

高畠町新庁舎ネットワーク設計構築業務
仕様書

令和5年5月
高畠町

目次

1. 背景・目的	4
2. 業務概要	4
2.1. 業務名	4
2.2. 履行場所	4
2.3. 契約期間	4
2.4. 事業範囲	4
2.5. 納品成果物	5
2.6. その他	7
3. 全体スケジュール	7
4. 現行ネットワーク概要	8
5. 新庁舎ネットワーク構築の基本要件	8
5.1. 構築方針	8
5.2. 構築事業の概要	9
5.3. 調達機器仕様	10
5.3.1. 基本事項	12
5.3.2. 新庁舎コアスイッチ仕様	12
5.3.3. 新庁舎サーバスイッチ仕様	13
5.3.4. 新庁舎フロアスイッチ仕様	14
5.3.5. 新庁舎エッジスイッチ仕様	14
5.3.6. メディアコンバータ	15
5.3.7. 本庁舎設置 VPN ルータ（出先機関接続用）	15
5.3.8. 出先機関設置 VPN ルータ（本庁舎接続用）	16
5.3.9. ファイアウォール（LGWAN 接続用、セキュリティクラウド接続用、分離用）	17
5.3.10. 無線 LAN コントローラ仕様	18
5.3.11. 無線 LAN アクセスポイント仕様（LGWAN 接続系、インターネット接続系兼用）	18

5.3.12.	公衆無線 LAN アクセスポイント仕様.....	18
5.3.13.	無線 LAN アクセスポイント給電用スイッチ.....	19
5.3.14.	認証サーバ (RADIUS サーバ) 兼無線 LAN 電子証明書発行サーバ仕様	20
5.3.15.	DHCP サーバ兼 AD サーバ仕様	21
5.3.16.	ネットワーク監視サーバ仕様.....	21
5.3.17.	UPS (無停電電源装置)	21
6.	業務内容に関する要件.....	22
6.1.	全体管理業務要件	22
6.2.	現行ネットワーク調査業務要件	22
6.3.	設計業務要件	22
6.4.	構築・移行業務要件	23
6.5.	運用・保守業務要件	26

1. 背景・目的

本業務は、令和7年5月開庁予定の新庁舎におけるネットワーク環境を新たに構築するものである。新庁舎ネットワークでは、総務省が示す「自治体情報システム強靱化向上モデル」に基づいたセキュリティを確保することや、新庁舎移転後のスマートな執務環境の実現に向けペーパーレス化による行政事務の電子化をはじめとする事務の効率化、自治体情報システムの標準化・共通化等、近年の高度化・複雑化するネットワーク要件への対応が必要となる。また、本町では各部署が管理する独立した個別システムが多数存在しているため、システム管理者の負担は増加する傾向にあり、運用の集約化及び簡素化についても喫緊の課題である。

このことから、新庁舎ネットワークについては、強固なセキュリティを確保するとともに、シンプルで将来実施されるシステムの追加や変更等に柔軟に対応できることや、維持管理の省力化が可能なネットワークとすることで、行政事務の効率化や住民サービスの向上を図るとともに、災害時においても継続して稼働できるネットワークを構築することを目的として本事業を行うものである。

2. 業務概要

2.1. 業務名

高島町新庁舎ネットワーク設計構築業務

2.2. 履行場所

高島町内（高島町役場（現庁舎、新庁舎）及び出先機関）

※現在の出先機関の一覧を別紙に示す。

2.3. 契約期間

設計・構築分：契約締結の翌日から令和7年5月31日まで

運用・保守分：令和7年6月1日から令和12年5月31日まで

※運用・保守の契約は、令和7年6月1日付けで別途締結する。

2.4. 事業範囲

本事業に係る業務内容については、全体管理業務、現行ネットワーク調査業務、設計業務、構築・移行業務、運用・保守業務の5種類に分類する。

(1) 全体管理業務

作業実施計画書の作成、進捗管理、品質管理、課題管理等を実施し、プロジェクトの包括的な管理を行うこと。具体的な要求仕様については、「6.1. 全体管理業務要件」に記載する。

(2) 現行ネットワーク調査業務

現庁舎のシステム・ネットワーク環境（マイナンバー利用事務系、LGWAN 接続系、インターネット接続系、個別システム）の調査・関係者へのヒアリング等を実施し現行ネットワークの構成、システム通信要件等を明らかにすること。具体的な要求仕様については、「6.2. 現行ネットワーク調査業務要件」に記載する。

(3) 設計業務

現行ネットワーク調査結果を基に、現行システム稼動における通信要件を全て履行できる設計とし、新庁舎ネットワークにて稼動するサーバ群及びクライアントの要件を確認した上で、適正なネットワーク機器を調達し、設計を行うこと。

また、LAN 配線工事等は本業務の対象外となるが、構築に必要となる配線は指示書を作成し、必要に応じて配線工事業者と調整を行うこと。具体的な要求仕様については、「6.3. 設計業務要件」に記載する。

(4) 構築・移行業務

新庁舎本体工事の進捗に合わせ、遅延なくネットワークを構築すること。ケーブル接続・機器動作確認、回線疎通確認、移行後のシステム稼動確認、監視確認等の作業について詳細な計画を立てること。具体的な要求仕様については、「6.4. 構築・移行業務要件」に記載する。

(5) 運用・保守業務

新庁舎ネットワークを基盤とした各情報システムの安定稼動のために確実な運用と保守体制を確保すること。迅速な保守対応が必須となるため、セキュリティ確保を前提としてリモート保守による提案を認めることとする。具体的な要求仕様については、「6.5. 運用・保守業務要件」に記載する。

2.5. 納品成果物

下記表に示す成果物の提出時期については、発注者と協議の上決定すること。

表 2-5 納品成果物

No	成果物	内容
全体管理業務		
1	作業実施計画書	全体スケジュール（本業務対象外となる回線敷設等を含む）、体制表、レビュー計画、マイルストーン等を記載すること。
2	課題管理表	発注者及び受注者で発生した課題に関して、対応期限、対応者、リスク、検討結果等を記載すること。
3	打合せ議事録	各打合せの議事録を作成すること。
現行ネットワーク調査業務		

