別紙２

複合施設ネットワーク基本設計書

目次

1 概要

新図書館等複合施設（以下、複合施設）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を、それぞれの館で敷設するのではなく複合施設として一体的に整備する事により、導入・運用コストの削減を図ると共に、共通化したシステム利用による組織全体の運用負担の軽減、組織間の連携、情報共有化が密に行える環境を整備する。併せて、来館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事で、県民・市民が幅広く活用できるネットワークとする。

1-1 ネットワーク

複合施設ネットワークで提供するシステム及び、サービスを利用するネットワーク（ＩＰ接続するネットワーク）、複合施設ネットワークの設備のみを利用（複合施設ネットワークを中継路として利用）するネットワーク※（レイヤ２接続するネットワーク）を対象とし、有線、無線どちらも利用可能なネットワークの設計を行う。

※複合施設ネットワークとの接点部分及び接続点間の経路設計までを設計範囲とする。

表 1-1.1 対象ネットワーク一覧

項番	ネットワーク名	備考
1	新図書館業務システムネットワーク （略称：新図書館ネットワーク）	ＯＰＡＣ用ネットワーク含む 高知県立図書館移動図書館用ネットワーク含む
2	点字図書館業務システムネットワーク （略称：新点字図書館ネットワーク）	ボランティア用ネットワークを含む
3	こども科学館（仮称）業務システムネットワーク （略称：こども科学館ネットワーク）	ボランティア用ネットワークを含む
4	複合施設内公衆無線・有線ネットワーク （略称：来館者ネットワーク）	
5	複合施設内業務委託業者用ネットワーク※1 （略称：委託業者ネットワーク）	
6	音声系ネットワーク※2	
7	データセンターネットワーク	新図書館情報システムのハウジング先ネットワーク

項番	ネットワーク名	備考
８	高知県立図書館（以下「県立図書館」）ネットワーク※3 （略称：県立図書館ネットワーク）	ＯＰＡＣ用ネットワーク含む 一部既存設備流用
９	高知市民図書館（以下「市民図書館」）ネットワーク　【本館※3分館・分室、移動図書館】 （略称：市民図書館ネットワーク）	ＯＰＡＣ用ネットワーク含む 一部既存設備流用
１０	高知県庁行政ネットワーク※4	未定
１１	高知市役所行政ネットワーク （略称：高知市行政ネットワーク）	レイヤ２接続

※１・・・委託業者ネットワークは、ＩＰ設計及び接続環境の設計のみを対象範囲とし、委託業者ネットワークで利用する機器等の設定や設置等は対象外である。

※２・・・ＩＰ(アドレス)関連、ＱｏＳ関連の設計、及び音声機器接続方法等に関しての協議、検討のみを対象とし、システム自体の設計及び構築は、建築業者側（音声系システム構築業者）で行う。

※３・・・平成２８年３月の本稼働前までの間（実際は複合施設への引越しまで)、複合施設ネットワークと接続。ネットワークとしては、高知市民図書館分館・分室と同じ扱いとする。

※４・・・複合施設ネットワークとは独立したネットワークとして整備予定。ＶＬＡＮ接続の対象とするかは詳細設計で検討する。

1-2 インフラシステム

複合施設ネットワークのインフラシステムとして、以下システム（又はサーバ機能）を構築対象とする。

表 1-2.2 対象システム一覧

項番	システム区分	対象システム	備考
1	インフラ系	認証基盤システム (Active Directory)	
		情報共有システム (グループウェア)	
		館内向け情報配信システム (デジタルサイネージ)	
		その他基盤システム	プレゼンス※1，内部ＤＮＳ，ＮＴＰ，ＤＨＣＰ※2

項番	システム区分	対象システム	備考
2	運用・管理系	ウイルス対策管理	
		総合死活監視システム	
		ＯＳパッチ管理※2	
		バックアップ管理※2	
		仮想化環境管理※2	
3	インターネット公開系	ＣＭＳ	
		公開サーバ関連	公開ＤＮＳ, メール, Ｗｅｂ※3

※１・・・複合施設ネットワークでの独立したシステムとして構築を実施するかどうかは、詳細設計にて建築業者側（音声系システム構築業者）と協議の上、決定する。

※２・・・詳細設計にて検討し、必要に応じて構築対象とする機能。

※３・・・情報公開(複合施設ホームページ)用Ｗｅｂサーバ。

1-3 構築フェーズ

ネットワークの構築は、新図書館情報システム等の稼働時期である暫定稼働と、複合施設の完成時期である本稼働の、二段階のフェーズで実施する。

① 暫定稼働ネットワーク構築（平成２７年３月稼働予定）
新図書館情報システム等の構築に合わせ、新図書館情報システムを稼働させる事を予定しているデータセンター間のネットワークと、システムを利用する各既存図書館のネットワーク及び、新図書館情報システム等に関連するインフラシステムの構築を行う。

② 本稼働ネットワーク構築（平成２８年３月稼働予定）
複合施設完成（平成２７年８月入館開始予定）に伴い、複合施設内のネットワーク及び複合施設で稼働させるインフラシステムの移設・構築を行う。

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

複合施設ネットワークの基幹として核となるスイッチ（以降コアスイッチという）を配置する。

本スイッチを中心に、職員用ネットワークやサーバネットワーク等の業務系ネットワークを構成する。業務系以外のネットワークは、セキュリティを考慮し、複合施設外部との通信の境界に配置するファイアウォール下に構成する。

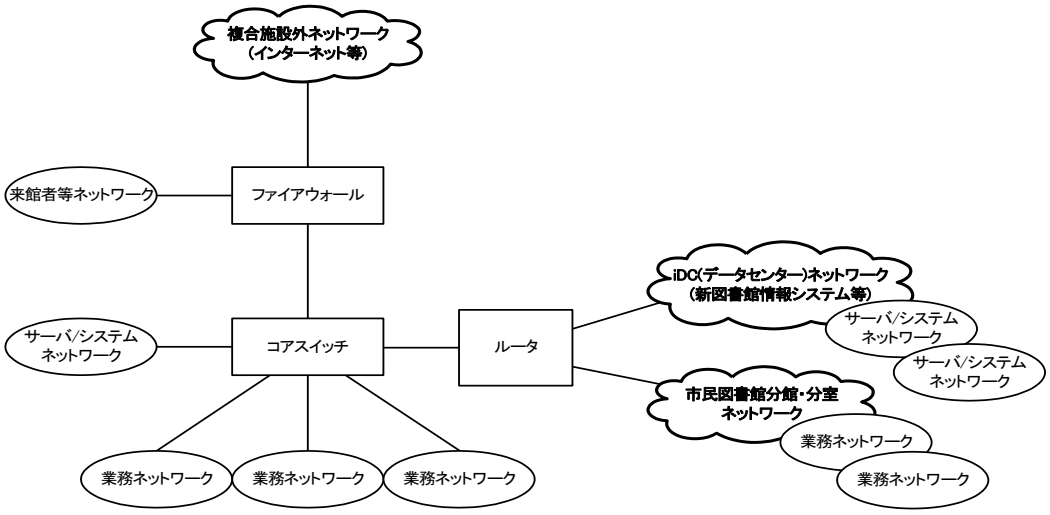

図 2-1-1.1 論理構成概要

2) セグメント

複合施設のＩＰネットワークでは、組織単位や利用者単位での通信制御や、いずれの利用者からの通信であるかを容易に判別できるようにする為、組織単位や利用用途を単位としたセグメント（ルータやファイアウォール等を介さずに端末同士が直接通信可能なネットワークの範囲）分けを行う。

基本設計段階での構築予定セグメントの一覧を、「表 2-1-1.1」に記載する。

表 2-1-1.1　主要セグメント一覧

項番	セグメント区分	セグメント名	用途
１	クライアント	新図書館業務セグメント	新図書館業務端末用ネットワーク
２	クライアント	新図書館ＯＰＡＣセグメント	新図書館ＯＰＡＣ端末用ネットワーク
３	クライアント	新点字図書館セグメント	新点字図書館職員端末用ネットワーク
４	クライアント	新点字図書館ボランティアセグメント	新点字図書館ボランティア端末用ネットワーク
５	クライアント	こども科学館(仮称)セグメント	こども科学館(仮称)職員用ネットワーク
６	クライアント	こども科学館(仮称)ボランティアセグメント	こども科学館(仮称)ボランティア端末用ネットワーク
７	クライアント	来館者セグメント	来館者持込み端末用ネットワーク
８	クライアント	委託業者セグメント※1	委託業者ネットワーク【プラネタリウム用ほか】
９	サーバ	インフラサーバセグメント	インフラサーバ用ネットワーク
１０	サーバ	新図書館用サーバセグメント	新図書館専用サーバ用ネットワーク
１１	サーバ	新点字図書館用サーバセグメント	新点字図書館専用サーバ用ネットワーク
１２	サーバ	こども科学館(仮称)用サーバセグメント	こども科学館(仮称)専用サーバ用ネットワーク
１３	システム	システム管理セグメント	システム管理用ネットワーク
１４	システム	音声ネットワーク	音声(ＩＰ電話等)用ネットワーク
１５	サーバ	新図書館情報システムセグメント	新図書館情報システムサーバ用ネットワーク
１６	サーバ	公開サーバセグメント	公開サーバ(Ｗｅｂ，メール等)用ネットワーク
１７	サーバ	データセンターサーバセグメント	新図書館情報システム以外のサーバ用ネットワーク
１８	クライアント	県立図書館業務セグメント(新)※2	県立図書館業務端末用ネットワーク
１９	クライアント	県立図書館ＯＰＡＣセグメント(新) ※2	県立図書館ＯＰＡＣ端末用ネットワーク

