5 医院信息平台设计

5.1 平台需求分析

基于电子病历的医院信息平台主要解决两方面的问题，首先是实现医院信息系统应用整合的需求，其次是医院信息系统基础设施整合的需求。

5.1.1 医院信息系统应用整合需求

目前，我国医院信息系统应用仍未达到信息充分共享、业务协同和医疗智能化发展的要求。因此，建立医院信息平台就是为了实现院内应用系统的互联互通，形成全院级的病人主索引和电子病历，并在此基础上实现对医院信息资源的二次利用，为患者提供公众服务，建立与外部系统互联的统一接口，满足区域的信息共享与协同以及医疗行为监管的要求。

根据业务梳理和分析，医院信息系统分为临床服务域、医院管理域以及平台应用域。其中临床服务域、医院管理域包括大量的医院基本业务系统。基于电子病历的医院信息平台需支持医院信息系统中纵向和横向的数据交换及信息共享。

从纵向看，在医院内部病人的电子病历信息，是一个纵向不断增加的信息集合，准确和连续的病历信息是高质量医疗活动的基础和保障。在医院外部，病人电子病历需要向区域卫生信息平台提供最新的治疗记录和检验报告，需要向上级医疗卫生部门上报重要的个案信息和管理统计信息。

从横向看，医院内部各科室使用的应用系统，也需要大量的信息交换，比如计费和门诊药房系统之间需要共享病人信息、交费记录、药品信息等。医生工作站系统需要和手术系统共享手术安排信息和病人体征信息等等。

医院信息协同的需求越来越普遍，医院和其他医疗相关机构之间的协同和信息交换、医院和病人的信息交换和沟通需求催生了许多新应用，如远程医疗、病人自我服务等。这些新应用需要在信息共享的基础上实现业务流程的整合和业务协同。如果没有平台的支持，无法做到对业务流程的有效监控管理及流程优化。

数据仓库和数据挖据是实现临床决策支持和管理决策支持的基础。要建立数据

仓库需要从现有业务系统中抽取数据，经过加工处理形成全院的临床和管理数据仓库，在此基础上进行数据挖掘，为医疗服务质量改进和管理水平提升提供决策支持。

5.1.1.1 全院级应用系统互联互通的需求

医院信息系统应用整合的首要需求是实现各医院应用系统之间的互联互通：

- 从集成的层面上，需要考虑三个层面：数据层面、应用/服务层面和流程层面。即各应用系统在数据层面可以相互交换，在应用层面可以互相调用，在流程层面可以协同在一起实现全院级的业务协同；
- 从集成的手段上，包括点对点集成和通过平台来集成。要实现全院级集成，应当通过平台化的手段来实现。

互联互通的核心是数据层面和应用层面的整合。具体来说，重点要解决医院信息系统的系统异构集成、数据共享和数据交换传输标准等关键性技术问题。全院各个应用系统均与医院信息平台互联，并通过医院信息平台实现相互之间的数据交换和应用服务的调用。

5.1.1.2 形成全院级病人主索引的需求

医院信息整合要解决的关键问题是患者信息的不统一。目前医院各个应用系统均有患者基本信息，但是数据的标准不统一，维护的方式不统一。临床医疗活动均是以患者为主线的，如果患者的信息不统一是无法实现电子病历等数据整合的。因此，必须要建立全院级统一的病人主索引，并以此为基础实现医院数据层面的整合，包括电子病历的数据整合以及医院业务和管理数据的整合。

5.1.1.3 建立全院级电子病历的需求

电子病历信息分散在 HIS、CIS、LIS、RIS/PACS 等各应用系统中。没有整合的电子病历，临床医疗服务人员无法了解服务对象的完整医疗活动情况。临床医疗服务人员需要通过全院级的电子病历去记录和查阅服务对象在所有医疗活动中产生的信息，掌握这些信息有利于提高医疗水平、降低医疗风险。

5.1.1.4 医院信息资源二次利用的需求

以电子病历为核心的医院信息平台还可以整合医疗业务和医院管理的数据，即建立全院级的信息资源中心。信息资源中心不仅能直接服务于医院业务应用，也可以用于二次利用。二次利用包括三个方面：医院管理辅助决策、医院临床辅助决策

以及临床教学和科研。

5.1.1.5 为患者提供公众服务的需求

基于医院内部系统协同、数据的整合及信息资源的二次利用，可以通过电子化的手段为患者提供信息服务，方便患者就医。例如，可以通过短信或电子邮件把检验报告的结果发送给患者，患者无需去医院取检验报告；甚至可以在门户网站上提供诊疗信息查询功能，这样患者可以查询到历次的处方、检验报告、检查报告等诊疗信息；患者可以在家预约挂号。

5.1.1.6 与外部系统互联的需求

在没有建立统一的医院信息平台以前，医院外部系统根据自己的需要直接与医院内部的某些系统进行单点的对接。例如医疗保险系统需要与 HIS 系统作接口，完成医保费用的结算和审核，区域检验中心与 LIS 系统作接口，区域影像中心与 RIS/PACS 系统作接口，卫生统计与病案系统作接口等。这样医院信息系统就会有多种不同的途径与外界对接。每个系统的数据、网络、安全等接入方式各不相同。给医院的运维造成很高的复杂性，特别是安全管理造成很大的隐患。

通过建立医院信息平台之后，医院信息平台成为与外部系统对接唯一的进出口。可以统一对外数据交换标准、提供多种灵活的对接技术、进行统一的运维，并且执行统一的安全策略。可以实现对医疗保险、新农合、公共卫生、区域卫生、第三方机构的统一对接和管理。

5.1.2 医院信息系统基础设施整合需求

系统基础设施为医院信息平台及各应用系统提供服务和支撑，应具有良好的伸缩性，以平台的方式来为所有系统提供统一服务，以满足医院不断变化的业务需求。

系统基础设施的设计，应充分考虑医院现有基础设施部署状况，并根据未来医院的发展，依据医院信息平台及各应用系统的需求，从计算能力、可管理性、可靠性/可用性、安全等角度来全面考虑。

系统软件基础设施包括：操作系统、数据库、基础软件、系统管理软件、安全及访问控制软件等。

系统硬件基础设施包括：服务器、存储、网络、安全及访问控制等相关的硬件基础设施。

服务器部署应具有较好的灵活性和伸缩性，通过虚拟化以及其他技术的应用来整合物理服务器资源，为医院信息平台及各应用系统提供硬件支撑和服务。

存储基础设施集中存放医院内外部应用数据。数据的可管理性、安全性、高效性非常重要，直接影响着医院服务的效率和业务的连续。因此，在存储设备建设过程中要除了要考虑存储系统的可靠性、安全性、性能等因素，还要顾及整个存储系统的统一管理、数据的本地保护和异地容灾备份。

鉴于医院业务涉及公民的生命安全、个人隐私、医学资料等关键信息，对网络架构的性能、稳定、安全、容灾、管理等都提出了很高的要求，以满足医院 7×24 小时连续服务、大容量医学影像数据传输、随时随地的无线业务终端接入、数据信息的保密和网络安全性方面的需求。

此外，系统基础设施的构建，应该从医院信息系统整体来进行考虑。服务器、存储和网络，应当统一进行规划，采取统一管理、统一运维等手段，以提供更好的服务水平。

5.2 平台体系架构概要

5.2.1 设计原则

医院信息平台体系架构设计应遵循以下原则：

- 基于医院信息化现状，实现信息共享与业务协同。即医院信息平台的建设不是一个推翻现有应用重建的过程，而是基于现有信息系统和现有的系统数据，通过医院信息平台来整合信息，并实现系统之间的业务协同。
- 基于企业信息架构分层设计思路。按照企业信息架构理论和方法，以分层的方式设计医院信息平台，不同的层次解决不同的问题。
- 覆盖医院信息系统建设全生命周期。不仅包括从技术角度医院信息平台本身如何设计和建设，还包括医院信息平台项目管理、系统运维以及相关的信息安全保障体系。
- 全面支持电子病历相关业务规范与标准体系。从数据层面遵循《电子病历

基本架构与数据标准》，即医院信息平台上保存的电子病历数据符合该标准；在电子病历生成和使用上符合电子病历相关业务规范。

5.2.2 总体架构

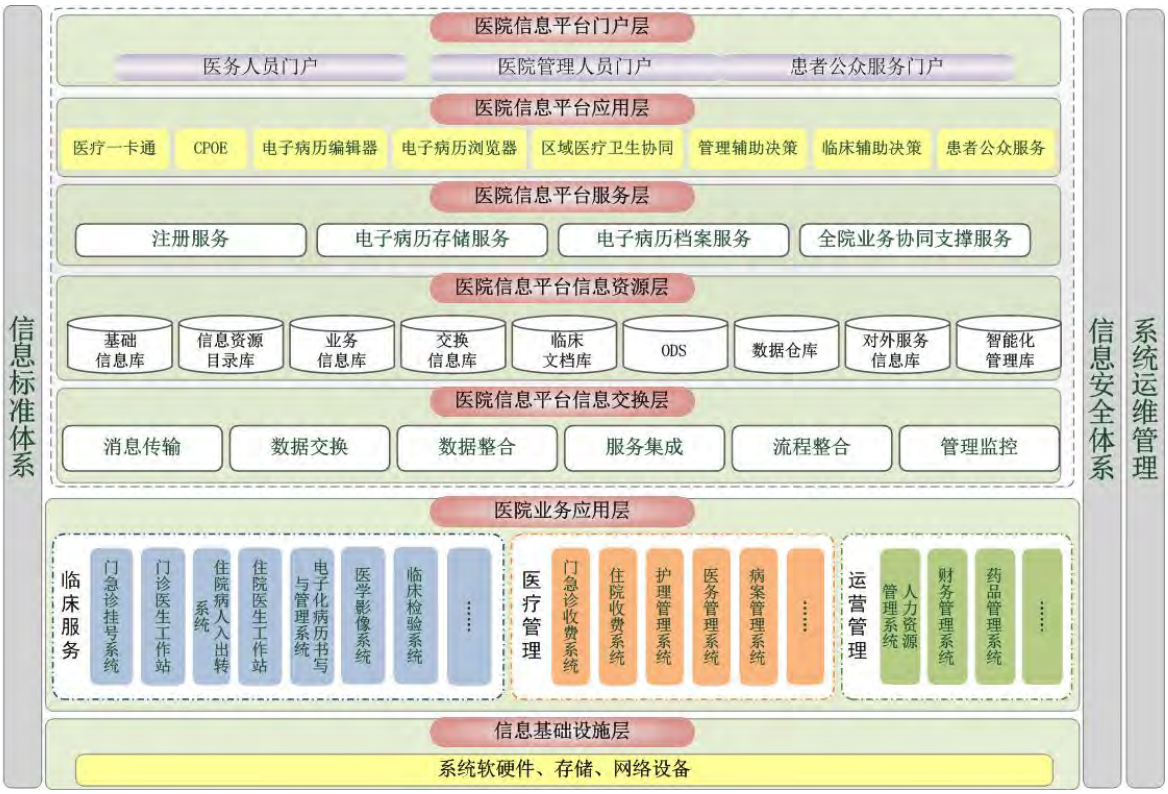

图 5-1　医院信息平台总体架构

如上图所示，医院信息平台的总体架构设计分为九个部分，包括：医院信息平台门户层、医院信息平台应用层、医院信息平台服务层、医院信息平台信息资源层、医院信息平台信息交换层、医院业务应用层、信息基础设施层以及信息标准体系、信息安全体系与系统运维管理。其中图中上半部分包括的医院信息平台门户层、医院信息平台应用层、医院信息平台服务层、医院信息平台信息资源层、医院信息平台信息交换层是属于医院信息平台的软件部分，主要服务于医院信息系统应用整合的需求；医院业务应用层是目前医院内部的业务应用系统，是医院信息平台的基础；信息基础设施层以及标准规范和信息安全与系统运维管理服务于医院业务应用系统和医院信息平台，信息基础设施层主要服务于医院信息系统基础设施整合的需求。

医院信息平台信息交换层，主要用于实现全院级应用系统互联互通的需求；医院信息平台信息资源层，主要服务于建立全院级的病人主索引的需求、建立全院级电子

病历的需求，并为医院信息二次利用、为患者提供公众服务、与外部互联奠定数据基础；医院信息平台应用层包含了建立在医院信息平台信息资源层、医院信息平台服务层、医院信息平台信息交换层的基础上的全院级应用。

5.2.2.1 医院信息平台门户层

门户层是整个医院信息平台对内和对外使用和展示的界面，根据不同的使用者可以分为：

1）医务人员门户：针对医务人员，提供 Web 应用的统一入口，医务人员所有的医院 Web 应用在该门户上使用。详见**第六章中基于平台的应用。**

2）医院管理人员门户：针对医院管理人员，提供 Web 应用的统一入口，医院管理人员所有的医院 Web 应用在该门户上使用。特别是提供统一的管理辅助决策和临床辅助决策应用。详见**第六章中基于平台的应用。**

3）患者公众服务门户：针对患者，提供各项信息化的医疗服务。详见**第六章中患者公众服务部分。**

医院信息平台门户层的具体支撑技术，请详见**本章平台基础设施架构设计中的门户服务器部分。**

5.2.2.2 医院信息平台应用层

医院信息平台应用层基于医院信息平台，通过基础业务数据的交换、共享和整合，结合实际的医疗业务和管理需要，建立扩展应用。主要包括：医疗一卡通、计算机化医嘱录入（CPOE）、智能电子病历编辑器、电子病历浏览器、区域医疗卫生协同、管理辅助决策支持、临床辅助决策支持和患者公众服务等。

医院信息平台应用层的具体内容，请详见**第六章基于平台的应用与协同部分。**

5.2.2.3 医院信息平台服务层

医院信息平台服务层的主要任务是为平台提供各种服务。医院信息平台服务层的具体内容，请详见**本章的平台软件架构中的注册服务、患者主索引、电子病历存储服务、电子病历档案服务、全院业务支撑服务等部分。**

5.2.2.4 医院信息平台信息资源层

医院信息平台信息资源层用于整个平台各类数据的存储、处理和管理，主要包

括：信息目录库、基础信息库、业务信息库、临床文档信息库 CDR、交换信息库、操作数据存储 ODS、数据仓库、对外服务信息库、智能化管理信息库。

医院信息平台信息资源层的具体内容，请详见**本章的平台软件架构中的数据架构部分。**

5.2.2.5 医院信息平台信息交换层

医院信息平台信息交换层的主要任务以满足临床信息、医疗服务信息和医院管理信息的共享和协同应用为目标，采集相关业务数据，并对外部系统提供数据交换服务，包括与区域平台的数据交换。

信息交换层为整个平台的数据来源提供了技术基础和保障，通过信息标准、交换原则的制定，对业务系统提供标准的信息交换服务，确保数据交换过程的安全性、可靠性，实现数据在系统平台范围内自由、可靠、可信的交换。

医院信息平台交换层的具体内容，请参考**本章的平台软件架构中的医院信息系统集成部分。**

5.2.2.6 医院业务应用

医院业务应用是医院信息平台的基础。包括三大类业务系统：医疗服务系统、医疗管理系统以及运营管理系统。业务应用层要接入到医院信息平台，向平台提供诊疗数据，同时，也要从平台获得业务协同支持。

（1）临床服务系统

临床服务系统是指以病人为中心，实现患者临床诊疗活动全过程的数字化运作。主要包括门急诊挂号系统、门诊医生工作站、分诊管理系统、住院病人入出转系统、住院医生工作站、住院护士工作站、电子化病历书写与管理系统、合理用药管理系统、临床检验系统、医学影像系统、超声/内镜/病理管理系统、手术麻醉管理系统、临床路径管理系统、输血管理系统、重症监护系统、心电管理系统、体检管理系统。

（2）医疗管理系统

医疗管理系统是指对医院医疗活动和医疗费用进行全过程监控，保障医院医疗活动的质量和安全，合理控制医疗费用。主要包括门急诊收费系统、住院收费系统、护理管理系统、医务管理系统、院感/传染病管理系统、科研教学管理系统、病案管理系统、医疗保险/新农合接口、职业病管理系统接口、食源性疾病上报系统接口。

（3）运营管理系统

运营管理系统是指医院“物流、资金流、信息流、业务流”的统一管理。主要包括人力资源管理系统、财务管理系统、药品管理系统、设备材料管理系统、物资供应管理系统、预算管理系统。

5.2.2.7 信息基础设施层

信息基础设施层是支撑整个医院信息平台运行的基础设施资源，主要包括各类系统软件、系统硬件、数据存储、网络设备、安全设备等。

医院信息基础设施层的具体内容，请详见**本章的平台基础设施架构概要、平台基础设施架构设计部分。**

5.2.2.8 信息安全体系与系统运维管理

信息安全体系与系统运维管理是整个平台建设和运作的重要组成部分，也应该贯穿项目建设的始终。其中，信息安全不仅包括技术层面的安全保障（如网络安全、系统安全、应用安全等），而且还包括各项安全管理制度，因为只有在一系列安全管理的规章制度实行的前提下，技术才能更好地为安全保障作出贡献。同时，完善的系统的运维管理也是系统稳定、安全运行的重要保障。

信息安全体系与系统运维管理的具体内容，请详见**第 7 章安全保障体系部分和第 9 章运维管理部分。**

5.2.2.9 标准规范

标准规范应该是贯穿于医院信息化建设的整个过程，通过规范的业务梳理和标准化的数据定义，要求系统建设必须遵循相应的规范标准来加以实施，严格遵守既定的标准和技术路线，从而实现多部门（单位）、多系统、多技术、以及异构平台环境下的信息互联互通，确保整个系统的成熟性、拓展性和适应性，规避系统建设的风险。

5.2.3 平台软件架构概要

医院信息平台软件架构在功能上，覆盖总体架构上面的 4 个层次，即医院信息平台应用层、医院信息平台信息资源层、医院信息平台服务层、医院信息平台信息交换层。医院信息平台应用层的功能请参考**第六章。**

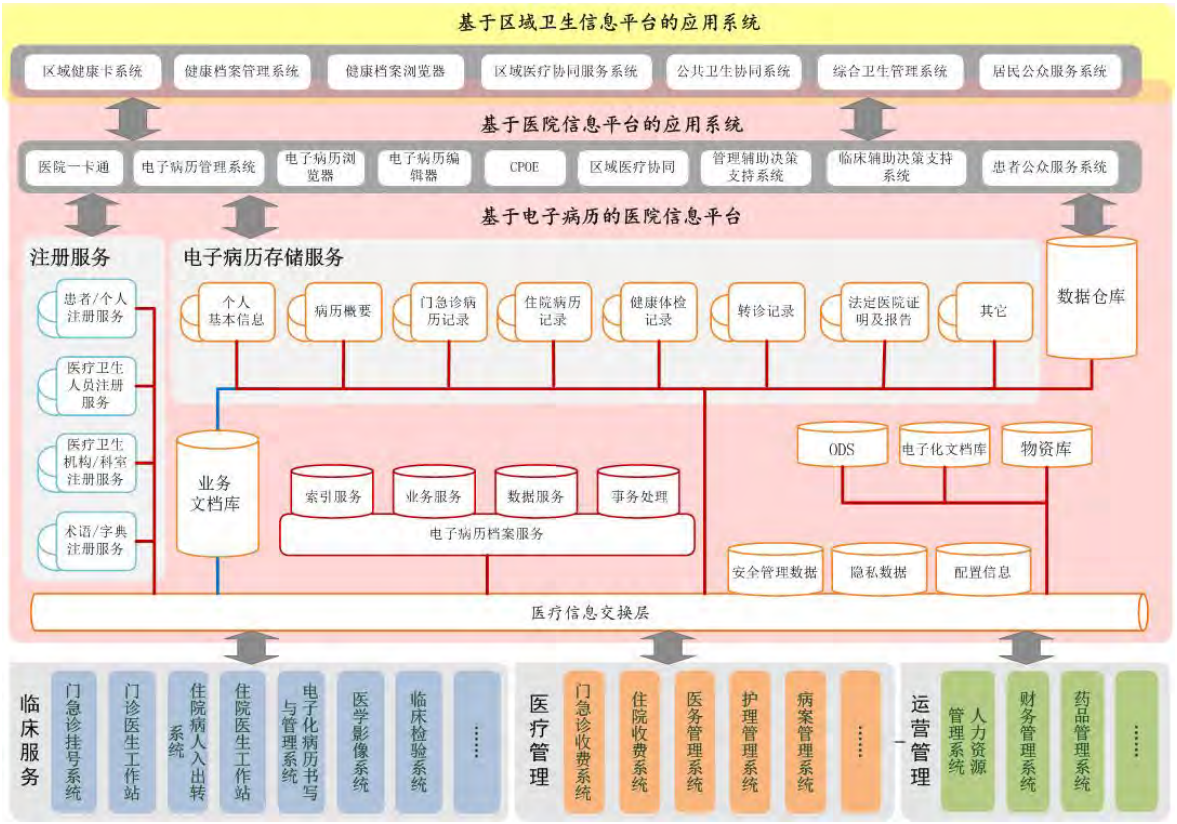

图 5-2　软件架构图

医院信息平台软件架构包括四个层面：图的核心部分是医院信息平台及基于医院信息平台的应用系统；医院信息平台接入临床服务、医疗管理和运营管理各业务应用系统；医院信息平台对外接入区域卫生信息平台。医院信息平台内部又可细分为医院信息平台服务层和医疗信息交换层。

医院信息平台包括以下功能组件：

（1） 注册服务

注册服务包括对患者、医疗卫生服务人员、医疗卫生机构（科室）、医疗卫生术语的注册管理服务，系统对这些实体提供唯一的标识。针对各类实体形成各类注册库（如个人注册库、医疗卫生机构注册库等），每个注册库都具有管理和解决单个实体具有多个标识符问题的能力。注册库具有一个内部的非公布的标识符。

（2） 电子病历与临床数据存储（CDR）

电子病历是由医疗机构以电子化方式创建、保存和使用的，重点针对门诊、住院患者（或保健对象）临床诊疗和指导干预信息的数据集成系统。是居民个人在医疗机构历次就诊过程中产生和被记录的完整、详细的临床信息资源。按照以患者为

中心建立的 EMR 文档的存储带来了临床数据存储库 CDR(Clinical Data Repository)的形成。

（3） 电子病历浏览器

电子病历浏览器（即 EMR 浏览器）是为终端用户提供的访问个人电子健康记录的应用程序，提供电子病历的展现，建议采用 Web 方式实现。电子病历浏览器的目标是建立一个用户友好的环境，在该环境下被授权的医护专业人员或患者可以方便地访问电子病历中保存的相关数据。电子病历信息主要由临床信息组成，电子病历浏览器可以根据使用者的特定需求提供不同医疗卫生领域的调阅展示服务。

（4） 全院业务协同支撑服务

医院信息平台基于 SOA 架构设计，将各种类型的协同工具服务组件化，统一在信息平台上进行注册，提供服务调用适配器接口或 Web Service，以便平台的其他应用程序和组件利用协同组件工作。

（5） 医院信息交换层

医院信息平台的主要作用包括：

- 接入医院业务系统。
- 实现医院信息的统一管理：病人主索引、电子病历、决策支持数据、业务协同数据、对外服务数据、区域卫生共享和协同数据。
- 实现医院业务系统之间的协同。
- 基于以上三点，开发新型的应用，包括医疗一卡通、电子病历共享、医院管理服务决策支持、临床辅助决策、医院业务协同、对外公众服务、区域卫生共享和协同应用。

5.2.4 平台基础设施架构概要

基础设施架构对应总体架构图中的医院信息基础设施层。基础设施架构是支撑整个医院信息平台运行的基础设施资源、软硬件及网络等资源，主要包括三个方面的内容：系统软件、系统硬件及网络环境等。

