

総社市新庁舎等ネットワーク構築業務
基本仕様書

令和5年5月

総社市総合政策部市政情報課

1. 概要

本仕様書は、総社市新庁舎等ネットワーク構築業務で構築する総社市役所新庁舎（以下「新庁舎」という。）における情報システムの基盤となるネットワーク及びインフラシステムについて、その基本的な仕様、考え方を定めるものである。

情報システムの基盤となるネットワーク及びインフラシステムについては、職員間の連携・情報共有が密に行え、また、システムの運用管理にかかる負担を可能な限り軽減できる環境とする。

1-1. ネットワーク

本市のネットワークは、総務省から示された「自治体情報システム強靱性向上モデル」に基づき、「三層の対策」を徹底している。新庁舎ネットワークは表1-1. 1のネットワークで構成する。各ネットワークは論理的又は物理的に独立させる。

表1-1. 1 新庁舎ネットワーク一覧

項番	ネットワーク名	説明
1	基盤ネットワーク	項番2~4の各セグメント並びに管理セグメントを集約他する基幹系ネットワーク。
2	中間系ネットワーク	ネットワークのコントロール、認証管理、資源配布、ファイルの受け渡し等を行うネットワーク。
3	住民情報系ネットワーク	住民情報システムを運用するネットワーク。住基ネット、LGWAN、住民情報系ベンダークラウドとの特定通信のみ接続する。
4	LGWAN 接続系ネットワーク	一般事務、財務会計システム、グループウェア等、非住民情報系システムを運用するネットワーク。岡山情報ハイウェイを通じ、LGWANと接続する。
5	インターネット接続系ネットワーク	インターネットを活用した情報収集や外部とのメールのやり取りを行うためのネットワーク。岡山県セキュリティクラウドを通じ、インターネットと接続する。
6	公衆無線 LAN	来庁者に対しインターネット接続環境を提供する。利用にあたっては認証を必要とする。（外部サービス利用）

1-2. インフラシステム

新庁舎ネットワークのインフラシステムとして、以下のシステム・機能を構築する。

本調達により構築するシステムを○、既存サービスを利用するものを●で表す。

表 1-2. 1 新庁舎インフラシステム

項番	区分	システム機能名称	対象ネットワーク			
			住民	LG	ネット	公衆
1	基盤システム					
	(1)	共通仮想基盤		○	○	○
	(2)	認証システム (Active Directory)		○	○	
	(3)	認証システム (RADIUS)		○	○	
	(4)	内部 DNS		○	○	
	(5)	環境分離型インターネット接続環境 (Soliton Secure Gateway 採用)			○	
	(6)	分離ネットワーク間ファイル転送環境		○	○	
	(7)	メール送受信システム		○	○	
2	アプリケーション・利用者向けサービス					
	(1)	グループウェアシステム		●		
	(2)	ファイルサーバ		○		
3	運用・管理					
	(1)	統合型 IT 運用管理システム		○	○	
	(2)	バックアップ管理システム		○	○	
	(3)	ウイルス対策システム		○	○	

1-3. クライアント PC 数

新庁舎で稼働予定のクライアント PC (住民情報系, LGWAN 接続系, インターネット接続系) の数は下表のとおり。

表 1-3. 1 各ネットワーククライアント PC 数

項番	ネットワーク	クライアント PC 数
1	住民情報系 (仮想端末)	300
2	LGWAN 接続系	865
3	インターネット接続系	65

2. ネットワーク基本設計

2-1. ネットワーク構成

2-1-1. 論理構成

(1) 基本構成

庁舎内に住民情報系ネットワーク, LGWAN 接続系ネットワーク, インターネット接続系ネットワーク, 公衆無線 LAN を構成する。

各ネットワークは設置する機器, 利用目的を踏まえ, サーバセグメント, クライアントセグメン

ト、DMZ などのセグメントに分割し、それぞれのセグメントに対し、適切にセキュリティ対策を実施する。

サーバセグメントは各ネットワークで利用するインフラシステム及びその他のサーバ群を設置するセグメントとする。クライアントセグメントは各ネットワークのインフラシステム及びその他システムを利用するための端末や印刷機器等を設置するセグメントとする。DMZ は各ネットワークが外部ネットワークと通信する必要のあるサーバ等を設置するためのセグメントとする。