1	現行ネットワーク構成図	現行ネットワークの調査をした上で、個別システムのネットワークを含めた、新庁舎構築・移行に影響する現行の網羅的なネットワーク構成図を作成すること。
2	現行 IP アドレス表	新庁舎構築・移行で現行 IP アドレスから変更した場合の影響がわかるように、個別システムを含めた現行の IP アドレス表を作成すること。
3	現行ネットワークルーティング設計書	新庁舎構築・移行におけるルーティング設計を行う上で、現行のルーティング設計（ポリシーベースルーティング等を含む）を記載すること。
設計業務		
1	ハードウェア等調達仕様書	新庁舎ネットワーク構築に必要なハードウェア等の調達仕様・条件等を記載すること。
2	配線敷設指示書	新庁舎の配線工事業者向けに、ケーブルの調達・敷設に関する設計仕様・条件等を作成すること。
3	機器一覧	新庁舎において、導入する機器種別やハードウェア・ソフトウェアのサポート期限等を一覧化し記載すること。
4	機器設置図	新庁舎、出先機関を含めた機器設置箇所、ラック内設置箇所を記載すること。
5	基本設計書	ネットワーク基盤の位置付けや新規システムを収容する場合にどの基盤に収容するか等のポリシー・ルールを記載すること。
6	詳細設計書	基本設計書に基づき、ネットワーク機器のパラメータ設定根拠や ACL (Access Control List) 等の通信制御ポリシー等を記載すること。
7	新庁舎ネットワーク構成図	個別システムのネットワークを含めた、新庁舎のネットワーク構成図を記載すること。
8	新庁舎 IP アドレス表	新庁舎でのサーバ・端末セグメントや IP アドレス採番ルール等を記載すること。
9	新庁舎ネットワークルーティング設計書	セキュリティゾーン（マイナンバー利用事務系、LGWAN 接続系、インターネット接続系、外部ネットワーク、DMZ 等）が異なる場合のルーティング設計や新規通信要件発生時における機器設定変更箇所等を記載すること。
10	監視設計書	監視対象機器、監視項目、ポーリング間隔等を記載すること。
構築・移行業務		
1	テスト実施計画書・成	テストにおけるネットワーク確認項目、テスト環境の妥当性、テストと本番ネットワークの環境差異、合否判定、及び作業完了後の成績を


	績書	記載すること。
2	移行方針書	移行作業の方針、移行過渡期における構成、通信制約、リスク等を網羅的に記載すること。
3	移行スケジュール表	機器毎、拠点毎の作業日程や移行日・予備日等を記載すること。
4	移行実施計画書・成績書	移行作業におけるネットワーク確認項目、合否判定、システム側での確認項目、及び作業完了後の成績を記載すること。
5	移行手順書	移行実施時の作業手順、設定コンフィグ等を記載すること。また、職員向け無線 LAN、AD (Active Directory) サーバ導入に伴う端末設定変更 (証明書インストール等) 並びに接続の手順書を作成すること。
運用・保守業務		
1	研修資料	システム、ネットワーク管理者となる職員に対し、本町のネットワークの概要や監視システムを利用した簡易的なネットワーク接続状況の確認方法等が理解できる資料
2	運用マニュアル	障害発生時の連絡先や作業手順等を記載すること。

2.6. その他

- (1) 受注者は、本業務に係る費用一切を含むものとして契約すること。そのため、本業務の履行に係る作業場所及び什器等並びにハードウェア及びソフトウェア等の作業環境は受注者側の負担で用意するものとする。
- (2) 本仕様書に定義する各種要件仕様を満たす範囲において、より信頼性や柔軟性に優れた構成案がある場合には、その内容及び当該案との違いを提案書にて説明すること。

3. 全体スケジュール

本業務の全体スケジュールは図3のとおり。本業務の構築・移行は令和7年3月上旬より開始可能となる予定である。受注者は必要に応じて、新庁舎本体工事の工程会議に出席して構築日程等を調整し、遅延なく進めることとする。

		令和5年度				令和6年度				令和7年度			
		5-6	7-9	10-12	1-3	4-6	7-9	10-12	1-3	4	5	6	
本体工事	建築工事												
	移転										★		

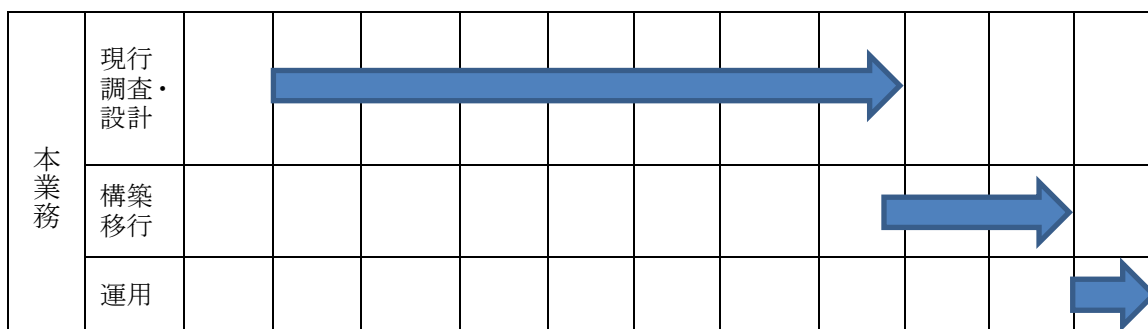


図3 全体スケジュール

4. 現行ネットワーク概要

本町のネットワーク系統は、下表のとおり大きく6つに分離されている。

表4 現行ネットワーク系統一覧

No	ネットワーク系統	概要
1	マイナンバー利用事務系	住民情報・税務・介護/福祉/子育て等基幹業務系システムに接続する。
2	LGWAN系	人事給与・財務会計・水道料金等の内部情報系システムに接続する。
3	インターネット系	山形県・市町村情報セキュリティクラウド経由でインターネットに接続する。
4	個別システム系	個別にネットワークを配置して、ローカル環境・専用回線・インターネットにて使用する。(戸籍、国保、防災システム等)
5	教育系	学校職員用の事務システム等に接続する。(現在の庁内ネットワークには収容されていない)
6	公衆利用系	一般回線で直接インターネットに接続する。来庁者等の職員以外の利用者がインターネットを閲覧するために使用する。

5. 新庁舎ネットワーク構築の基本要件

5.1. 構築方針

新庁舎ネットワークは、出先機関や各個別システムとの通信の中核となり、高い耐障害性と耐災害性、強固な情報セキュリティ対策、今後も発生すると考えられる将来的なネットワーク要件の変更に柔軟な拡張性を備える必要があるため、以下を基本(必須)要件とする。

- (1) 総務省の地方公共団体における情報セキュリティポリシーに関するガイドラインに準拠し、現行同様にマイナンバー利用事務系、LGWAN 接続系、インターネット接続系の論理的に独立した3層のネットワーク構成とし、強固なセキュリティ対策を備えること。
- (2) 現行ネットワークで稼働中の既存システムがすべて問題なく稼働できること。
- (3) 24時間365日の安定稼働が継続可能な高性能・高信頼性のネットワークであること。
- (4) ネットワーク管理者の管理・運用・庁内ネットワークのトラブルシューティングに係る負荷を低減するシンプルなネットワークであること。
- (5) 各個別システムの管理・運用の向上、及び通信量の増加等に柔軟な対応ができるネットワークであること。
- (6) 来庁者の利便性及び職員の業務効率が向上するネットワークであること。
- (7) 運用後にセキュリティ等の新たな機能や機器の追加が容易に行えるネットワークであること。

