武雄市新庁舎情報システム構築業務システム基本仕様書

１．概要

本仕様書は、武雄市新庁舎情報システム構築業務で構築する武雄市役所新庁舎（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（以下「新庁舎情報システム」という。）について、その基本的な仕様、考え方を定めるものである。

新庁舎情報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する環境を整備する。併せて、来庁者も利用できる公衆無線 LAN によりインターネット接続サービスを提供することで、市民が幅広く活用できる新庁舎とする。

１－１．ネットワーク

新庁舎ネットワークは表１－１．１の LAN で構成する。各 LAN 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	概要
1	基盤ネットワーク	項番２～４の各セグメントを集約する基幹ネットワーク。
2	住民情報系 LAN	住民情報オンラインシステムを運用する LAN。 杵藤電子計算センターとのみ接続。
3	内部業務系 LAN	財務会計システム等の個別業務システムを運用する LAN。 佐賀県公共ネットワークを通じ、LGWAN と接続する。
4	情報共有系 LAN	インターネットを利用した情報収集等を行うための LAN。接続する端末は一般事務・汎用事務を行う。 佐賀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。
5	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。 利用にあたってはユーザー登録を必要とする。

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。

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	対象セグメント			
			住民	内部	情報	公衆
1	基盤システム					
	(1)	認証システム（ActiveDirectory）		○	○	
	(2)	認証システム（RADIUS）			○	
	(3)	内部 DNS		○	○	

	(4)	NTP		○	○	
	(5)	DHCP		○	○	○
	(6)	仮想デスクトップ環境（RDS 接続環境）			○	
2	アプリケーション・利用者向けサービス					
	(1)	情報共有システム（グループウェア）		○		
	(2)	情報共有システム（ファイルサーバー）		○		
3	運用・管理					
	(1)	デバイス管理システム		○	○	
	(2)	死活監視システム		○	○	
	(3)	バックアップ管理システム		○	○	
	(4)	ウィルス対策管理システム		○	○	

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 LAN、内部業務系 LAN、情報共有系 LAN、公衆無線 LAN を構成する。

各 LAN は設置する機器、利用目的を踏まえ、サーバーセグメント、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。

サーバーセグメントは各 LAN で利用するインフラシステム及びその他のサーバー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 LAN 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 LAN が外部ネットワークと通信する必要のあるサーバー等を設置するためのセグメントとする。

＜住民情報系 LAN＞

住民情報系 LAN は杵藤電子計算センターと接続する。

ネットワークの論理構成は、原則として従来の武雄市役所本庁を引き継ぐものとし、変更の必要がある場合は杵藤電子計算センターと協議する。

＜内部業務系 LAN＞

既存の出先部署で使用する業務用ネットワークは内部業務系 LAN と接続する。

佐賀県公共ネットワーク（LGWAN、国保連合会、防災ネットワーク）を内部業務系 LAN と接続する。

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うえで、特定通信としてインターネットと通信できるものとする。

＜情報共有系 LAN＞

インターネットとの接続は佐賀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、内部業務系 LAN と通信できるものとする。

＜公衆無線 LAN＞

公衆無線 LAN 用のインターネット接続回線を用意する。

原則として、公衆無線 LAN はインターネットとのみ通信を行うものとし、内部業務系 LAN、情報共有系 LAN との通信は行わない。

2）LAN 及び各 LAN 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　構築予定セグメント一覧

項番	LAN 名称	区分	セグメント名
1.1	住民情報系 LAN	クライアント	住民端末セグメント
2.1	内部業務系 LAN	サーバー	内部サーバーセグメント
2.2	内部業務系 LAN	クライアント	内部クライアント１Ｆセグメント
2.3	内部業務系 LAN	クライアント	内部クライアント２Ｆセグメント
2.4	内部業務系 LAN	クライアント	内部クライアント３Ｆセグメント
2.5	内部業務系 LAN	クライアント	内部クライアント４Ｆセグメント
2.6	内部業務系 LAN	クライアント	内部クライアント６Ｆセグメント
2.7	内部業務系 LAN	DMZ	内部 DMZ
3.1	情報共有系 LAN	サーバー	情報サーバーセグメント
3.2	情報共有系 LAN	クライアント	情報クライアント１Ｆセグメント
3.3	情報共有系 LAN	クライアント	情報クライアント２Ｆセグメント
3.4	情報共有系 LAN	クライアント	情報クライアント３Ｆセグメント
3.5	情報共有系 LAN	クライアント	情報クライアント４Ｆセグメント
3.6	情報共有系 LAN	クライアント	情報クライアント６Ｆセグメント
3.7	情報共有系 LAN	DMZ	情報 DMZ
4.1	公衆無線 LAN	サーバー	公衆サーバーセグメント
4.2	公衆無線 LAN	クライアント	公衆クライアント１Ｆセグメント
4.3	公衆無線 LAN	クライアント	公衆クライアント２Ｆセグメント
4.4	公衆無線 LAN	クライアント	公衆クライアント３Ｆセグメント
4.5	公衆無線 LAN	クライアント	公衆クライアント４Ｆセグメント
4.6	公衆無線 LAN	クライアント	公衆クライアント６Ｆセグメント
4.7	公衆無線 LAN	DMZ	公衆 DMZ