項番	セグメント区分	セグメント名	用途
２０	クライアント	市民図書館業務セグメント(新)※3	市民図書館業務端末用ネットワーク
２１	クライアント	市民図書館ＯＰＡＣセグメント(新) ※3	市民図書館ＯＰＡＣ端末用セグメント

※１・・・委託業者毎に異なるセグメントの構築を行う可能性がある。

※２・・・平成２８年３月の本稼働前までの間（実際は複合施設への引越しまで)、複合施設ネットワークと接続。

※３・・・分館・分室、移動図書館毎に異なるセグメントの構築を行う。(従来は本館及び全分館・分室で同一セグメント）但し、本館（暫定稼働中）及び分室（鏡図書室、土佐山図書室）以下については同一セグメントとする。

3)　ネットワークアドレス

＜ネットワークアドレスの管理＞

複合施設ネットワークの各セグメントでＩＰ通信が行えるよう、一部のセグメント（複合施設ネットワークで提供するサービス等を利用しないセグメント。高知市役所行政ネットワーク等）を除きネットワークアドレスを割当てる必要がある。ネットワークアドレスは、アドレス競合を避ける為、複合施設のネットワーク管理者が一括で管理する（複合施設ネットワークに接続する委託業者整備のネットワークを含む)。

＜利用するネットワークアドレス＞

複合施設ネットワークで利用するネットワークアドレスは、以下と競合しないアドレスで、プライベートアドレス（公開サーバは除く）を利用する。

- 既存県立図書館ネットワーク
- 既存市民図書館ネットワーク
- 高知新聞社ネットワーク
- 高知県情報ハイウェイ教育ＶＰＮ

＜サブネットマスク＞

サブネットマスク（ネットワークアドレスの中で、ネットワーク部分とホスト部分を識別する為の数値）は、ネットワークの運用・管理でのオペレーションミスを避ける為に、特別な理由を除き、２４ビットもしくは１６ビットとする。

＜ＩＰアドレスの割当て規則＞

各機器へのＩＰアドレス割当て規則は、特別用途のセグメントを除き全サブネットで共通化する。また、各ネットワークアドレス内の割当て範囲も、機器の用途や種別毎に明確に定め、ＩＰアドレスからどのような機器が利用しているか容易に判別できるようにして、運用・管理の軽減化を図る。

4)　ＶＬＡＮ構成

複合施設ネットワークでは、ＶＬＡＮ（バーチャルＬＡＮ）機能（ポートＶＬＡＮ，タグＶＬＡＮ）を利用して、各ネットワークを論理的に分割した状態（混在させない＝セキュリティが保たれた状態）で中継路となる幹線やスイッチを共用できるようにする。また、本機能により、複合施設の各ネットワークとは独立したネットワーク（高知市行政ネットワーク等）を、複合施設ネットワークを利用して構築できる。そのため、複合施設ネットワークと独立したネットワークも物理的に接続できる環境を設け、複合施設ネットワークと独立したネットワークを、ケーブルを別途に敷設することなく施設内に展開する為の機能としても利用する。

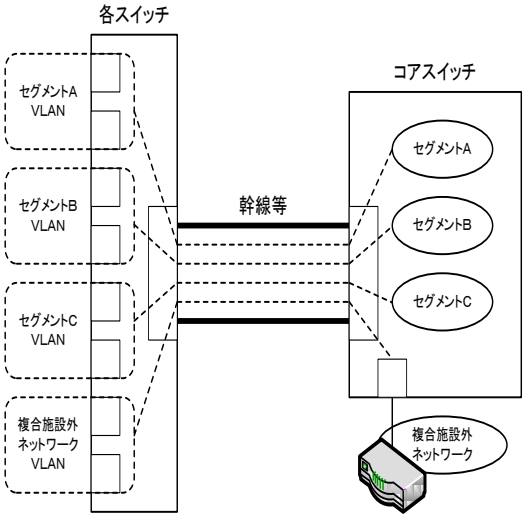

図 2-1-1.2 ＶＬＡＮイメージ

5)　無線ＬＡＮネットワーク

無線ＬＡＮネットワークは、各ネットワーク毎にＳＳＩＤ（無線ネットワークの識別子）を設け、各端末等は各々が所属するネットワークに割当てられた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機能を利用し、有線との接続箇所（アクセスポイント又は無線ＬＡＮコントローラとスイッチの接続箇所）において、各々のネットワーク（セグメント）に割当てたＶＬＡＮとＳＳＩＤの紐付けを行う。

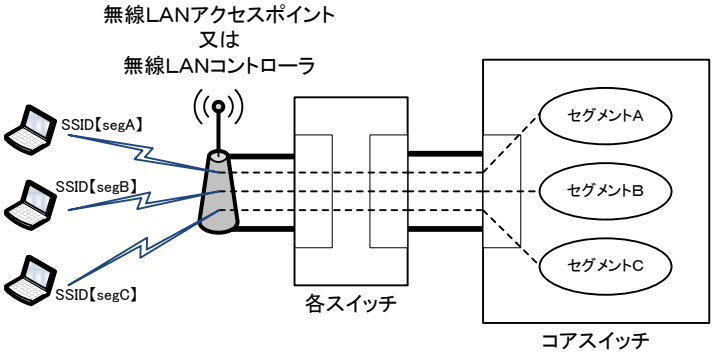

図 2-1-1.3 無線ＬＡＮ通信概要

6)　経路制御

複合施設内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のみを基本的に利用する事とし、経路の冗長化等で必要な場合のみ部分的（冗長経路で接続された装置間の間のみ等）にダイナミックルーティングを利用する。なお、各ゲートウェイ機器の経路情報（設定）が煩雑にならない事を考慮したネットワークアドレスの割当て設計を行う。

2-1-2 物理構成

1) ネットワークトポロジ

複合施設４Ｆサーバ室に基幹となるスイッチ（コアスイッチ）を設置し、本スイッチを基点としたスター形の構成で複合施設ネットワークを形成する。

複合施設内各フロア（Ｍ３Ｆ、Ｍ４Ｆ、Ｍ５Ｆ、及び４Ｆの一部配線は除く）は、フロア内配線（無線ＬＡＮアクセスポイント向けを含む）を収容するスイッチ（以降幹線スイッチという）を設け、本スイッチを経由してコアスイッチと接続する。

Ｍ３Ｆ、Ｍ４Ｆ、Ｍ５Ｆは、それぞれのフロア内配線（無線ＬＡＮアクセスポイント向けを含む）を集約するスイッチ（以下、エッジスイッチ）を設け、直下のフロアの幹線スイッチに接続する構成とし、コアスイッチー幹線スイッチーエッジスイッチの多段接続を行う。

各フロアの一部の支線についても同様の多段構成としてエッジスイッチに収容する構成とし、幹線スイッチの配線収容本数の分散化を図る。上記構成の例外として、４Ｆの一部支線については、サーバ室に設置するエッジスイッチに収容し、本スイッチをコアスイッチに直接接続する。

サーバ室内は、幹線スイッチの接続構成と同様、用途毎（基本はセグメント毎）にスイッチ（各サーバスイッチ、外部接続用スイッチ等、以降総称としてシステム系スイッチという）を設け、それぞれの該当機器（サーバ等）を収容し、コアスイッチと接続する。