新庁舎ネットワークイメージは以下図を想定している。

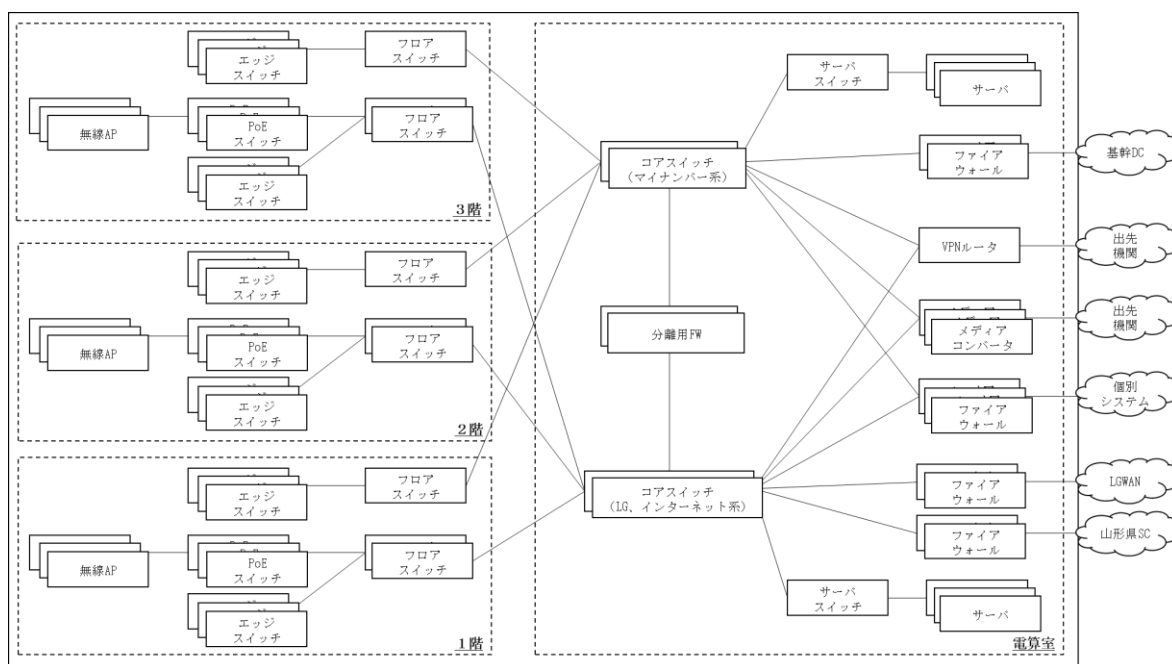


図 5-1 新庁舎ネットワークイメージ図

※新庁舎ネットワーク構成は今後の基本・詳細設計により決定する。

5.2. 構築事業の概要

「5.3. 調達機器仕様」に基づき、次の通り構築すること。

- (1) 新庁舎は地上3階建てとなる。

- (2) 2階に電算室を設け、本町が所管する各システムとコアスイッチ、並びにサーバ収容スイッチを設置する。なお、電算室のラックは7架を予定している。
- (3) 各階 EPS 内に中継ラックを設け、フロアスイッチを設置する。フロアスイッチにて各端末接続用スイッチ（エッジスイッチ）を収容する。
- (4) エッジスイッチはフロア内の各機の側面に接続することも可能とするが、業務に支障が生じないようにファンレス等静穏性に優れた機器とすること。
- (5) コアスイッチから各階 EPS 内フロアスイッチまでの配線は、10Gbps に対応した光ケーブルで構成する。
- (6) 各階 EPS 内フロアスイッチからエッジスイッチ、エッジスイッチから端末等までは、カテゴリ 6a 以上のケーブルを使用する。
- (7) 出先機関の高畠消防署、公立高畠病院、げんき館、高畠町営体育館、高畠町文化ホールについては、電算室のラック内ネットワーク機器から光ケーブルでそれぞれの施設に接続する。また、移行過渡期で新庁舎と現庁舎を接続予定であるが、同様に光ケーブルで接続する。
- (8) 各ケーブルの両端には、接続元と接続先を記載したタグ付けを行う。
- (9) 庁内のマイナンバー利用事務系端末は有線 LAN とするが、LGWAN 接続系、インターネット接続系端末は無線 LAN とすること。
- (10) 提案機器とソフトウェア（ライセンス）の構成は、安定稼動を実現するために、メーカーの推奨構成及び推奨値を遵守すること。
- (11) 庁内 LAN は以下のセグメントに分離し、一部の特定通信を除いて、相互に通信ができないようにすること。
 - ・マイナンバー利用事務系セグメント
 - ・LGWAN 接続系セグメント
 - ・インターネット接続系セグメント
 - ・その他（ネットワーク監視セグメント、公衆無線 LAN サービス等）
- (12) 特定通信はファイアウォールやネットワーク機器の ACL 等で制御し、送信元、宛先 IP アドレス及び送信元、宛先ポート番号を指定して通信できるようにすること。

5.3. 調達機器仕様

本業務で調達する機器は、以下を想定している。

表 5-3 新庁舎調達機器一覧

No	機器種別	数量	備考
1	コアスイッチ（マイナンバー利用事務系）	2	スタック構成
2	コアスイッチ（LGWAN 接続系、インターネット接続系兼用）	2	スタック構成

3	サーバスイッチ（マイナンバー利用事務系）	2	予備機 1 台含む
4	サーバスイッチ（LGWAN 接続系、インターネット接続系兼用）	2	予備機 1 台含む
5	1 階フロアスイッチ（マイナンバー利用事務系）	2	予備機 1 台含む
6	1 階フロアスイッチ（LGWAN 接続系、インターネット接続系兼用）	3	予備機 1 台含む
7	2 階フロアスイッチ（マイナンバー利用事務系）	1	
8	2 階フロアスイッチ（LGWAN 接続系、インターネット接続系兼用）	2	
9	3 階フロアスイッチ（マイナンバー利用事務系）	1	
10	3 階フロアスイッチ（LGWAN 接続系、インターネット接続系兼用）	2	
11	エッジスイッチ	82	予備機 4 台含む
12	メディアコンバータ	18	
13	本庁舎設置 VPN ルータ（出先機関接続用）	1	
14	出先機関設置 VPN ルータ（本庁舎接続用）	20	
15	LGWAN 接続用 FW	2	
16	セキュリティクラウド接続用 FW	2	
17	マイナンバー利用事務系分離用ファイアウォール	2	
18	無線 LAN コントローラ	2	
19	無線 LAN アクセスポイント（LGWAN 接続系、インターネット接続系兼用）	30	予備機 1 台含む
20	公衆無線 LAN アクセスポイント	31	予備機 1 台含む
21	無線 LAN アクセスポイント給電用スイッチ	12	予備機 2 台含む
22	認証サーバ（RADIUS）兼無線 LAN 電子証明書発行サーバ	2	
23	DHCP サーバ兼 AD サーバ	2	
24	ネットワーク監視サーバ	1	
25	電算室ラック用 UPS	必要数	
26	各階（1～3 階）EPS ラック用 UPS	必要数	

