自身の消費電力、および接続機器へ給電可能な電力容量（PoE バジェット）の仕様を明示すること。
- (2) デスク下や什器への設置を考慮し、静音性（ファンレス）に優れ、コンパクトな筐体であること。

#### 3.6.4. 管理要件

- (1) 障害切り分けやセキュリティ維持のため、最低限の管理機能（Web GUI 等による VLAN 設定、ポート状態監視）を持つ「インテリジェントタイプ」または「スマートスイッチ」であることが望ましい。

### 3.7. 公共 NW ルータ

公共ネットワーク（佐賀県公共ネットワーク）および庁舎内ネットワークとの安全かつ安定した相互接続を実現するため、高い信頼性とセキュリティ、処理性能を有するルータであること。なお、本機器で集約できる FW については可能な限り集約すること。参考機器は FortiGate 100F とし、同等以上の性能・機能を備えること。

※ なお、公共ネットワークと庁舎内ネットワーク間のセキュリティ境界は、本機器が提供する FW 機能により統合的に管理することを基本とする。

### 3.8. 佐賀 IDC 設置センターL3 スイッチ

- (1) 佐賀 IDC 内に設置し、庁舎側ネットワークと IDC 内ハウジング機器との L3 接続を提供する装置であること。
- (2) VRF 等により論理分離された複数系統の経路制御に対応できること。
- (3) ルーティング（スタティック/ダイナミック）の方式は本市と協議のうえ決定すること。
- (4) 監視・運用のため、SNMP、Syslog、CLI、Web GUI 等による管理が可能であること。高度機能（VRF、BGP 等）の利用に追加ライセンスが必要な場合は、その体系を明示すること。
- (5) 旧 IDC 側 L3 スイッチからの設定移行、切替手順、切戻し手順を作業計画書に明記し、本市の承認を得て実施すること。
- (6) IDC 内作業に必要な入館手続、作業時間、立会い条件等を本市および佐賀 IDC と協議のうえ確定し、当該条件を遵守して作業を実施すること。

## 4. 非機能要件

### 4.1. 全般

- (7) 端末が 600 台以上収容可能なネットワークとすること。
- (8) ネットワークシステムを構成する有線機器は、すべてワイヤースピード以上の速度とすること。
- (9) 無線 LAN のアクセスポイントは、原則として「3.3.1. (1)」の要件（Wi-Fi 6 準拠）を満たすこと。Wi-Fi 6E 対応機器については、同項の定めに基づき、追加提案として評価する。
- (10) ポート数は端末の増設を想定し、各フロアスイッチにおいて、本稼働開始時点での使用ポート数（無線 AP、有線端末含む）に対し、概ね 20%の空きポート（PoE 給電ポート

を含む)を確保する設計とすること。

#### 4.2. 耐障害性

- (1) コアスイッチを冗長構成とし、障害発生時に影響を及ぼさないこと。
- (2) ネットワーク内においてループを検視した場合はスイッチのポートが自動で閉塞する等ネットワーク停止が拡大しない対策をとること。
- (3) 無線接続およびダイナミック VLAN に必要な認証装置は冗長化を行い、機器の不具合で市役所業務特に窓口業務が停止することがないように構築を行うこと。
- (4) 無線ネットワークが障害により停止した際に備えて、業務内容、想定人数を踏まえて、AP (アクセスポイント) の配置密度を高め、1 台の AP 障害時も周辺 AP でカバーできる冗長性等を確保すること。
- (5) 一つのスイッチに障害が発生した際に、複数の箇所に影響を及ぼす設計をしないこと。また、特定の部署の機能がすべて停止することがないように、可能な限り隣接する無線 AP、有線 LAN は複数のスイッチから分散して配線を行うこと。また電波設計において無線のカバーエリアに可能な限り冗長性を持たせること。
- (6) 各機器のコンフィグ、設定はバックアップ取得を行うこと。

#### 4.3. セキュリティ

- (1) 嬉野市情報セキュリティポリシーおよび総務省セキュリティ強靱化ガイドラインを遵守すること。
- (2) 各ネットワーク (特に番号利用系ネットワーク) においては、情報漏洩等を防ぐ観点から、セキュリティの高いネットワークを構築すること。
- (3) 各機器および管理用コンソールはパスワードにおけるアクセス制御を行うこと。またパスワードはそれぞれ異なるものとする。
- (4) 利用しないサービスは停止させること。
- (5) 不正端末接続を防止するために、認証機能を実装すること。また、よりセキュリティ性を向上させるため、LGWAN 系端末は端末証明書で認証すること。
- (6) 許可されていない端末の接続は島ハブ、無線アクセスポイントおよびフロアスイッチにて遮断すること。

### 5. 配線等要件

#### 5.1. 配線について

- (1) LAN ケーブルは、カテゴリ 6A 以上の規格のものとする。
- (2) 光ケーブルが必要な区間は将来的なスイッチの 10Gbps 以上の対応を見込み、提案において必要な本数敷設すること。

- (3) 配線箇所は有線端末を設置する場所および会議室や共用スペースを主として各執務室の予備回線や複合機等のネットワーク接続する機器に対して配線が不足することがないよう設計すること。
- (4) 有線 LAN 配線は端末数、部署数などから計算した必要数を用意し、情報コンセントもしくは島ハブを設置すること。

### 5.3. EPS

- (1) 設置するネットワーク機器の停電対応として、非常用発電機が起動し、安定給電を開始するまでの時間（約 2 分間）をカバーできる容量を持つ無停電源装置を準備すること。

## 6. ネットワーク監視要件

### 6.1. 全般

- (1) 導入する機器は必要に応じて監視システムからの監視(SMNP 監視、SMNP trap 監視等)を受け入れられる設定にすること。

## 7. 既存ネットワーク・サーバの移転・接続要件

### 7.1. 全般

- (1) 本業務の対象外となるサーバ、ネットワーク機器、回線等がかつ継続して移転後庁舎においても必要となるものについて、移設作業は各保守業者が行うものとするが、移転に必要なスケジュール計画、設置場所、配線、電源等の設計は本業務にて行うこと。また必要となる LAN ケーブル、導入機器に必要な OA タップ等は本業務で用意すること。
- (2) 既存機器の移設に必要なラック内の LAN ケーブル、電源ケーブルの必要な取り回しを支援し、サーバ室や EPS 室の電源容量設計も行うこと。
- (3) 各サーバのアプリケーションは各保守ベンダーもしくは本市職員が行うものとするが、ネットワークの疎通確認は既存業者と協力して行うこと。
- (4) 各課に独自に設置されている通信機器、回線をサーバ室もしくは EPS へ集約して設置できるよう配線・構築を行うこと。また必要な配線ルートを設計し、建築の詳細設計に反映できるよう提案すること。

### 7.2. 各課の個別回線について

各課で個別に調達している回線については、可能な限り移転時に回線を集約できるものは集約できるようにネットワークの設計時に最適なアドバイスを行うこと。