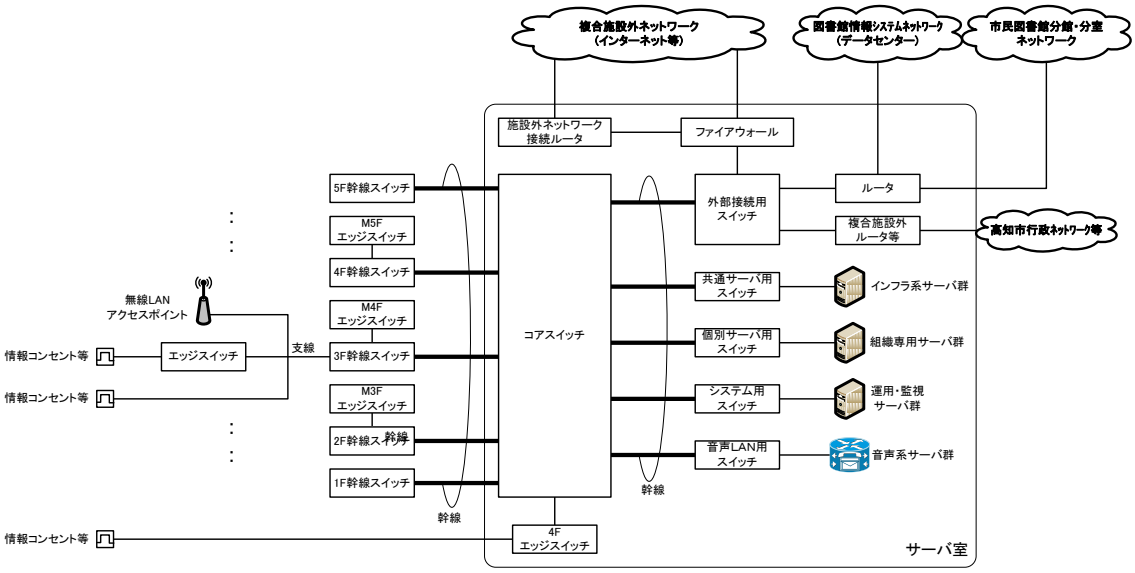

図 2-1-2.1 物理構成概要

2)　通信（リンク）速度

光ファイバーケーブルで接続する部分（幹線）は１０Ｇｂｐｓ（１０ＧＢａｓｅ－ＳＲ）、ＬＡＮケーブルで接続する部分は１０Ｍ／１００Ｍ／１Ｇｂｐｓ（スイッチ側で自動認識）とする。

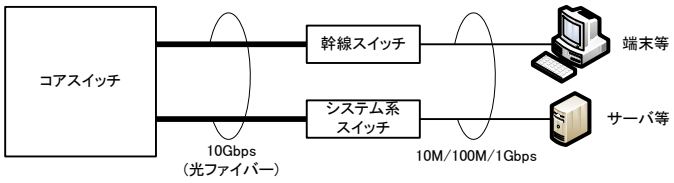

図 2-1-2.2 通信速度

3)　敷設ケーブル

・ 幹線

コアスイッチと幹線スイッチを接続する幹線ケーブルは、光ファイバーケーブルを敷設する。敷設するケーブルは、マルチモード（ＧＩ型）で、４芯（複合施設ネットワークで利用）＋必要予備芯数※とする。

なお、終端はスプライスユニットに収容し、コアスイッチ及び幹線スイッチと同一箇所に設置する。

※予備芯数は詳細設計にて検討する。

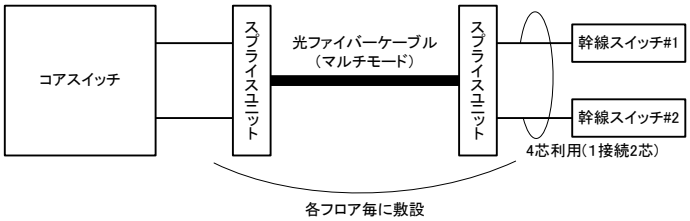

図 2-1-2.3 幹線ケーブル敷設概要

・ 支線

幹線スイッチからエッジスイッチ、幹線／エッジスイッチからＬＡＮアウトレット（情報コンセント等）及び無線ＬＡＮアクセスポイント向けのＬＡＮケーブルは、カテゴリ６又はそれ以上のカテゴリのものを敷設する事とし、幹線スイッチとエッジスイッチ間は二本、その他は一本ずつ敷設する。

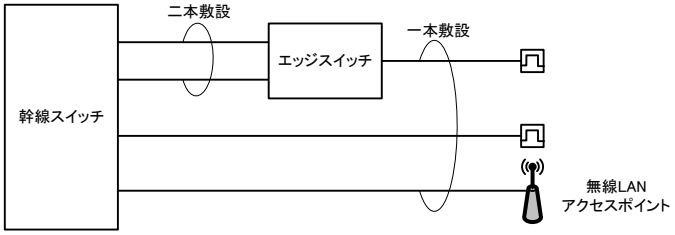

図 2-1-2.4 支線ケーブル敷設概要

敷設予定の支線本数は以下の通り。

表 2-1-2.1 支線敷設本数(予定)

フロア	敷設区間	本数	フロア合計
１Ｆ	幹線スイッチ～エッジスイッチ	18	101
	幹線スイッチ～ＬＡＮアウトレット	4	
	幹線スイッチ～無線アクセスポイント	13	
	エッジスイッチ～ＬＡＮアウトレット	66	
２Ｆ	幹線スイッチ～エッジスイッチ※1	24	137
	幹線スイッチ～ＬＡＮアウトレット	14	
	幹線スイッチ～無線アクセスポイント	27	
	エッジスイッチ～ＬＡＮアウトレット	72	
Ｍ３Ｆ	エッジスイッチ～ＬＡＮアウトレット	24	40
	エッジスイッチ～無線アクセスポイント	16	
３Ｆ	幹線スイッチ～エッジスイッチ※1	32	191
	幹線スイッチ～ＬＡＮアウトレット	30	
	幹線スイッチ～無線アクセスポイント	26	
	エッジスイッチ～ＬＡＮアウトレット	103	
Ｍ４Ｆ	エッジスイッチ～ＬＡＮアウトレット	29	44
	エッジスイッチ～無線アクセスポイント	15	
４Ｆ	幹線スイッチ～エッジスイッチ※1	22	134
	幹線スイッチ～ＬＡＮアウトレット	12	
	幹線スイッチ～無線アクセスポイント	22	
	エッジスイッチ～ＬＡＮアウトレット	43	
	サーバ室エッジスイッチ～ＬＡＮアウトレット	35	
Ｍ５Ｆ	エッジスイッチ～ＬＡＮアウトレット	14	27
	エッジスイッチ～無線アクセスポイント	13	
５Ｆ	幹線スイッチ～エッジスイッチ	4	22
	幹線スイッチ～ＬＡＮアウトレット	10	
	幹線スイッチ～無線アクセスポイント	8	
	エッジスイッチ～ＬＡＮアウトレット	未定	

フロア	敷設区間	本数	フロア合計
ＲＦ	５Ｆ幹線スイッチ～無線アクセスポイント	1	1
合計			697

※１・・・M階エッジスイッチ分含み

・ サーバ室

サーバ室は、コアスイッチとシステム系スイッチ（音声系との接続は未定）間は、光ファイバーケーブル（マルチモード、ＧＩ型）を敷設、その他はＬＡＮケーブル（カテゴリ６以上のグレード）を敷設し、接続する。

4) 冗長化構成

複合施設ネットワークでの基盤となる装置は、ネットワークの障害による業務の停止を、防止もしくは最小限に留める為、ハードウェアを冗長化する。

冗長化の対象機器は以下の通りとする。なお、冗長化されたスイッチ等へ接続する機器（クライアント系機器を除く）は、両方のスイッチへ同時に接続する構成（ＮＩＣ）を基本構成とする。

・ 主要スイッチ（コア、幹線、システム系）
スタック接続（複数のスイッチを論理的に一台のスイッチとして扱えるようにする方式）＋リンクアグリゲーション構成
・ ファイアウォール
・ 端末認証サーバ
・ 無線ＬＡＮコントローラ
・ 統合認証サーバ（Active Directory）
・ 仮想サーバ環境
※仮想サーバ環境を構築対象とする場合での冗長化構成は、物理サーバを複数系統（ストレージは一系統で共用）準備し、片系が故障した場合は稼働していた仮想サーバを、別系の物理サーバに動的に復元・稼働させる。（仮想環境の冗長化機能で実現）
※仮想サーバ環境について、構築対象とするか、また、構築対象で冗長構成とするかは詳細設計以降にて検討する。

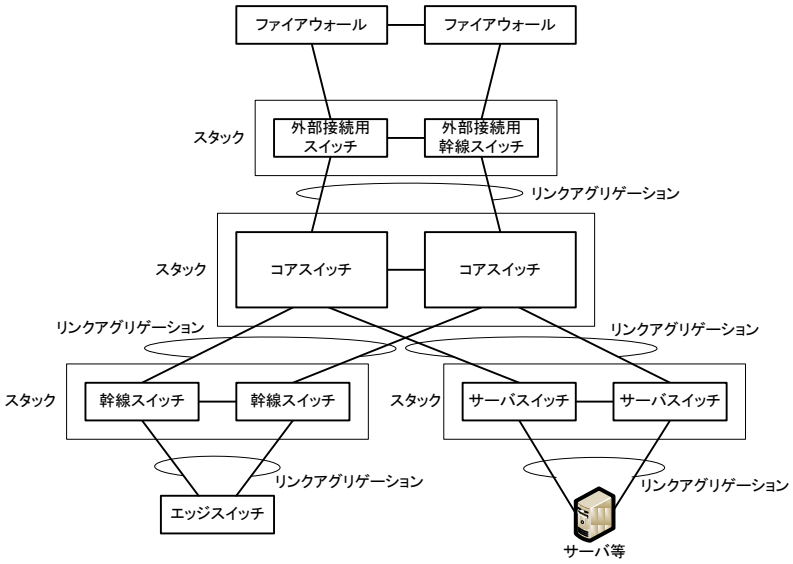

図 2-1-2.5 冗長化構成概要

構成上、ハードウェアの冗長構成が取れないものや、冗長化を構成してもネットワークの停止を避ける事が不可能な装置は、予備機を確保しておき、すぐに交換可能な体制を整える。
予備機が必要なものは以下の通りとする。