※上表に加えて、必要な数量や機器、SFP/SFP+、スタックモジュール、ライセンス等があれば合わせて調達すること。

※上表の機器を調達する際は、令和 12 年 5 月 31 日までのメーカ保守も含めること。

※現行ネットワークを調査した結果次第では、上表の数量や機器は変更となる可能性がある。

5.3.1. 基本事項

- (1) 機器については、コンシューマモデルではなく法人モデルで構成すること。
- (2) 本業務における機器の調達については、全て新品であること。

5.3.2. 新庁舎コアスイッチ仕様

- (1) 19 インチラックに設置できる規格であること。
- (2) 1000BASE-T インタフェースを 40 ポート以上有すること。
- (3) SFP/SFP+スロットを 4 ポート以上有すること。
- (4) ポートのオートネゴシエーションと固定設定 (100M/1000M Full/Half) の両方が設定可能であること。
- (5) MDI/MDI-X 自動認識と固定設定の両方が設定可能であること。
- (6) リンクアグリゲーション (IEEE802.3ad LACP (Link Aggregation Control Protocol) /Manual Configuration) の機能を有していること。
- (7) ループバックインタフェースが設定可能であること。
- (8) VLAN (ポートベース、IEEE802.1Q タグベース) が設定可能であること。
- (9) VLAN 登録可能数は、4,094 以上であること。
- (10) IEEE 802.1D (STP (Spanning Tree Protocol))、IEEE 802.1w (RSTP (Rapid STP)) に準拠していること。
- (11) BPDU ガード、BPDU フィルタ、スパニングツリーポートファストの機能を有すること。
- (12) ループガード (LDF (Loop Detection Frame) 検出/MAC アドレススラッシング検出/受信レート検出) が設定可能であること。
- (13) ループ検出時にポート LED が点滅するなど、視覚的にループが発生したことを知らせる機能を有すること。
- (14) IEEE802.1x に準拠していること。
- (15) SNMP (Simple Network Management Protocol) v1/v2c/v3 に準拠していること。
- (16) ポートミラーリング、リモートミラーリングが設定可能であること。
- (17) MAC アドレス登録可能数は、16,000 以上であること。
- (18) スイッチング・ファブリックは、673Gbps 以上であること。
- (19) ARP 登録可能数は、4,000 以上であること。
- (20) 機器本体に syslog を保存可能であること。また、外部 syslog サーバに syslog を転送できること。
- (21) NTP クライアント機能を有すること。また、自身を NTP サーバとして動作できること。

- (22) CLI (Command Line Interface) と GUI (Graphical User Interface) の両方で機器の操作が可能であること。
- (23) スタック機能を有し、複数の筐体を1台の仮想スイッチとして扱うことができること。
- (24) スタックポートは、SFP/SFP+スロット、10/100/1000BASE-Tポート、100/1000/2.5G/5GBASE-Tポートのいずれにも対応していること。
- (25) スタック接続している機器間で、コンフィグ、MACアドレステーブル、ARPテーブル、ルーティングテーブル等を同期できること。
- (26) DHCP リレーエージェントが設定可能であること。
- (27) ACL、ルートフィルタ、QoS、グレースフルリスタートの機能を有すること。
- (28) スタティックルーティング、RIPv1/v2、OSPFv2、BGP、ポリシーベースルーティングが設定可能であること。
- (29) ルーティングテーブルの登録可能数は、13,000以上であること。

5.3.3. 新庁舎サーバスイッチ仕様

- (1) 19 インチラックに設置できる規格であること。
- (2) 1000BASE-T インタフェースを48ポート以上有すること。
- (3) SFP スロットを4ポート以上有すること。
- (4) ポートのオートネゴシエーションと固定設定 (100M/1000M Full/Half) の両方が設定可能であること。
- (5) MDI/MDI-X 自動認識と固定設定の両方が設定可能であること。
- (6) リンクアグリゲーション (IEEE802.3ad LACP/Manual Configuration) の機能を有していること。
- (7) VLAN (ポートベース、IEEE802.1Q タグベース) が設定可能であること。
- (8) VLAN 登録可能数は、4,094以上であること。
- (9) IEEE 802.1D (STP)、IEEE 802.1w (RSTP) に準拠していること。
- (10) BPDU ガード、BPDU フィルタ、スパニングツリーポートファストの機能を有すること。
- (11) ループガード (LDF 検出/MAC アドレススラッシング検出/受信レート検出) が設定可能であること。
- (12) ループ検出時にポート LED が点滅するなど、視覚的にループが発生したことを知らせる機能を有すること。
- (13) IEEE802.1x に準拠していること。
- (14) SNMPv1/v2c/v3 に準拠していること。
- (15) ポートミラーリング、リモートミラーリングが設定可能であること。
- (16) MAC アドレス登録可能数は、16,000以上であること。
- (17) スwitチング・ファブリックは、336Gbps以上であること。

- (18) 機器本体に syslog を保存可能であること。また、外部 syslog サーバに syslog を転送できること。
- (19) NTP クライアント機能を有すること。また、自身を NTP サーバとして動作できること。
- (20) CLI と GUI の両方で機器の操作が可能であること。

5.3.4. 新庁舎フロアスイッチ仕様

- (1) 19 インチラックに設置できる規格であること。
- (2) 1000BASE-T インタフェースを 48 ポート以上有すること。
- (3) SFP/SFP+スロットを 4 ポート以上有すること。
- (4) ポートのオートネゴシエーションと固定設定 (100M/1000M Full/Half) の両方が設定可能であること。
- (5) MDI/MDI-X 自動認識と固定設定の両方が設定可能であること。
- (6) リンクアグリゲーション (IEEE802.3ad LACP/Manual Configuration) の機能を有していること。
- (7) VLAN (ポートベース、IEEE802.1Q タグベース) が設定可能であること。
- (8) VLAN 登録可能数は、4,094 以上であること。
- (9) IEEE 802.1D (STP)、IEEE 802.1w (RSTP) に準拠していること。
- (10) BPDU ガード、BPDU フィルタ、スパニングツリーポートファストの機能を有すること。
- (11) ループガード (LDF 検出/MAC アドレススラッシング検出/受信レート検出) が設定可能であること。
- (12) ループ検出時にポート LED が点滅するなど、視覚的にループが発生したことを知らせる機能を有すること。
- (13) IEEE802.1x に準拠していること。
- (14) SNMPv1/v2c/v3 に準拠していること。
- (15) ポートミラーリング、リモートミラーリングが設定可能であること。
- (16) MAC アドレス登録可能数は、16,000 以上であること。
- (17) スイッチング・ファブリックは、506Gbps 以上であること。
- (18) 機器本体に syslog を保存可能であること。また、外部 syslog サーバに syslog を転送できること。
- (19) NTP クライアント機能を有すること。また、自身を NTP サーバとして動作できること。
- (20) CLI と GUI の両方で機器の操作が可能であること。