系统软件包括：操作系统、数据库、基础软件、系统管理软件、安全及访问控制软件等。

系统硬件基础设施包括：服务器、存储、安全及访问控制等相关的硬件基础设施。

网络环境包括网络设备、安全设备、容灾备份等。

5.2.4.1 硬件基础设施架构概要

硬件基础设施包括：服务器、存储、网络、安全及访问控制等相关的硬件基础设施：

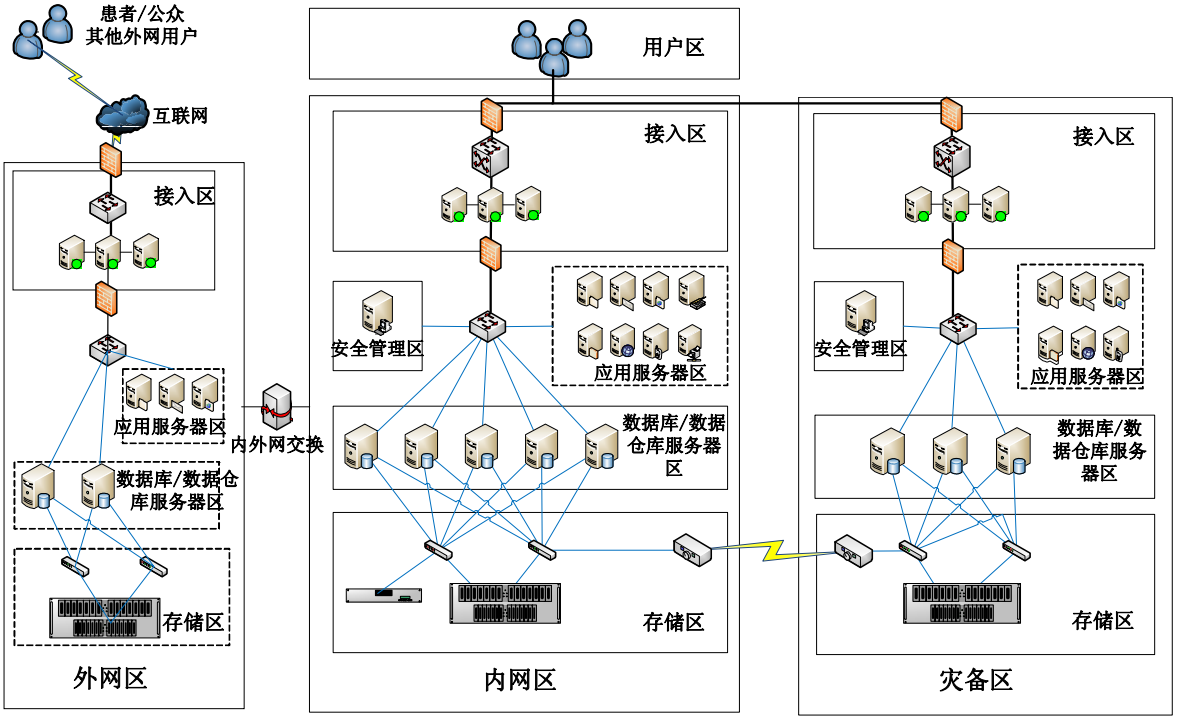

图 5-3 系统硬件基础设施架构图

在存储架构、网络架构中，将分别进行更为深入的描述，详细内容请参见相关章节。本节中主要描述服务器相关的架构。

服务器部署应具有较好的灵活性和伸缩性，通过虚拟化以及其他技术的应用来整合物理服务器资源，为医院信息平台及各应用系统提供硬件支撑和服务。

医院信息平台的服务器部署，主要包括 Web 服务器、应用服务器、数据库服务器等支撑医院信息平台和各应用系统的运行所需的服务器。这些不同类型的服务器与物理服务器之间不存在一一对应的关系，可以通过虚拟化技术实现灵活部署。系统管理、安全等系统则可能部署在单独的服务器上。

随着医院信息化水平的不断提高，医院信息平台及各应用系统所涉及的数据重要性突显，对于业务连续性的要求也更高。在系统基础设施的设计中，应充分考虑采用集群、冗余和备份等技术，来实现高可用性。对于较大规模的医院，可以建立灾备中心。当医院主数据中心发生故障或异常时，利用灾备中心继续提供服务。

不同规模的医院，所对应的系统硬件基础设施的规模也不同。在服务器部署、存储架构、网络架构等章节中，针对不同规模的医院提出了相应的解决方案，具体参见相关章节。

5.2.4.2 存储架构概要

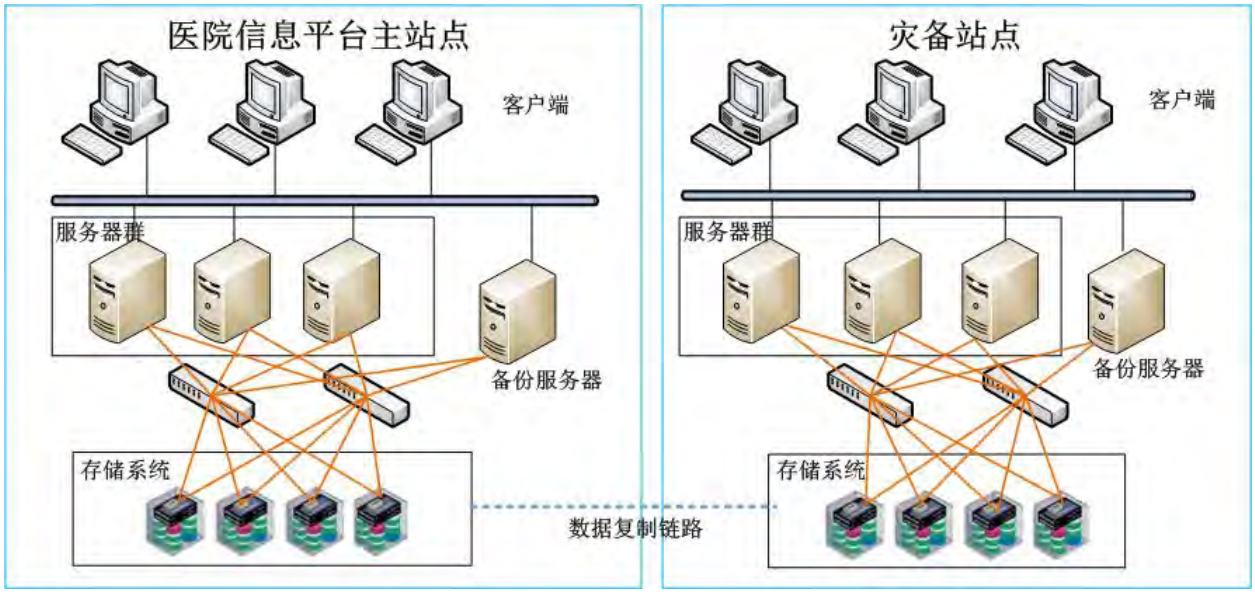

图 5-4 存储架构

根据医院信息平台数据存储的需求，整个存储系统的架构从三个层次来构建，主要包括：

1） 可靠的存储网络

为了支撑前端应用服务器的业务高效、稳定、安全运转，要求后端存储网络具备可靠的传输性能和安全性。

2） 本地数据的统一化存储和保护

存储系统能够兼容已有的存储系统，并纳入统一的管理平台下，实现存储系统的统一化管理和维护，同时为了保证业务的连续性，要求存储系统提供数据的安全保护。

3） 应用级数据容灾

为了减少人为或自然因素所导致的应用或系统中断，要求在存储系统具有应用级数据容灾功能，以保证医院业务的连续性。

5.2.4.3 网络架构概要

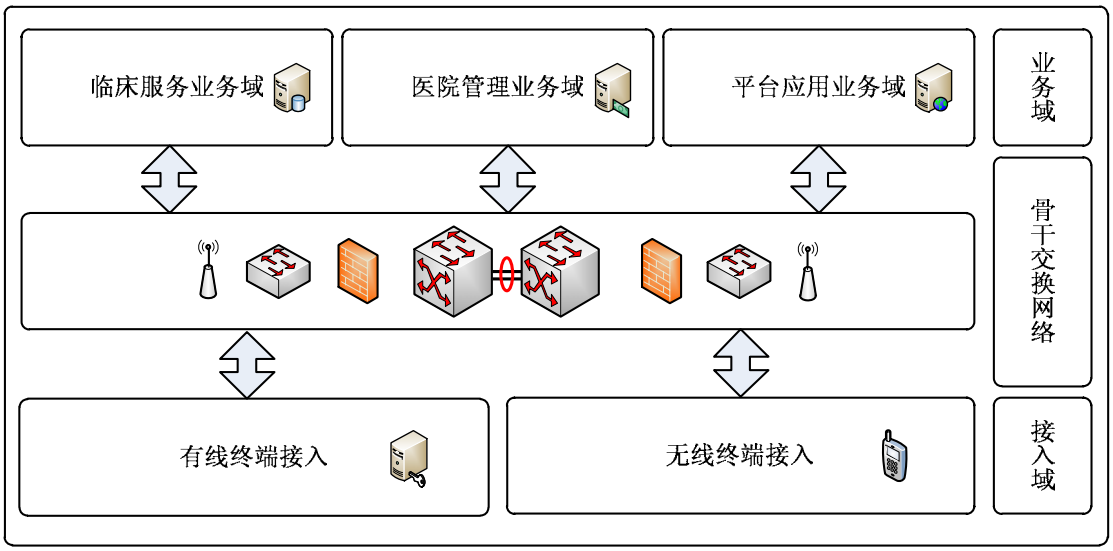

图 5-5 网络架构图

按照医院信息平台建设的设计框架，网络架构设计需满足医院 7×24h 连续服务、大容量医学影像数据传输，随时随地的无线业务终端接入，数据信息的保密和入网安全性方面的需求。医院信息平台网络架构主要由业务域、骨干交换网络和接入域构成。

骨干交换网络：用于连接业务域和接入域，为医患人员提供可靠、高速、安全、管理以及具备容灾抗灾能力的多业务承载网。包括网络设备、安全设备以及其他相关设备。

业务域：由临床服务、医院管理、平台应用三大子域构成，通过骨干交换网络与接入域进行通信，并为最终用户提供后端的服务，会承担较大的并发访问量，发生意外将可能导致全院业务中断。在设计中主要考虑冗余容灾及安全保护。

接入域：物理上由有线接入域和无线接入域构成，通过骨干交换网络访问业务域，是医院人员进行相关操作的第一线，面临的环境较为复杂且不好控制。在设计中主要考虑用户身份的真实性，敏感数据的保护以及非法接入及非法外联的防范。

按业务可将网络区域划分为：内网中心服务器区、外网中心服务器区(DMZ)、数据灾备区、骨干网络区、医疗专网出口区、互联网出口区、网络安全管理区、门诊终端接入区、住院终端接入区、医技终端接入区、无线终端接入区、行政终端接入

区、其他终端接入区，提供更强的策略控制及安全管理能力，具体设计参见网络架构设计章节。

5.2.5 平台安全体系概要

基于电子病历的医院信息平台安全体系框架需在国家政策、法律法规要求的指引的前提下，以安全基础设施为依托，与平台的业务流程、应用架构和数据资源紧密结合，从安全技术、安全管理为要素进行框架设计说明，它是平台安全保障体系的指导性架构。

基于电子病历的医院信息平台安全体系框架如下图所示：

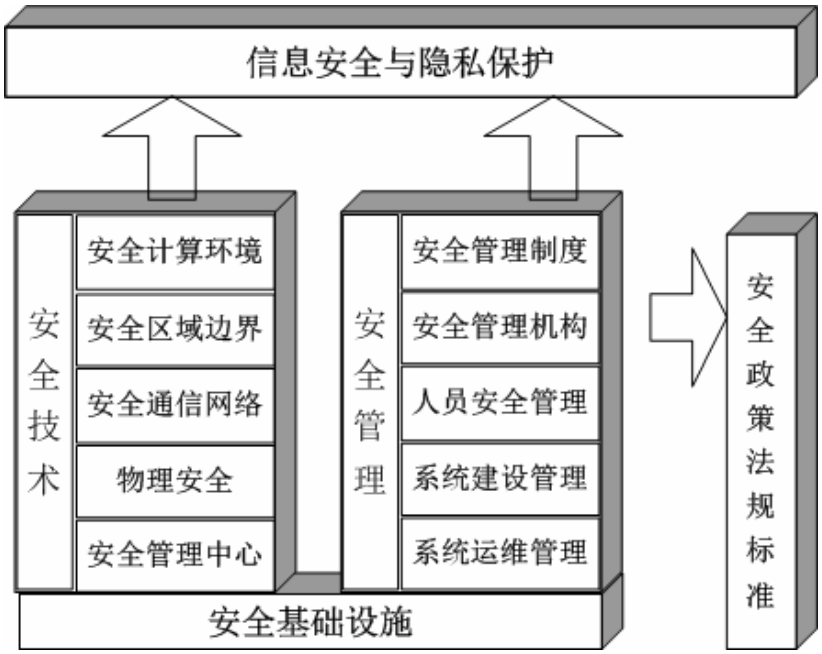

图 5-6 医院信息平台的信息安全体系总体框架

基于电子病历的医院信息平台安全体系总体框架包括：安全基础设施、安全技术、安全管理三部分：

◆ 安全技术

✧ 安全计算环境：安全计算环境解决基于电子病历的医院信息平台的计算机系统硬件和系统软件以及外部设备及其连接部件的系统安全，包括用户身份真实有

效、资源的访问控制、主机安全审计、重要数据的完整和可用性及数据的存储与备份恢复方面的安全。

✧ 安全区域边界：安全区域边界首先确立基于电子病历的医院信息平台的边界，并确定医院信息平台所在的安全计算环境与安全通信网络之间部件的安全，包括网络结构、边界的访问控制、协议过滤、安全审计、恶意代码防护及边界的入侵监控等。

✧ 安全通信网络：安全通信网络解决基于电子病历的医院信息平台所在的安全计算环境用于信息传输实施安全保护的部件的安全，包括数据传输的完整性和保密性、网络可信接入、抗抵赖等。

✧ 物理安全：物理安全是基于电子病历的医院信息平台所依附的设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏过程。

✧ 安全管理中心：安全管理中心是实现围绕基于电子病历的医院信息平台所制定的安全策略及所依托的安全计算环境、安全区域边界和安全通信网络上的安全机制得到统一管理，强制其策略下发及实现的过程管理等。

◆ 安全管理

安全管理建设需以基于电子病历的医院信息平台所服务对象为基础，来建立完善的安全管理体系，即建立相应的信息安全管理机构、制定相应的信息安全管理制度、设置平台运行所需的人员、岗位，建立对系统在运行开发过程中的制度，同时通过日常巡检、咨询、评估等运行管理来发现安全隐患并予以改进与提升。

◆ 安全基础设施

安全基础设施主要为基于电子病历的医院信息平台安全运行所需的防护部件，通过安全基础设施的安全互联、接入控制与边界防护、区域安全、通信安全、数据传输安全和安全管理等，为形成一体化的安全防护体系奠定基础。

5.3 平台软件架构设计

医院信息平台的使用对象主要是医务人员，最终的服务对象是居民和患者。医务人员为了更好的为居民和患者提供可靠的、可及的、连续的医疗服务，需要依赖平台提供的众多服务。平台软件架构包括注册服务、电子病历档案服务、电子病历存储服务，电子病历浏览器、全院级业务协同支撑服务、医院信息交换层等组成部分。

5.3.1 注册服务

注册服务用于医院信息平台各种共享服务资源的注册，通过服务资源的发布－发现－访问机制，实现服务资源共享。注册服务是医疗信息闭环系统中最基础的服务之一。

注册服务包括对患者、医疗卫生服务人员、医疗卫生机构（科室）、医疗卫生术语的注册管理服务，系统对这些实体提供唯一的标识。针对各类实体形成各类注册库（如个人注册库、医疗卫生机构注册库等），每个注册库都具有管理和解决单个实体具有多个标识符问题的能力。注册库具有一个内部的非公布的标识符。

5.3.1.1 患者注册

患者注册的目的

患者注册用于对前来医院就诊患者的基本信息进行管理，通过对病患者基本信息的统一管理，可以实现对患者信息最完整的保存，可以解决患者信息在各个系统中的不一致问题，以避免重复录入患者基本信息的情况。

患者注册服务在医院信息平台上，形成一个患者注册库，安全地保存和维护患者的诊疗标识号、基本信息，并可为医疗就诊及公共卫生相关的业务系统提供人员身份识别功能。

患者注册库主要扮演着两大角色。其一，它是唯一的权威信息来源，并尽可能地成为唯一的患者基本信息来源。其二，解决跨越多个信息系统时患者身份唯一性识别问题。患者注册服务是医院信息平台正常运行所不可或缺的，只有通过统一的患者注册管理，才能确保记录在医院各个信息系统中的患者被唯一地标识，各类诊疗业务数据通过统一管理的患者注册记录关联起来，最终形成患者在机构内的全局

共享诊疗信息记录。

患者注册信息模型

患者注册信息的主要内容按照卫生部 2009 年《电子病历基本架构与数据标准》的规定，应包括该标准的 H.02 服务对象标识、H.03 人口学、H.04 联系人、H.05 地址、H.06 通信、H.07 医保等数据组。

具体数据规定如下：

表 5-1 患者注册信息

临床数据组	数据元标识符（DE）	数据元名称	重复次数	定义	数据元值的数据类型	表示格式	数据元允许值
H.02 服务对象标识	HR01.01.002.01	标识号-类别代码	1..1	特定环境下本人身份标识（证明文件）号码的类别代码	S	N2	CV0100.03 个体标识号类别代码
	HR01.01.002.02	标识号-号码	1..1	特定环境下本人身份标识（证明文件）号码	S	N..30	
	HR01.01.002.03	标识号-生效日期	0..1	特定环境下本人身份标识（证明文件）号码的生效日期	D	D8	
	HR01.01.002.04	标识号-失效日期	0..1	特定环境下本人身份标识（证明文件）号码的失效日期	D	D8	
	HR01.01.002.05	标识号-提供标识的机构名称	0..1	提供本人身份标识的机构或单位的名称	S	AN..70	
	HR02.01.001.01	姓名-标识对象	0..1	姓名的标识对象,如本人姓名、户主姓名、母亲姓名、丈夫姓名等，默认值为本人姓名	S	A..20	CV0100.01 姓名类别代码
	HR02.01.001.02	姓名-标识对象代码	0..1	姓名的标识对象代码	S	N2	CV0100.02 姓名标识对象代码
	HR02.01.002	姓名	1..1	本人在公安户籍管理部门正式登记注册的姓氏和名称	S	A..30	
	HR42.01.012	病人类型代码		标识病人类型的代码	S	N1	病人类型代码

临床数据组	数据元标识符（DE）	数据元名称	重复次数	定义	数据元值的数据类型	表示格式	数据元允许值
H.02.001 个体生物学标识	HR51.03.003	ABO 血型	1..1	标识本人按照 ABO 血型系统决定的血型类别代码	S	N1	CV5103.02ABO 血型代码
	HR51.03.004	RH 血型	1..1	标识本人按照 Rh 血型系统决定的血型类别代码	S	N1	0.Rh 阳性 1.Rh 阴性 3.不详
H.02.002 个体危险性标识	HR01.03.001.01	个体危险性名称	1..1	个体危险性标识的名称	S	AN..20	
	HR01.03.001.02	个体危险性代码	1..1	个体危险性标识的类别代码	S	N2	个体危险性标识代码
H.03 人口学	HR02.02.001	性别代码	1..1	标识本人生理性别的代码	S	N1	GB/T 2261.1-2003 个人基本信息分类与代码 第 1 部分 人的性别代码
	HR02.03.001	年龄（岁）		人的生存年数，计量单位为岁	N	N..3	
	HR02.04.001	国籍代码	0..1	标识本人所属国籍的代码	S	AN3	GB/T 2659-2000 世界各国和地区名称代码
	HR02.05.001	民族代码	1..1	标识本人所属民族类别的代码	S	N2	GB 3304-1991 中国各民族名称的罗马字母拼写法和代码
	HR02.06.003	婚姻状况类别代码	1..1	本人当前婚姻状况类别的代码	S	AN1	GB/T 2261.2-2003 个人基本信息与分类代码 婚姻状况代码

临床数据组	数据元标识符（DE）	数据元名称	重复次数	定义	数据元值的数据类型	表示格式	数据元允许值
	HR02.07.011.01	职业编码系统名称	0..*	标识职业编码系统的名称，如国标职业类别代码、传染病报告职业类别代码	S	AN..50	
	HR02.07.011.02	职业代码	0..*	标识本人当前职业类别的代码	S	AN..3	GB/T 6565-1999 职业分类与代码
	HR02.08.001	文化程度代码	0..1	标识本人受教育的最高程度类别的代码	S	N2	GB/T 4658-1984 文化程度代码
	HR30.00.001	出生日期	1..1	本人出生当天的公元纪年日期	D	D8	
	HR30.00.005	出生地	0..1	出生时地址的详细描述，包括省（自治区、直辖市）、市（地区）、县（区）、乡（镇、街道办事处）	S	AN..120	
H.04 联系人	HR01.01.002.01	标识号-类别代码	0..1	特定环境下本人身份标识（证明文件）号码的类别代码	S	N2	CV0100.03 个体标识号类别代码
	HR01.01.002.02	标识号-号码	0..1	特定环境下本人身份标识（证明文件）号码	S	N..30	
	HR01.01.002.03	标识号-生效日期	0..1	特定环境下本人身份标识（证明文件）号码的生效日期	D	D8	
	HR01.01.002.04	标识号-失效日期	0..1	特定环境下本人身份标识（证明文件）号码的失效日期	D	D8	
	HR01.01.002.05	标识号-提供标识的机构名称	0..1	提供本人身份标识的机构或单位的名称	S	AN..70	

临床数据组	数据元标识符（DE）	数据元名称	重复次数	定义	数据元值的数据类型	表示格式	数据元允许值
	HR02.01.001.01	姓名-标识对象	0..1	姓名的标识对象,如本人姓名、户主姓名、母亲姓名、丈夫姓名等，默认值为本人姓名	S	A..20	CV0100.01 姓名类别代码
	HR02.01.001.02	姓名-标识对象代码	0..1	姓名的标识对象代码	S	N2	CV0100.02 姓名标识对象代码
	HR02.01.002	姓名	1..1	本人在公安户籍管理部门正式登记注册的姓氏和名称	S	A..30	
H.05 地址	HR02.07.006	工作单位名称	0..*	本人工作单位的组织机构名称	S	A..70	
	HR03.00.003	标识地址类别的代码	0..*	标识地址类别的代码	S	N1	CV0300.01 地址类别代码
	HR03.00.004.01	地址-省（自治区、直辖市）	0..*	地址中的省、自治区或直辖市名称	S	A..20	
	HR03.00.004.02	地址-市（地区）		地址中的市或地区名称	S	A..20	
	HR03.00.004.03	地址-县（区）		地址中的县或区名称	S	A..20	
	HR03.00.004.04	地址-乡（镇、街道办事处）		地址中的乡、镇或城市的街道办事处名称	S	A..20	
	HR03.00.004.05	地址-村（街、路、弄等）		地址中的村或城市的街、路、里、弄等名称	S	A..20	
	HR03.00.004.06	地址-门牌号码		地址中的门牌号码	S	AN..20	
	HR03.00.005	邮政编码	1..1	由阿拉伯数字组成，用来表示与地址对应的邮局及其投递区域的邮政通信代号	S	N6	
	HR03.00.006	行政区划代码	1..1	标识中华人民共和国县级及县级以上行政区划的代码	S	N6	

临床数据组	数据元标识符（DE）	数据元名称	重复次数	定义	数据元值的数据类型	表示格式	数据元允许值
H.06 通信	HR04.00.001.01	联系电话-类别	0..*	联系电话所属者类别的名称	S	A..20	
	HR04.00.001.02	联系电话-类别代码	0..*	标识联系电话所属者类别的代码	S	N1	CV0400.01 联系电话类别代码
	HR04.00.001.03	联系电话-号码	0..*	电话号码，包括国际、国内区号和分机号	S	N..20	
	HR04.00.002	电子邮件地址	0..*	本人的电子邮箱名称	S	AN..20	
H.07 医保	HR02.09.001.01	医疗保险-类别	0..*	本人参加的某个医疗保险的类别名称	S	A..20	
	HR02.09.001.02	医疗保险-类别代码	0..*	本人参加的某个医疗保险的类别代码	S	N2	CV0209.01 医疗保险类别代码