・住民情報系ネットワーク

住民情報系ネットワークは、システム運用上必要な場合、相応のセキュリティを確保したうえで、特定通信として LGWAN、住基ネット、住民情報系ベンダークラウドと通信できるものとする。

・LGWAN 接続系ネットワーク

LGWAN 接続系ネットワークは、システム運用上必要な場合、相応のセキュリティを確保したうえで、特定通信として住民情報系ネットワーク及びインターネット接続系ネットワークと通信できるものとする。

・インターネット接続系ネットワーク

インターネットとの接続は岡山県セキュリティクラウドを利用する。

システム運用上必要な場合、相応のセキュリティを確保した上で、LGWAN 接続系ネットワークと通信できるものとする。

・公衆無線 LAN

NTT が提供する「おかやま Wi-Fi」を利用予定である。アクセスポイントの設置は別業務にて行う。

(2) ネットワーク構成及び各ネットワークのセグメント構成

新庁舎の情報通信ネットワークでは、通信制御や機器の運用管理を容易にするため、適切にセグメントを分割する。

基本設計段階での構築予定セグメントは下表のとおり。

表 2-1-1. 1

項番	ネットワーク名	区分	セグメント名
1.1	基盤	サーバ	管理用セグメント
2.1	中間系	サーバ	サーバセグメント
3.1	住民情報系	サーバ	サーバセグメント
3.2	住民情報系	クライアント	クライアントセグメント
4.1	LGWAN 接続系	サーバ	サーバセグメント
4.2	LGWAN 接続系	クライアント	庁内クライアントセグメント
4.3	LGWAN 接続系	クライアント	出先機関クライアントセグメント
4.4	LGWAN 接続系	DMZ	内部 DMZ
5.1	インターネット接続系	サーバ	サーバセグメント

5.2	インターネット接続系	クライアント	クライアントセグメント
5.3	インターネット接続系	DMZ	DMZ
6.1	公衆無線 LAN	クライアント	公衆クライアントセグメント

(3) ネットワークアドレス

・ネットワークアドレスの管理

各セグメントにおけるネットワークアドレスは、アドレス競合を避けるため、情報ネットワークシステム管理者が管理する。

・利用するネットワークアドレス

住民情報系ネットワークで利用するネットワークアドレスは、基幹システム保守事業者が定めるネットワーク設計に従う。

LGWAN 接続系ネットワークで利用するネットワークアドレスは、既存設備の設計を踏襲し、出先機関と競合しないものとする。

インターネット接続系ネットワークで利用するネットワークアドレスは、既存設備の設定変更をできる限り不要とするため、既存設備の設計を踏襲する。

公衆無線 LAN で利用するネットワークアドレスは、外部サービス提供事業者が定めるネットワーク設計に従う。

・サブネットマスク

サブネットマスクは、ネットワークの運用・管理における負担軽減を図るため、原則として 24 ビットとする。ただし、現在 16 ビットとしているものもある。

・IP アドレスの割り当て規則

各セグメントで機器等に割り当てるホストアドレスは、運用管理の負担軽減を図るため、機器の用途や種別ごとに割り当てのルールを定める。このルールは住民情報系ネットワークを除く全セグメントで共通のものとする。

(4) LAN 構成

新庁舎ネットワークでは、VLAN 機能（ポート VLAN，タグ VLAN）を利用し、各 LAN を論理的に分割した状態で、中継器となる幹線やスイッチを共用できるようにする。