5.3.5. 新庁舎エッジスイッチ仕様

- (1) 非金属壁面へマグネット取り付けが可能であること。
- (2) 1000BASE-T インタフェースを 16 ポート以上有すること。

- (3) ポートのオートネゴシエーションと固定設定 (100M/1000M Full/Half) の両方が設定可能であること。
- (4) MDI/MDI-X 自動認識が設定可能であること。
- (5) VLAN (ポートベース、IEEE802.1Q タグベース) が設定可能であること。
- (6) VLAN 登録可能数は、4,094 以上であること。
- (7) IEEE 802.1D (STP)、IEEE 802.1w (RSTP) に準拠していること。
- (8) BPDU 透過の機能を有すること。
- (9) ループ構成を検知し、該当ポートを自動的に無効にするループ防止機能を有すること。
- (10) ループ検出時にポート LED が点滅するなど、視覚的にループが発生したことを知らせる機能を有すること。
- (11) IEEE802.1x に準拠していること。
- (12) SNMPv1/v2c/v3 に準拠していること。
- (13) ポートミラーリングが設定可能であること。
- (14) 機器本体に syslog を保存可能であること。また、外部 syslog サーバに syslog を転送できること。
- (15) CLI または GUI で機器の操作が可能であること。
- (16) ファンレス等静穏性に優れた機器とすること。

5.3.6. メディアコンバータ

- (1) 19 インチラックに設置できる規格であること。
- (2) ファイバ芯数は 2 芯仕様とすること。
- (3) 通信速度は 1000Mbps に対応していること。
- (4) リンク連動 (リンクパススルー) 機能を有していること。
- (5) MDI/MDI-X 自動認識が設定可能であること。
- (6) SNMPv1/v2c/v3 に準拠していること。

5.3.7. 本庁舎設置 VPN ルータ (出先機間接続用)

- (1) 19 インチラックに設置できる規格であること。
- (2) 1000BASE-T の WAN インタフェースを 2 ポート以上有すること。
- (3) 1000BASE-T の LAN インタフェースを 5 ポート以上有すること。
- (4) ポートのオートネゴシエーションと固定設定 (100M/1000M Full/Half) の両方が設定可能であること。
- (5) MDI/MDI-X 自動認識と固定設定の両方が設定可能であること。
- (6) リンクアグリゲーション (IEEE802.3ad LACP/Manual Configuration) の機能を有していること。
- (7) ループバックインタフェースが設定可能であること。

- (8) VLAN (ポートベース、IEEE802.1Q タグベース) が設定可能であること。
- (9) IEEE 802.1D (STP)、IEEE 802.1w (RSTP) に準拠していること。
- (10) BPDU ガード、BPDU フィルタ、スパニングツリーポートファストの機能を有すること。
- (11) IEEE802.1x に準拠していること。
- (12) SNMPv1/v2c/v3 に準拠していること。
- (13) MAC アドレス登録可能数は、4,096 以上であること。
- (14) 機器本体に syslog を保存可能であること。また、外部 syslog サーバに syslog を転送できること。
- (15) NTP クライアント機能を有すること。また、自身を NTP サーバとして動作できること。
- (16) CLI と GUI の両方で機器の操作が可能であること。
- (17) DHCP リレーエージェントが設定可能であること。
- (18) ACL、ルートフィルタ、QoS の機能を有すること。
- (19) スタティックルーティング、RIPv1/v2、OSPFv2、BGP、ポリシーベースルーティングが設定可能であること。
- (20) PPP/PPPoE に準拠していること。
- (21) VPN 機能として IPsec 機能を有すること。また、暗号化に際してハードウェア処理の機能を有していること。
- (22) IPsec 以外の VPN として L2TPv2、L2TPv3、SSL VPN (OpenVPN)、GRE、もしくはこれらに準ずる機能を有すること。
- (23) WAN サービスとして、ADSL、CATV、FTTH、フレッツ・サービス (IPv4 PPPoE/IPv6 IPoE/IPv4 over IPv6)、インターネット VPN、IP-VPN、広域イーサネット、移動体データ通信サービスに対応していること。

5.3.8. 出先機関設置 VPN ルータ (本庁舎接続用)

- (1) 19 インチラックに設置できる規格であること。
- (2) 1000BASE-T の WAN インタフェースを 1 ポート以上有すること。
- (3) 1000BASE-T の LAN インタフェースを 4 ポート以上有すること。
- (4) ポートのオートネゴシエーションと固定設定 (100M/1000M Full/Half) の両方が設定可能であること。
- (5) MDI/MDI-X 自動認識と固定設定の両方が設定可能であること。
- (6) リンクアグリゲーション (IEEE802.3ad LACP/Manual Configuration) の機能を有していること。
- (7) ループバックインタフェースが設定可能であること。
- (8) VLAN (ポートベース、IEEE802.1Q タグベース) が設定可能であること。
- (9) IEEE 802.1D (STP)、IEEE 802.1w (RSTP) に準拠していること。
- (10) BPDU ガード、BPDU フィルタ、スパニングツリーポートファストの機能を有すること。

- (11) IEEE802.1x に準拠していること。
- (12) SNMPv1/v2c/v3 に準拠していること。
- (13) MAC アドレス登録可能数は、4,096 以上であること。
- (14) 機器本体に syslog を保存可能であること。また、外部 syslog サーバに syslog を転送できること。
- (15) NTP クライアント機能を有すること。また、自身を NTP サーバとして動作できること。
- (16) CLI と GUI の両方で機器の操作が可能であること。
- (17) DHCP リレーエージェントが設定可能であること。
- (18) ACL、ルートフィルタ、QoS の機能を有すること。
- (19) スタティックルーティング、RIPv1/v2、OSPFv2、BGP、ポリシーベースルーティングが設定可能であること。
- (20) PPP/PPPoE に準拠していること。
- (21) VPN 機能として IPsec 機能を有すること。また、暗号化に際してハードウェア処理の機能を有していること。
- (22) IPsec 以外の VPN として L2TPv2、L2TPv3、SSL VPN (OpenVPN)、GRE、もしくはこれらに準ずる機能を有すること。
- (23) WAN サービスとして、ADSL、CATV、FTTH、フレッツ・サービス (IPv4 PPPoE/IPv6 IPoE/IPv4 over IPv6)、インターネット VPN、IP-VPN、広域イーサネット、移動体データ通信サービスに対応していること。

5.3.9. ファイアウォール (LGWAN 接続用、セキュリティクラウド接続用、分離用)