患者注册的流程

患者注册的主要流程为，当患者前来就诊时，对患者基本信息进行收集，调用医院信息平台的患者注册服务进行注册，患者注册服务根据传入的基本信息同患者主索引库中信息进行比对并计算匹配度，匹配度会有三个结果：完全匹配、完全不匹配、可能匹配，根据匹配度会有三种结果返回给注册调用者：

1）完全匹配。说明已经存在此患者的基本信息，直接返回此患者已经存在的主索引记录；

2）完全不匹配。说明没有此患者的基本信息，那么为此患者生成一个新的主索引记录并返回给调用者；

3）可能匹配。则需要注册者根据匹配列表进行人工选择，确定是否已有此病人的记录。

表 5-2 患者注册中所涉及的功能

患者注册操作	描述
查询患者信息服务	根据部分信息查找患者
获取患者 ID 服务	根据所有符合要求的患者信息返回患者 ID
注册新患者服务	添加一个新的患者信息
更新患者信息服务	根据患者 ID 更新其它信息
作废患者信息服务	作废某位患者信息及其相关 ID
患者身份匹配服务	根据模糊身份匹配算法，对数据中心患者身份进行合并
注册异常处理	回滚处理

5.3.1.2 医疗卫生服务人员注册

医疗卫生服务人员注册的目的

医疗卫生服务人员注册用于对医疗单位内部所有医疗卫生服务人员的基本信息进行注册和管理。医疗卫生服务人员包括医生、护士、医技人员、药事人员等全部提供医疗卫生服务的医务人员，通过对医疗卫生服务人员基本信息、专业信息的记录，可以实现对医疗卫生服务人力资源的全面掌控、统一管理、合理配置。

医疗卫生服务人员注册库，是一个单一的目录服务。系统为每一位医疗卫生服

务人员分配一个唯一的标识，并提供给平台以及与平台交互的系统和用户所使用。

医疗卫生服务人员注册信息模型

医疗卫生服务人员注册信息的主要内容按照卫生部 2009 年《电子病历基本架构与数据标准》的规定，应包括该标准的 H.09 卫生服务者数据组。

具体数据规定如下：

表 5-3 医疗卫生服务人员注册信息

临床数据组	数据元标识符（DE）	数据元名称	重复次数	定义	数据元值的数据类型	表示格式	数据元允许值
H.09 卫生服务者	HR22.01.100	服务者姓名	1..1	卫生服务提供者的姓名	S	A..30	
	HR22.01.101.01	服务者职责（角色）	1..1	标识服务者在某项活动中的职责和角色，如接诊医师、收费员、化验员	S	A..30	
	HR22.01.101.02	服务者职责（角色）代码	0..*	标识服务者在某项活动中的职责和角色的代码	S	N2	服务者职责（角色）代码 NA
	HR22.01.102	服务者医师资格标志	0..1	标识服务者所具备的医师资格,如主任医师、副主任医师	S	A..30	
	HR22.01.103	服务者学历	0..1	标识服务者求学的经历，如本科、大专	S	A..30	
	HR22.01.104	服务者所学专业	1..*	标识服务者所学的学业门类，如公共卫生专业、卫生管理专业等	S	A..30	
	HR22.01.105	服务者专业技术职称	1..*	标识服务者的专业技术等级，如高级、中级等	S	A..30	
	HR22.01.106	服务者职务	1..*	标识服务者所担任的职务工作	S	A..30	

医疗卫生服务人员注册流程

医疗卫生服务人员注册流程是，首先建立医疗卫生服务人员注册中心，将医疗机构全部医疗卫生服务人员的信息整理后批量注册；当有新的医疗卫生服务人员加入或离职，资格提升，或吊销从业许可证，那么需要及时通过人事系统调用医疗卫生服务人员注册服务，对相关信息进行更新。

作为医疗机构内医疗卫生服务人员信息的唯一管理者，医疗卫生服务人员注册服务向授权管理、访问控制及其它需要使用医疗卫生服务人员信息的业务系统提供信息发布服务。感兴趣的系统可以订阅医疗卫生服务人员注册服务。

表 5-4 医疗卫生服务人员注册中所涉及的服务功能

医疗卫生服务人员注册操作	描述
查询医疗卫生服务人员信息服务	根据部分信息查找医疗卫生服务人员
获取医疗卫生服务人员 ID 服务	根据所有符合要求的人员信息返回医疗卫生服务人员 ID
注册医疗卫生服务人员服务	添加一个新的医疗卫生服务人员信息
更新医疗卫生服务人员信息服务	根据医疗卫生服务人员 ID 更新其它信息
医疗卫生服务人员身份匹配服务	根据模糊身份匹配算法，对数据中心医疗卫生服务人员身份进行匹配合并

医疗卫生服务人员角色管理

基于角色的访问控制(Role-based Access Control，RBAC)，其组成要素有资源、权限、角色、用户，控制的实质是在用户和权限之间建立一种机制，以角色为单元来分配系统的权限，用户通过扮演角色获得了对资源的访问权限。

在医院的实际应用中可以按照相关人员的工作内容及所需要访问的系统资源来划分出多个业务角色，每个角色被赋予对一定资源的访问控制权限。角色之间的权限可以交叉，用户所获得的权限为其扮演的所有角色的权限并集。角色可以继承，通过继承的方式下级角色拥有上级角色的授权，以此构建出完整的角色树。应用系统根据角色信息和资源访问控制列表(Access Control List，ACL)确定相关人员的功能权限。用户的身份认证可以借助数字证书由医院信息平台和第三方机构共同完成。

角色对资源的访问分为公共和私有两种类型，私有类型的访问控制权限其继承者不能拥有，公共类型的访问控制权限其继承者通过继承自动拥有。

角色可以根据控制的资源粒度划分为平台级角色和应用级角色。平台级角色是整个全院信息系统的基础角色，独立于具体的应用系统之上，它在比较粗的粒度上控制平台级资源的访问。应用级角色针对特定应用的角色，它可以是应用内独立的角色，也可以是继承于平台级角色。应用角色是在比较细力度上控制应用级资源的访问。从平台角色继承的应用角色自动具有平台级角色的公共权限，可以访问平台级的公共资源。

对应于角色的划分，角色的管理也分为平台角色管理和各应用的角色管理。平台角色管理负责平台级资源的访问控制，应用角色管理负责各应用内部资源的访问控制，继承自平台角色的应用角色在访问平台资源时可以以父类角色访问。

医院可以按工作角色建设医疗卫生服务人员 RA 管理中心，分别设置医生、护士、药师、检验、管理等多个医务角色，每个角色可被赋予相应的权限和某一个保密等级。角色按照医疗卫生服务人员的工作内容采用面向对象的方法来定义。角色对象存储在 RA 服务器中。角色信息应按照国家有关规定根据医疗卫生服务人员注册信息确定。

医疗卫生服务人员的责任、权利和执业时效等应符合国家及卫生部相关法律、法规和办法，例如《中华人民共和国执业医师法》、《医师执业注册暂行办法》、《医师资格考试暂行办法》、《医师外出会诊管理暂行规定》、《中华人民共和国护士管理办法》、《乡村医生从业管理条例》等等，同时身份认证应遵从卫生部的《卫生系统电子认证服务管理办法（试行）》等办法。

5.3.1.3 医疗卫生机构（科室）注册

医疗卫生机构（科室）注册的目的

医疗卫生机构（科室）注册用于对医疗卫生机构（科室）的基本信息进行管理，通过对医疗卫生机构（科室）基本信息的统一管理，可以向基于医疗信息平台建设的各应用系统、患者提供完整、统一的医疗卫生机构（科室）信息。

通过建立医疗卫生机构（科室）注册库，提供各相关医疗机构及医疗机构所有科室的综合目录，系统为每个机构、科室分配唯一的标识，可以解决医疗活动中医疗卫生服务场所唯一性识别问题，从而保证在医疗业务活动中涉及的不同系统中使

用统一的规范化的标识符，同时也满足与各医疗卫生机构服务机构的互联互通要求以及维护居民健康档案信息的统一标识需求。

医疗卫生机构（科室）注册信息模型

医疗卫生机构（科室）注册信息的主要内容按照卫生部 2009 年《电子病历基本架构与数据标准》的规定，应包括该标准的 H.08 卫生服务机构数据组。

具体数据规定如下：

表 5-5 医疗卫生机构（科室）注册信息

临床数据组	数据元标识符（DE）	数据元名称	重复次数	定义	数据元值的数据类型	表示格式	数据元允许值
H.08 卫生服务机构	HR21.01.100.01	机构名称	1..1	卫生服务机构的组织机构名称	S	AN..70	GB/T17538-1998 全国干部、人事管理信息系统数据结构
	HR21.01.100.02	机构组织机构代码	0..*	卫生服务机构的组织机构代码	S	N22	
	HR21.01.100.03	机构负责人（法人）	0..*	卫生服务机构负责人的姓名	S	A..30	
	HR21.01.100.04	机构地址	0..*	卫生服务机构的地址	S	A..100	
	HR21.01.100.05	科室名称	0..*	卫生服务机构内就诊科室的名称	S	AN..50	
	HR21.01.100.06	机构角色	0..*	标识机构在某项活动中的角色，如转出机构、转入机构	S	AN..50	
	HR21.01.100.07	机构角色代码	0..*	标识机构在某项活动中角色的代码	S	N2	机构角色代码 NA

表 5-6 医疗卫生机构（科室）注册中所涉及的服务功能

医疗卫生机构（科室）注册操作	描述
列出医疗卫生机构（科室）服务	根据条件返回满足要求的医疗卫生机构（科室）列表
查询医疗卫生机构（科室）服务	根据部分信息查找医疗卫生机构（科室）
获取医疗卫生机构（科室）ID 服务	根据所有符合要求的信息返回医疗卫生机构（科室）ID
注册医疗卫生机构（科室）服务	添加一个新的医疗卫生机构（科室）
更新医疗卫生机构（科室）信息服务	根据医疗卫生机构（科室）ID 更新其它信息
废除医疗卫生机构（科室）	根据相关要求作废指定医疗卫生机构（科室）信息

5.3.1.4 术语注册

术语注册的目的

术语注册用于从数据定义层次来解决各系统的互操作问题。术语的范围包括医疗卫生领域所涉及到的各类专业词汇，以及所遵循的数据标准。

建立术语和字典注册库，用来规范医疗卫生事件中所产生的信息含义的一致性问题。术语可由平台管理者进行注册、更新维护；字典既可由平台管理者又可由机构内各应用系统来提供注册、更新维护。

各应用系统使用术语和字典库，根据术语和字典库的更新频率，及其数据量级，可以通过在线、离线两种方式来获取服务。如果选择离线方式，那么需要考虑到更新频率和更新策略的问题。对于更新频率较多且数据量较大的术语和字典，应采用订阅发布机制来完成。

术语注册信息模型

基于 UDDI/WSDL 的注册服务参考实现采用基于 XML 表示的注册信息，其数据结构中包括四个核心部分：业务实体（bussinessEntity）、业务服务（businessService）、绑定模板（bindingTemplate）和技术模型（tModel），它们的结构及相互之间的关系如下图所示：

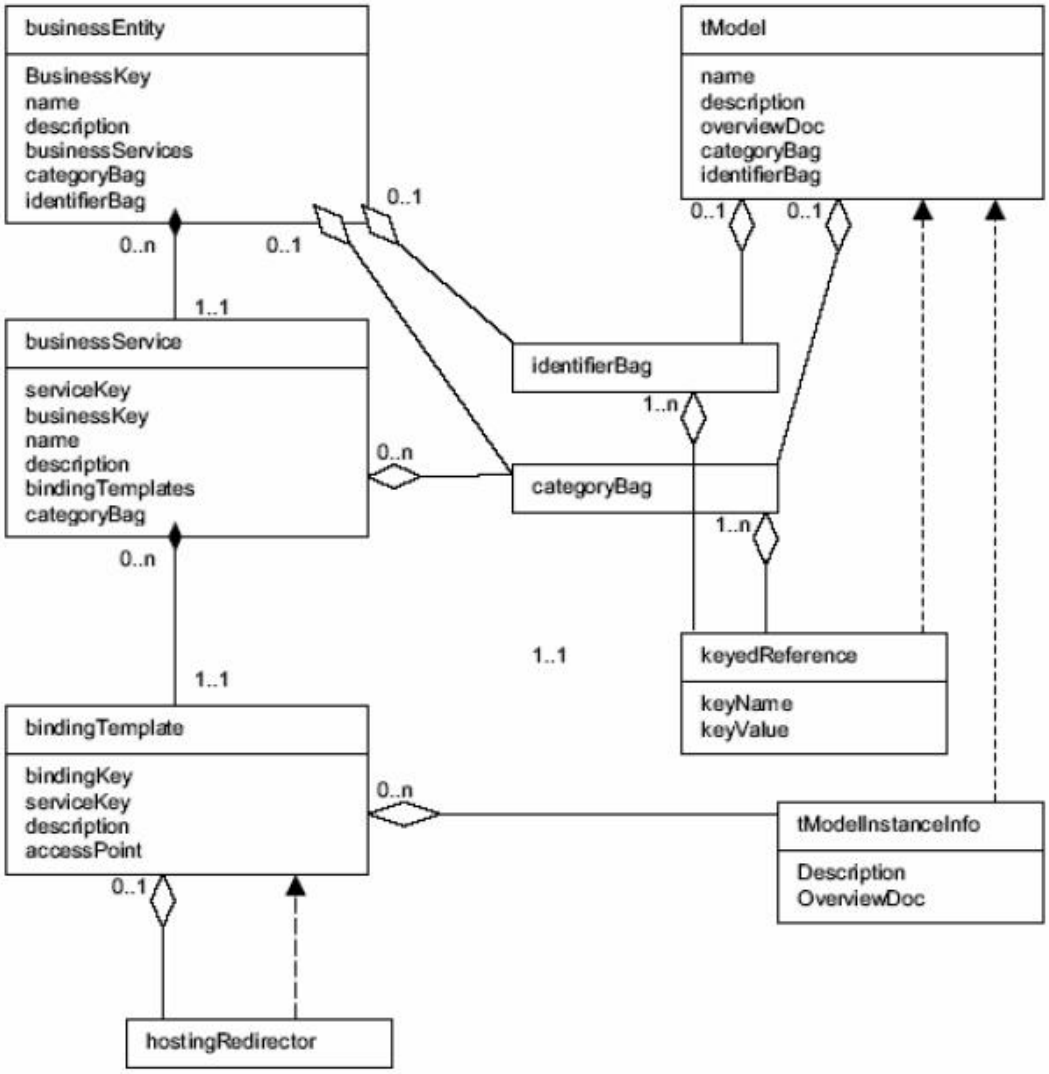

图 5-7 注册服务

其中业务实体用于对提供服务的单位、机构等的基本情况进行描述，同时包含有该单位或机构提供服务资源的描述信息－业务服务。

业务服务用于对服务资源的内容、分类体系等基本信息进行描述，同时包含有对服务资源技术信息的描述内容－绑定模板。

绑定模板用于描述服务资源的访问信息。服务资源访问信息以服务描述语言（WSDL）进行描述。

技术模型相对独立于其它三个部分，用于描述服务资源相关的技术规范、协议、命名空间等信息。

术语注册的流程

术语注册的流程是，首先对各系统所使用的专业词汇、遵循标准进行收集和整理，当全部术语确定后，将其注册入术语库。由于某些术语是可以不断扩充的，随着业务的发展，需要加入新的数据，此时首先应该通过术语注册申请服务来进行增加新术语的申请操作，术语管理者进行评判通过后，才可以正式加入术语库。

表 5-7 术语注册中所涉及的服务功能

医疗卫生术语和字典注册操作	描述
列出术语和字典服务	根据条件返回满足要求的术语及字典列表
查询卫生术语和字典服务	根据部分信息查找术语和字典信息
注册卫生术语和字典服务	添加一个新的医疗卫生术语或字典
更新卫生术语和字典信息服务	根据术语和字典 ID 更新其它信息

5.3.2 患者主索引

注册服务中的患者注册一般通过建立患者主索引 MPI(Master Patient Identifiers)来实现。

5.3.2.1 患者主索引和机构级患者主索引（EMPI）

患者主索引 MPI，是指在特定域范围内，用以标识该域内每个患者实例并保持其唯一性的编码。患者唯一标识是指用于临床实际业务并且能够辅助进行患者信息唯一性识别，在该域或跨域各涉众均可见的患者唯一编码。患者主索引服务是指为保持在多域或跨域中用以标识患者实例所涉及的所有域中患者实例的唯一性，所提供的一种跨域的系统服务。各地可采用身份证、社保卡、医保卡、市民卡、健康卡等来进行唯一标识的加载与识别。

MPI 是一个十分宽泛的概念，但它通常是和患者主 ID 域的建立联系在一起的。这个主 ID 域相对其他的 ID 域，通常可以在更大的范围内适用，是一个“机构级别”的 ID 域。将多个患者 ID 域分级包含入一个“患者主 ID 域”中的方法，可以被看作是交叉索引的一个特殊用法，其中的各个 ID 域中的 ID 都和主 ID 域中的 ID 建立交叉索引关系。下图描述了两种可能采用的配置方式。

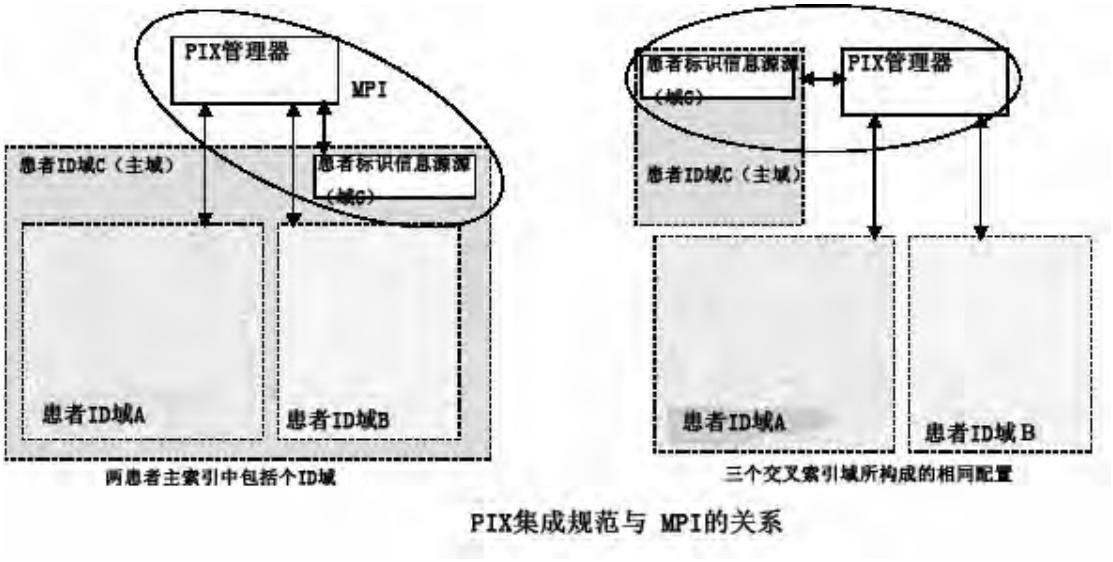

图 5-8 PIX 集成规范与 MPI 的关系

如上图所示，一个典型的 MPI 方式中的患者主 ID 域（域 C），可以被认为是 PIX（患者标识交叉索引）方式中的一个普通的患者 ID 域。是否将一个覆盖全机构范围的系统（如临床数据仓库）作为“主 ID 域”仅仅是一个结构选择。另外，有时候这种结构假设，域 A 中的系统不仅要管理域 A 中的 ID，还需要知道域 C 中的 ID。在 PIX 集成规范中，某个系统被设计部署为跨多个 ID 域进行工作，这是另外一种结构的选择。以这种角度看，被称作“MPI”的实体（图中用椭圆圈起）实际上是患者标识信息源角色和 PIX 管理器角色的混合体。

PIX 集成规范可以和一个已经部署了 MPI 的环境共存，还可以进一步为此环境提供更大的扩展性。PIX 规范还支持很多其他部署配置方式，尤其是在一个覆盖其他 ID 域的主 ID 域并不是必需的情况下（例如，存在多个域的联合体，但其中并没有主 ID 域）。

在本文中，MPI 一般指医院内部使用的患者主索引，EMPI（Enterprise master patient identifiers，机构级 MPI）通常指区域范围内使用的患者主索引。

MPI 信息的主要内容按照卫生部 2009 年《电子病历基本架构与数据标准》的规定，应包括该标准的 H.02 服务对象标识、H.03 人口学、H.04 联系人、H.05 地址、H.06 通信等数据组。其中主要元素包括：患者主 ID、业务系统 ID、患者 ID、姓名、性别、出生日期、出生地、民族、母亲姓名、婚姻状况、身份证号、住址、电话等。

5.3.2.2 患者标识交叉索引

不同医疗机构采用不同的标识码标识同一个患者，当患者在不同医疗机构间转诊需要交换转诊或协作信息进而共享医疗文档时，首先要求能够准确识别患者的身份，这就需要一个交叉索引系统，把患者在不同医疗机构的标识码通过索引联系起来，在需要访问某个系统时可以提供患者在该系统的识别码。

下图展示不同系统通过交叉索引系统注册和提供患者标识，从而顺利完成跨机构信息访问的任务。

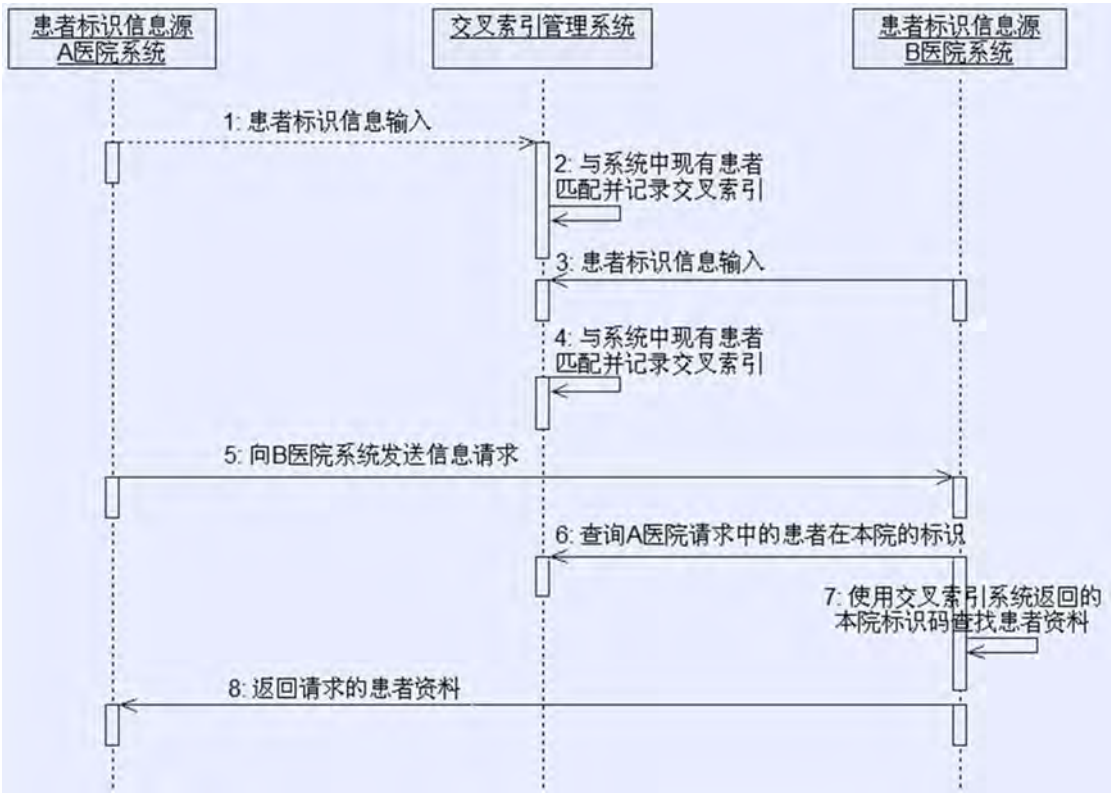

图 5-9 交叉索引注册和使用

1） A 医院向交叉索引管理系统输入患者标识信息。

2） 交叉索引系统将输入的信息与系统中的现有患者进行匹配，形成 A 医院患者标识与现有患者的交叉索引。

3） B 医院向交叉索引管理系统输入患者标识信息。

4） 交叉索引系统将输入的信息与系统中的现有患者进行匹配，形成 B 医院患者标识与现有患者的交叉索引。

5） A 医院系统需要访问一位患者在 B 医院的资料，向 B 医院系统发送请求。

6） A 医院的请求中只有 A 医院的患者标识，因此 B 医院收到请求后首先到

交叉索引管理系统查询该患者在本院的标识。

7） B 医院系统获得请求的患者在本院的标识后可以在本院系统查找该患者的资料。

8） B 医院系统将结果回复给请求的 A 医院系统。

如上面的一般场景所述，交叉索引系统主要提供索引注册和索引查询服务，另外还有一些保证系统运转的系统管理和维护需求。

上述内容描述了患者标识交叉索引在跨机构业务上的应用，而在一个机构内跨应用系统（不同开发商的产品）间的业务上也可参考使用，此时不同的域就是指不同的应用系统，可根据实际情况确定如何使用患者标识交叉索引。