(5) 無線 LAN

無線 LAN は、ネットワーク毎に SSID を設け、各端末等は SSID を利用して無線通信を行う。アクセスポイントは、複数の SSID での通信を同時に行えるようマルチ SSID 機能を有し、有線との接続箇所（アクセスポイント又は無線 LAN コントローラーとスイッチの接続箇所）において、各ネットワークに割り当てた SSID と VLAN の紐づけを行う。

(6) 経路制御

各ネットワークの経路制御（ルーティングプロトコル）は、スタティックルートを基本とする。経路の冗長化や業務システム上、必要な場合のみダイナミックルーティングを利用する。また、ネット

ワークアドレスの設計は、経路情報の設定が煩雑にならないよう考慮する。

2-1-2. 物理構成

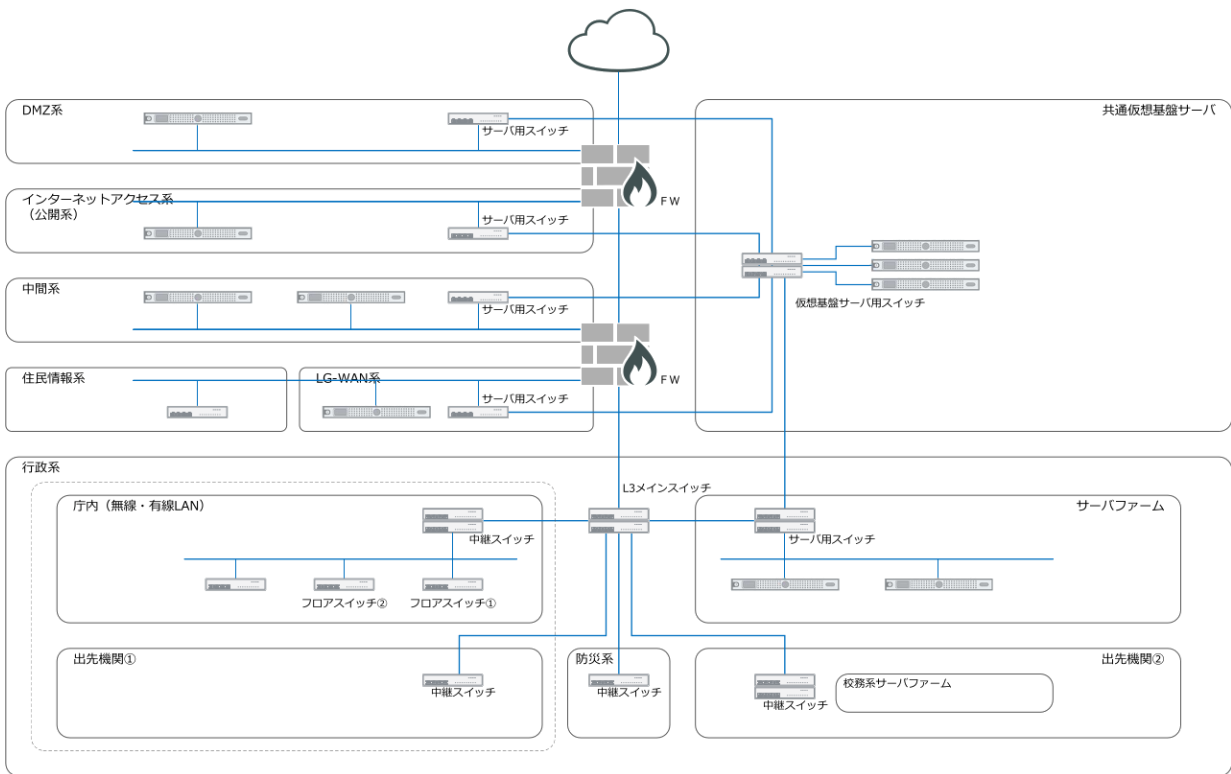
(1) 物理構成概要（ネットワークトポロジー概要）

新庁舎6階サーバ室に基幹となるL3スイッチ（メインスイッチ）を設置する。メインスイッチを基点として、スター型構成により新庁舎情報ネットワークシステムを構築する。各階にフロア内配線及び無線LANアクセスポイント接続を収容するスイッチ（フロアスイッチ）を設け、本スイッチを経由してメインスイッチと接続する。