- (1) 19 インチラックに設置できる規格であること。
- (2) 1000BASE-T インタフェースを 8 ポート以上有すること。
- (3) ポートのオートネゴシエーションと固定設定 (100M/1000M Full/Half) の両方が設定可能であること。
- (4) SNMPv1/v2c/v3 に準拠していること。
- (5) ファイアウォールスループットは、5.8Gbps 以上であること。
- (6) ファイアウォール同時セッション数は、700,000 以上であること。
- (7) 機器本体に syslog を保存可能であること。また、外部 syslog サーバに syslog を転送できること。
- (8) NTP クライアント機能を有すること。また、自身を NTP サーバとして動作できること。
- (9) CLI と GUI の両方で機器の操作が可能であること。
- (10) DHCP リレーエージェントが設定可能であること。
- (11) ACL、ステートフルパケットインスペクションの機能を有すること。
- (12) スタティックルーティングが設定可能であること。

5.3.10. 無線 LAN コントローラ仕様

- (1) 本庁舎、出先機関を含めて、無線 LAN コントローラによる集中管理を実現できるような設計、構築を行うこと。
- (2) アクセスポイント設置場所については、本町と別途協議した場所に設置すること。
- (3) 無線 LAN コントローラの収容アクセスポイント数は、ライセンス追加により拡張可能とすること。
- (4) 無線 LAN コントローラは、異なるセグメントに設置した無線 LAN アクセスポイントも管理できるよう設計すること。
- (5) 無線 LAN コントローラとの通信が切れた場合においても、無線 LAN アクセスポイント自体は通信が継続、端末等の接続にも影響ないように構成出来ること。
- (6) 無線 LAN コントローラ同士で冗長化が可能であること。

5.3.11. 無線 LAN アクセスポイント仕様 (LGWAN 接続系、インターネット接続系兼用)

- (1) 無線 LAN アクセスポイントの導入範囲は本庁舎の 1 階～3 階の全エリアとすること。
- (2) セキュリティレベルごとに SSID を分離し、それぞれ最適な認証方式、暗号化方式を設定すること。
- (3) アクセスポイント設置場所については、本町と別途協議した場所に設置すること。
- (4) 無線ネットワークに接続する機器の台数が増え、同一セグメント内に多数のクライアント端末が配置されることによる、ブロードキャストトラフィックの増大を抑制するために、同一 VLAN にはクライアント端末がおおよそ 200 台程度となるよう、無線 VLAN の設計を行うこと。
- (5) 利用可能周波数帯は 2.4GHz/5GHz を同時に利用できること。
- (6) 対応規格は、IEEE802.11a/b/g/n/ac/ax であること。
- (7) 100/1000/2.5G/5GBASE-T (RJ-45、PoE 受電) に対応したインタフェースを 1 ポート以上有すること。
- (8) LAN インタフェースは、タグ VLAN (IEEE802.1Q) に対応し、業務内で必要とされる VLAN 数に対応可能なこと。
- (9) PoE+ (IEEE802.3at) に対応していること。
- (10) 通信暗号化の規格である、WPA2 および WPA3 に対応していること。

5.3.12. 公衆無線 LAN アクセスポイント仕様

- (1) 無線 LAN アクセスポイントの導入範囲は本庁舎の 1 階～3 階の全エリアとすること。
- (2) セキュリティレベルごとに SSID を分離し、それぞれ最適な認証方式、暗号化方式を設定すること。
- (3) 庁内無線 LAN (LGWAN 接続系、インターネット接続系) アクセスポイント、無線 LAN ネットワークとは分離すること。

- (4) アクセスポイント設置場所については、本町と別途協議した場所に設置すること。
- (5) 無線ネットワークに接続する機器の台数が増え、同一セグメント内に多数のクライアント端末が配置されることによる、ブロードキャストトラフィックの増大を抑制するために、同一 VLAN にはクライアント端末がおよそ 200 台程度となるよう、無線 VLAN の設計を行うこと。
- (6) 利用可能周波数帯は 2.4GHz/5GHz を同時に利用できること。
- (7) 対応規格は、IEEE802.11a/b/g/n/ac/ax であること。
- (8) 100/1000/2.5G/5GBASE-T (RJ-45、PoE 受電) に対応したインタフェースを 1 ポート以上有すること。
- (9) LAN インタフェースは、タグ VLAN (IEEE802.1Q) に対応し、業務内で必要とされる VLAN 数に対応可能なこと。
- (10) PoE+に対応していること。
- (11) 通信暗号化の規格である、WPA2 および WPA3 に対応していること。
- (12) 総務省「Wi-Fi 提供者向け セキュリティ対策の手引き」に則り、来庁者が安全に利用できるセキュリティ対策を行うこと。
- (13) 公衆無線 LAN の不正利用防止のため、メール認証、SNS アカウント認証などの複数の認証方式が選択可能なこと。

5.3.13. 無線 LAN アクセスポイント給電用スイッチ

- (1) 無線 LAN アクセスポイント (LGWAN 接続系、インターネット接続系兼用と公衆無線 LAN の両方) への電源供給は PoE 給電を原則とし、アクセスポイントを接続するスイッチから給電を行うこと。
- (2) 非金属壁面へマグネット取り付けが可能であること。
- (3) 1000BASE-T インタフェースを 16 ポート以上有すること。
- (4) ポートのオートネゴシエーションと固定設定 (100M/1000M Full/Half) の両方が設定可能であること。
- (5) MDI/MDI-X 自動認識が設定可能であること。
- (6) VLAN (ポートベース、IEEE802.1Q タグベース) が設定可能であること。
- (7) VLAN 登録可能数は、4,094 以上であること。
- (8) IEEE 802.1D (STP)、IEEE 802.1w (RSTP) に準拠していること。
- (9) BPDU 透過の機能を有すること。
- (10) ループ構成を検知し、該当ポートを自動的に無効にするループ防止機能を有すること。
- (11) ループ検出時にポート LED が点滅するなど、視覚的にループが発生したことを知らせる機能を有すること。
- (12) IEEE802.1x に準拠していること。

- (13)SNMPv1/v2c/v3 に準拠していること。
- (14)ポートミラーリングが設定可能であること。
- (15)機器本体に syslog を保存可能であること。また、外部 syslog サーバに syslog を転送できること。
- (16)CLI または GUI で機器の操作が可能であること。
- (17)ファンレス等静穏性に優れた機器とすること。
- (18)PoE+に対応していること。
- (19)PoE 供給電力は 180W 以上であること

5.3.14. 認証サーバ (RADIUS サーバ) 兼無線 LAN 電子証明書発行サーバ仕様

- (1) 職員が利用する有線 LAN 端末に MAC 認証機能を提供すること。
- (2) 職員が利用する無線 LAN 端末にクライアント証明書を利用する IEEE802.11x 認証機能を提供すること。
- (3) 認証に用いるアカウントは 500 以上登録できること。
- (4) ネットワーク認証装置の認証数拡張は、ライセンス追加により拡張可能とすること。
- (5) 100/1000BASE-T インタフェースを 4 ポート以上有すること。
- (6) 認証アカウント毎に最終認証成功日時を記録できること。記録した日時の情報は検索条件として利用でき、その結果は CSV ファイルとしてエクスポートできること。
- (7) パスワードの有効期限、及びパスワードの変更禁止期間を設定できること。パスワード有効期限切れが近づいたことを、電子メールにより管理者・利用者に通知できること。
- (8) 認証連続失敗によりアカウントロックできること。アカウントロックに至る失敗回数、連続失敗カウントのリセットやロックの解除までの秒数は管理者により指定できること。
- (9) ゲストユーザアカウント登録機能を持つこと。
- (10)MAC アドレス毎に最終認証成功日時を記録できること。その結果を CSV ファイルとしてエクスポートできること。
- (11)認証局 (CA : Certificate Authority) 機能を有し、クライアント証明書、及びサーバ証明書を発行できること。
- (12)Web ブラウザからの申請・承認ワークフローにより、安全かつ確実にクライアント証明書の配布が可能であること。
- (13)外部の AD サーバにあるアカウント情報を参照し、認証情報として利用することができる機能を有すること。
- (14)設定情報のバックアップ・リストアが可能であること。
- (15)サーバ同士で冗長化が可能であること。