5.3.2.3 MPI 服务功能

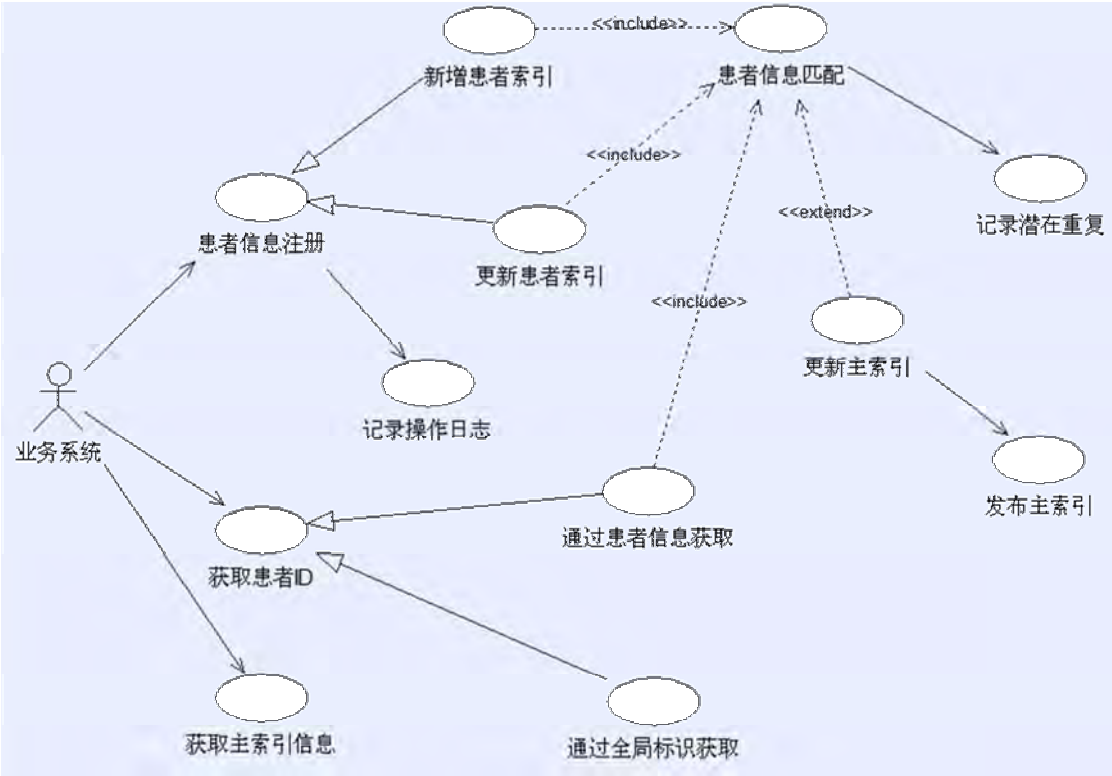

图 5-10 患者标识交叉索引系统服务用例

患者信息注册

业务系统希望把一个患者的索引加入到交叉索引系统时，向交叉索引系统传送请求注册消息，消息中包含待注册的患者信息，主要元素包括：业务系统 ID、患者 ID、姓名、性别、出生日期、出生地、民族、母亲姓名、婚姻状况、身份证号、住址、电话等。

交叉索引系统通过匹配规则检查系统中是否已存在该患者的索引，按照新增索引或更新索引两种情况分别处理。

新增索引需要在交叉索引系统中记录业务系统的索引，同时产生主索引。如果该患者在交叉索引系统中有潜在重复的记录，还需要记录潜在重复信息。

更新索引需要更新匹配的业务系统的索引，同时更新主索引。

主索引更新时，需要对订阅主索引的系统发布更新的主索引。

登记患者流程图示如下：

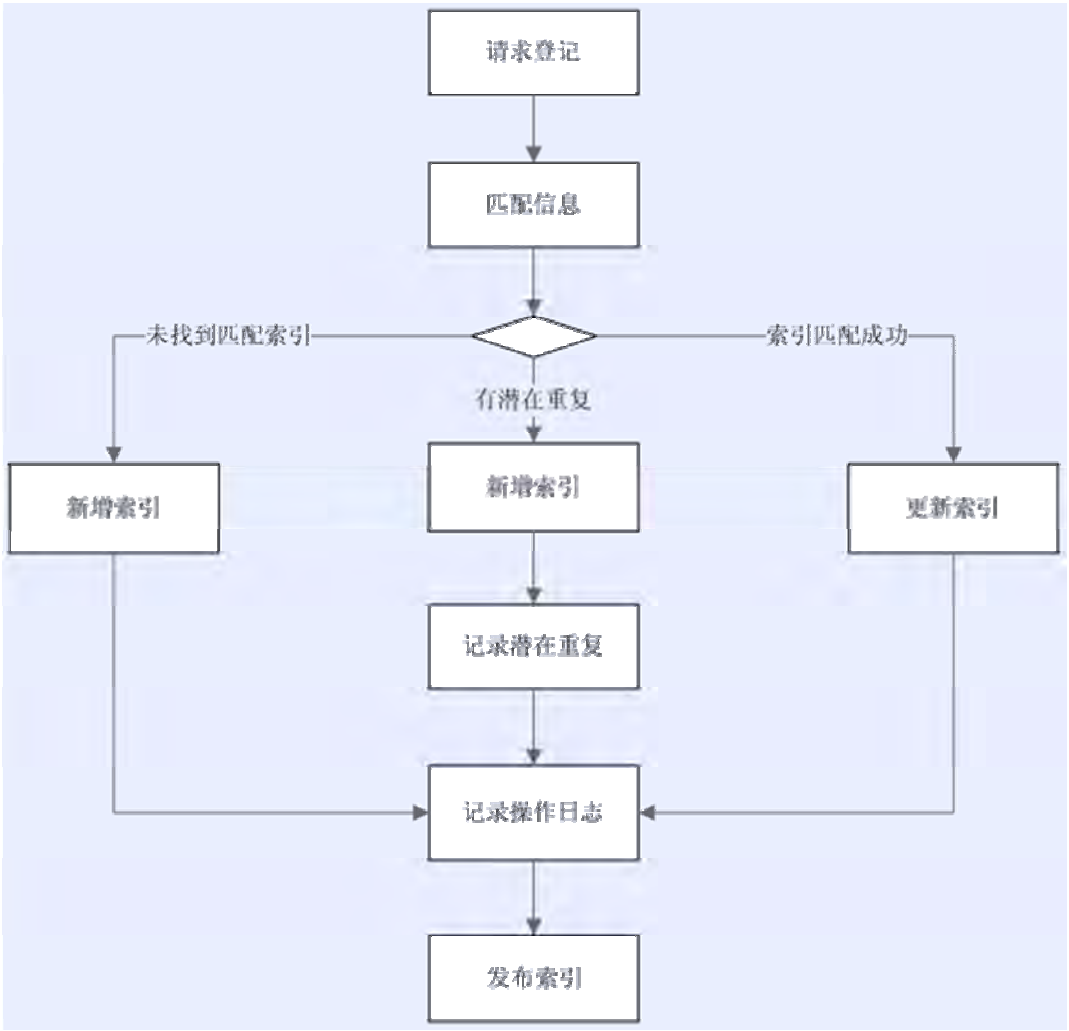

图 5-11 登记患者流程

患者信息匹配

接收到外部系统登记患者的请求信息后，交叉索引系统首先使用业务系统号＋患者局部 ID（LID）查找，如果存在精确匹配的索引，只需要对原索引信息进行更新即可，如果没有找到精确匹配的患者索引，则需要根据患者的其它信息和

系统中的记录进行匹配。

交叉索引匹配引擎首先通过预定义的匹配条件选定一批相近的记录，对每个记录计算匹配度，再根据这组记录的匹配度确定请求登记的信息属于新患者、现有患者或者潜在重复患者。这里所说的潜在重复是指两个患者的信息匹配度比较高但还不足以判定为同一个人。

患者信息匹配流程如下：

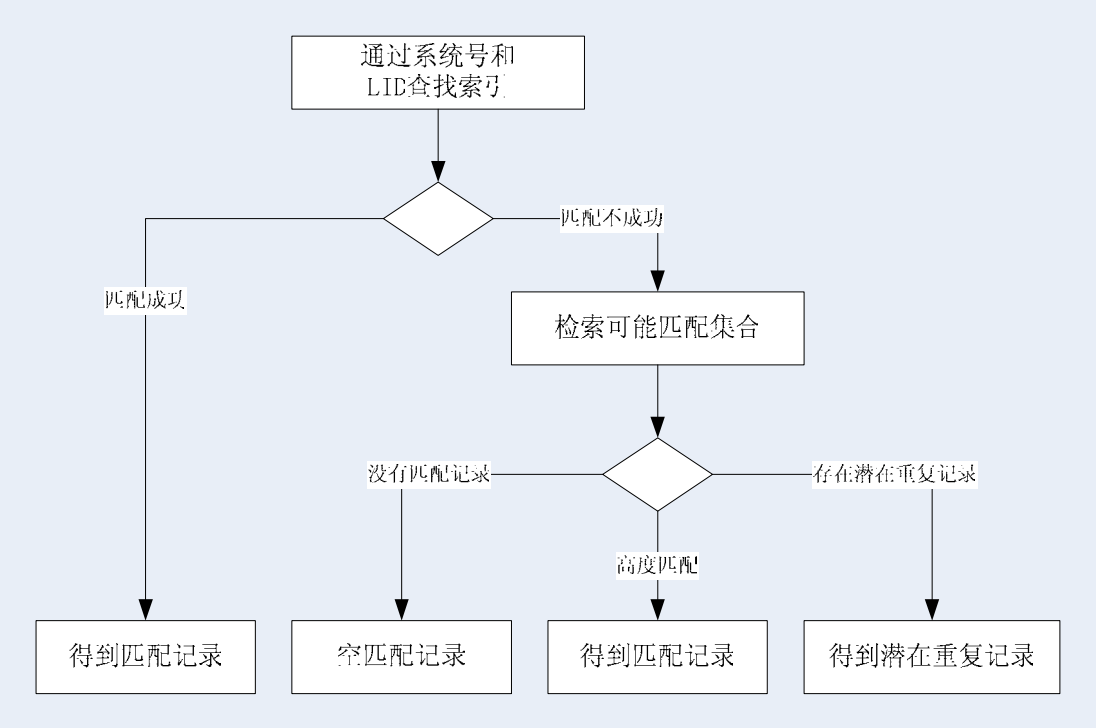

图 5-12 登记患者流程

更新主索引

在交叉索引系统新增或更新一个患者的索引信息后，同时需要对主索引进行更新。向交叉索引提供患者信息注册的系统可能拥有不同的信息可信度，因此其提供的信息对主索引的影响有所不同。更新操作根据新的信息对主索引每个字段记录的信息进行评价，确定该字段的最佳值。

记录潜在重复

匹配引擎检测到申请登记的患者和现存索引存在潜在重复时，需要对潜在重复的情况进行记录，并返回给业务系统或系统管理员进行处理。

发布主索引

业务系统可以向交叉索引系统订阅主索引，便于在以后的应用中加快应用，提高信息准确性，交叉索引系统在对一个患者的主索引更新或增加新索引后，需要向订阅主索引的业务系统发布更新。

记录操作日志

交叉索引系统业务记录发生的变化都需要记录操作日志，并能实现回退。

需要记录的业务操作：

表 5-8 需记录的业务操作

新增局部索引	更新局部索引	合并索引
新增主索引	更新主索引	取消索引合并
索引自动匹配	取消自动匹配	

获取患者交叉索引

交叉索引系统的主要功能是为业务系统提供业务系统交叉索引表，业务系统可以通过两种方式获取交叉索引：通过全局标识获取、通过患者信息获取。

如果业务系统中记录了患者全局标识，交叉索引系统可以直接检索到该患者的交叉索引表。

当业务系统仅提供患者本地信息向交叉索引系统检索交叉索引时，交叉索引系统首先要进行患者信息匹配，在交叉索引库中查找可以匹配的病人。如果能够精确匹配，则返回该患者的交叉索引；如果仅能匹配到潜在重复，则返回潜在重复信息，由业务系统进一步选择；如果匹配失败，则返回空记录。

获取患者主索引信息

交叉索引系统存储了患者在多个系统中的标识信息，并由此维护一个主索引，记录最准确的患者基本信息，该信息可以提供给业务系统使用，提高业务系统中患者信息的质量。

获取患者主索引信息的使用方法要求与获取患者交叉索引类似，可以由业务系统提供全局标识获取，也可以由业务系统提供患者本地信息获取。

5.3.2.4 MPI 管理功能

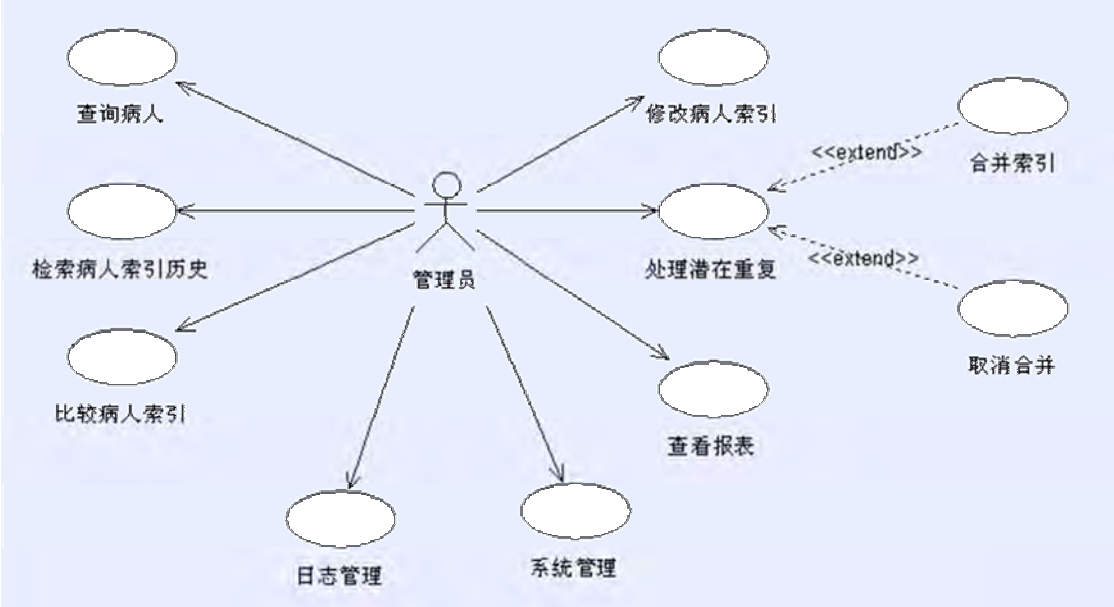

图 5-13 患者标识交叉索引系统管理用例

查询患者

允许系统管理操作人员使用全局患者标识或业务系统本地患者标识检索患者；或者输入患者部分信息，如姓名、性别、出生日期、身份证号等检索患者，检索结果以列表形式返回给操作员。

检索患者索引历史

以直观的形式显示指定患者的全部索引，浏览索引详细内容，并查看索引创建、更新的过程记录。

比较患者索引

对选定的局部索引或主索引进行信息比较，检查两条记录的匹配度和差异性，生成差异报告。

修改患者索引

提供操作界面满足管理后台对现有索引进行修正的要求。

处理潜在重复

对潜在重复的索引进行合并或取消重复标记的操作，首先由系统提供潜在重复记录的差异报告，然后由管理员处理。

系统自动匹配的索引或者人工合并的索引可以由管理员进行拆分。

查看报表

提供操作界面查看系统中需要管理员处理的信息报表，包括潜在重复报表、默认匹配报表，也提供管理员人工处理的信息报表，如合并操作报表。

系统管理

系统允许参数设置，包括业务系统权重设置、病人信息字段权重设置。

使用权限管理，即使用系统的用户及其相应操作权限管理。

系统字典管理，包括病人资料涉及的多种标准字典和系统自定义字典。

日志管理

日志分类浏览，需分类的日志类型：索引注册、索引更新、系统匹配、潜在重复、手工拆分、手工合并。

对日志显示设定限定条件，包括：日志时间、患者 ID。

日志导出，导出为 XML 文件，并可以在日志浏览器中打开显示内容。

5.3.2.5 患者新增/更新流程

当患者标识建立、修改、合并后，或在基本信息关键字被修改后，患者标识源向 PIX 管理器传送患者标识和基本信息。PIX 管理器在接收到患者标识源发送的消息后，对患者信息进行相应的增、改，检查是否存在重复并进行相应的处理。服务流程图示如下：

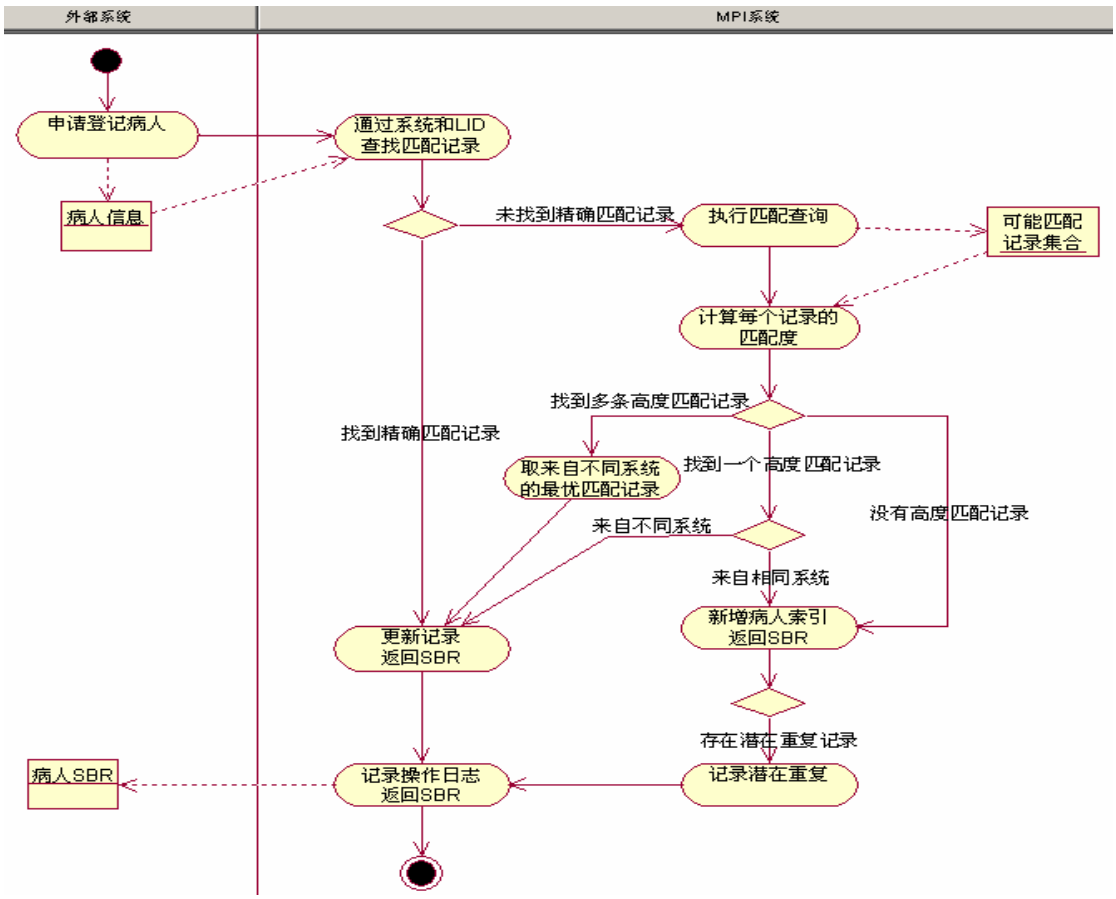

图 5-14 患者新增/更新流程

需要指出的是：当不同系统的患者 ID（不同 ID 域的 ID）进行匹配计算时，很少有患者基本信息完全一致的情况（MPI 信息匹配度为 1）。基本上当两个 ID 信息匹配度大于某一个值时(如大于 0.95)，就可认为该两个 ID 是指向同一个人。任何匹配算法都不可能保证匹配精度为 100%。

为了尽可能提高 PIX 系统的可信度，一般情况下应以卫生部 2009 年《电子病历基本架构与数据标准》的相关要求建立身份信息框架，对部分重要关键词排序，并适当考虑关键词的关联关系，以求得尽可能高的匹配精度。

5.3.3 电子病历档案服务

5.3.3.1 索引服务

索引服务全面掌握医院信息平台所有关于居民的诊疗信息事件，包括患者何时、在哪个科室、接受过何种医疗服务，并产生了哪些文档。索引服务主要记录

两大类的信息，一是医疗卫生事件信息，另一为文档目录信息。

医院信息平台用户在被授权的情况下，可以通过电子病历档案服务提供的索引服务从基本业务系统查看某患者的诊疗事件信息，以及事件信息所涉及的文档目录及摘要信息。再结合电子病历存储服务可以实现文档信息的即时展示，使用户更多的了解患者既往的健康情况，为本次医疗服务提供相应的辅助参考作用。

5.3.3.2 数据服务

数据服务提供功能性的支持，以执行正确的数据访问过程和与不同的注册服务、存储服务、业务管理或辅助决策服务交互所需的转换。通常，电子病历档案服务可以与平台内部组件相互作用。它依赖于基于标准的通信机制，并使用交换层来执行这种相互作用，或者使用更为直接或私有化的接口机制来访问或更新数据到任何一种注册服务、存储服务。数据服务用在两个场景里：记录和获取电子病历数据的在线业务场景，加载和管理电子病历存储库和注册信息的管理功能场景。数据服务所包含的主要服务组件有：

1.复制服务

在现有的医院信息平台平台内的系统或数据库之间提供数据复制功能。

2.数据仓库服务

数据仓库服务管理从不同的存储库中抽取和插入数据，经过抽取、转换和装载等加工处理后，提供生成医院信息平台范围内使用的各种数据分析利用资源。

3.键值管理服务

当数据访问来自不同数据源时，会出现这样的情况，即某个主索引键或次索引键在源系统间不唯一或不存在。键值管理服务将在电子病历存储库插入和更新操作期间生成和管理这些键值。

4.数据访问服务

为不同的注册库、电子病历系统或辅助服务相关的数据访问过程的正确调用提供支持。它存储着有关数据结构和调用过程的元数据，以在运行 I-IPs 的语境中或数据维护类型过程中执行存储库的操作。

5.3.4 电子病历存储服务与临床数据存储库

电子病历是由医疗机构以电子化方式创建、保存和使用的，重点针对门诊、住院患者（或保健对象）临床诊疗和指导干预信息的数据集成系统。是居民个人在医疗机构历次就诊过程中产生和被记录的完整、详细的临床信息资源。