フロアスイッチは末端の機器を接続するためのスイッチ（エッジ集約スイッチ、エッジスイッチ）接続する。

サーバ室内は各ネットワーク用の用途（サーバ接続用、外部ネットワーク接続用など）ごとにスイッチ（サーバスイッチ）を設け、それぞれ該当する機器を収容し、メインスイッチと接続する。

図2-1-2. 1 概念図



(2) 通信速度（リンク速度）

光ファイバで接続する幹線部分の通信速度（リンク速度）は10Gbpsとする。

SFP+DACケーブルで接続する場合の通信速度（リンク速度）は10Gbpsとする。

LANケーブルで接続する部分の基本の通信速度（リンク速度）は10M/100M/1Gbpsの中から、機器同士が自動的に選択できるものとする。

フロアスイッチー無線アクセスポイント間の接続については、100M/1G/2.5G/5Gbpsの中から、共通仮想基盤/バックアップサーバスイッチ間の接続については、100M/1G/2.5G/5G/10G

bps の中から機器同士が自動的に選択できるものとする。

(3) 敷設ケーブル

・幹線

メインスイッチとフロアスイッチを接続する幹線ケーブルは、マルチモード対応 2 芯以上の光ファイバケーブルとする。

・支線 (LAN ケーブル)

各機器間を接続する LAN ケーブルの規格は、基本カテゴリ 6A 以上のものとする。

エッジ集約スイッチとエッジスイッチ間、エッジ集約スイッチ又はエッジスイッチと各端末等の機器間を接続する LAN ケーブルの規格については、カテゴリ 5e 以上のものとする。

・サーバ室

サーバ室内の機器のうち、メインスイッチとサーバスイッチ間、サーバスイッチと各種サーバ等機器は必要に応じて LAN ケーブル、SFP+DAC ケーブル、光ファイバケーブル等にて接続する。

(4) 冗長化構成

新庁舎情報ネットワークシステムの基盤部分となるメインスイッチ、フロアスイッチ等の通信機器及び通信経路については、可用性を向上させるため、冗長化する。冗長化を想定している機器、通信経路は下表のとおり。

表 2-1-2. 1 冗長化対象設備

項番	設備名称	備考
1	メインスイッチ	スタック接続
2	サーバスイッチ (一部のみ)	スタック接続
3	フロアスイッチ	スタック接続
4	メインスイッチ～サーバスイッチ経路	リンクアグリゲーション
5	メインスイッチ～フロアスイッチ経路	リンクアグリゲーション

※スタック接続：複数のスイッチを 1 台のスイッチのように扱う技術。

※リンクアグリゲーション：複数の物理ポートを束ねて 1 つの論理ポートとして扱う技術。

2-1-3. その他

サーバ室内に新規で 48U 型サーバラックを 7 基設置。

収納する各種サーバ、通信機器、UPS 等の各機器の配置は詳細設計で検討する。

2-2. 外部ネットワーク

2-2-1. 住民情報系ベンダークラウド

(1) 住民情報系ベンダークラウドの概要

住民情報系ベンダークラウドは、岡山情報ハイウェイに繋がる、住民情報系ベンダーが運営する

データセンターサービスである。

(2) 住民情報系ベンダークラウドとの接続

住民情報系ベンダークラウドとの接続は岡山情報ハイウェイ経由で行う。
ネットワークの論理設計については、既存設備を踏襲するものとする。

2-2-2. 岡山情報ハイウェイ (LGWAN 等)

(1) 岡山情報ハイウェイネットワークの概要

岡山情報ハイウェイネットワークは、岡山県が運用する県内全域を結んだ高速大容量の光ファイバ網で構成された情報通信ネットワークであり、LGWAN 等の通信インフラとして利用されている。