- 幹線スイッチ、M階エッジスイッチ
- エッジスイッチ
  予備機は、２４ポートモデルタイプ、１０ポートモデルタイプの二種類。
- 各ルータ

2-2 外部ネットワーク

複合施設ネットワークと関連する外部ネットワークについて、その接続方法や接続構成等について記載する。

なお、各外部ネットワーク接続に利用するアクセス回線は、同品目の回線を利用するサービスを用いて接続する場合、アクセス回線を共用する事が可能である。回線の共用利用については詳細設計で検討する事とし、基本設計では、各接続に別々の回線を用いる構成として設計する。

2-2-1 ｉＤＣ（データセンター）

1) ｉＤＣの概要

暫定稼働開始時期との関係上、新図書館情報システム及び関連するその他インフラ系システムは、複合施設以外の場所で構築し稼働させる必要がある。

稼働場所は、「新システム基本設計書 別紙 5-1 システム運用・維持管理計画書」に記載の運用要件を備えたｉＤＣハウジング設備を利用する。

2) ｉＤＣとの接続

ｉＤＣは、フレッツ光ネクスト（品目はスーパーハイスピード隼を予定）をアクセス回線とし、フレッツＶＰＮワイドを利用して施設間の接続を行う。

データセンターと接続を予定している施設を以下に記載する。

表 2-2-1.1 接続施設一覧

接続施設	アクセス回線	備考
複合施設	フレッツ光ネクスト スーパーハイスピード隼	
既存図書館	フレッツ光ネクスト ハイスピード	一部回線速度未定

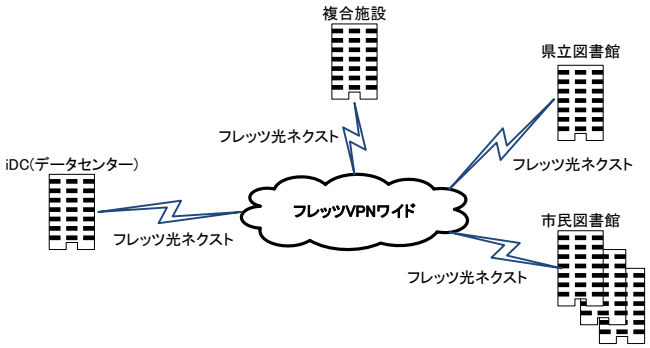

図 2-2-1.1 ｉＤＣ接続構成

2-2-2 既設図書館ネットワーク

1) 既存図書館の整備範囲

既存図書館（県立図書館、市民図書館全館）で、新図書館情報システムを利用する為に複合施設ネットワークに接続する。また、併せて、既存図書館のネットワークについての整備も行う。

既存図書館の主な整備内容は以下の通りである。

① ルータを新設し、各館に二系統あるネットワーク（業務系とＯＰＡＣ系）を収容して複合施設ネットワークと接続する。

※ 市民図書館本館及び鏡、土佐山の各分室のネットワークは、現行通り高知市役所に集約し、高知市役所に設置するルータ（複合施設で手配）から、複合施設ネットワークに接続する。（業務系及びＯＰＡＣ系ともに現行と同じく同一ネットワークとなる）

② 館内のスイッチの更新（配線は基本既存のものを流用し、不足する分のみ配線を敷設）。

※ 県立図書館、市民図書館本館へは、既存スイッチの流用及び複合施設に設置予定のスイッチを暫定利用し、両館の複合施設への引越しに伴って移設を行う。

2) ネットワーク構成

各館で現行利用している（市民図書館本館及び、鏡、土佐山分室は除く）、高知市役所手配のフレッツ光ネクスト回線を共用※し、フレッツＶＰＮワイドサービスを利用して、複合施設及びｉＤＣと接続する。

以下に、各館で利用するアクセス回線速度（品目）及び接続時期の一覧と、構成概要を記載する。

※ 現行利用している回線のＯＮＵ配下にスイッチを設置し、本スイッチに既存ルータ及び新設するルータを収容して回線を共用で利用できる構成にする。

表 2-2-2.1 アクセス回線速度と接続時期

接続施設	アクセス回線	接続時期
県立図書館	フレッツ光ネクスト ハイスピード	暫定稼働テスト開始前～本稼働開始前
高知市役所 （市民図書館本館・ 鏡・土佐山）	フレッツ光ネクスト （品目未定）	暫定稼働テスト開始前 （本館は本稼働開始前まで）
市民図書館 分館・分室１９箇所	フレッツ光ネクスト ハイスピード	暫定稼働テスト開始前
市民図書館移動図書館	フレッツ光ネクスト	本稼働開始前