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 LAN で利用するネットワークアドレスは、杵藤電子計算センターが定めるネットワーク設計に従う。

内部業務系 LAN で利用するネットワークアドレスは、現行の庁内 LAN の設計を踏襲し、既存の出先部署と競合しないものとする。

情報共有系 LAN 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、運用管理が適切に行うことができるよう設計する。

＜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。

＜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 LAN 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 LAN 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４階サーバー室に機関となる 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（幹線スイッチ）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。

幹線スイッチの配下にフロアスイッチを設ける。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（島ハブ、エッジスイッチ）接続する。

サーバー室内は各 LAN 用の用途（サーバー接続用、外部ネットワーク接続用など）ごとにスイッチ（サーバースイッチ）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。

２）通信速度（リンク速度）

光ファイバーで接続する幹線部分の通信速度（リンク速度）は 10Gbps とする。

LAN ケーブルで接続する部分の通信速度（リンク速度）は 10Mbps/100Mbps/1Gbps 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 12 芯以上の光ファイバーケーブルとする。光ファイバーケーブルの終端はメインスイッチ及び幹線スイッチと併せて設置するスプライスユニットに収容し、各スイッチと接続する。

＜支線＞

幹線スイッチとフロアスイッチを接続する LAN ケーブルはカテゴリ６以上のものを使用する。フロアスイッチ～島ハブ・エッジスイッチ、島ハブ・エッジスイッチ～端末等機器を接続する LAN ケーブルはカテゴリ５e 以上のものとする。

＜サーバー室＞

サーバー室内の機器のうち、メインスイッチとサーバースイッチ間、サーバースイッチと各種サーバー等機器は必要に応じて LAN ケーブル、光ファイバーケーブルにて接続する。

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、幹線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	幹線スイッチ	スタック接続
3	メインスイッチ～幹線スイッチ経路	リンクアグリゲーション
4	幹線スイッチ～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。

２－２　外部ネットワーク

２－２－１　杵藤電子計算センター

１）杵藤電子計算センターの概要

杵藤電子計算センターは、杵藤地区広域市町村圏組合を構成する市町のうち、武雄市・鹿島市・嬉野市・大町町・江北町・白石町の基幹系業務を共同処理する施設である。

２）杵藤電子計算センターとの接続

杵藤電子計算センターの基幹業務システムとの接続するための通信回線の整備ついては別途検討する。

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　佐賀県公共ネットワーク（LGWAN、佐賀県 SC、国保連 NW、防災 NW）

１）佐賀県公共ネットワークの概要

佐賀県公共ネットワークは、佐賀県及び県内市町が共同で運用する情報通信ネットワークであり、LGWAN、国保連合会、防災システム、佐賀県セキュリティクラウドの通信インフラとして利用されている。

２）佐賀県公共ネットワークとの接続

現庁舎に引き込まれている佐賀県公共ネットワークの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 と武雄市文化会館、各町公民館、市立小中学校事務室、競輪事業所、水道庁舎を結ぶネットワーク。CATV 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、存続する必要がない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

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（アクセスポイント、無線 AP）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）及び、IEEE802.11a/n/ac（5GHz 帯）を同時に利用できるものとする。但し、電波干渉等の影響により通信速度の低下を考慮し、5GHz 帯の利用を前提とした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 LAN は以下のとおり。LAN ごとに SSID を設けた上、SSID は当該 LAN に割り当てられる VLAN に紐づけられ、他の LAN との通信の混在は起きないようにする。

- 内部業務系 LAN
- 情報共有系 LAN

- 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。

- 内部業務系 LAN 及び情報共有系 LAN：WPA2 エンタープライズ
- 公衆無線 LAN：認証完了まではオープン（認証サーバーとの SSL 通信）とし、認証後に WPA2 による暗号化通信を行う。

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以下のとおり。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
１F	１０
２F	１０
３F	１０
４F	１０
６F	１０

２－４　セキュリティ

２－４－１　端末認証

内部業務系 LAN、情報共有系 LAN、公衆無線 LAN 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。

各 LAN で想定する認証方法は以下のとおり。

（１）公衆無線 LAN

・WEB 認証

新庁舎公衆無線 LAN の利用者登録を行う｡来庁者は利用端末を新庁舎公衆無線 LAN に接続し、認証サーバーへアクセスする。認証画面に事前登録時に設定した ID、パスワードを入力し、ユーザー認証及びインターネット接続の認可を行う。