(2) 岡山情報ハイウェイとの接続

現庁舎に引き込まれている岡山情報ハイウェイ接続施設行き自設ケーブルを新庁舎に引き直す。

2-2-3. 既設出先部署ネットワーク

(1) 既設出先部署ネットワークの概要

現庁舎の庁内 LAN と各出張所、各会館、各公民館、市立小中学校、市立幼稚園、市立認定こども園、その他の本市の施設を結ぶネットワーク。自設ケーブル及び一部通信事業者の VPN 接続サービスで接続されている。

(2) 既設出先部署ネットワークとの接続

既設出先部署ネットワークについては、出先部署での設定変更を伴わない、現在の構成をそのまま引き継ぐものとする。ただし、新庁舎に移転する出先部署については、存続する必要があることを確認した上で廃止する。

2-2-4. インターネット接続

(1) 既設インターネット接続の概要

CATV 事業者提供の回線にてインターネットへ接続するネットワーク。
インターネットには、岡山県セキュリティクラウドを通じ、接続される。

(2) 生徒系 (GIGA スクール) インターネット接続の概要

生徒系については、専用回線として CATV 事業者提供の 10 回線を使用し、直接インターネットへ接続される。

(3) 現庁舎に引き込まれている各インターネット回線を新庁舎に引き直す。

2-2-5. 外部ネットワーク接続

上記の外部施設等との接続に必要な光ファイバケーブルの引込みは別業務にて行う。

2-3. 無線 LAN

2-3-1. 無線 LAN 構成概要

新庁舎無線 LAN は、利用者（職員、来庁者）の利便性及びセキュリティ対策を踏まえて利用可能エリアを設定する。無線 LAN アクセスポイントの配置は、利用可能エリアでの確実な利用を満たすものとする。

アクセスポイントの設定変更等を円滑に行うため、無線 LAN コントローラーによる集中管理機能を導入する。

2-3-2. 伝送規格

無線 LAN では、IEEE802.11b/g/n（2.4GHz 帯）、IEEE802.11a/n/ac（5GHz 帯）及び、IEEE 802.11ax（2.4GHz/5GHz/6GHz 帯）を同時に利用できるものとする。

ただし、クライアント側の対応状況、電波干渉等の影響による通信速度の低下を考慮し、5GHz 帯の利用を前提としてアクセスポイントを配置する。

2-3-3. 無線 LAN を利用可能な LAN

無線 LAN を利用可能なネットワークは以下のとおり。ネットワークごとに SSID を設けた上、SSID は当該ネットワークに割り当てられる VLAN に紐づけられ、他のネットワークとの通信の混在は起きないようにする。

- ・ LGWAN 接続系ネットワーク
- ・ インターネット接続系ネットワーク
- ・ 公衆無線 LAN

2-3-4. 無線セキュリティ通信

無線 LAN 端末が利用するセキュリティ規格は次のものを想定している。

- ・ LGWAN 接続系ネットワーク、インターネット接続系ネットワーク：WPA2 エンタープライズ
- ・ 公衆無線 LAN：「おかやま Wi-Fi」の規格に準ずる。

2-3-5. 無線通信のトラフィック経路

無線 LAN のトラフィック経路については詳細設計で検討する。

2-3-6. アクセスポイントの電源供給

アクセスポイントへの電源供給は 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。

2-3-7. アクセスポイントの設置予定台数

アクセスポイントの設置予定台数は下表のとおり。各フロアの設置台数は詳細設計で変更する可

能性がある。

表 2-3-7. 1 アクセスポイント設置予定台数

設置フロア	設置予定台数
1 F	6
2 F	6
3 F	6
4 F	6
5 F	5
6 F	6

2-4. セキュリティ

2-4-1. 端末認証

LGWAN 接続系ネットワーク，インターネット接続系ネットワークに対し，セキュリティを確保するため，端末認証機能を利用する。

公衆無線 LAN に対しては，現在利用中である岡山県が推進する公衆無線 LAN サービス「おかやま Wi-Fi」を継続利用とし，認証について同サービスの機能を利用する。