接続施設	アクセス回線	接続時期
	ハイスピード（予定）	

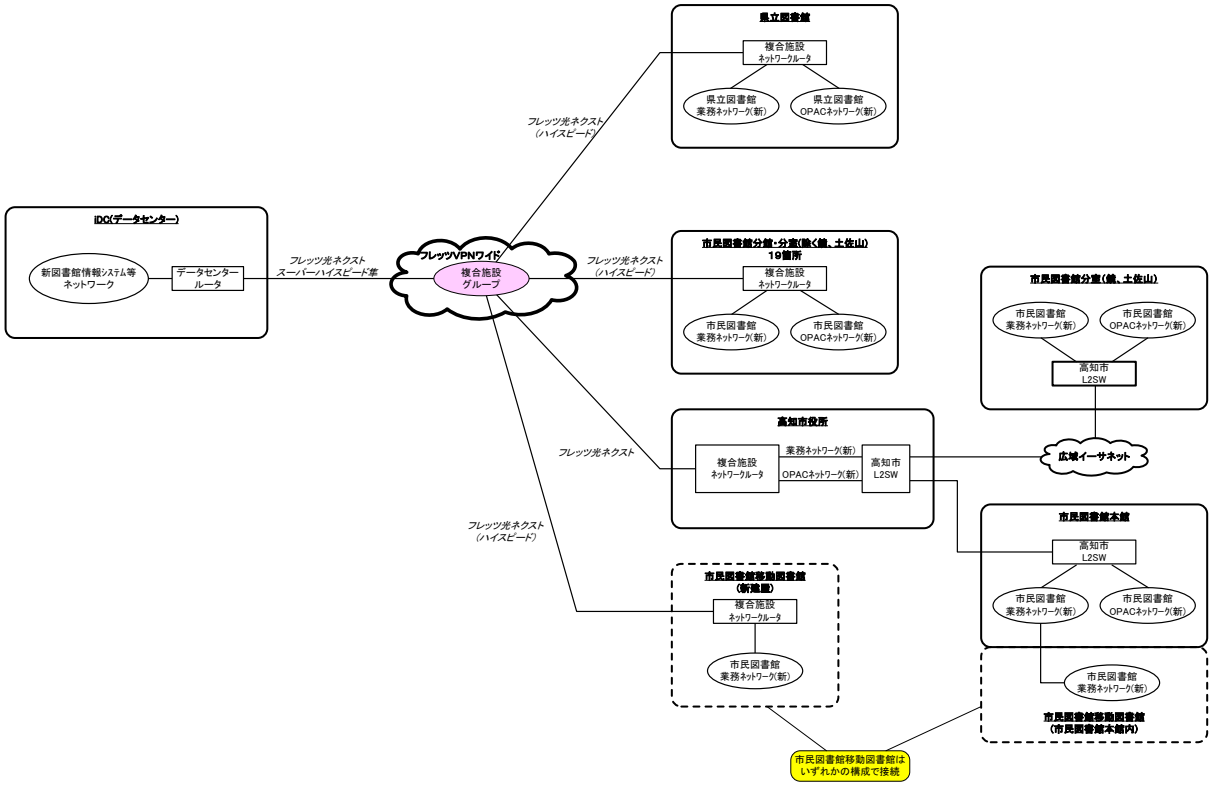

図 2-2-2.1 既存図書館接続構成（暫定稼働時）

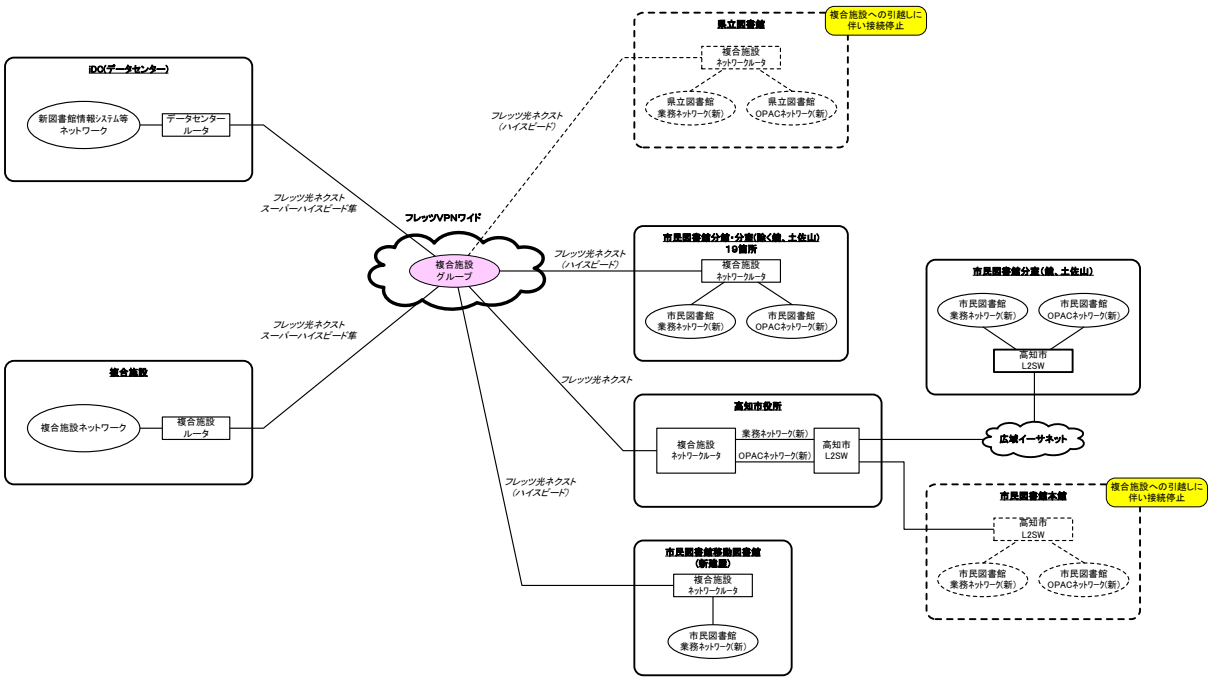

図 2-2-2.2 既存図書館接続構成（本稼働時）

3)　市民図書館各館の責任分解点

市民図書館各館（本館、鏡、土佐山除く）は、既設設備を流用してネットワークの整備を行うが、既設設備は管理元が設備により異なる為、各設備の責任分解点を明確にした上で、構築・運用保守を行う必要がある。以下に、各設備の責任分解点を記載する。
※以下は想定している内容である。装置の手配区分も含め、詳細設計の段階で高知市情報政策課と協議の上、最終決定する。

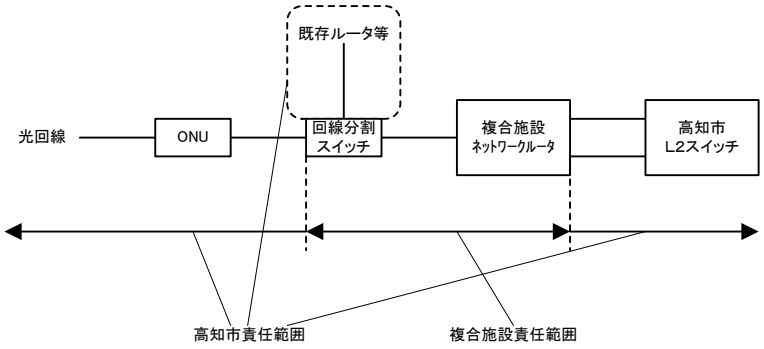

図 2-2-2.3 責任分解点【高知市役所】

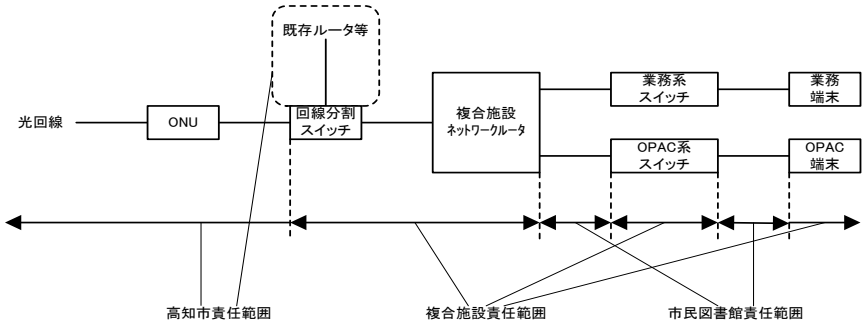

図 2-2-2.4 責任分解点【分館・分室　※鏡、土佐山除く】

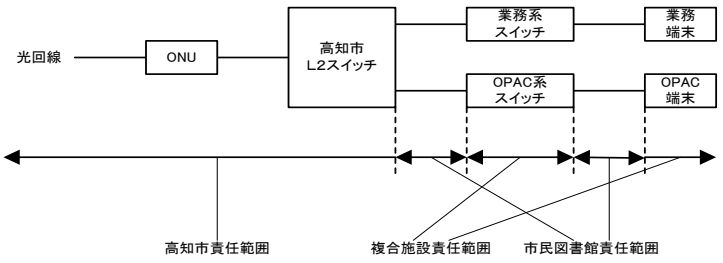

図 2-2-2.5 責任分解点【本館、鏡、土佐山　※本館は光回線接続ではない】

2-2-3 インターネット

インターネットへは、複合施設からの接続と、データセンターからの二系統の接続構成とする。

複合施設側のインターネット接続は、複合施設内の各端末及び、既存図書館端末（本稼働開始直前以降）からインターネットへのアクセス用に利用し、データセンターのインターネット接続は、インターネットから、各公開サーバ（ＤＮＳ、メール、Ｗｅｂ、新図書館情報システムＷｅｂ）へのアクセスと、データセンター内各サーバ及び既存図書館端末（本稼働開始直前まで）からのインターネットへのアクセスに利用する。

複合施設側のインターネット接続は、グローバルＩＰアドレスを２つ以上固定で割当てられるようプロバイダー契約し、２００Ｍｂｐｓ以上の光回線（ベストエフォート型）を利用して接続を行う。

データセンター側のインターネット接続は、データセンターが提供するプロバイダーサービスを利用し、１００Ｍｂｐｓ以上での接続（ベストエフォート型でＵＴＰによる構内接続）を行う。グローバルＩＰアドレスは、新図書館情報システム公開Ｗｅｂ用、デジタルアーカイブ公開Ｗｅｂ用、グループウェア用、複合施設の公開ＤＮＳ・メール・Ｗｅｂ用兼、インターネットアクセス用と、４つ割当て（予定）を行う。

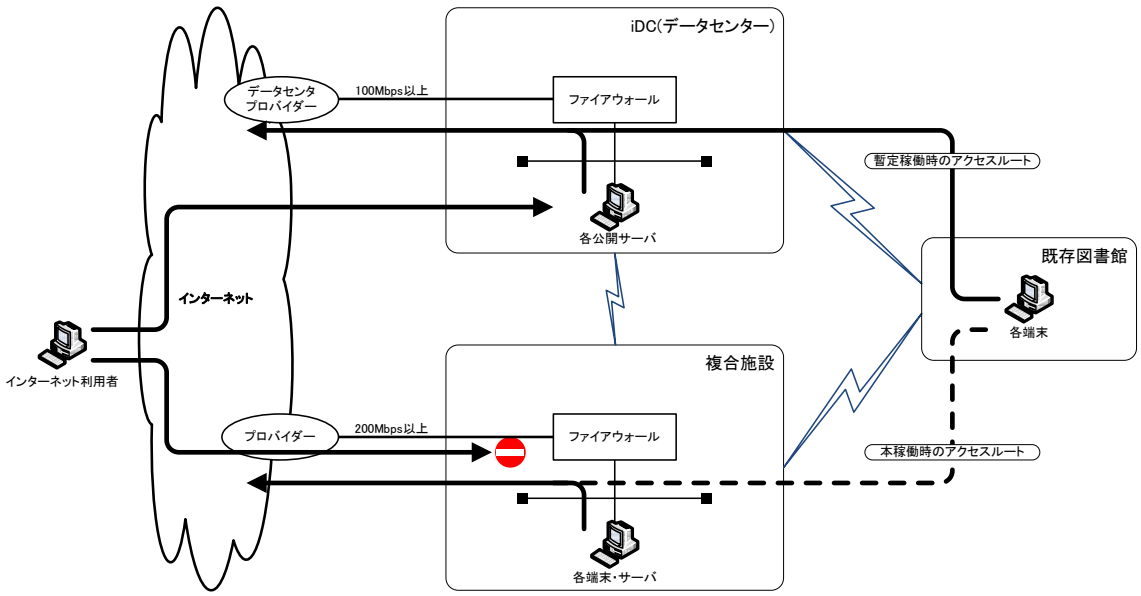

図 2-2-3.1 インターネット接続構成

2-2-4 高知県庁行政ネットワーク

高知県庁行政ネットワークへは、高知県庁行政ネットワークを管理する高知県情報政策課が手配する、回線及びルータを利用して接続する。ルータ以降の整備（高知県庁行政ネットワーク用端末利用場所までの配線敷設やスイッチの手配、設置等）は複合施設側で行う。配線等は複合施設ネットワークとは別整備とし、複合施設ネットワークとの接続は行わない。