なお、アカウントの登録・管理・運用の方法については詳細設計で検討する。

（２）内部業務系 LAN、情報共有系 LAN

・IEEE802.1X

認証サーバーに対し、サプリカント（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、認証サーバー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。

２－４－２　LAN 間通信ポリシー

各 LAN 間の通信ポリシーについては表２―４―２．１のとおりとする。

表２－４－２．２　LAN 間通信ポリシー

		送信側			
		住民情報系 LAN	内部業務系 LAN	情報共有系 LAN	公衆無線 LAN
受信側	住民情報系 LAN	―――	×	×	×
	内部業務系 LAN	×	―――	△	×
	情報共有系 LAN	×	△	―――	×
	公衆無線 LAN	×	×	×	―――

―――：同一 LAN

○：通信を許可、×：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）情報共有系 LAN

原則として、情報共有系 LAN 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。

情報共有系 LAN からのインターネットアクセスは、佐賀県セキュリティクラウドを経由するものとし、Web フィルタリング等のセキュリティ対策を実施する。

（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。どの通信を許可するのかについては、詳細設計で検討する。

公衆無線 LAN からのインターネットアクセスは専用回線を利用し、通信速度の確保を図る。

３　インフラシステム機能設計

３－１　基盤システム

３－１－１　認証システム（Active Directory）

- 内部業務系 LAN、情報共有系 LAN 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ーとして利用する。

３－１－２　認証システム（RADIUS、IEEE802.1X）

- 内部業務系 LAN、情報共有系 LAN の Windows 端末の認証を行う。

３－１－３　内部 DNS

- 内部業務系 LAN、情報共有系 LAN のネットワーク機器、端末、サーバー等の名前解決に利用する。
- 情報共有系 LAN のインターネットアクセスに対し､外部 DNS のキャッシュを保持する。

３－１－４　NTP

- 内部業務系 LAN、情報共有系 LAN のネットワーク機器、端末、サーバー等の時刻同期に利用する。

３－１－５　DHCP

- 内部業務系 LAN、情報共有系 LAN の端末に対し、動的に IP アドレスを割り当てる。

３－１－６　仮想デスクトップ環境（RDS 接続環境）

- 既に情報共有系 LAN に構築済みの RDS 接続環境を利用し、内部業務系 LAN の端末から Web サイトの閲覧やインターネットメールの送受信を行う。
- 既存環境については新庁舎への移設が必要である。

３－２　アプリケーション・利用者向けサービス

３－２－１　情報共有システム（グループウェア）

- 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。
- 内部業務系 LAN に設置する。

３－２－２　情報共有システム（ファイルサーバー）

- 内部業務系 LAN に､業務上が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。

３－３　運用・管理システム

３－３－１　デバイス管理システム

- 内部業務系 LAN、情報共有系 LAN 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等を行う。

３－３－２　死活監視システム

- 内部業務系 LAN、情報共有系 LAN に接続するネットワーク機器、サーバー、システムの死活監視を行う。

３－３－３　バックアップ管理システム

- 内部業務系 LAN､情報共有系 LAN 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。

３－３－４　セキュリティ対策管理システム

- 内部業務系 LAN、情報共有系 LAN で利用する端末、サーバーに対し、ウィルス対策、不正アクセ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・ソフトウェア構成およ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　データ移行・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	システム名	利用 LAN	備考
1	インターネット接続環境 （RDS 接続環境）	内部業務系	1U サイズサーバー×４ 2U サイズサーバー×１ 2U サイズ UPS×２
2	財務会計システム	内部業務系	1U サイズサーバー、2U サイズサーバー 2U サイズ UPS、1U サイズ NAS
3	設計・積算システム	内部業務系	1U サイズサーバー、1U サイズ UPS
4	要支援者台帳管理システム	内部業務系	1U サイズサーバー、1U サイズ UPS
5	地籍管理システム	内部業務系	2U サイズサーバー、2U サイズ UPS
6	家屋評価支援システム	内部業務系	タワー型サーバー、据え置き型 UPS
7	生活保護システム	内部業務系	タワー型サーバー、据え置き型 UPS
8	教育用ネットワークシステム	教育系(※)	2U サイズスプライシングユニット×１ 1U サイズサーバー×５ 2U サイズ NW 監視サーバー×１ 3U サイズサーバー×１ 1U サイズ Firewall×１ 1U サイズ L3SW×１ 1U サイズコンソール×1 1U サイズ UPS×１ 2U サイズ UPS×２

			ノート PC×１、コンパクト PC×２ 8 ポートハブ×１

それぞれの移行に際し、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。

内部業務系 LAN については、既存ネットワークの設計を引き継ぐこととしているため、移設の際に各サーバーの設定変更作業は不要なものとする。

教育用ネットワークシステムについても、市内小中学校間接続及びインターネット接続のための商用回線は現在のものを引き継ぐため、設定変更作業は不要とする。

６－３　研修計画

別途システム構築実施計画書で定める。

６－４　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。

６－５　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。