各 LAN で想定する認証方法は以下のとおり。

(1) LGWAN 接続系ネットワーク，インターネット接続系ネットワーク

・IEEE802.1X 認証

認証サーバに対し，サブリカント（認証クライアント）をインストールした端末から認証要求を行い，認証サーバの定める認証方式で認証を行う。認証方式は ID/パスワードを利用する EAP-PEAP，クライアント証明書を利用する EAP-TLS などがある。認証方式については詳細設計で検討する。

(2) 公衆無線 LAN

・WEB（メールアカウント又は SNS アカウント）認証

「おかやま Wi-Fi」ネットワーク接続時に表示されるポータル画面からのログイン時，メールアドレス又は SNS アカウントを使用した認証を行う。

2-4-2. ネットワーク間通信ポリシー

各ネットワーク間については，アクセスポイント，無線 LAN コントローラー，ファイヤーウォール等で通信制御を行う。

ネットワーク間の通信ポリシーについては下表のとおりとする。

表 2-4-2. 1 ネットワーク間通信ポリシー

		送信側			
		住民情報系	LGWAN 接続系	インターネット系	公衆無線 LAN
受信側	住民情報系		△	×	×
	LGWAN 接続系	△		△	×
	インターネット系	×	△		×
	公衆無線 LAN	×	×	×	

×：通信禁止，△特定通信のみ許可

2-4-3. インターネットアクセスのセキュリティ

(1) インターネット接続系ネットワーク

原則として、インターネット接続系ネットワークにおけるインターネットアクセスは Web アクセスに限定する。業務上必要な場合は、セキュリティ確保を条件として、限定的に他の通信を許可する。

インターネット接続系ネットワークからのインターネットアクセスは、岡山県セキュリティクラウドを経由するものとするが、Web フィルタリングサーバを設置する等、新たに独自のセキュリティ対策を導入、実施する。

(2) 公衆無線 LAN

公衆無線 LAN については、利用者の利便性を鑑み、Web アクセス以外の通信も許可するものとし、詳細は「おかやま Wi-Fi」で提供されるセキュリティを遵守する。

3. インフラシステム機能設計

3-1. 基盤システム

3-1-1. 共通仮想基盤

LGWAN 接続系の基盤システムならびにインターネット接続系サービス等をホストする仮想基盤を構築する。また、将来的に個別システムも仮想基盤上に移設、クラウドサービスとの連携も見据えた共通仮想基盤として設計、構築を行う。

3-1-2. 認証システム (Active Directory)

LGWAN 接続系ネットワーク、インターネット接続系ネットワークの Windows ドメイン管理を行い、Windows 端末へのログイン認証を行う。

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。

他システムと連携可能な認証サーバとして利用する。

3-1-3. 認証システム (IEEE802.1X, RADIUS)

LGWAN 接続系ネットワーク、インターネット接続系ネットワークにおいて、正当な端末以外が LAN に参加することを防ぐ為、IEEE802.1X 規格に基づき、それぞれ Windows 端末に対し、証明書ベースの RADIUS 認証等を行う。

3-1-4. 内部 DNS

LGWAN 接続系ネットワークのネットワーク機器、端末、サーバ等の名前解決に利用する。インターネット接続系ネットワークのインターネットアクセスに対して名前解決、DNS 情報のキャッシュ保持に利用する。

3-1-5. 環境分離型インターネット接続環境 (Soliton Secure Gateway 採用)

インターネット接続ゲートウェイアプリケーションに接続可能な専用ビューア (ブラウザ) を利用し、LGWAN 接続系ネットワークの端末内に用意される内部から分離された環境から Web サイトの閲覧やインターネットメールからの添付ファイル等の受け渡しを行う。

3-1-6. 分離ネットワーク間ファイル転送環境 (FileZen S 採用)

