

# 武雄市教育系基盤システム構築業務システム基本仕様書

## 別紙：現行ネットワーク基本仕様（抜粋）

### 1 ネットワーク基本設計

#### 1-1. ネットワーク構成

##### 1-1-1. 論理構成

###### 1) 基本構成

武雄市役所（以下、「市役所」という）及び各小中学校（16校）に校務系ネットワーク、校務外部接続系ネットワーク、学習系ネットワーク、管理ネットワークを構成する。

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ー等を設置するためのセグメントとする。

###### <校務系ネットワーク>

市役所及び各小中学校で使用する校務システムは校務系ネットワークと接続する。

ネットワークの論理構成は、原則として従来の教育系基盤システムを引き継ぐものとするが、インターネットとの通信ができない構成とする。

###### <校務外部接続系ネットワーク>

市役所及び各小中学校で使用するインターネット通信が必要な校務システムは校務外部接続系ネットワークと接続する。

クラウドサービス（校務シェアボード、SEI-Net等）へ接続する場合は、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。

###### <学習系ネットワーク>

教員及び児童生徒が学習活動で利用する学習系システムは学習系ネットワークと接続する。

クラウドサービスへ接続する場合は、相応のセキュリティを確保した上で、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。

### 2) ネットワーク及び各ネットワークセグメント構成

教育系基盤システムでは、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 1-1-1. 1 構築セグメント一覧

項番	LAN 名称	区分	セグメント名
1.1	校務系ネットワーク	サーバー	サーバーセグメント
1.2	校務系ネットワーク	クライアント	市役所クライアントセグメント
1.3	校務系ネットワーク	クライアント	武雄小学校クライアントセグメント

1.4	校務系ネットワーク	クライアント	御船が丘小学校クライアントセグメント
1.5	校務系ネットワーク	クライアント	朝日小学校クライアントセグメント
1.6	校務系ネットワーク	クライアント	若木小学校クライアントセグメント
1.7	校務系ネットワーク	クライアント	武内小学校クライアントセグメント
1.8	校務系ネットワーク	クライアント	西川登小学校クライアントセグメント
1.9	校務系ネットワーク	クライアント	東川登小学校クライアントセグメント
1.1	校務系ネットワーク	クライアント	橘小学校クライアントセグメント
1.11	校務系ネットワーク	クライアント	山内東小学校クライアントセグメント
1.12	校務系ネットワーク	クライアント	山内西小学校クライアントセグメント
1.13	校務系ネットワーク	クライアント	北方小学校クライアントセグメント
1.14	校務系ネットワーク	クライアント	武雄中学校クライアントセグメント
1.15	校務系ネットワーク	クライアント	武雄北中学校クライアントセグメント
1.16	校務系ネットワーク	クライアント	川登中学校クライアントセグメント
1.17	校務系ネットワーク	クライアント	山内中学校クライアントセグメント
1.18	校務系ネットワーク	クライアント	北方中学校クライアントセグメント
2.1	校務外部接続系ネットワーク	サーバー	校務外部接続系サーバーセグメント
2.2	校務外部接続系ネットワーク	クライアント	市役所クライアントセグメント
2.3	校務外部接続系ネットワーク	クライアント	武雄小学校クライアントセグメント
2.4	校務外部接続系ネットワーク	クライアント	御船が丘小学校クライアントセグメント
2.5	校務外部接続系ネットワーク	クライアント	朝日小学校クライアントセグメント
2.6	校務外部接続系ネットワーク	クライアント	若木小学校クライアントセグメント
2.7	校務外部接続系ネットワーク	クライアント	武内小学校クライアントセグメント
2.8	校務外部接続系ネットワーク	クライアント	西川登小学校クライアントセグメント
2.9	校務外部接続系ネットワーク	クライアント	東川登小学校クライアントセグメント
2.1	校務外部接続系ネットワーク	クライアント	橘小学校クライアントセグメント
2.11	校務外部接続系ネットワーク	クライアント	山内東小学校クライアントセグメント
2.12	校務外部接続系ネットワーク	クライアント	山内西小学校クライアントセグメント
2.13	校務外部接続系ネットワーク	クライアント	北方小学校クライアントセグメント
2.14	校務外部接続系ネットワーク	クライアント	武雄中学校クライアントセグメント
2.15	校務外部接続系ネットワーク	クライアント	武雄北中学校クライアントセグメント
2.16	校務外部接続系ネットワーク	クライアント	川登中学校クライアントセグメント
2.17	校務外部接続系ネットワーク	クライアント	山内中学校クライアントセグメント
2.18	校務外部接続系ネットワーク	クライアント	北方中学校クライアントセグメント
3.1	学習系ネットワーク	サーバー	サーバーセグメント
3.2	学習系ネットワーク	クライアント	市役所クライアントセグメント
3.3	学習系ネットワーク	クライアント	武雄小学校クライアントセグメント
3.4	学習系ネットワーク	クライアント	御船が丘小学校クライアントセグメント
3.5	学習系ネットワーク	クライアント	朝日小学校クライアントセグメント