与某一具体临床活动相关的临床活动的信息与数据记录形成了相对独立的电子病历（EMR）文档。而在临床活动过程中产生的对医疗活动的文字、图像、或多媒体的电子格式记录文档均称之为 EMR 文档。

EMR 文档集：由多个 EMR 文档组成的一组与某个临床业务活动相关的文档集合称为 EMR 文档集。

电子病历存储服务具体由临床数据存储库 CDR(Clinical Data Repository)来实现。。

5.3.4.1 EMR 文档标准

2009 年 12 月 31 日卫生部颁布了《电子病历基本架构与数据标准(试行)》。它是我国卫生领域制定、发布的首部国家级具有中西医结合特点的电子病历业务架构基本规范和数据标准。主要包括两部分内容，第一部分是“电子病历基本架构”，包括（1）电子病历的基本概念和系统架构，（2）电子病历的基本内容和信息来源；第二部分是“电子病历数据标准”，包括（3）电子病历数据结构，（4）电子病历临床文档信息模型，（5）电子病历临床文档数据组与数据元标准，（6）电子病历临床文档基础模板与数据集标准。EMR 文档应当从内容与架构上遵循《电子病历基本架构与数据标准》的要求。

EMR 文档本身采用何种存储结构本身取决于各个供应商自行定义，但作为电子病历我们需要将 EMR 文档实现 CDR(Clinical Data Repository)存储服务模式。在基于电子病历的医院信息平台建设时我们建议 EMR 文档格式应当建议遵循 HL7CDA 标准。

HL7 临床文档架构（Clinical Document Architecture，CDA）是一项基于 XML 的标记标准（置标标准），旨在规定用于交换的临床文档的编码、结构和语义。CDA 基于 HL7 参考信息模型（Reference Information Model，RIM）以及第 3 版 HL7 数据类型（Data Types）。CDA 文档在本质上具有持久性。CDA 标准规

定，CDA 文档内容由强制性的文本部分和可选性的结构化部分构成；其中，前者保证的是对于文档内容的人工解释，而后者则旨在用于软件处理。结构化部分依赖于各种编码系统（coding systems）来表示概念，如医学术语系统命名法（Systematized Nomenclature of Medicine，SNOMED）和 LOINC（Logical Observation Identifiers Names and Codes）。

5.3.4.2 EMR 文档的基本内容

根据 2010 年 3 月颁布的《电子病历基本规范（试行）》规定，电子病历包括门（急）诊电子病历、住院电子病历及其他电子医疗记录。电子病历内容应当按照卫生部《病历书写基本规范》执行。电子病历的基本内容由门（急）诊病历与住院病历两部分组成。

门（急）诊病历内容包括门（急）诊病历首页（门（急）诊手册封面）、病历记录、化验单（检验报告）、医学影像检查资料等。

住院病历内容包括住院病案首页、入院记录、病程记录、手术同意书、麻醉同意书、输血治疗知情同意书、特殊检查（特殊治疗）同意书、病危（重）通知书、医嘱单、辅助检查报告单、体温单、医学影像检查资料、病理资料等。

各项书写内容的详细规定详见 2010 年 3 月 1 日开始实施的《病历书写基本规范》。

5.3.4.3 EMR 文档类型

EMR 文档包含的各类临床活动描述的信息与数据，其信息与内容的描述形式总的来说可以分为结构化、非结构化、多媒体（含扫描病历）或这三种形式的混合体。

结构化 EMR 文档是指在对临床信息进行记录时，所包含的临床信息包含各种可识别的临床知识内容，每一个元素节点都有对应的清楚临床知识定义，能够被临床知识分析或科研作为一个临床信息进行分析。

非结构化 EMR 文档指临床信息由自然语言或字符串组成，未进行临床知识标识，只能进行全文检索或者自然语言处理引擎进行分析和利用的 EMR 文档。

多媒体 EMR 文档指文档内包含图像、动画、视频、声音等多媒体文件。

通常在 EMR 文档中可能是这三种形式的混合体。

5.3.4.4 EMR 文档结构

电子病历主要由临床文档组成，临床文档是电子病历中各类业务活动记录的基本形式。临床文档中的数据存在着一定的层级结构关系，其中有包含与被包含的关系，也有按同类属性相互嵌套的关系。临床文档的结构化和标准化，是电子病历实现语义层数据交换与共享的基本要求。

电子病历数据结构用于规范描述电子病历中数据的层次结构关系，即电子病历从临床文档到数据元的逐步分解、或从数据元到临床文档的逐步聚合关系。

电子病历数据结构分为四层（见图 1）：

（1）临床文档：位于电子病历数据结构的最顶层，是由特定医疗服务活动（卫生事件）产生和记录的患者（或保健对象）临床诊疗和指导干预信息的数据集合。如：门（急）诊病历、住院病案首页、会诊记录等。

（2）文档段：结构化的临床文档一般可拆分为若干逻辑上的段，即文档段。文档段为构成该文档段的数据提供临床语境，即为其中的数据元通用定义增加特定的约束。结构化的文档段一般由数据组组成，并通过数据组获得特定的定义。本标准中未明确定义文档段，但隐含了文档段概念。

（3）数据组：由若干数据元构成，作为一个数据元集合体构成临床文档的基本单元，具有临床语义完整性和可重用性特点。数据组可以存在嵌套结构，即较大的数据组中可包含较小的子数据组。如：文档标识、主诉、用药等。

（4）数据元：位于电子病历数据结构的最底层，是可以通过定义、标识、表示和允许值等一系列属性进行赋值的最小、不可再细分的数据单元。数据元的允许值由值域定义。

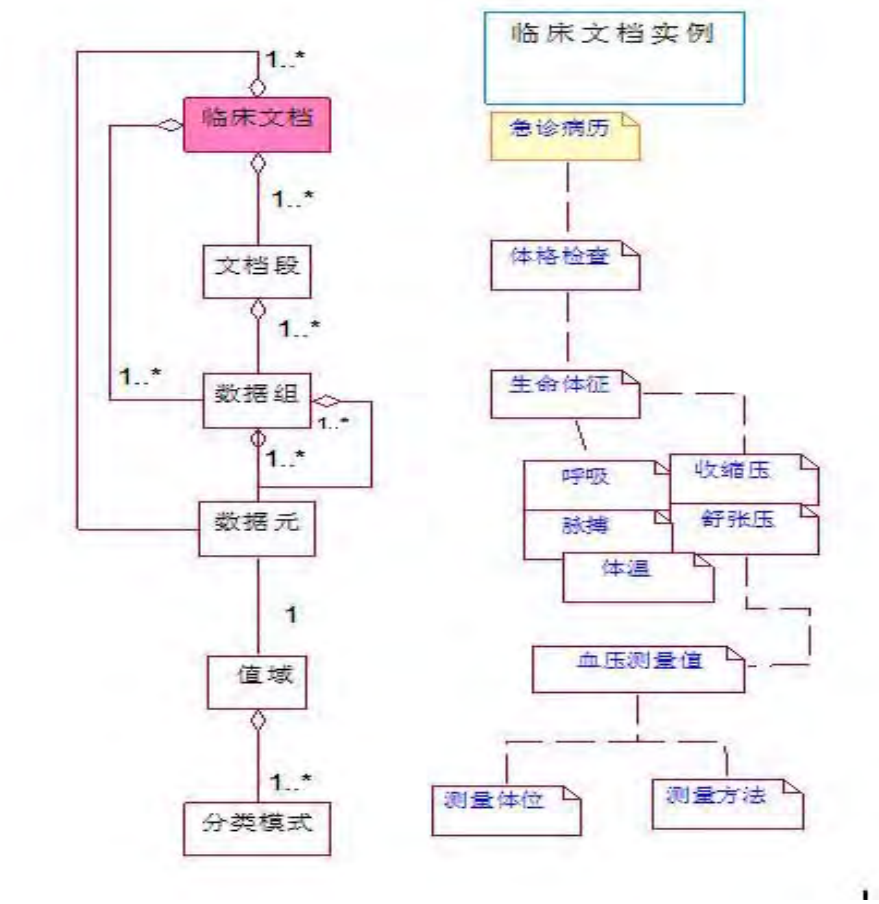

图 5-15 电子病历数据结构

详细的数据元定义参见《电子病历基本架构与数据标准》。

EMR 文档作为重要的患者临床信息的重要载体，应当遵从《电子病历基本架构与数据标准》数据内容框架及数据元定义。并以符合 HL7 CDA 标准作为组织 EMR 文档的结构机构实现文档存储或者以符合 HL7 CDA 标准实现 EMR 文档的组织。

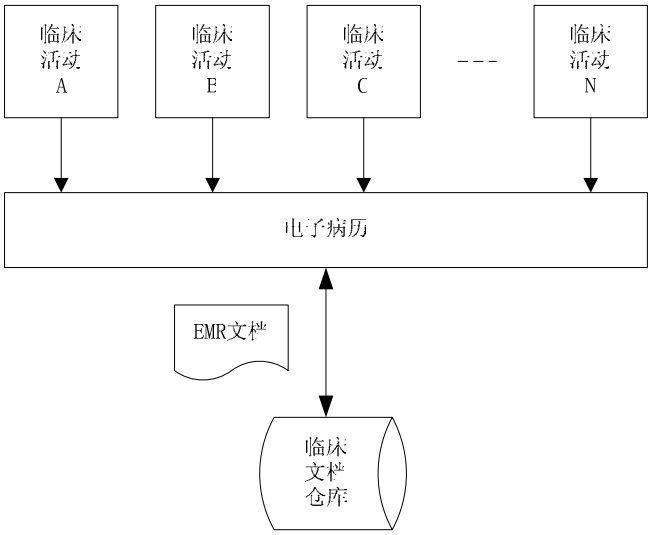

图 5-16 EMR 文档是患者临床信息的重要载体

EMR 文档存储应当以患者为中心，围绕患者的所发生的实际临床业务活动组织文档，基于已注册的 EMR 文档分类进行文档的分类、标识。平台业务用户可根据实际授权情况进行 EMR 文档的全部、部分、单个文档的调阅与应用。

5.3.4.5 临床数据存储库

临床数据存储库（CDR Clinical Data Repository）是 EMR 文档存储中心，它将一个患者在某一医疗机构内发生的所有临床活动所产生的临床文档集中存储在一个物理或虚拟的存储内，方便各种临床业务角色在使用该患者某一或某些临床活动的 EMR 文档时进行调阅。

CDR 是所有的病人医疗结果和其他临床数据的一个中心存储仓库，而且是在电子病历的中心。单个病人信息随着时间的增加信息量也随之增长，为了可长期获得该病人的信息，需要对其信息进行长期存储。这时，就出现异构下的数据的长期管理问题。而医疗文档库，就是把医院信息系统中各个业务系统的数据库的信息抽取出去，通过归档的形式形成一个静态的文档，把它放在中间的文档库。来自多个系统、由不同厂家建立的，全部收集起来归入文档库。CDR 对于电子病历来讲是一个非常核心的部件。CDR 是一个面向主题的、集成的、可变的、当前的细节数据集合，用于支持企业对于即时性的、操作性的、集成的全体信息的需求。

5.3.4.5.1 以患者为中心的 EMR 文档存储

患者在某一医疗机构内发生的各类临床活动形成的 EMR 文档集应当在患者主索引（MPI）的指引下进行汇总归集，并通过 MPI 完成 EMR 浏览器及非电子病历编辑器环境下的患者 EMR 文档浏览。

5.3.4.5.2 EMR 文档数据来源

所有的临床活动所产生的信息记录均为 EMR 文档的数据来源，基于电子病历的医院信息平台将各个系统中产生的临床活动数据与信息进行集成与共享后，通过生成规定格式的 EMR 文档进行归档与储存。与临床业务活动相关的各部分数据分别来源于基于平台上的各个分子系统，把反映临床业务活动的最终状态的数据进行集中、集成后统一合并到 EMR 文档中。

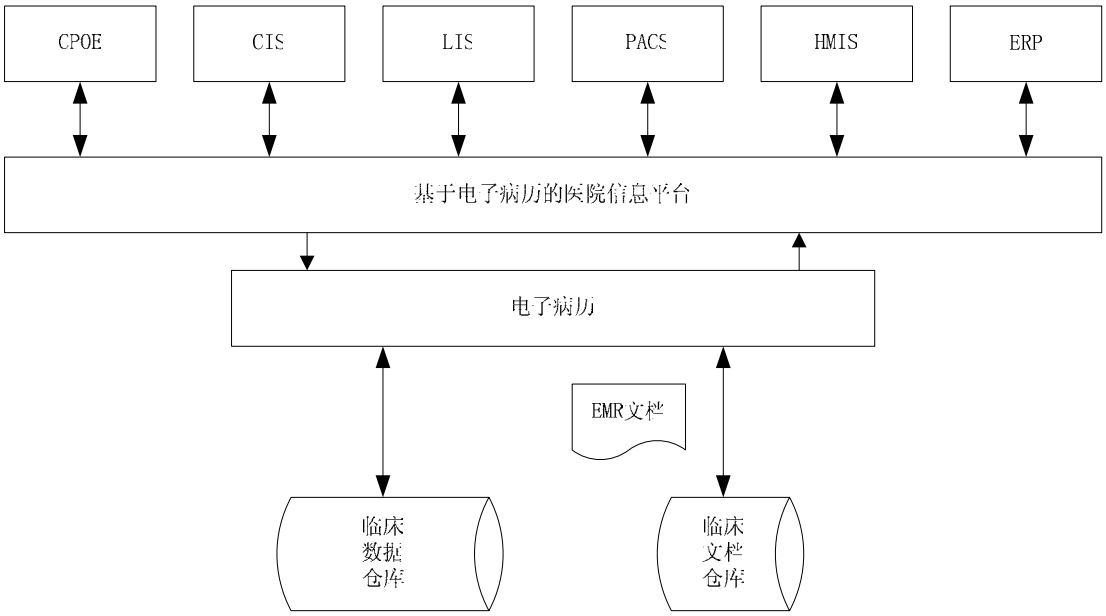

图 5-17 EMR 文档的来源

5.3.4.5.3 EMR 文档注册

每一类需要在临床文档仓库中进行存储的 EMR 文档都需要在 CDR 中进行注册。并且还需要在 CDR 中注册其文档的模板信息与数据。而在实际临床业务活动发生过程中所产生的 EMR 文档都能够通过注册系统对应其使用的文档模板

信息与数据。

EMR 文档产生并完成注册后，随着临床业务活动的发生逐个生成 EMR 文档并通过 CDR 进行存储。

5.3.4.5.4 临床数据存储库与临床文档存储库

EMR 文档以符合 HL7 CDA 的文档结构的方式产生后按照以患者为中心的索引方式进行存储，形成临床数据存储库。由于患者的临床数据是以 EMR 文档的方式进行存储并以 HL7 CDA 的方式进行组织，这样组织的存储方式也称之为临床文档存储库。临床文档存储库（Clinical Document Repository，CDR）是临床数据存储库（CDR Clinical Data Repository）的表现形式之一，并非唯一表现形式。

5.3.4.5.5 EMR 文档版本管理

患者的临床业务活动的发生时一个持续并且连续的过程，并且主观描述部分，或者非数据接口内的数据内容会因为某些特定条件下发生修订或者修改，这是 EMR 文档作为临床活动发生情景的真实记录数据应当能够客观的反应出各种主客观数据或者描述的变化与修改过程，这时就对 EMR 文档提出了文档版本的管理要求。

EMR 文档版本管理应当支持文档变化的痕迹跟踪，以及痕迹审计。反应出 EMR 文档在不同提交时间戳时的文档实际状态。

5.3.5 电子病历浏览器

电子病历浏览器（即 EMR 浏览器）是为终端用户提供的访问个人电子健康记录的应用程序，提供电子病历的展现，建议采用 Web 方式实现。电子病历浏览器的目标是建立一个用户友好的环境，在该环境下被授权的医护专业人员或患者可以方便地访问电子病历中保存的相关数据。电子病历信息主要由临床信息组成，电子病历浏览器可以根据使用者的特定需求提供不同医疗卫生领域的调阅展示服务。

5.3.5.1 电子病历浏览器的设计要求

- **常规设计要求**
  - 用户可以访问同一患者信息，无需考虑是从哪个工作站登录的；
  - 向用户提供访问患者纵向记录的窗口，必须能够显示所有CDR存储库中的数据；
  - 对于电子病历浏览器来说，注册库应该是信息平台标识符的唯一来源，尤其在选择患者和医疗机构或者解析服务位置标识时；
  - 提供能够使用信息平台中的患者注册服务来检索患者信息的功能；
  - 提供在客户记录间方便的导航能力，同时维持特定用户会话的语境信息如用户ID、密码和患者标识信息；
  - 提供记住活跃患者的列表能力，提供优化机制以访问活动名录（预先查询，缓存等）中的患者记录；
  - 纵向记录服务包含的电子病历索引应当是任何和所有（即纵向的）患者电子病历查询的起点（即第一级的）。电子病历浏览器应使用户能“下钻”到由LRS索引的任何特定事件、文档或其他公布的条目；
  - 对于给定的患者来说，提供代表客户电子病历内容的概览视图；
  - 提供不同方式的视图，如按日期、按服务提供者、按服务地点排序的按事件访问客户电子病历，或者按视图中展现的特定域来访问电子病历；
  - 提供方便灵活的信息导航特征，如，改变列表中分类顺序、改变列的位置、可变更可视长度等；
  - 提供医师在患者就诊期间或在就诊的上下文环境中获得对患者健康记录的访问。为了有助于这些方案的应用，电子病历浏览器需要易于使用和导航，易于学习，高效提供数据和有效地与信息平台交互以访问所呈现的数据。；
- **隐私和安全设计要求**

- 患者健康相关信息属于个人隐私，电子病历浏览器需要通过安全、保密、访问控制等手段，提供健康信息的隐私保护和数据安全保护；
- 为安全起见，电子病历浏览器利用信息平台的安全机制，即用户应该在信息平台上注册并被全域所知晓；
- 通过应用保持在接入层中可用于用户电子病历访问的政策、规则和控制，提供与用户交互的能力，以执行认证和授权访问控制；
- 提供应用辖区许可管理的政策的特征，例如紧急情况下的处置，许可收集等；
- 在适当的系统安全日志机制内，记录所有导致访问或更新信息平台系统任何组件的系统/用户事务日志。；

▪ **集成/技术要求**

- 电子病历浏览器应用通过执行电子病历互操作性框架标准化消息来访问所有信息平台服务；
- 所有与信息平台的交互都依赖于国家电子病历标准。包括数据消息通信标准，术语标准，协议和其他技术标准；
- 可以在任意支持当前工业标准的Web浏览器客户端的台式/便携式/无线计算设备上运行；
- 建议采用行业认可的基于web方式的方案，该方案可以最小化拥有成本，包括维护和开发成本。例如，使用Web界面，不需要将代码下载到客户端计算设备，而是使用运行时编译对象或脚本语言如Java、.Net或JavaScript；
- 基于公认的web门户技术，提供了灵活、开放、组件驱动、面向服务的应用架构，如基于web的门户和端口小程序技术；
- 能易于整合到现有PoS应用用户接口环境，该环境基于开放W3C标准的互操作技术，如HTML，HTTP，XML等；

- 能在用户界面级整合到现有PoS应用，采用上下文环境管理技术和标准，例如CCOW等，在一个或多个软件应用间进行传递用户会话和患者标识。

- **性能/可伸缩性要求**
  - 高性能的客户数据访问，在网络通常的情况下，任何单一访问信息平台进行数据调阅通信必须在5秒内在终端用户屏幕上响应；
  - 能够支持信息平台下规划的所有用户；
  - 能够支持一个信息平台内预计用户基数的用户请求/事务的高峰容量；
  - 用松散耦合的软件部件支持基于服务的N层架构（即非客户服务器模式）的概念、设计和实现，允许容易地变更或增加新功能；。

5.3.5.2 电子病历浏览器的分类

在Gartner关于CPR（Computer-based patient record）系统的分代模型的基础上对电子病历浏览器进行了分类，以此为基础建立描述电子健康记录功能分代的通用语言。此模型的发布是作为“基于计算机的患者记录系统的互操作路线图”的研究报告的一部分，报告者为Gartner公司(www.gartner.com)的Wes Richel（ID号：G00129914），2005年12月29日。

1) 第一代电子病历浏览器解决方案——调阅浏览器

第一代电子病历浏览器以调阅服务为主要目标，通过电子病历浏览器调阅患者的健康相关信息。这种解决方案中，调阅患者信息有两种方式：一种是基于IE浏览器直接浏览；第二种是通过IE控件嵌入医疗机构业务系统。

- 基于IE浏览器直接浏览

这种浏览方式直接通过IE浏览，不受医疗业务系统功能限制，用户在任何地方授权登录后都能够浏览权限范围内的电子病历信息，能够有多种浏览方式，但只能阅读，不能做任何处理和操作。

- 通过IE控件嵌入医疗机构业务系统

这种浏览方式通过控件将浏览器嵌入医疗业务系统，对于浏览器使用者，只是看到同样的一个界面，不会产生在使用两个界面/系统的感觉。浏览服务是通过中心的服务得到，与所嵌入的应用程序的配置无关，不能直接调阅所嵌入的医疗业务系统的数据；可以引用所被嵌入的应用程序的当前病人信息；可以对病人医疗记录进行重新排序、归类等工作，但不能直接更新医疗记录。

2) 第二代电子病历浏览器解决方案——专业用户浏览器

第二代电子病历浏览器即为专用用户界面（Specialized UI），这类应用程序提供高级的功能，不仅是电子病历数据的浏览，也提供处理电子病历数据的能力。例如：对于PACS供应商提供的DICOM影像浏览器，该浏览器需要提供相应的工具来管理、传输和转换图像。

专用用户界面具有一般电子病历浏览器所具有的特征，但局限于特定的临床域（如诊断图像）而不是提供系统之外跨域的纵向记录。尽管这看起来可能是一个重要的限制，但是有两个方法可以弱化这个问题。

第一个方法是在专用用户界面和功能更丰富的浏览器之间采用“语境共享”（也称语境管理），例如CIS浏览器。语境共享是技术术语，就是说允许两个独立的应用程序共享有限的有关每个系统中发生了什么（语境）的知识。典型地，这些应用程序共享简单的数据元素，如哪个患者的信息正在被用户浏览。如果用户用CIS选择不同的患者，该患者的标识符就“共享”或“传送”给PACS浏览器，使得该浏览器可以将视图切换到同一个患者。对于用户来说，这可以看作是一次自动同步，省去用户手动切换的麻烦。同样，如果CIS知道一个特定的诊断成像的检查ID，DI浏览器不仅能转换到正确的患者对象，而且能把与用户选择的特定检查相关联的图像显示出来。

第二个方法是利用web技术（HTTP）的链接和重定向能力。在这个方法中，一个应用程序包括到相应的对象（例如DI研究）的链接。显然，这一知识不得不在两个主应用程序间直接共享，而不是通过对应的浏览器。一旦用户选择其中的一个链接，主程序将通过与链接关联的URL重定向到其他程序，调用专有的浏览器来显示所需图像。

DICOM图像浏览器是专用UI最典型的实例，但是并不是唯一的例子。对于浏览扫描文档或者是位图文档（如pdf浏览器）或音视频频来说也有类似的方案。

3) 第三代电子病历浏览器解决方案——定制化浏览器

第三代电子病历浏览器是定制的UI（Tailored UI）包括一些倾向于基于门户平台开发一个定制的系统的项目。从一整套用户自定义的需求开始，开发人员建立一个全新的用户界面，包括界面具有所需功能，所要求的观感和客户化特征。依靠所使用的门户技术，许多功能特征由工具直接提供，发人员能集中致力于屏幕流、观感设计和各种数据元素间的交叉链接。

第三代电子病历浏览器的优点是能够按照用户的要求定制，避免了不必要的复杂性和多余的功能。它也使得创建的UI在图形、语言支持以及在与信息平台、其他非电子病历存储库和临床系统（像前述的专用UI）的无缝集成方面遵循已存在的指南。