LGWAN 接続系ネットワークのクライアント端末とインターネット接続ゲートウェイアプリケーションに接続可能な専用ビューア (ブラウザ) との間でファイルの受け渡しを行う。必要に応じて無害化処理を施す。

3-1-7. メール送受信システム (Soliton FileZen S/DigitalArts m-FILTER 採用)

LGWAN 接続系ネットワークのクライアント端末でメールの送受信を行う。LGWAN メールとインターネットメールで同一のメールクライアントを利用し、LGWAN メールについては送受信可能、インターネットメールについては送信、受信は無害化処理を施した後に行う。

3-2. アプリケーション・利用者向けサービス

3-2-1. グループウェアシステム

メール、掲示板、スケジュール管理、ファイル共有などの機能を有し、職員間のコミュニケーション支援、情報共有を行うシステム。

LGWAN 接続系ネットワークに設置する。

クラウドに整備している既存システムを利用する。

3-2-2. ファイルサーバ

LGWAN 接続系ネットワークに、業務上必要なデータを保存するための共有ストレージを構築する。

ユーザー認証システムと併せて、共有フォルダに対するアクセス権限を設定可能とする。

共通仮想基盤上へ構築する。

3-3. 運用・管理システム

3-3-1. 統合型 IT 運用管理システム

LGWAN 接続系ネットワーク、インターネット接続系ネットワークに接続する端末の情報収集、遠隔管理、利用可能デバイス管理、資産管理、ウイルス対策管理等を行う。

3-3-2. バックアップ管理システム

LGWAN 接続系ネットワーク、インターネット接続系ネットワークで利用するインフラシステムのバックアップについて、スケジュール管理、バックアップからの復旧、バックアップデータの削除等を管理する。

3-3-3. ウイルス対策システム

LGWAN 接続系ネットワーク、インターネット接続系ネットワークで利用するサーバに対し、ウイルス対策等を実施する。

4. 構成

新庁舎情報ネットワークシステムにおけるハードウェア・ソフトウェア構成及びネットワーク構成については、別途詳細設計で検討する。

5. 運用・維持管理計画

新庁舎情報ネットワークシステムにおける運用・維持管理計画については、詳細設計及び構築の進捗を踏まえ、別途システム構築実施計画書で定める。

6. 構築実施計画

6-1. 導入・稼働に必要な作業

別途システム構築実施計画書で定める。

6-2. システム移行

既存システムのうち、新庁舎への移設が必要な物について以下の表に定める。

表 6-2. 1 移行対象システム

項番	ネットワーク	システム名	仮想基盤上に構築予定のもの
1	LGWAN 接続系ネットワーク	戸籍システム	
2	LGWAN 接続系ネットワーク	地籍管理システム	○
3	LGWAN 接続系ネットワーク	積算システム	○
4	LGWAN 接続系ネットワーク	企業会計システム	○
5	LGWAN 接続系ネットワーク	農家台帳システム	○
6	LGWAN 接続系ネットワーク	財務会計システム	○

7	LGWAN 接続系ネットワーク	道路台帳システム	
8	LGWAN 接続系ネットワーク	路線価システム	
9	LGWAN 接続系ネットワーク	家屋評価システム	
10	LGWAN 接続系ネットワーク	例規検索システム	○
11	LGWAN 接続系ネットワーク	二要素認証用システム	○
12	LGWAN 接続系ネットワーク	見守り支援システム	

それぞれのシステムの移行は原則として、システム導入業者、保守業者が行う。

移行に際し、必要な手順・スケジュールについては別途システム構築実施計画書で定める。

6-3. データ移行

別途システム構築実施計画書で定める。

6-4. 研修計画

別途システム構築実施計画書で定める。

6-5. 作業スケジュール

別途システム構築実施計画書で定める。

6-6. 進捗管理・リスク管理の方法

新庁舎情報ネットワークシステム構築に係る進捗管理及びリスク管理については、別途システム構築実施計画書で定める。