5.3.15. DHCP サーバ兼 AD サーバ仕様

(1) DHCP サーバ仕様

- ① 有線 LAN、無線 LAN にアドレスの自動払い出し機能を提供すること。
- ② アドレスの同時払い出しが 1,000 以上可能であること。
- ③ 端末追加に対して即時で対応できる拡張性を持つこと。
- ④ 特定の MAC アドレスに対して特定の IP アドレスを静的に付与する機能を有すること。
- ⑤ IP アドレスの使用率が閾値を超えた場合、通知する機能を有すること。
- ⑥ 設定情報のバックアップ・リストアが可能であること。

(2) AD サーバ仕様

- ① マイナンバー利用事務系、LGWAN 接続系、インターネット接続系の Windows ドメイン管理を行い、Windows 端末へのログイン認証を行うこと。Windows 端末の動作について、グループポリシーによる管理を行うこと。
- ② 他システムと連携可能な認証サーバとして利用できるようにすること。
- ③ Windows ドメインの設定については、既存設定を踏襲するものとし移行作業を受注者が実施すること。
- ④ 設定情報のバックアップ・リストアが可能であること。

5.3.16. ネットワーク監視サーバ仕様

- (1) 新庁舎ネットワークを構成する通信機器及びサーバ等を含め死活監視ができること。
- (2) 新庁舎ネットワークを構成する通信機器・機器等の負荷監視項目について、閾値を設定し監視できること。最低でもネットワークトラフィック負荷、CPU 使用率が監視できること。
- (3) マイナンバー利用事務系、LGWAN 接続系、インターネット接続系の機器をそれぞれ監視できること。
- (4) 機器間の物理接続や論理接続を GUI で確認できること。HUB や端末を含めて接続状況が可視化できること。
- (5) 有線ネットワークだけでなく、無線ネットワークも接続状況を可視化できること。
- (6) 障害発生を早急に発見できる仕組みを設けること。
- (7) 監視対象追加に対して即時で対応できる拡張性を持つこと。
- (8) 設定情報のバックアップ・リストアが可能であること。

5.3.17. UPS（無停電電源装置）

- (1) 電算室並びに EPS のラックに、瞬間電圧低下対策として UPS を導入すること。
- (2) UPS は収容ラック全体を対象とした容量とすること。
- (3) 収容ラックの消費電力増加に備え、UPS の容量を拡張可能とすること。

6. 業務内容に関する要件

6.1. 全体管理業務要件

- (1) 委託する業務範囲は、本業務に関する契約期間にわたる全ての作業工程における管理業務全般とする。
- (2) 受注者は、本業務の遂行にあたり、本町及び各事業者との間で生じる各種調整事項について、積極的に協力・調整を行うこと。特に、現行ネットワーク保守業者や回線業者、庁内ネットワーク上で稼動する全ての現行システム保守業者及び建設工事請負者とは、作業において密接な関わりがあるので、十分な調整を図ること。
- (3) テスト・構築・移行・保守作業等において、関係事業者による作業等依頼する必要がある場合は、発注者と調整すること。
- (4) 本仕様書に記載がない事項であって、本業務の遂行、新庁舎ネットワーク及びシステムの安定稼動、個別システム・ネットワークとの接続に必要と認められる対応については、発注者と協議・検討の上実施すること。
- (5) 発注者から本業務に係る技術的な助言を求められた際は、速やかに対応し、回答を行うこと。また、受注者は本業務に係るネットワーク構築に必要な技術動向、製品動向等の情報を積極的に提供すること。
- (6) 受注者は、本仕様書の対象業務及び利用する技術に関する十分な知識、理解及び経験のある作業者を配置し、従事させること。

6.2. 現行ネットワーク調査業務要件

- (1) 現庁舎のネットワーク、個別システムに関して現状調査・分析を実施し、課題の抽出を行うこと。
- (2) 現在のネットワーク、システムに関する把握している情報（IPアドレス等）については調査時に提供する。提供した情報を参考に、システム保守業者等へのヒアリングや現地調査を実施すること。
- (3) 各個別システムが必要とする VLAN 種別、帯域、回線種別等を確認し、要件として整理すること。
- (4) 課題抽出については、現庁舎の各セグメントにおける有線/無線 LAN 及びネットワーク機器、稼動する全てのシステム、各課が個別で契約する通信回線及び機器を対象とすること。
- (5) 現状調査・分析の際は、各課・デジタル推進係と協議の上、統合や廃止可能な回線・ネットワーク機器を整理すること。

6.3. 設計業務要件

- (1) 基本設計で必要と考えている事項を以下の通り示す。

- ① IP アドレス設計
- ② ルーティング設計
- ③ 物理構成設計
- ④ 論理構成設計
- ⑤ 情報セキュリティ設計
- ⑥ 移行設計
- ⑦ 運用設計
- ⑧ 設置設計

(2) 詳細設計では、基本設計を基に新庁舎ネットワークで運用される各機器等の主要な設定項目について設定内容の方針や理由を記述すること。

- ① 導入ネットワーク機器の物理・論理設計（VLAN、ACL 等）
- ② 導入システムの物理・論理設計（ネットワーク管理システム等）

(3) 関係する既存システムとの調整では、既存システム単位に詳細な事前調整を行い、要件を整理した上で設計承認を得た後に構築・移行を進めること。以下に、既存システムとの調整が必要と考える事項を示す。

- ① 各既存システムが接続するネットワーク系統（マイナンバー利用事務系、LGWAN 接続系、インターネット接続系）、必要帯域等について確認すること。
- ② 各既存システムの IP アドレスを確認し、調整すること。
- ③ 各既存システムの情報セキュリティポリシー要件（通信元端末の限定等）を確認し、必要な設計を行うこと。
- ④ 各既存システムのパラメータ設計支援（DNS、NTP 等）を行うこと。
- ⑤ 現行ネットワークで接続している LGWAN 専用線、山形県・市町村情報セキュリティクラウド専用線等の接続について、現行ネットワーク保守業者、山形県事務局との調整の上、必要な技術支援と対応を行うこと。