なお、上記の整備区分、構成とするかは、詳細設計で再度高知県側と協議を行った上で判断する。

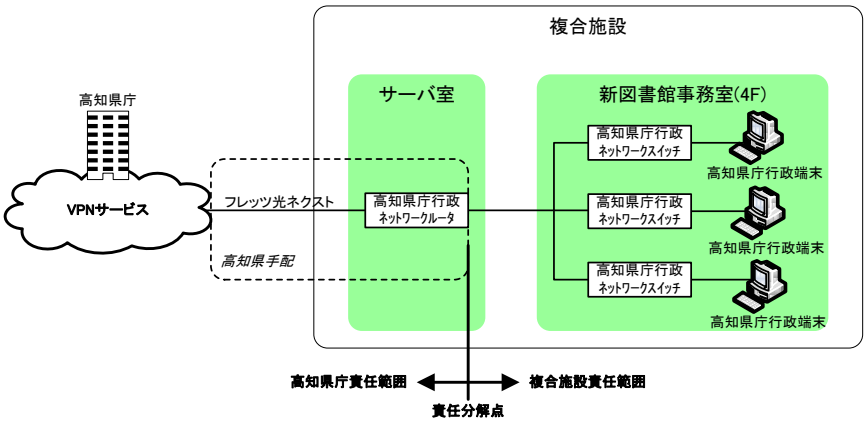

図 2-2-4.1 高知県行政ネットワーク接続構成

2-2-5 高知市行政ネットワーク

複合施設で利用する、高知市行政ネットワークは、高知市情報政策課が手配する高知市行政ネットワーク用ルータを、サーバ室に設置し複合施設ネットワークのスイッチ（外部接続用スイッチ）と接続する。本接続を基点に、各フロアに設置される高知市行政ネットワーク端末が接続される最寄のスイッチまで、高知市行政ネットワーク用のＶＬＡＮを展開して、高知市行政ネットワークを形成する。（高知市行政ネットワークとの接続は、前述の通りレイヤ２接続とし、複合施設ＩＰネットワークとの接続は行わない）

なお、高知市行政ネットワーク用ルータに付帯する高知市手配の設備（スイッチや回線のＯＮＵ等）は、高知市行政ネットワーク用ルータと同一箇所に設置できる環境を複合施設側で用意する。

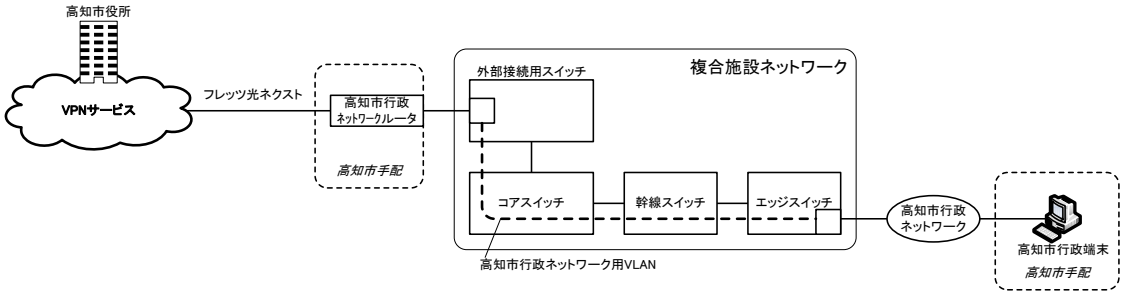

図 2-2-5.1 高知市行政ネットワーク接続構成

2-2-6 リモートアクセス

高知市民図書館移動図書館車から、移動体通信を利用した新図書館情報システムの利用は、移動体通信提供業者が提供するデータ通信を利用したインターネット経由でのＶＰＮ接続にて行う。

クライアントとなる端末は限定し、ＶＰＮサーバは、ファイアウォール（またはインターネット接続用のルータ）のＶＰＮ機能を利用する。

ＶＰＮ方式は、ＳＳＬ－ＶＰＮ（相性を考慮しトンネルモードを利用）又は、専用クライアントソフトを利用したＩＰｓｅｃとする。

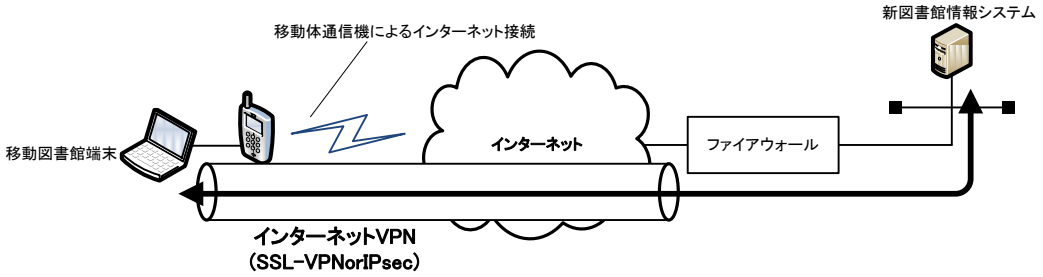

図 2-2-6.1 リモートアクセス概要図

2-2-7 高知新聞社

高知新聞記事検索データベースの利用のための、高知新聞社との接続については、フレッツ光ネクスト（品目はハイスピードを予定）を利用し、現行の県立図書館との接続で利用しているＶＰＮサービス【フレッツＶＰＮワイド】の新たな利用者として参加する。

なお、本接続については複合施設ネットワークとＶＬＡＮ接続するかを含め、詳細設計段階にて、高知新聞社と打合せを行い最終的に構成を決定することとする。

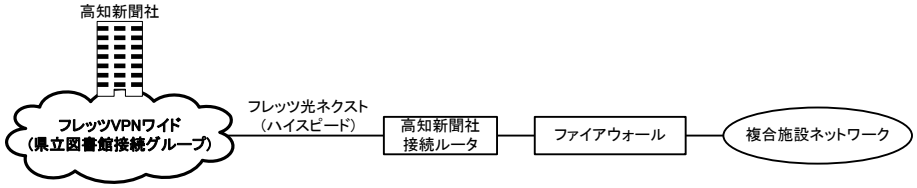

図 2-2-7.1 高知新聞社接続構成

2-3 無線ＬＡＮネットワーク

2-3-1 無線ＬＡＮ構成概要

複合施設無線ＬＡＮは、利用者（職員、来館者共）が施設内のどこでも利用できる事を前提とした無線ＬＡＮアクセスポイント（以降アクセスポイント又はＡＰという）の配置構成とし、アクセスポイントの配置間隔は、５ＧＨｚ帯での利用及びＩＰ電話の利用を考慮して、密な間隔で配置する。なお、アクセスポイントは集中管理型とし、無線ＬＡＮコントローラからの一元管理を行う。

2-3-2 伝送規格

利用する伝送規格は、ＩＥＥＥ８０２．１１ｂ／ｇ／ｎ（２，４ＧＨｚ帯）及び、ＩＥＥＥ８０２．１１ａ／ｎ（５ＧＨｚ帯）の同時利用（デュアルバンド）とする。

但し、電波干渉等の影響によるスループットの低下を考慮し、５ＧＨｚ帯を優先して利用するようにアクセスポイント等を設定する。

2-3-3 無線ＬＡＮ対象セグメント

無線ＬＡＮ利用対象セグメントは以下とし、セグメント毎にＳＳＩＤを設ける。

なお、ＳＳＩＤは、当該セグメントに割当てれらているＶＬＡＮに紐付けるようにする。

- 新図書館業務セグメント
- 新点字図書館セグメント
- 新点字図書館ボランティアセグメント
- こども科学館（仮称）セグメント
- こども科学館（仮称）ボランティアセグメント
- 来館者セグメント
- 音声ネットワークセグメント