第三代电子病历浏览器的一个应用例子是医生门户。个性化是医生门户的重要特点，个性化允许每个医生有自己独特的浏览和显示格式。系统的高级用户更希望通过客户化来加快工作流程，快速而方便地访问数据。显示管理是将完全不同的信息以高效的浏览方式恰当地汇集到一起。医生可以从一个视图浏览源于不同系统的数据。这有助于医学诊断，缩短查找信息的时间和方便使用。根据角色对工作流客户化被视作门户的一个重要特征。

4) 第四代电子病历浏览器解决方案——互动式浏览器

第四代电子病历浏览器能够提供基本的数据录入功能，这些功能对电子病历浏览器用户有意义深远的影响。这类用户界面向电子病历浏览功能补充了几个“增值”的特点，这些特点有利于方案的应用，如：

- 业务调度——能够请求和修改跨越大量服务点的操作预约、会诊预约和其他医疗就诊预约；
- 病例管理——能够浏览和管理与治疗患者特定问题的连续医疗（如：糖尿病）有关的多次就诊和事件。

这些功能要由基于规则和算法来支持，这样有助于医生完成任务并且避免一

些并不轻微的错误(如:药物过敏反应),甚至能针对情况提出更适合的变通(如:CAT扫描与简单的X光)。

解决方案和决策支持算法完全依赖于患者可靠的和结构化的临床数据的可用性,这样可以完全发挥其潜能和优势。它们是从前的电子病历浏览器和UI的自然进化产品,并且为电子病历的可用性的提高提供了强有力的论据。

5.3.5.3 电子病历浏览器的应用

通过对各类电子病历浏览器解决方案的分析,可以看到每代解决方案都有自己的适用场景和角色,实际项目中可以针对不同用户的需求提供相应的功能,以满足不同场景和角色。

- IE浏览器服务:基于IE浏览器比较适合为外网用户提供浏览服务,比如,患者能够通过上网输入查询条件,查询自己的电子病历。
- 嵌入浏览服务:嵌入浏览服务通过控件嵌入医疗业务应用系统,医疗卫生服务人员不需要在两个界面切换,对于其提供只有一个应用界面的一体化的嵌入浏览服务;
- 专业浏览服务:专业浏览服务适用需要对浏览信息进行处理,比如,影像浏览时需要对影像进行放大、缩小、旋转、动态播放等,就需要进行信息处理;
- 定制浏览服务:定制浏览服务针对不同用户个性化需求提供不同的浏览显示和浏览内容,比如,临床医生希望能够按照科室浏览患者,或者按照疾病类别进行浏览。
- 互动式浏览服务:互动式浏览服务除提供一般浏览服务的功能外,还可提供数据的采集录入。比如,医生在工作站中医嘱录入——能申请检查(如:诊断成像,操作和检验),处方和调配药物,都能被浏览器获知并存储于数据中心。

5.3.5.4 电子病历浏览器的功能

1) 浏览器展示

- J2EE的B/S应用

浏览器展示信息以JAVA类包(jar)形式提交，在J2EE下集成。

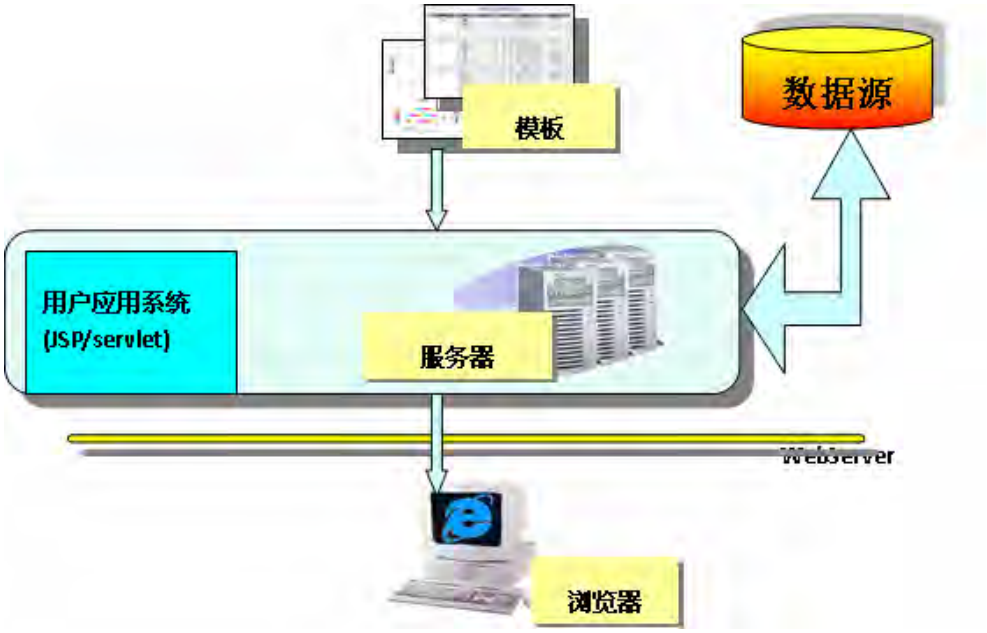

图 5-18 J2EE 的 B/S 应用

上图中，服务器是个逻辑概念，并没有一个物理的服务器在运行。它是作为应用服务器上的一个应用提交，或者直接向应用程序员提交JAR包。应用程序在JSP中可使用Tablib或直接调用开放的JAVA API就可以方便应用浏览器提供的各项功能以达到最高的运行效率，同时还能够与应用程序一起统一部署。

- 非J2EE的B/S应用

非J2EE机制的WEB应用集成浏览器采用Web Service的方式，

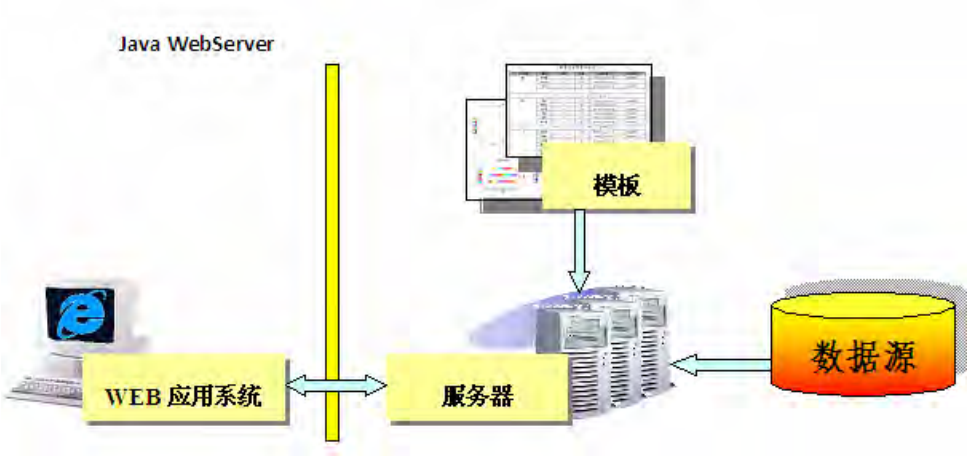

图 5-19 非 J2EE 的 B/S 应用

在应用系统的后台运行服务器，向其它WEB应用提供Web Service，通过URL访问机制传递参数并获得运算完成的HTML结果流（或Excel、PDF、WORD流），然后再由该应用发布到浏览器上。在非J2EE应用服务器上，可采用专门的WEB服务转发程序。

- 控件方式嵌入应用

采用可选的Windows展现控件可将浏览器应用于Windows GUI程序中。还可以将浏览器显示的数据生成成Excel/PDF/WORD流再采用第三方控件展现在GUI应用界面中。

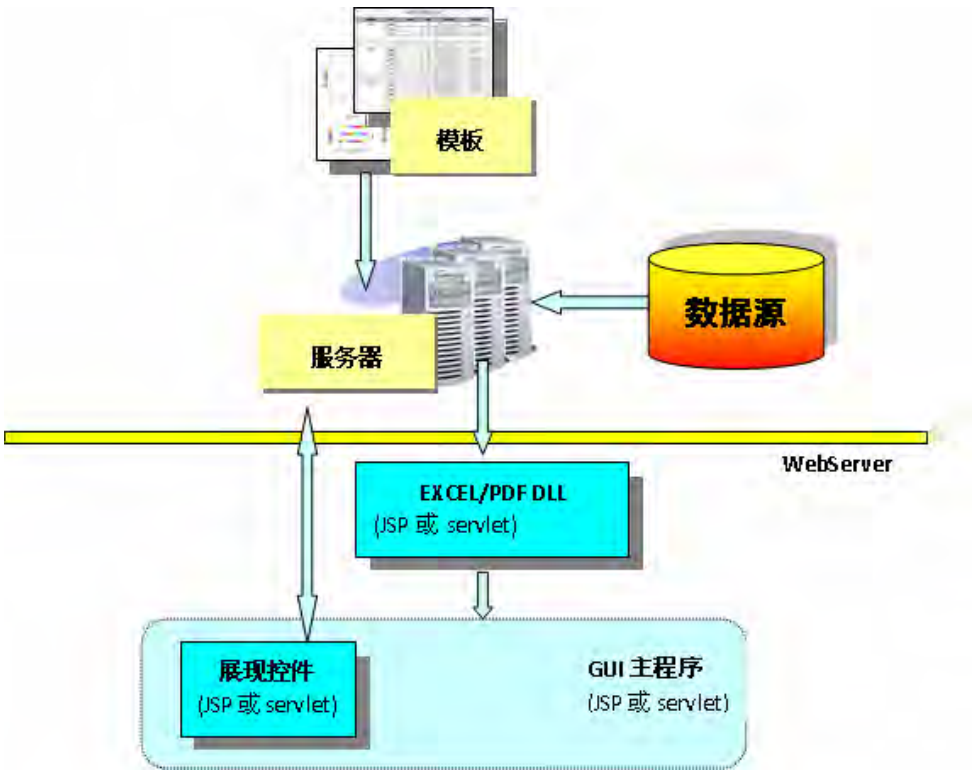

图 5-20 控件方式嵌入应用

2) 联机填报

浏览器服务器程序在后台根据绘制好的配置文件生成可以填写的HTML表单，用户直接在浏览器中填写，提交后再由浏览器服务器根据填写内容和配置文件将数据写入数据库。

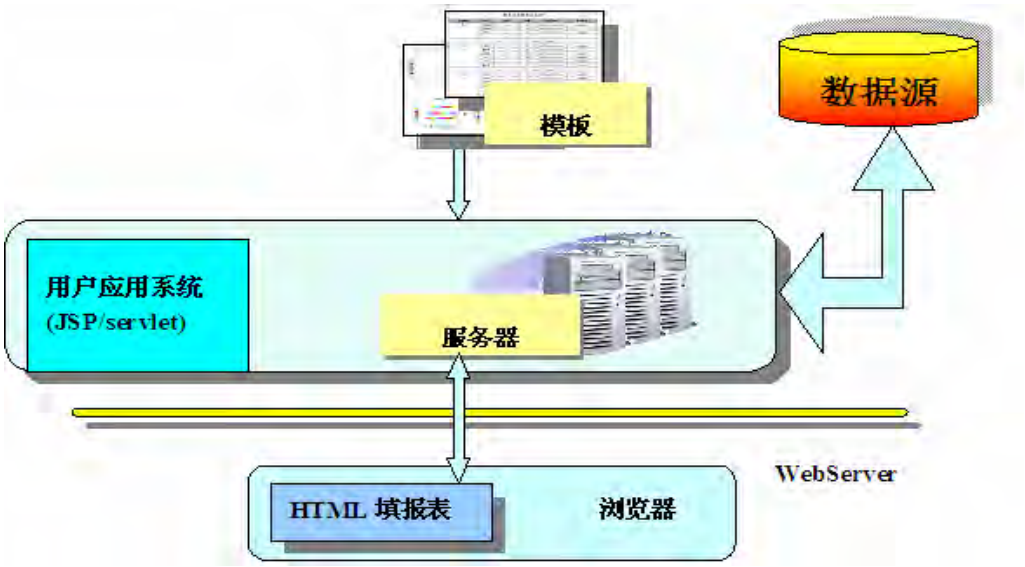

图 5-21 联机填报

3) 浏览器配置

基于可选的集成（远程）设计支持包，填报设计器可被集成于用户的统一门户管理之下（B/S或C/S均可，B/S下需采用WebStart机制启动设计器），模板文件可送交远程的资源管理服务自行处理，同时可通过支持包中附带的HTTP-JDBC接口连接远程的数据库进行设计和预览,而非直连到数据库上(在WEB端设计时原则上根本就不允许直接到数据源上），从而保证数据文件（资源）与数据都能够接受统一的门户权限管理。

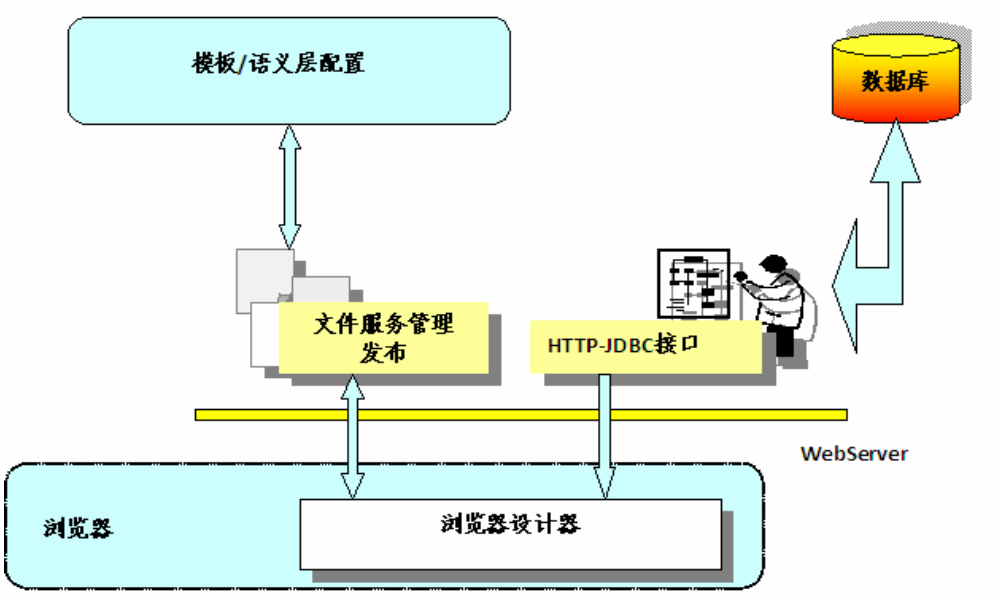

图 5-22 浏览器配置

4) 信息安全控制

为了进行权限的控制，提供了登录的机制。即用户进行连接之前，必须进行登录，登录后系统即可读取该用户的会话变量，并传递给远程服务器。远程服务器根据会话变量返回该用户有权限使用的所有数据库连接，并将会话变量传递给文件服务器，由文件服务器动态组织出该用户有权限读取的语义层文件内容，并将该语义层文件以流的方式传输到客户端。由此实现了不同的用户享有不同的数据库连接，不同的用户读取不同的语义层内容，实现了更高层面的权限控制，从而满足信息安全、患者隐私信息保护等要求。

文件服务器的作用是接受文件访问请求，根据会话变量，判断请求的合法性，然后处理文件请求，返回处理结果。

5.3.6 全院业务协同支撑服务

随着网络、通讯、软件技术的快速发展，特别是医院内部网络系统的不断完善，出现了多种支持医院协同工作的技术。比如，信息门户，业务管理（BPM）和工作流管理系统（Workflow Management System），即时通讯工具（IM），呼叫中心（Call Center），短信平台（SMS），视频流媒体服务，电子邮件(email)，信息门户（Portal）等技术；这些技术适用不同的协同过程模式和业务协同环境。比如 BPM（Business Process Management）适合于事先定义完成的业务处理过程，业务步骤明确，人员责任明确，比如门诊诊疗过程，疾病的临床路径，住院流程，药品供应流程等；即时通讯工具适用于医院内部人员之间的在线交流共享信息等非正式的快速沟通交流，提高工作效率；呼叫中心适于与预约挂号和咨询服务等病患和医院之间的沟通服务，电子邮件适合于更广泛的动态联系的协同过程。

基于电子病历的医院信息平台基于 SOA 架构设计，将各种类型的协同工具服务组件化，统一在信息平台上进行注册，提供服务调用适配器接口或 WebService，以便平台的其他应用程序和组件利用协同组件工作。下图描述了基于电子病历和 SOA 架构的医院协同支撑服务平台的组成部分及其关系。

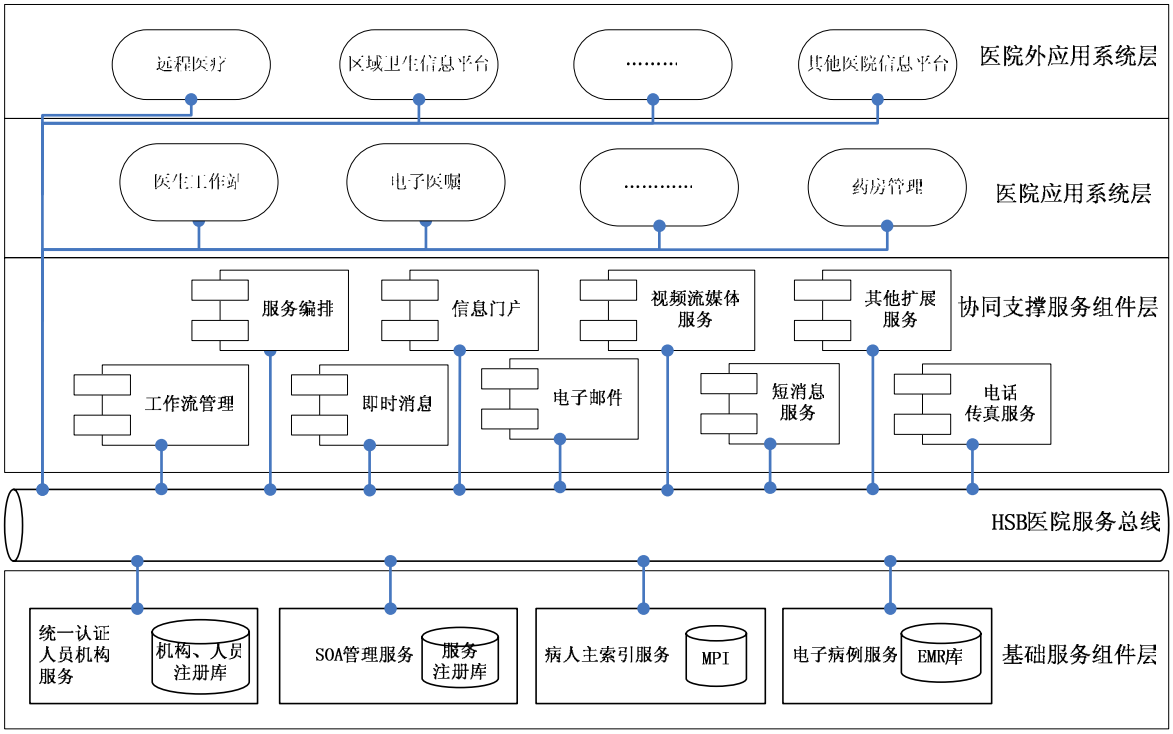

图 5-23 基于电子病历及 SOA 的医院协同支撑服务组成

从上图可以看出，基础支撑服务组件包括：统一认证人员机构服务、SOA管理服务、病人主索引服务和电子病历服务等；协同支撑服务组件包括：业务过程管理、工作流管理、服务编排、即时消息、信息门户、视频流媒体服务、电子邮件服务组件、短消息服务组件和电话传真服务以及其他服务扩展。这些组件都插接在 HSB 医院服务总线上，供医院内部应用系统和医院外部应用系统调用。协同组件之间也可以通过服务总线项目调用，实现多种通讯方式的集成。

业务协同支撑服务组件从应用对象的角度可分为系统协同支撑服务组件和人员协同支撑服务组件，以下分别作出简要描述。

5.3.6.1 系统协同支撑服务组件

业务过程管理

业务过程管理（Business Process Management，BPM）定义为：在一定的空间和时间范围内，由一组任务组成，这些任务被设计用来共同创造特定的产品或服务，并保证实现组织的总体目标。

工作流管理

目前工作流标准主要由 WfMC 和 OASIS 维护，WfMC 发布的工作流标准包括：XPDL，BPML，没有人参与的工作流过程包括 BPEL（Business Process Execution Language），意为业务过程执行语言，是一种基于 XML 的，用来描写业务过程的编程语言，被描写的业务过程的每个单一步骤则由 Web 服务来实现。

BPEL 语言说明了业务过程的行为特性，过程的活动是 Web 服务。人员交互并不在其范围内。虽然在分布式商业应用中广泛采用了 Web 服务，但是缺乏人员交互是应用于真实世界业务过程的一大差距。为了填补这个差距，BPEL4People 扩展了 BPEL，从只能编排 Web 服务，扩展为同时支持对 Web 服务和基于角色的人工活动进行编排。

工作流引擎是医院协同支撑服务的核心部件，具体实现技术不做限制，应该能够支持 XPDL，BPEL4People 标准。

服务编排

服务编排服务组件是指将 Web 服务组件编排在一个处理流程并支持其执行的组件。应该支持 BPEL 标准，WebService，WSDL，SOAP 协议。服务编排组件可以通过可视化编辑工具设计 BPEL。

5.3.6.2 人员协同支撑服务组件

视频流媒体服务

视频流媒体服务组件能够介入远程视频会诊室的扩音设备来控制各扩音器,会议室上各摄像机,显微镜,B 超等的视频信号和高清晰混音器的音频信号输入到视频流媒体服务器，其含内置密码并对输入的音视频信号进行数字化,采用先进的音视频数据压缩格式 H.264 标准的码流，经授权的用户在连入该区域专用网络的计算机或手机上使用浏览器收看视频会议实况,多媒体会议室之间可以互动讨论。

远程视频会诊(会议)系统将远程会议室的影像信息通过该区域系统专网与视频会议系统连结，将不同地域的几个会诊(会议)室和视频会诊(会议)活动影像在同一时间内在同一显示屏幕显示出来，这样在视频会议内就可以通过大屏幕投影观看同一时间内的多个会议室视频会诊(会议)。医学专家可以通过计算机与远程（异地）会诊(会议)室的视频会活动交流，同时将影像通过显示设备。

视频流媒体服务组件可以嵌入到远程医疗系统软件中，实现在会诊中调阅电子病历，检验的医学影像等功能。

信息门户

信息门户服务组件，一般由内容管理系统（CMS）提供，可以定义频道，发布文档和信息，支持全文信息检索和查询，信息门户也是页面集成的工具，应该支持 JRS168，JRS286 和 WSRP 标准。通过 Portlet 集成医院内部信息系统的 web 页面。

信息门户提供网络博客功能，提供医学保健知识信息频道，支持与医学专家在线交流等功能。也可以通过信息门户预约挂号，或则预约检查。病人可在信息门话上浏览检验解决报告。

即时消息

即时消息（Instant Message），是指 QQ，MSN，ICQ 等网络即时交流的实时通讯工具，医院 IM 需要具备开放性，可集成性和可扩展性要求。

开放性：应该支持开放的 IM 标准如 XMPP，以实现不同 IM 产品的相互联结。

可集成性：包括能够与医院组织机构管理的集成，能够从组织机构中同步组织机构和人员信息，并自动在 IM 中建立帐号。提供客户端程序和 ActiveX 浏览器插件或 web 客户端，以实现和业务系统的页面集成。需要提供 WebService 接

口能够注册到服务总线上并被其他服务调用。

可扩展性：系统应具有较大的可扩展性，以适应不同规模医院的用户数量的变化。

即时消息系统应具备的功能包括：

会话功能：IM 即时消息，收发文件，截图，表情符，字体，清屏，自定义组，邀请，在线人员查看；

文件、消息管理：文件管理,离线传文件,未读消息管理

消息广播：医院广播，科室及广播

人性化设置：我的部门,常用联系人,部门优先,个人优先,我的部门、我的联系人,最近联系人

IM 互通：能够与 MSN，QQ 等常用 IM 工具相互联通

多客户端：WEB 客户端,手机客户端

个人设置：基本资料,联系方式,详细资料,用户自定义头像

语音视频聊天：支持点对点语音、视频传输、多路语音、多路视频

协同：电子白板，文件共享，网页共享，程序共享等功能

组织结构：树形显示组织架构树形结构形像显示，优先级设置，部门按优先级排序，部门管理 添加、修改、删除部门

用户管理：创建及管理用户，创建、修改、删除用户（可批量添加）， 用户资料登记 设置用户姓名，性别，职位，邮箱等基本资料，优先级设置 设置人员在组织架构中的排列顺序