3.6	学習系ネットワーク	クライアント	若木小学校クライアントセグメント
3.7	学習系ネットワーク	クライアント	武内小学校クライアントセグメント
3.8	学習系ネットワーク	クライアント	西川登小学校クライアントセグメント
3.9	学習系ネットワーク	クライアント	東川登小学校クライアントセグメント
3.1	学習系ネットワーク	クライアント	橘小学校クライアントセグメント
3.11	学習系ネットワーク	クライアント	山内東小学校クライアントセグメント
3.12	学習系ネットワーク	クライアント	山内西小学校クライアントセグメント
3.13	学習系ネットワーク	クライアント	北方小学校クライアントセグメント
3.14	学習系ネットワーク	クライアント	武雄中学校クライアントセグメント
3.15	学習系ネットワーク	クライアント	武雄北中学校クライアントセグメント
3.16	学習系ネットワーク	クライアント	川登中学校クライアントセグメント
3.17	学習系ネットワーク	クライアント	山内中学校クライアントセグメント
3.18	学習系ネットワーク	クライアント	北方中学校クライアントセグメント
4.1	管理ネットワーク	サーバー	サーバーセグメント

### 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>

校務系ネットワーク、及び学習系ネットワークは、既存設備の設定変更をできる限り不要とするため、現行の教育系基盤システムの設計を踏襲する。変更の必要がある場合は武雄市と協議する。

校務外部接続系ネットワーク、及び管理ネットワークは現行の教育系基盤システムの設計を踏襲し、既存のシステムと競合しないものとする。

#### <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。ただし、学習系ネットワークのサブネットマスクは、既存設備の台数を加味し22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。

### 4) LAN 構成

教育系基盤システムでは、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 は学習系ネットワークのみとし、ネットワークに SSID を設け、各端末等は SSID を利用して無線通信を行う。また、SSID の隠蔽や許可された端末以外が接続されないようにセキュリティ対策を行う。

## 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。

### 1-1-2. 物理構成

#### 1) 物理構成概要（ネットワークトポロジー概要）

市役所 4 階サーバー室に基幹となるスイッチ（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教育系基盤システムを構築する。

市役所と各小中学校は既存の CATV 網で接続する。

各小中学校はサーバー室に市役所と接続する VPN 装置を設け、スイッチ（拠点メインスイッチ）及び無線 LAN アクセスポイント接続を収容するスイッチ（PoE スイッチ）と接続する。

拠点メインスイッチの配下にフロアスイッチを設け、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）と接続する。

#### 2) 通信速度（リンク速度）

市役所及び各小中学校内の通信速度（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

LAN ケーブルは基本的に既存流用とするが、市役所と協議の結果、追加又は更新が必要な箇所については LAN ケーブルを敷設する。また、LAN ケーブルはカテゴリ 6 以上のものとする。

### 1-2 外部ネットワーク

#### 1-2-1 拠点間ネットワーク

##### 1) 拠点間ネットワークの概要

市役所と各小中学校（16 拠点）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) 拠点間ネットワークとの接続

各小中学校ネットワークについては、現在の構成や設定をそのまま引き継ぐものとする。なお、山内東小学校、山内西小学校、山内中学校の CATV 回線は増強する見込みであり、その契約及び調整は市役所にて実施する。

### 1-3 インターネット接続

#### 1-3-1 インターネット接続の概要

インターネット接続は、校務外部接続系ネットワークと学習系ネットワークで利用する。

校務外部接続系ネットワークは、インターネットを利用した校務システムが継続利用出来るような設定を行う。

学習系ネットワークは、利用者（職員、児童生徒）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、既存設置場所に設置するものとする。

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。

#### 1-3-2 無線 LAN の伝送規格

無線 LAN 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。

#### 1-3-3 無線 LAN を利用可能なネットワーク

無線 LAN を利用可能なネットワークは以下のとおり。各小中学校に 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。

- 学習系ネットワーク

#### 1-3-4 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。

- 暗号化：WPA2 エンタープライズ
- 認証方式：基本は IEEE802.1X 認証とするが、対応が困難な機器は MAC 認証とする。

#### 1-3-5 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。

#### 1-3-6 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。

#### 1-3-7 アクセスポイントの設置台数

アクセスポイントの設置台数は以下のとおり。設置台数は詳細設計で変更する可能性がある。

表 1-3-7. 1 アクセスポイント設置台数

拠点	設置台数
武雄小学校	33
御船が丘小学校	39

朝日小学校	32
若木小学校	19
武内小学校	21
西川登小学校	22
東川登小学校	22
橘小学校	23
山内東小学校	29
山内西小学校	27
北方小学校	42
武雄中学校	46
武雄北中学校	24
川登中学校	26
山内中学校	27
北方中学校	36

## 1-4 セキュリティ

### 1-4-1 端末認証

校務系ネットワーク、学習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。

各ネットワークで想定する認証方法は以下のとおり。

#### (1) 校務系ネットワーク

##### ・IEEE802.1X

認証サーバーに対し、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。

##### ・MAC 認証

クライアント証明書が利用出来ない機器を対象とする。認証サーバーに対し MAC 登録を行い認証する。

#### (2) 学習系ネットワーク

##### ・IEEE802.1X

認証サーバーに対し、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。

##### ・MAC 認証

クライアント証明書が利用出来ない機器を対象とする。認証サーバーに対し MAC 登録を行い認証する。

### 1-4-2 ネットワーク間通信ポリシー

各ネットワーク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. 1 ネットワーク間通信ポリシー

		送信側			
		校務	外部	学習	管理
受信側	校務	——	△	×	△
	外部	△	——	×	△
	学習	×	×	——	△
	管理	△	×	△	——

——：同一ネットワーク

×：通信禁止、△特定通信のみ許可

### 1-4-3 インターネットアクセスのセキュリティ

#### (1) 校務外部接続系ネットワーク

原則として、校務外部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、インターネットを利用した校務システムへのアクセスに限定する。

## (2) 学習系ネットワーク

学習系ネットワークについては、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、既存のモバイルデバイス管理 (MDM) 及び Web コンテンツフィルタリングを利用する。