2-3-4 無線セキュリティ通信

無線ＬＡＮ端末が利用する無線通信のセキュリティ規格は以下とする。

- 業務系セグメント：ＷＰＡ２－ＰＳＫ、又はＷＰＡ２－エンタープライズ
- 音声系セグメント：ＷＥＰ、又はそれ以上のセキュリティ規格
- 来館者セグメント：認証はオープン（ＳＳＬ通信)、認証後はＷＰＡ２でも使えること

※認証については、2-4-1 端末認証に記載の認証を利用予定である。

2-3-5 無線通信のトラフィック経路

無線ＬＡＮクライアントからの通信トラフィック経路は、無線ＬＡＮコントローラ経由の通信と、アクセスポイントからの直接通信のいずれかを選択可能となる。どちらを採用するかについては、詳細設計にて他の装置との兼ね合い（セキュリティ事項等）を検討した上で、判断する。

2-3-6 アクセスポイントの電源供給

アクセスポイントの電源はＰｏＥ（Power over Ethernet）給電とし、アクセスポイントを接続するスイッチから供給を行う。
※スイッチは、１ポートで最大３０Wを出力可能なＩＥＥＥ８０２．３ａｔ（ＰｏＥ＋）規格に対応のものとする。

2-3-7 アクセスポイントの予定設置台数

現状で設置を予定しているアクセスポイントの設置台数は以下の通りである。

表 2-3-7.1 アクセスポイント設置台数(予定)

設置フロア	設置台数
１Ｆ	13
２Ｆ	27
Ｍ３Ｆ	16
３Ｆ	26
Ｍ４Ｆ	15
４Ｆ	22
Ｍ５Ｆ	13
５Ｆ	8
ＲＦ	1
合計	141

2-4 セキュリティ

2-4-1 端末認証

業務ネットワークへの不正アクセスの抑止や、利用者の特定を目的として、一部のネットワークは端末認証機能を利用する。認証は、多様な認証プロトコルに対応する事が可能なよう、統合認証サーバとは別立てで専用の認証サーバを設ける。

なお、認証はクライアント系の端末が接続されるネットワークのみを対象とし、システム系で利用するネットワークは対象外とする（複合施設外のネットワークも対象外)。また、認証方法は、同じネットワークであれば、基本的には有線、無線に関わらず同じ方法での認証を行う。

各ネットワークで想定している認証方法は以下の通りである。

1) 来館者ネットワーク

・ Ｗｅｂ認証

来館者の持込み端末を、来館者ネットワークに接続後、ブラウザを起動して認証画面にアクセスし、ＩＤ、パスワード認証を行い、インターネット等へのアクセスを許可する。

なお、本認証にあたってのアカウントの管理・運用方法は、詳細設計にて以下の検討を行う。

- アカウント作成方法及び作成手順
  利用者自身で自己登録可能なシステムを導入する
- 利用者へのアカウントの提供方法
- アカウントの有効期限
  一定の期限を設け再認証を行う
- アカウントの管理
  有効期限を持たす場合での期限切れアカウントの取扱い（削除等）

2) 業務系ネットワーク

以下の認証を利用する。

・ ＩＥＥＥ８０２．１ｘ(ＥＡＰ－ＰＥＡＰ)＋ＭＡＣバイパス認証

サーバ、端末(クライアント)の双方向で認証を行う方法。サーバ側は証明書を用いた認証で、クライアント側はユーザＩＤ/パスワードでの認証。

・ ＭＡＣアドレス認証
機器のＭＡＣアドレスを認証に用いる方法。

※原則ＩＥＥＥ８０２．１ｘ（ＥＡＰ－ＰＥＡＰ）＋ＭＡＣバイパス認証を使用するが、ネットワークの重要度に応じてＭＡＣアドレス認証も併用する。

2-4-2 セグメント間の通信ポリシー

セグメント間の通信ポリシーは、以下を基本ポリシーとしてコアスイッチへのアクセスフィルター、ファイアウォールへのアクセスポリシーを設定する。
※ インターネットへは全てのセグメントからのアクセスを許可する。

表 2-4-2.1 セグメント間基本通信ポリシー

項番	通信元セグメント	アクセス許可セグメント
1	新図書館業務セグメント 市民図書館業務セグメント	新図書館情報システムセグメント 新図書館用サーバセグメント インフラサーバセグメント 公開サーバセグメント ｉＤＣサーバセグメント
2	新図書館ＯＰＡＣセグメント 市民図書館ＯＰＡＣセグメント	新図書館情報システムセグメント（ＯＰＡＣのみ） インフラサーバセグメント（一部のサーバへのみ） ｉＤＣサーバセグメント（ウイルス対策のみ）
3	新点字図書館セグメント	新点字図書館用サーバセグメント 新点字図書館ボランティアセグメント インフラサーバセグメント 公開サーバセグメント
4	新点字図書館ボランティアセグメント	新点字図書館セグメント 新点字図書館用サーバセグメント
5	こども科学館（仮称）セグメント	こども科学館（仮称）用サーバセグメント こども科学館（仮称）ボランティアセグメント インフラサーバセグメント 公開サーバセグメント
6	こども科学館（仮称）ボランティアセグメント	こども科学館（仮称）セグメント こども科学館（仮称）用サーバセグメント
7	来館者セグメント	
8	ｉＤＣサーバセグメント	全セグメント（来館者、委託業者セグメント除く）
9	インフラサーバセグメント	業務系全セグメントとＯＰＡＣセグメント
１０	新図書館用サーバセグメント	新図書館業務セグメント 市民図書館業務セグメント
１１	新点字図書館用サーバセグメント	新点字図書館セグメント 新点字図書館ボランティアセグメント
１２	こども科学館（仮称）用サーバセグメント	こども科学館（仮称）セグメント こども科学館（仮称）ボランティアセグメント

項番	通信元セグメント	アクセス許可セグメント
１３	システム管理セグメント	全セグメント
１４	音声ネットワーク	※プレゼンス機能を利用する場合は、各業務セグメントへのアクセスを許可。

2-4-3 インターネットアクセスのセキュリティ

インターネットアクセスにおけるセキュリティポリシー及び、利用するセキュリティ機能について以下に記載する。

1) インターネットアクセスポリシー

インターネットへのアクセスポリシーは以下を基本ポリシーとし、ファイアウォールにてアクセス制限を行う。

表 2-4-3.1 複合施設からのインターネットアクセス

項番	アクセス元	アクセスポリシー
1	各業務系セグメント システム系セグメント 各ボランティアセグメント 各委託業者セグメント	基本は制限無しとし、明確に不要な通信のみを遮断 （Ｗｉｎｄｏｗｓファイル共有、ＲＰＣ等）
2	来館者セグメント	Ｗｅｂアクセスのみ等、必要最低限の通信のみを許可

表 2-4-3.2 インターネットから複合施設へのアクセス

項番	アクセス先	アクセスポリシー
1	公開サーバ群 新図書館情報システム	公開するサービスで必要な通信のみを許可
2	グループウェアサーバ	高知市・高知県グローバルアドレスからグループウェアサーバへのＨＴＴＰ又はＨＴＴＰＳ通信のみ許可
3	その他	全て遮断

2) Ｗｅｂフィルタリング

インターネットへのＷｅｂアクセスは、不正なサイト等へのアクセスを防止する事を目的として、Ｗｅｂフィルタリングを実施する。

Ｗｅｂフィルタリングは、ファイアウォール又はルータのオプション機能を利用し※、利用者端末への設定等を行わずに利用できるようにする。

本フィルタリングは、複合施設ネットワーク内からインターネットへＷｅｂアクセスする全ての端末機器を対象とする。但し、全ての機器を同じ制限設定にはせず、利用端末や利用者の用途に応じて制限内容を変更する。（業務用は制限を緩めにする、来館者用は制限を厳しくする等）

※但し、詳細設計でのセキュリティ設計で、きめ細かい制御が必要と判断された場合は、専用のアプライアンス機等で稼働対応する。

3)　不正侵入検知/防御（ＩＰＳ）

インターネットからの不正な侵入を防ぐ事を目的に、不正侵入検知/防御（ＩＰＳ）を利用する。

ＩＰＳは、ファイアウォールのオプション機能を利用し、インターネットから公開サーバへアクセスする際に機能するよう設定し、侵入を検知した場合のデフォルトアクションは通信遮断とする。なお、誤検知が多い場合は、デフォルトアクションを見直す事とする。

4)　スパム対策

スパムメール対策として、アンチスパム機能を利用する。

アンチスパムは、ファイアウォールのオプション機能を利用する事とし、公開メールサーバのメール受信時に機能するよう設定する。

スパムと判断されたメールは、スパムと判別された事を示すタグを付与して公開メールサーバへ送信し、スパムメールの処理（削除等）は実際にメールを受信するメールソフトにて行うようにする。

5)　ウイルス対策

ウイルス対策は、来館者端末及び、一部の委託業者セグメント（委託業者が独自で整備したセグメント）の端末を除き、ウイルス対策ソフトがサポートしている全てのＯＳを搭載する全ての端末にソフトをインストールする。