6.4. 構築・移行業務要件

(1) 共通要件

- ① 新庁舎開庁（令和 7 年 5 月）までに、機器ケーブル接続、回線疎通確認、機器動作確認、通信確認、監視確認等、新庁舎での稼働テストを完了させること。特に構築・移行可能時期（令和 7 年 3 月上旬予定）から新庁舎開庁までの期間が短い
ため、構築・移行可能時期までの可能な限り本番環境を模擬した環境でのテスト、
構築・移行の確実な実施計画、作業時の切戻し判断基準・切戻し手順、作業不芳
時のリトライ計画も考慮すること。

- ② テスト環境、テストツール、テスト項目の網羅性、テスト合否判断基準等を明確にすること。

(2) 構築要件

構築時に必要と考える事項を示す。

① 新庁舎ネットワーク

- (ア) ネットワーク機器等の調達、搬入、設置、設定作業
- (イ) ネットワーク機器等の動作確認 (単体テスト)
- (ウ) ネットワーク機器等と敷設された通信ケーブルの結線作業
- (エ) 通信ケーブル結線後の動作確認 (結合テスト)

② 外部機関

- (ア) 新規調達機器と既存機器の入替作業
- (イ) 新庁舎との接続テスト

また、外部機関の総合交流プラザ、二井宿地区公民館、屋代地区公民館、亀岡地区公民館、和田地区公民館、生涯学習館の6施設に関しては、上記(ア)(イ)の作業に加え、現庁舎の無線LANアクセスポイントを流用し、設定変更・移設作業も実施すること。

(3) 移行要件

- ① 移行の際は、移行手順書を作成・提示し、本町の承諾を得た上で、移行作業を実施すること。また、移行にあたって、既存システム等の設定変更が必要となる場合は、既存システム運用業者への説明・設定変更支援を実施すること。
- ② 新庁舎建設に伴い、新庁舎内の新ネットワーク基盤の構築を行うが、職員や各システムの新庁舎への移転は段階的に行っていく予定である。そのため、現庁舎ネットワークと新庁舎ネットワークは並行稼動することを前提とするため、現庁舎ネットワークと新庁舎ネットワークの接続を行い、構築を進めること。
- ③ 新庁舎開庁後、令和7年5月31日までの安定稼動を保障すること。開庁後、令和7年5月31日までのネットワーク環境不安定については、調査・設定変更を繰り返し行い、ネットワーク環境を安定させること。
- ④ 新庁舎に移転完了・安定稼動を確認した後に、現庁舎ネットワークとの切り離しを行うこと。
- ⑤ 無線LAN、ADサーバ導入に伴う端末の設定変更、並びに証明書のインストール作業は本業務の対象外となるが、作業手順は移行手順書の内容に含めること。

また、本業務、本体工事、配線工事との工事区分は以下を想定している。

表 6-4 工事区分

No	項目	本業務	本体	配線
----	----	-----	----	----

			工事	工事
1	電算室ラックのネットワーク機器（スタックモジュール、SFP/SFP+等含む）の調達、設置、動作試験	○		
2	電算室ラックの調達及び設置取付			○
3	電算室ラックのUPSの調達及び設置取付	○		
4	電算室ラック内、ラック間等のケーブル調達、配線			○
5	電算室・各階EPSの電源及び接地		○	
6	各階EPSのフロアスイッチの調達、設置、動作試験	○		
7	各階EPSラックの調達及び設置取付		○	
8	各階EPSラックのUPSの調達及び設置取付	○		
9	電算室から各階EPSへのケーブル用配管		○	
10	電算室から各階EPSへのケーブル調達、配線			○
11	各階EPSから各室LANソケットへの配管		○	
12	各階EPSから各室LANソケットへのケーブル調達、配線			○
13	各室LANソケットの設置		○	
14	無線LANアクセスポイントの調達、設置、動作試験	○		
15	各階EPSから無線LANアクセスポイントへの配管		○	
16	各階EPSから無線LANアクセスポイントへのケーブル調達、配線			○
17	エッジスイッチの調達、設置、動作試験	○		
18	各階EPSからデスク島（エッジスイッチ）までの配線			○
19	エッジスイッチから端末・プリンタ等へのケーブル調達、配線			○
20	電算室サーバと執務室端末とのエンドツーエンドの動作試験	○		
21	新庁舎から自営光接続拠点・現庁舎までの配管・設備			○
22	新庁舎から自営光接続拠点・現庁舎までのケーブル調達、配線			○
23	新庁舎と自営光接続拠点・現庁舎との接続試験	○		
24	現庁舎から新庁舎への運搬（文書、什器、備品）			○
25	現庁舎から新庁舎への運搬（ラック内機器、端末、プリンタ等）※ラックからのアンラッキング作業含む	○		
26	現庁舎不要物品の廃棄			○

6.5. 運用・保守業務要件

- (1) 開庁日の駆け付け時間は、4時間以内を目標とすること。但し、保守回線を利用したリモート保守により、オンサイト保守と同様の保守レベルを提供できる場合は、リモート保守でも代替可とする。
- (2) リモート保守を認める場合でも、機器交換等オンサイト保守が必要となる場合は、迅速にオンサイト保守を実施できるようにすること。
- (3) 本業務で導入する通信機器等について、簡易的なネットワーク接続状況の確認方法等が理解できる資料を整備し、納品すること。
- (4) ネットワーク障害や情報セキュリティインシデント発生時に備え、連絡先と対応方針を明確にすること。
- (5) 障害発生時の対応は開庁日を原則とするが、特に緊急時連絡として24時間365日の連絡体制を確立すること。
- (6) ネットワークの運用や変更、情報セキュリティ等に関する各種相談、問い合わせに確実に対応すること。
- (7) 機器の故障、ソフトウェアのバグ、パッチ適用、バージョンアップ、メーカーサポート終了等に関する情報の速やかな提供と適用の必要性について、本町の職員と協議すること。
- (8) ネットワーク機器のsyslogを収集、保管すること。
- (9) 冗長構成になっている機器は、冗長構成健全性の監視も行うこと。
- (10) ネットワーク障害が発生した場合に備え、障害の状況、原因箇所が把握できる仕組みを構築すること。ネットワーク障害の原因の切り分け、調査、復旧作業、確認作業において、支援または対応を行うこと。

また、新庁舎ネットワーク基盤に係る運用・保守作業は以下を想定している。

表 6-5 運用・保守作業一覧

No	保守作業	頻度・発生タイミング
1	電話・メール等による技術的問合せ	開庁日 8:30～17:15
2	障害発生時の障害切り分け、原因究明、復旧作業	24時間 365日
3	ネットワーク機器定期点検（報告書作成含む）	4回/年
4	定例会開催	4回/年
5	法令点検（電源復旧時の機器動作確認）	1回/年
6	UPSのバッテリー交換	随時
7	ネットワーク機器の軽微な設定変更、マイナーバージョンアップ、セキュリティパッチ適用	随時