权限设置：角色设置，可组合创建、修改、删除三种权限，群组管理员分配，给人员赋于群管理员角色。

电子邮件服务

邮件系统是医院 IT 基础服务，应提供如下功能：查新邮件，写邮件(支持 HTML 格式编辑，带附件)，发邮件(立即发送、定时发送、群发)，取外部邮箱邮件(POP3/IMAP4/Hotmail)，邮件处理规则（自动转发、自动回复、自动处理、规则拒收），通讯录管理，私人通讯薄，邮件夹管理，语音邮件，视频邮件，网络硬盘（支持多级文件夹），共享网络硬盘，已读回执，删除邮件等功能。

为了实现电子邮件的收发，需提供电子邮件收发的服务组件，以实现与其他

系统的集成。

JavaMail API 是基于 Java 的邮件发送和接收的框架，可以跨平台实现邮件接收和发送。对于 Windows 平台也可采用.net API 实现邮件收发的 WebService 组件。

短消息服务组件

短消息服务是指通过手机发送的短信，短信服务可以通过直接连接电信运营商的短信 API 通过网络发送，还有通过短信 Modem 的方式直接发送短信。不管采用哪种方式，需要提供短信发送的服务组件的 WebService。

可以从患者主索引服务获取患者个人手机号码；可以从医疗卫生服务人员注册服务中获取医院内部员工的手机号码。

电话和传真服务组件

呼叫中心（Call Center）作为一种能充分利用最新通信手段和计算机技术的现代化服务方式，医院建立呼叫中心可以明显地改善服务水平和提高病人的满意度，利用呼叫中心可以开展的业务包括：

可以为医院提供多种跟用户沟通的方式，方便用户就诊。系统支持的跟用户沟通的方式包括：电话、传真、Internet、短消息、WAP 等。电话服务中，用户还可以选择自动语音服务和人工服务。

用户可以随时接触到专家级的咨询和诊断，预约挂号。

呼叫中心和电子病历系统集成，只要输入用户身份识别号（ID 号）就可以将用户的所有记录调出，从而为用户提供精确的诊断。

呼叫中心提供用户电话号码的识别功能，这种人性化的服务，使得用户一旦接通电话，系统就能认出用户是谁，使用户倍感情切。这样，当用户进行专家咨询时，就不必从头到尾向专家解释自己的病因、病史。

当用户受到不公正的待遇时，可以随时拨打医院的投诉热线，让用户摆脱那种在对医院和医护人员的被动服从的心理压力，提高患者的满意度。

呼叫中心提供的服务包括：

电话接入、分配、排队、语音导航、自动业务、传真，短消息服务，电话录音、呼叫，这些服务都可以作为基础通讯服务整合到医院工作流程中。

5.3.7 医院信息系统集成

5.3.7.1 医院信息集成的方法

医院信息集成包括三个方面的内容，即界面集成，数据集成，应用集成。这三种集成内容各解决不同方面的问题。界面集成含义是应用程序界面之间相互关联引用合成，采用技术包括 Portlet，ActiveX 插件，IFrame 等；数据集成是指应用系统的数据库系统之间的数据交换和共享，以及数据之间的映射变换，常采用 ETL（Extract Transform Load）工具实现；应用集成指应用程序之间实时或异步交换信息和相互调用功能，可以采用 CORBA，EJB，DCOM，WebService，RPC 等标准，采用消息中间件和企业服务总线等中间件实现。

从医院信息系统应用集成的架构来说，存在三种模式，即点对点，单体系统，基于 ESB（Enterprise Service Bus）集成。

点对点集成适合于少数系统之间的应用集成。n 那个系统集成的接口数量达 n*n 个，像医院这样复杂信息系统，采用点对点方式集成是不现实的。

单体系统，比如套装 ERP 软件供应商提供的 ERP 系统，整个系统有统一的数据模型和数据库（或分布式数据库），消除了各个系统之间的接口问题；但是，单体系统的修改和适应新业务的能力比较差，修改成本过高，也不适合目前企业重组和流程再造多发的市场经济竞争环境。

单体系统和点对点混合是目前医院主流的集成模式，比如医院管理信息系统由一家软件供应商提供，PACS，LIS 由其他供应商提供，还包括 ERP 系统，OA 系统，信息门户网站等异构系统。

企业服务总线（ESB）是一种体系结构模式，支持虚拟化通信参与方之间的服务交互并对其进行管理，是实施 SOA 的连接基础软件。使用 ESB 模式可以降低连接各个异构应用系统的工作量，降低相连的应用系统之间的耦合度，从而从本质上提高了整个系统的灵活性和面对变化的响应速度。它代理服务提供者和服务消费者之间的连接，即使它们并非完全匹配，也能够使它们进行交互，此模式可以使用各种中间件技术和编程模型实现。

在 ESB 模式中，服务交互的参与方并不直接交互，而是通过一个总线交互，该总线提供虚拟化和管理功能来实现和扩展 SOA 的核心定义。因此 ESB 模式使

请求者不用了解服务提供者的物理实现——从应用程序开发人员和部署人员的角度来看均是如此。

5.3.7.2 基于 ESB 的医院信息交换层组成

从需求分析可以看出医院信息平台需要一个信息交换层，医院信息交换层在整个医院信息系统的作用和地位如下：

- 在纵向信息集成中相当于 Infoway 的医疗信息交换层（HIAL），起到信息共享和数据交换的中间件作用。
- 支撑医院横向业务系统消息交换和信息共享，通过协同支撑服务来达到院内业务系统的互操作。
- 为未来建设 SOA 医院信息系统提供基础服务。

符合 SOA 架构的医院信息交换层一般采用医院服务总线（HSB）来实现。

5.3.7.3 医院服务总线

医院服务总线需支持主流的开放标准和规范，提供可靠的消息传输机制，建立服务之间的通信、连接、组合和集成的服务动态松耦合机制，为集成遗留系统和新建基于 SOA 的应用系统的服务集成提供了支撑。

并在此基础上，开发面向应用的业务适配器组件，实现各集成应用之间可管理的接口透明，为企业应用提供了便捷、一致、安全并符合标准的丰富接口，保证服务之间信息的可靠传送，实现不同操作系统，不同数据库、中间件运行平台及其基于这些平台之上开发的应用软件的服务集成。

HSB 应具备可插拔的服务协调、传输协议转换、消息转换和路由的能力，如下图所示：

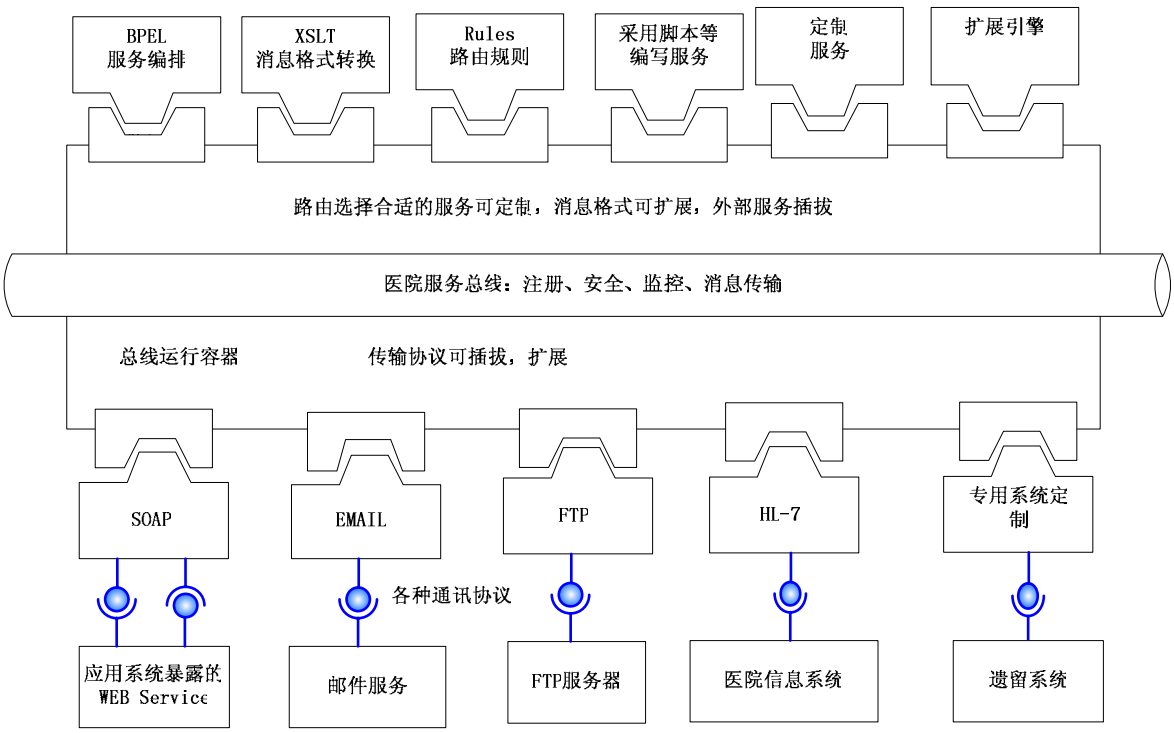

图 5-24 HSB 服务总线框架图

HSB 内置的服务组件包括：

- BPEL 服务编排组件能够实现采用 BPEL 语言编写的业务过程服务编排和组织，而不需要编译源代码和重新开发服务组件。
- XSLT 消息装换服务支持使用 XSLT 将输入 XML 格式的消息转变成目标 XML 格式。
- 规则引擎能够实现基于规则库的消息路由和智能化的服务调用
- 服务提供引擎开发 API 为总线二次开发服务

HSB 内置的传输组件包括：

- 使用 HTTP 传输的 SOAP 协议，能够连接 WebService 端点
- 使用 EMAI 传输协议，可以连接 POP3（SMTP）电子邮件服务器，监听受到的电子邮件并自动处理
- 使用 FTP 传输协议，可以连接 FTP 服务器，监听受到的文件并自动处理
- HL7 传输协议，可以读取使用 HL7 格式的 XML 文档，并将消息传入总线，发给其他服务。接口形式可以是 COM，XML 文件或者是能够产生 HL7 文档的代理程序

- 传输组件 API 提供接入遗留系统的二次开发能力

HSB 应具备如下特征：

- 支持广泛开放标准：符合 Web service、XSLT、XPATH、WS-Security、SSL、WPDL、BEPL4WS 等标准
- 可靠的服务事件传输：服务总线的可靠消息传输和异步通讯特征通过基于消息的基础中间件实现。服务总线应该支持 JMS 或 MSMQ 等接口的第三方消息中间件。总线服务器内部服务不通过消息队列传递消息通过内部的传输服务实现数据传输和调用，明显地提升了系统处理消息的性能
- 支持可插拔服务组件：支持引擎扩展和传输邦定扩展
- 内置丰富引擎组件：以实现组件包括 BPEL，XSLT，Rules，Script，SCA 组件等
- 支持多种传输构件：以实现组件包括 SOAP（HTTP），JMS（MSMQ），EMAIL，FTP，医院电子病历适配器等
- 支持集中管理和分布部署
- 安全策略：采用统一认证方式，与安全认证服务中心集成工作，建议采用支持 LDAP 标准的目录服务系统来管理注册库(组织,人员,术语等)，选用 KPI/CA 认证和口令认证等安全策略，安全策略是管理工具可以配置的
- 支持同步和异步服务调用：同步调用采用 web 服务直接调用，采用消息队列传输支持异步服务调用

5.3.7.3.1 医院服务总线功能

HSB 从功能上可以分为总线服务管理层、消息传输层、域服务器层，服务组件及适配器层共四个层次，如下图所示。

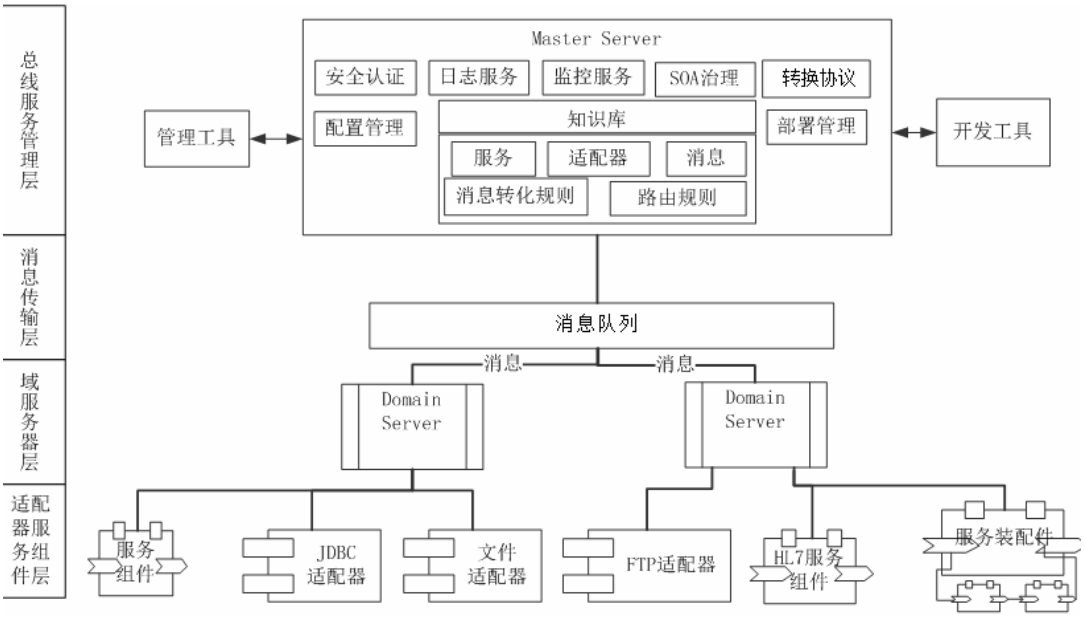

图 5-25 服务总线总体架构图

主域服务器（Domain Server）主要是对 SOA 架构中的基础资源进行管理，消息路由、转换，事件响应，安全机制，服务生命周期管理，监控功能等。主域服务器负责管理分布式域服务器，将域服务器的配置信息集中管理和发布。

主域服务器的核心部分是知识库。通过服务管理工具，对运行于医院内的服务进行注册，安全策略进行配置，注册新开发的业务服务组件和应用程序接口适配器，实现服务总线的二次开发和扩展。

下图显示了分布式部署服务总线的管理模式，服务器管理员可以集中式和分布是管理总线服务器。总线管理模块提供对域服务器信息的配置和管理提供基于 Web 方式的管理工具。

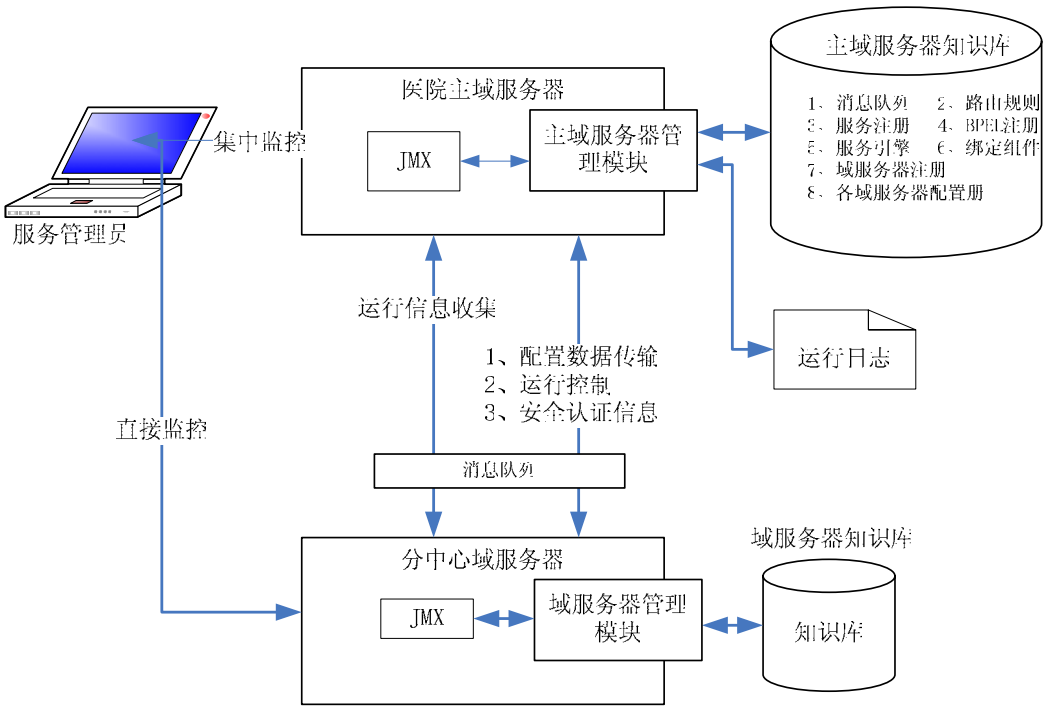

图 5-26 总线服务器的管理模式图

域服务器（Domain Server）和主域服务器是服务总线运行环境，主要面向业务领域运行，支持服务组合的运行、数据路由、数据转换与 Domain Server 的自治管理。

域服务器的管理功能包括：

- 资源注册管理：服务器注册，组件注册，使用消息队列注册；
- 部署管理：域服务器注册，服务器控制；
- 安全策略配置：通讯安全策略选择，安全策略包括，域服务器信任模式，消息传输加密模式，服务访问权限等；
- 服务状态管理：管理各个域服务器上管理的服务的生命周期管理，比如启动，停止；
- 服务发布和发现。

5.3.7.3.2 服务总线基础服务组件

表 5-9 HSB 基础服务清单

服务域名	服务名称	服务描述	接口方式
服务注册域	服务注册服务	查询，增加，修改 Web 服务和 WSDL 文件的功能	WebService SOAP
	机构注册服务	查询，增加，修改，删除医疗机构，药品供应商等	WebService SOAP
	消息格式注册服务	查询，增加，修改，删除 HSB 内部服务	WebService SOAP
	服务引擎注册服务	查询，增加，修改，删除 HSB 内部服务引擎，比如规则引擎，事件处理引擎，路由处理引擎	WebService SOAP
	绑定适配器注册服务	查询，增加，修改，删除适配器服务组件	WebService SOAP
医疗标准数据管理服务域	注册管理临床医疗基本术语和编码规范，例如：疾病术语编码；标准药品编码；诊疗项目编码；医用耗材编码等等	疾病术语编码维护服务，增加，废止，修改，启用，版本维护等功能	WebService SOAP
安全权限管理服务域	身份认证服务	认证用户的身份	WebService SOAP
	数字签字和验证服务	对 XML 文档进行数据签名，和验证签名是否被篡改，有效	WebService SOAP
	组织管理	管理医院组织机构和人员	WebService SOAP
	权限管理服务	管理服务和数据的授权	WebService SOAP
	日志服务	记录输入输出消息和调用的服务日志，为日志查询和审计的提供给出服务	WebService SOAP

5.3.7.3.3 服务总线与消息中间件集成

对于服务总线的使用者来说，消息队列的使用是不可见的。服务消费者，通过服务总线查询到可以调用某个服务提供者，但是该消费者并不知道具体使用了哪个真正的服务提供者，服务总线代替他完成这个工作：

首先，服务消费者向服务总线发出调用请求，总线通过 HTTP/WS 代理接受到该请求；然后，通过消息总线的消息规范化服务将消息规范化；接着，服务总线的服务管理找到能够提供该服务的服务提供者，将该消息发送到消息队列中，该消息传输可以使用发布/订阅的方式传输；最后，在另一台服务器上的服务接受到消息后，再转变成 SOAP 格式，再通过 HTTP/WS 代理调用真正的 Web service 服务提供者。

为了区分不同的事件类型（消息类型），采用消息主体方式进行分类：

1） 总线管理主题：用户管理服务总线的连接，传递服务注册信息

2） 服务生命周期管理主题：用户启动，停止，注册的应用 web 服务

3） 服务监控主题：收集服务运行信息

4） 服务调用主题：调用服务

5） 通过这些主题的设置可以完成服务的集中管理和监控。

5.3.7.3.4 适配器层

在服务层主要是各个参与流程协作的服务（或可以通过适配器代理的服务）的集合。适配器，是指把常用的服务接口转换为消息内部数据格式的代理组件。

通用的适配器一般包括 HTTP，JMS，EMAIL，FTP 等：

1） HTTP 适配器。支持服务组件的服务者和消费者登记和激活调用。支持标准：SOAP1.1 和 1.2，MIME 附件，WS-Addressing，基于 WSDL 发布，支持 WebService 服务消费者和提供者，SSL，WS-Security。

2） JMS 适配器。支持标准：JMS 接口，SSL；也应支持 C，C++，.NET 访问消息队列的 API。

3） EMAIL 适配器。提供服务总线收发电子邮件的功能，发送邮件也可以使用系统的通知服务实现。Email 服务也应提供 WebService 形式的接口

电子邮件收发服务。

4） FTP 适配器。提供服务总线使用 FTP 服务器的能力，读写 FTP 服务器传输目录中的文件，和定期轮询 FTP 目录中是否有新文件到达。

医院电子病历适配器，应参考电子病历相关业务规范与标准体系，在医院已建设的各业务系统的基础上建立电子病历适配器，实现电子病历和各业务系统之间的接口。

5.3.7.4 医院数据交换与共享

服务组件的开发分为：传统应用封装的服务组件，项目新开发的服务组件，和应用支撑服务组件三大类。

由于现存的大量的医疗信息系统并不是按照 SOA 架构设计开发的，即使采用服务封装的方法利用 HSB 进行集成，还是需要大量的资金投入和较长的开发周期。较为可行的电子病历库和 ODS 建设方法是通过医疗数据共享和交换组件实现。该组件需要具备 ETL 工具的各种数据源装载转换和清洗的功能，另外还需要与 HSB 集成，以实现数据共享服务的全程监控和管理，同时利用 HSB 的基础服务比如安全机制等。