2-5　トラフィック制御（ＱｏＳ）

複合施設内のトラフィック制御は、音声ＶＬＡＮの通信を最優先で通すよう構成する事とし、その他トラフィックは必要に応じ優先度合いを変更するようにする。

3 インフラシステム機能設計

複合施設ネットワークにおけるインフラシステムの機能（要件）概要について以下に記載する。

3-1 認証基盤システム【Active Directory】

① 複合施設ネットワークのＷｉｎｄｏｗｓドメイン管理を行い、Ｗｉｎｄｏｗｓ端末のログイン認証を行う。
② Ｗｉｎｄｏｗｓ端末の動作について、グループポリシー機能により管理を行う。
③ 他システムと連携可能な認証サーバとして利用する。

3-2 情報共有システム【グループウェア】

以下に記載の機能を利用する。

① 認証基盤システムとの連携機能
② 個人によるポータル作成機能
③ スケジュール管理機能
④ 個人による任意のメンバーのスケジュール一覧表示機能
⑤ 掲示板機能
⑥ 施設、備品予約管理機能
⑦ ファイル管理機能
⑧ メールサーバを利用しない各職員へのメッセージの送受信機能
⑨ Ｗｅｂメール（マルチアカウント対応）機能
⑩ 複合施設ネットワーク外へのメール送信機能。メール機能(ＳＭＴＰ)を有しない場合は、外部のメールサーバとの連携による複合施設ネットワーク外へのメール送信機能。
⑪ 公開メールサーバが受信したメールの受信機能
⑫ 任意のメンバーから成るグループで情報共有出来るポータル機能
⑬ 各機能の最新情報をトップページ表示機能
⑭ 柔軟なアクセス権の設定機能
⑮ 個別 ID 登録だけでない、Active Directory 連携機能
⑯ 複合施設外（インターネット）からのアクセスを可能とする（ファイアウォール等と連携）

3-3 情報配信システム【デジタルサイネージ】

以下に記載の機能を利用する。

① 2か所（こども科学館（仮称）内、図書館内）でのコンテンツの作成機能
② 簡便な操作でのデジタルサイネージのコンテンツの作成機能
③ コンテンツ再編集機能
④ 複数コンテンツの作成機能
⑤ 分単位でのデジタルサイネージのコンテンツ再生スケジュールを設定機能
⑥ 年間を通してのデジタルサイネージのコンテンツ再生スケジュール設定機能
⑦ 以下の形式のファイルを取込み、再生機能
・【静止画】　．ｊｐｇ．ｊｐｅｇ．ｂｍｐ．ｇｉｆ．ｐｎｇ
・【動画】　．ａｖｉ．ｍｐｅｇ．ｍｐｇ．ｗｍｖ．ａｓｆ
・【Ｆｌａｓｈ】．ｓｗｆ
・【ＰｏｗｅｒＰｏｉｎｔ】．ｐｐｔ．ｐｐｓ
・【HTML】．ｈｔｍ．ｈｔｍｌ
・【音声】　．ｗａｖ．ｍｐ３．ｗｍａ．ｍｉｄ．ｍｉｄｉ

3-4 その他基盤システム

3-4-1 プレゼンス機能

各業務端末にログインしたユーザー間で、チャットのようなリアルタイム通信機能（インスタントメッセージ機能）を実現する。

なお、建築の弱電設備（音声系システム構築業者）として設計を進めている構内電話を、従来型構内交換機（ＰＢＸ）ではなくＩＰネットワーク上で動作するサーバ（呼制御サーバ）として構築した場合、呼制御サーバのパッケージ機能に同機能を有する（又はオプション機能として有する）可能性がある。

複合施設ネットワークの詳細設計の段階において、構内電話のＩＰ化が確定され、かつ本機能を有する場合は、複合施設ネットワーク側で独立システムとして構築するのか、構内電話側の機能を流用して構築するのかを、建築の弱電設備側と協議・検討した上で判断する。

3-4-2 内部ＤＮＳ機能

① 複合施設ネットワーク内の各ネットワーク機器、システム、端末が名前解決時に利用する。
② 後述する複合施設独自ドメインのゾーン管理を公開ＤＮＳサーバとは別で行い、複合施設公開サーバへのアクセスを内側から行えるように、名前解決を可能にする。

3-4-3 ＮＴＰ機能

複合施設ネットワーク内の、各ネットワーク機器、各システム、端末の時刻同期サーバとして利用する。

3-4-4 ＤＨＣＰ機能

複合施設ネットワーク内の端末に対し、動的にＩＰアドレスの割当てを行う。

3-5 ウイルス対策管理

① パターンファイル等の更新について、集中管理を行う。
② 物理ＯＳ及び仮想ＯＳでウイルススキャンが可能で、スキャン結果・稼働状況をｓｙｓｌｏｇ等のログに記録を行う。
③ リアルタイムスキャンと、オンデマンドスキャンを行う。

3-6 総合死活監視システム

① 複合施設ネットワークの各システム、ネットワーク機器の死活監視を行う。
② 複合施設ネットワークの各システムのリソース監視を行う。
③ 複合施設ネットワークの主要な経路部分のトラフィック監視を行う。
④ 各システム及び、ネットワーク機器のログの集中管理を行う。（ｓｙｓｌｏｇ）
⑤ 上記監視において異常を検知した時に、アラートメール等にて各管理者へ通知を行う。
⑥ その他必要となる監視機能等については、詳細設計以降に機能設計を行う。

3-7 インターネット公開システム

3-7-1 公開Ｗｅｂ（複合施設公開ホームページ）・ＣＭＳ

① 複合施設公開ホームページとして稼動させ、県民・市民への広報を行う事を目的とし、各種コンテンツの公開を行う。その他新図書館情報システムとの連携等を行う。
② ＣＭＳ、その他新図書館情報システムとの連携を行う。

公開Ｗｅｂと連携するＣＭＳの機能として下記を利用する。

③ スクリーンリーダによるホームページ音声読み上げへの対応
④ 文字の拡大縮小・表示色の変更機能
⑤ コンテンツ公開の承認ワークフロー機能
⑥ システム管理者、コンテンツ管理者、コンテンツ作成者での権限設定機能

3-7-2 公開ＤＮＳ機能

複合施設ネットワークの構築において取得する、独自ドメインのゾーン情報を管理し、インターネットへ公開する各サーバの名前解決を行えるようにする。
（インターネットからの複合施設ホームページへのアクセスＵＲＬ、メール受信についてのメールアドレスには本独自ドメインを使用する。）

3-7-3 メール機能

上記の独自ドメインのメールサーバ（ＳＭＴＰ及びＰＯＰ又はＩＭＡＰ）として機能させる。新図書館情報システム、グループウェア等と連携を行い、インターネット側とのメールの送受信を行う。

4 構成

複合施設ネットワーク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、新システム基本設計書と共通の資料として、以下の資料に記載する。

- 「新システム基本設計書 別紙 4-1 システム構成」
- 「新システム基本設計書 別紙 4-2 機器基本要件」
- 「新システム基本設計書 別紙 4-4 システム構成（4-1 ハードウェア構成一覧-ネットワーク)」
- 「新システム基本設計書 別紙 4-5 システム構成（4-3 ネットワーク構成)」

5 複合施設ネットワーク運用・維持管理計画

複合施設ネットワークにおける運用・維持管理計画については、新システム基本設計書と共通の資料として、以下の資料に記載する。

- 「新システム基本設計書 別紙 5-1 システム運用・維持管理計画書」

6 複合施設ネットワーク 構築実施計画

6-1 導入・稼働に必要な作業

複合施設ネットワーク構築に関する作業項目を分類し一覧にしたものについては、新システム基本設計書と共通の資料として、以下の資料に記載する。

・「新システム基本設計書 別紙 6-1 システム実施構築計画（6-1 導入・稼働に必要な作業)」

6-2 データ移行

複合施設ネットワークのインフラシステムは新規構築システムとなり移行元システムが存在しないため、データ移行については考慮しない事とする。

6-3 研修計画

複合施設ネットワークに関する職員研修の概要、スケジュール、研修コース、対象者等については、新システム基本設計書と共通の資料として、以下の資料に記載する。

・「新システム基本設計書 別紙 6-3 システム実施構築計画（6-3 研修計画)」

6-4 作業スケジュール

複合施設ネットワーク構築スケジュール（線表）について、新システム基本設計書と共通の資料として、以下の資料に記載する。

・「新システム基本設計書 別紙 6-4 システム実施構築計画（6-4 作業スケジュール)」

6-5 進捗管理・リスク管理の方法

複合施設ネットワークにおける、進捗管理及びリスク管理については、新システム基本設計書と共通の資料として、以下の資料に記載する。

・「新システム基本設計書 別紙 6-5 システム実施構築計画（6-5 進捗管理・リスク管理の方法)」