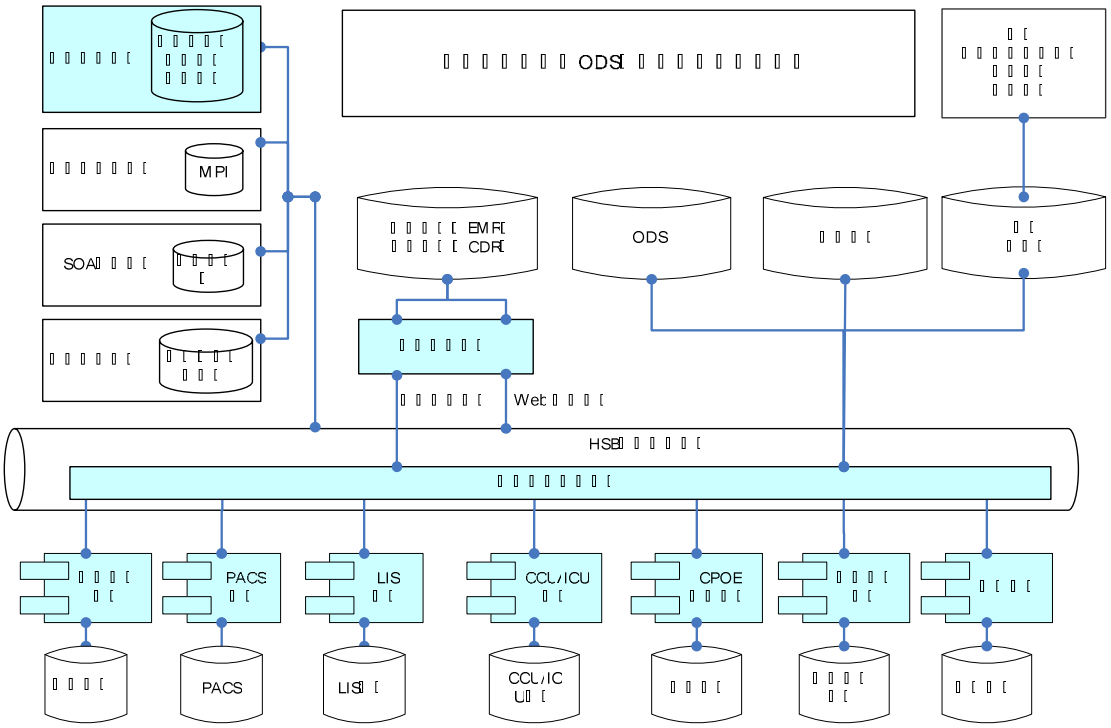

图 5-27 医院信息交换共享组件结构

医院数据交换和共享组件参考了国际 IHX 标准实现医疗 POS 系统信息交换。数据格式需遵照卫生部颁布的电子病历相关标准，参考 HL7 电子病历模版。

对于集成到 ODS 和数据仓库中的数据，可以采用数据库通用接口如 JDBC，ODBC 等实现数据抽取和加工装载。

5.3.7.4.1 设计开发工具

管理设计工具是数据交换平台的操作交互界面，设计的结果保存到配置库中。主要包括以下部分：服务模型，流程模型，规则模型，部署信息，权限信息。应该具备以下功能：

- 数据处理服务（任务）可视化配置
- 支持多种数据源，包括 WebService，XML，EXCEL，TXT，JDBC，ODBC，JMS 等。
- 数据加工流程可视化配置
- 数据库、文件、通讯等资源可视化配置
- 变量/规则的可视化配置
- 数据处理应用项目的可视化建立和部署
- 整合适配器的管理
- 数据加工过程的可视化监控

5.3.7.4.2 运行管理工具

管理服务器是数据交换平台的集中管理中心，主要具备如下功能：

- 服务模型管理
- 流程模型管理
- 规则模型管理
- 部署信息管理
- 响应管理工具的请求
- 通信信息的路由
- 运行环境和适配器的部署管理

5.3.7.4.3 运行引擎

运行环境是数据交换平台的运行引擎，它包括运行架构和基于其上的整合服务。主要具备以下功能：

- 变量的处理：自定义变量和函数处理数据转换和影射
- 动态规则的处理：支持基于 XML 文档属性判断的路由规则
- 整合加工任务处理：表复制，表路由，文件-表转换，表-表转换，表-文件的转换
- SQL 语句调用：SQL 函数调用，SQL 过程调用
- 流程的调动：数据流，变量流，处理流
- 运行环境之间的协同调度

5.3.8 数据架构

数据是进行信息资源建设的起点与目标。良好的数据架构是未来应用进行灵活扩充的基础保证。

医疗信息系统要适应业务的复杂多变，又需对海量数据作出高效反应。尤其是针对数据，要根据使用的对象不同，用不同方式快速的展现，而这些数据往往存储在多个数据库中。基于电子病历的医院信息平台的数据架构设计目标是：既能满足医疗机构内业务系统平滑开展协同过程，又能构建成以人为核心的电子病历可扩充构架，还能对医疗管理决策提供有效支撑。

5.3.8.1 总体架构

信息平台数据结构以临床文档库为中心，。对于各个业务系统产生的医疗业务信息、临床信息、医院管理信息，通过业务信息库进行整合；这些业务信息需要患者基本信息、医疗卫生从业人员注册信息和各种术语字典等基础信息的支撑，并以此形成电子病历信息；医院信息平台的重要特点是根据数据仓库中历史积累的数据实现决策支持；此外要有医院内部子系统之间的交换和对外信息交换数据库。

具体数据分布图如下所示：

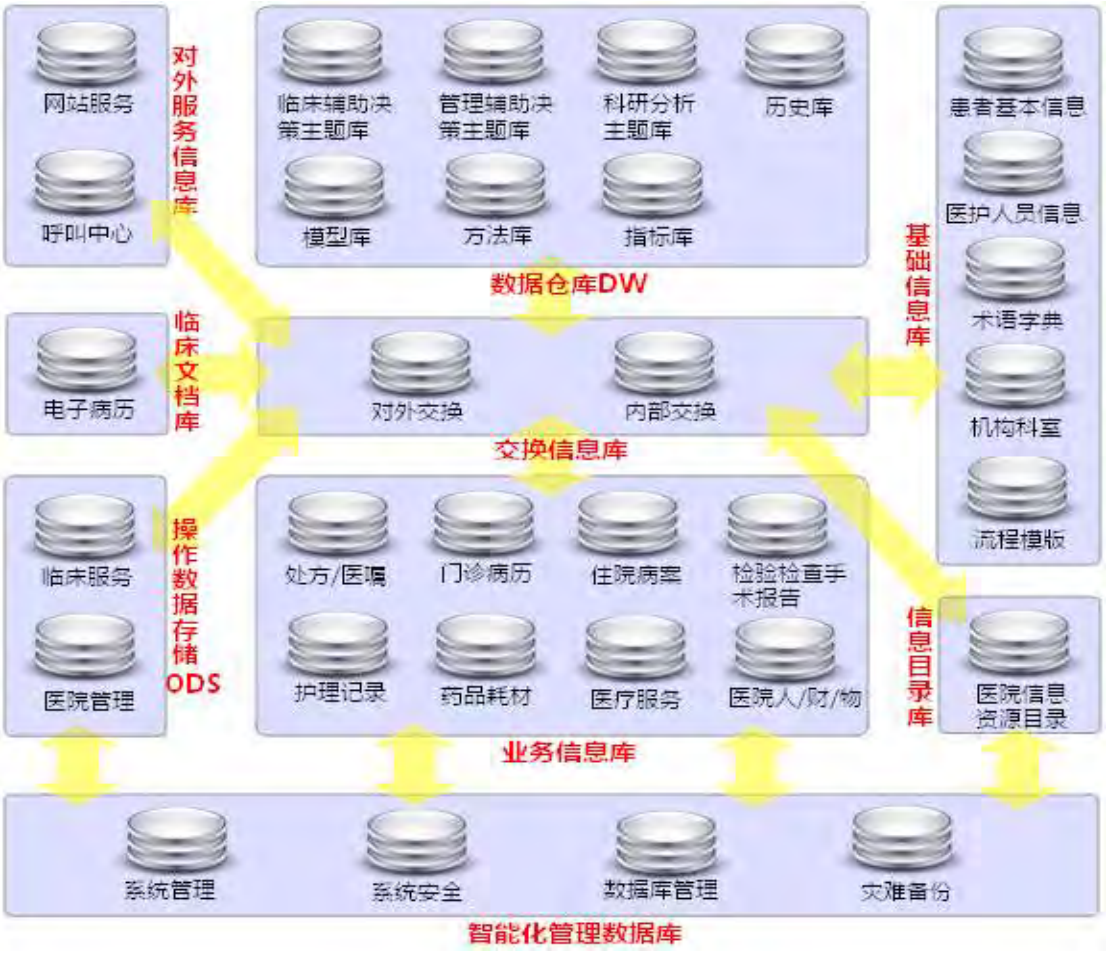

图 5-28 具体数据分布图

依照业界经验和最佳实践，基于电子病历的医院信息平台可以采用三层数据存储架构来进行未来的规划和建设，以完成不同的数据存储与统计分析服务目标。在具体技术实现时，应该从数据的生命周期、性能和经济性上综合考虑。

三层数据存储架构的划分如下表所示：

表5-10三层数据存储架构

数据存储层次	服务目标
数据采集与操作处理（OLTP DB）	■ 记录采集的原始数据记录 ■ 围绕原始数据进行的事务型操作 ■ 短期（如当天）实时查询与统计

数据存储层次	服务目标
CDR 及 ODS	■ 保存有效原始数据记录，以供历史数据查询，并共享给其他应用系统和省市区域信息平台 ■ 计算部分中间汇总表，提供主要的业务支撑服务 ■ 完成常规的智能分析，为用户提供操作指导
数据仓库(EDW)	■ 保留医院内部应用数据历史记录变更记录,可以做历史变更分析 ■ 可引入外部数据源，综合医院内所有的数据源历史记录，对医院进行跨业务跨应用的长期分析，提供决策依据

5.3.8.2 基础信息库

基础信息库集中了整个医院信息平台的基础信息和共享数据，是为各个子系统提供基础信息服务的。基础信息库包括了患者的人口学信息、医疗卫生人员的注册信息、以及各种医疗卫生、公共卫生术语字典数据及流程模板数据等。

病人基本信息是基础信息数据库中的核心内容之一。无论是电子病历、医疗业务、临床信息，还是疾病分析信息和公共卫生条线数据都是以病人基本信息为基础的。在此基础上，实现电子病历、医疗业务（含临床数据）的关联。

医护人员库是基础信息数据库中的另一个核心内容，以医护人员信息为基础。可以建立医院诊疗资源注册库，可以作为医院管理以及绩效考核的基础。

数据元字典是辅助各类医院业务、临床业务的基本数据元、代码集以及数据字典；以及包含了医院各种业务、流程说明模版的操作模型。

流程模版库是包含了医疗机构医疗业务、临床路径、管理流程、财务结算等所有信息系统正常运转、分布协同的规则库。通过流程模版库的流程引擎指导，能够明确患者在医疗机构内如何进行就医，临床医生如何对患者进行准确诊断，防保医生如何对疾病进行控制和分析，管理及后勤人员如何对医疗资源进行合理分配或者补充采购、财务结算人员如何统计和控制医院的收入和开支。流程模版库是医疗机构保证正常运转的核心，对各级医疗卫生人员和患者的医疗行为起着规范和指导作用。

5.3.8.3 医院信息资源目录库

在一个医疗机构网络中，并非所有的信息都被集中存放在一个物理存储中，

信息可能分布在医疗机构中的独立系统中。

为了解决上述情况的相关信息调用，信息资源目录库提供每条医疗信息记录的真实存放地址。在数据读取过程中，读取服务会通过信息资源目录库查询到真实存放地址，地址信息包括：存放服务器地址，存放服务名等信息。存放服务器都需要实现统一的基于WebServices的数据存储服务，同时使用非显性认证机制来解决安全问题。数据读取服务可以通过信息资源目录库直接到远端系统中读取相关数据。

在存放数据时，存放服务根据上传数据的情况，向信息资源目录库插入每条记录的地址信息，以提供将来读取需要。

信息资源目录库中的地址数据是存放在独立的数据表中，通过外键与EMR-Index联合。针对EMR-Index中的每一条数据，都可以查询到相应存放地址。

5.3.8.4 业务信息库

业务信息库是整个医院信息平台的数据基础，主要存储原始业务产生的数据，以未经过进一步加工的数据为主。包括诊疗业务流程产生的结果数据、医疗服务管理数据以及医院运营管理流程产生的结果数据。这些未经修改的数据，作为电子病历的备份存储，在以后发生任何疑问时，可调阅业务信息库中的数据进行核实。业务信息库中的数据要求在存储后不能被修改和删除，将作为系统的原始凭证被永久保留。从时效性和实际业务需求出发，业务信息库至少也要保存50年之内在线业务操作及结果数据。

医疗机构内部的业务数据分布于不同的信息系统自身的数据库之中，因此需要接入到覆盖整个医疗机构的信息平台上，以提供对原有业务数据的整合、利用服务，并为机构之间以及业务系统之间的联动提供支持。

业务系统通过设置交换信息库作为与信息平台的接入端代理，来实现业务系统与信息平台的互联互通性。体现在数据结构层面，就是业务信息库通过交换信息库实现数据的接入。

除了在信息平台上保存即时产生的，符合临床诊疗要求的各种业务原始数据以外，还需要以患者的基本信息为基础，整合患者历次就诊的就诊履历，完善患

者的医院电子病历。患者的基本信息保存在基础信息库中，电子病历保存在临床文档信息库中，也就是说，业务信息库根据基础信息库中的患者信息进行整合，并最终形成存储在临床文档信息库中的电子病历。

5.3.8.5 交换信息库

交换信息库是信息平台的数据转换枢纽，包括中心交换库和对外交换库。中心交换库的作用主要是对医疗机构内部信息系统业务数据的采集、整合以及医疗机构内部信息系统之间业务联动。对外交换库的作用主要是实现医院信息平台与区域信息平台的数据交互。

1) 中心交换库

考虑到医疗机构各个信息系统相对的独立性以及数据之间的关联性，我们在医院信息平台中设立中心信息交换数据库。中心交换库是采集医院各个业务信息系统的信息，并整合程电子病历信息的区域，也是各个业务信息系统基础信息和专业信息交换的信息存储区域。中心交换库存放各个信息系统交互的信息，包括了电子病历信息、基础信息（患者基本信息、医疗人员信息等）、专业信息（医疗业务、临床数据、检验检查报告以及影像数据等）。

2) 对外交换库

对外信息交换库是医院信息系统与区域卫生信息平台进行数据交换的信息存储区域。为保证系统的相对独立，我们设立对外信息交换数据库。对外交换库存储要推送到区域卫生信息平台的电子病历，同时也存储着从区域平台推送来的健康档案。在对外交换库中完成电子病历与健康档案的相互转换。

5.3.8.6 临床文档信息库 CDR

下图对临床文档存储库CDR在医院信息平台中的位置与地位做了描述：

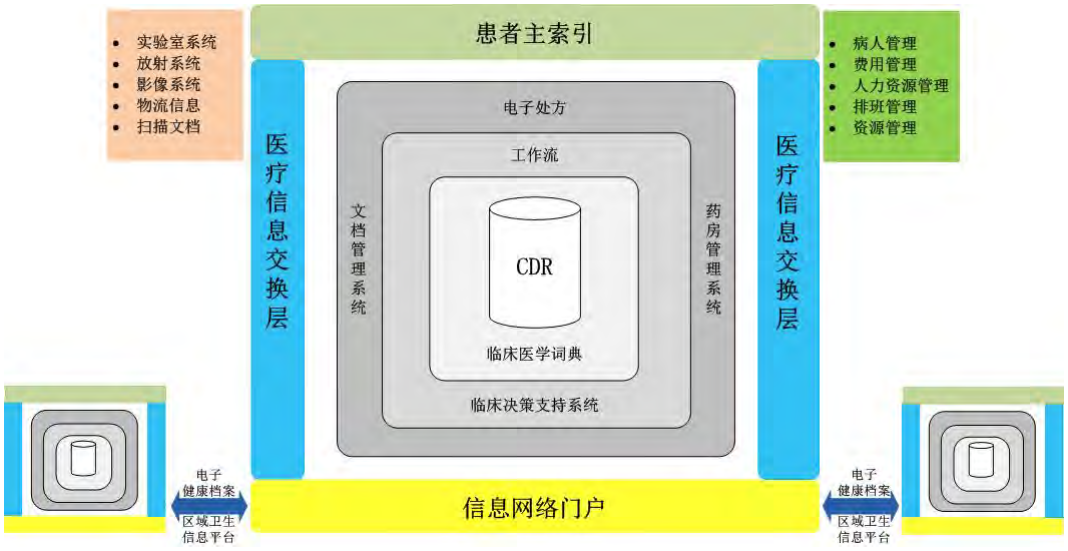

图 5-29 临床文档信息库

上图参照了美国的医疗卫生信息化组织（HIMSS）的智库HIMSS Analytics公司给出的一个EMR体系架构示意图。从图中可以看出，临床文档存储库CDR（Clinical Document Repository）是医院信息平台的核心构件。

CDR是医院为支持临床诊疗和全部医、教、研活动而以病人为中心重新构建的新的一层数据存储结构。它应该是物理存在的，而不仅仅是概念存在或者是逻辑存在。它是医院基于电子病历的信息平台的核心构件。它是否存在可以作为医院是否拥有真正电子病历系统的标志。它与直接支持医疗操作的前台业务信息库不同，其数据来自这些业务系统，但与前台业务流程无关。它也不是通常意义上的数据仓库，因为它的内容是随着医院业务活动动态变化的，并且直接支持医生/护士对病人临床记录的实时应用。

CDR独立存在主要用于实现：

1、 与复杂的业务处理流程分割

病人的临床信息来自医院现已存在的多种多样的应用系统。一般说来，它们是面向应用过程设计的，是由不同供应商提供的，具有不同的信息模型和软硬件平台，其功能必须满足管理与临床应用不同的过程要求，例如一个实验室系统。从医生开出医嘱，到条码打印和取得样本，样本传送与接受，上化验设备，化验过程的双向控制，化验结果的自动获取，报告的产出与确认，报告的发出与接受确实是十分复杂的。应用系统的数据结构设计必须满足这些要求，数据库内的化

验结果表达必然是复杂多变的。而电子病历仅仅关心化验报告的最终结果。因此，如果CDR仅仅保存从检验系统传递来的化验结果，那么电子病历系统就可以和复杂的业务处理流程相分割。如果电子病历系统中的化验结果要从检验系统中直接获取，就不得不关注上述的所有细节。

2、 透明、一致化的数据模型

CDR的独立存在使得一个统一的、透明的、一致化的电子病历信息模型的设计与实现成为可能。这样一个模型的存在对所有应用系统的开发商、对系统集成、对医生护士对病人信息的进一步应用都十分重要。

3、 应用系统升级容易

由于CDR和复杂的业务处理流程相分割，使得以后各应用系统（POS）的升级换代变得简单易行。而这种变化随着业务流程的变化和信息化水平的提高，是经常发生的，也是医院信息化发展进程中最让人头痛的问题。

4、 对医生/护士更友善，效率更高

医生/护士使用物理上保存的以病人为中心的电子病历记录比起使用分散在不同应用系统中的病人记录来更得心应手、更符合他们的思维习惯，应答速度会更快。特别是简单、统一、透明的信息模型的存在使得他们有可能根据自己临床工作的需要从CDR中剪裁出自己的病人临床记录子集。

5、 有利于电子病历深层次应用的开发推广

电子病历的存在不仅仅是要满足临床信息查询的需要，更重要的是要满足临床决策、教学、科研的深层次的要求，例如警告与提示系统、临床路径控制、循证医学支持等等。这些应用的开发，当面对一个数据相对稳定、信息模型简单清晰、与操作过程无关的存储库时，要简单得多。特别的，当服务点应用系统(Point of Service，PoS)发生变化时，也不会影响这些深层次的应用。

5.3.8.7 操作数据存储 ODS

CDR存储库的组织形式以患者电子病历为核心展开，其存储结构方式更多的以个人基本索引模式组织展开，以结果数据为主体，这样的组织形式在以个人视

角所见的电子病历中能够完整迅速的定位，但对纵向条线业务的支持却明显缺乏有力的索引组织，不能完全满足业务的需求。所以很多业务数据并不都在CDR存储库中存储，为了完成某些特定业务上的流程要求，可能产生很多中间数据，而这些中间数据都有赖ODS数据库实现其存储方式。

ODS数据库主要涵盖临床和管理数据，对数据即席查询、数据仓库、面向患者的公众信息服务以及区域卫生提供数据层支持。同时，ODS数据库支持整个医院范围内各业务系统的协同，可以与CDR结合作为院内临床及其他业务驱动的数据，为医院内平台级别的应用（非POS应用），如统一调阅等提供信息支撑。

ODS数据库主要是作为CDR存储库外的业务需求的补充。除了电子病历外，医院信息平台还需要支持一些其他业务，比如说妇幼保健等具体医疗业务。这些业务所需的一些信息可以从电子病历中抽取，但是同时另一部分信息可能和健康信息毫无关系只是为业务统计分析时使用，他们也有一定的业务流程，ODS就成为此类数据的存放场所。

ODS数据库还包含对这些业务数据的汇总、展现、统计查询等功能的支持，他不仅仅是一个单纯的存储服务，他可以依赖LRS实现共享和使用CDR存储库中已经存储信息的展示。

ODS、数据仓库和业务信息库的区别在于：业务信息库一般针对实时性非常强的事务性操作和这些操作所对应的业务数据。其特点是数据实时性很强，但数据规模不大。数据仓库一般针对很大规模的数据量。但是其数据为历史数据，时效性不强。ODS则介于二者之间。

ODS、业务信息库和数据仓库三者之间的区别如下：

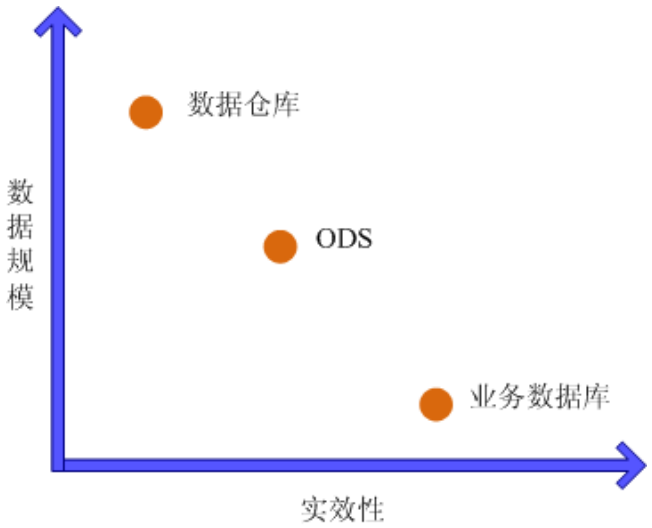

图 5-30 ODC、业务信息库和数据仓库三者间的区别

ODS、业务数据库和数据仓库三者在一个系统中的组合如下图所示：

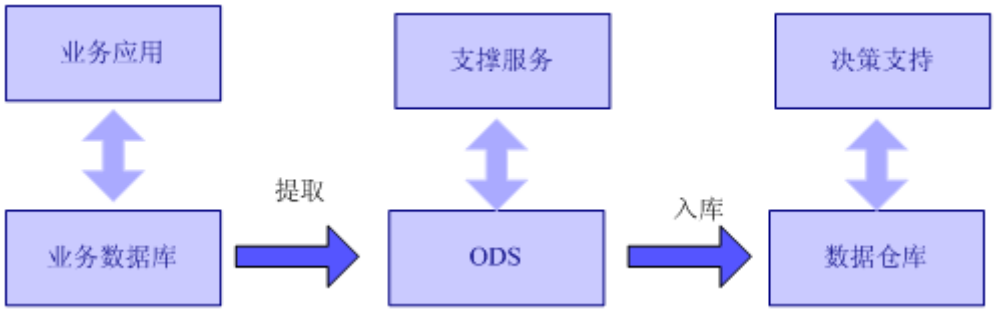

图 5-31 ODC、业务数据库和数据仓库三者组合图

如上图所示，ODS数据来源于在线业务系统的实时映像。映像数据保存周期为数据集市或数据仓库的装载周期。利用ODS系统，我们即可以允许历史数据在保存周期中进行更新，又可以随时对现有监测数据进行分析，满足应急性分析需求。数据从业务库抽取出来装载到ODS后，从ODS系统中进行数据清洗和转换从而完成在建立数据仓库/数据集市之前的数据准备工作。

为了不影响业务数据库的性能，一般ODS的数据库结构和业务数据库是完全一致的，这样数据可以高效的从业务数据库中抽取出来。ODS和数据仓库的数据库结构则往往区别较大。ODS的数据需要进行数据转换方可进入数据仓库。

5.3.8.8 数据仓库

数据仓库是在临床数据、医院管理类数据以及财务类数据采集的基础上对各类数据进行归类整合并加以利用。按其数据的性质大致可分为三类：卫生资源信

息、临床诊疗信息、卫生业务信息。其中卫生资源信息可作为卫生资源分布的基础数据；临床诊疗中与费用相关的信息可作为卫生资源消耗的基础数据；临床诊疗中的疾病数据和卫生业务信息可作为卫生资源需求的基础数据，医院的管理与决策可利用这些数据所产生的信息为相关的卫生决策进行支撑。

为快速的展示各种业务统计分析的报表及结果，必须首先对不同来源的数据按照主题的方式来进行组织和处理，按照业务统计分析的需求搭建数据仓库，实现对数据的多维管理。数据仓库包括相应的事实表和维度表，基于上述业务统计分析的要求，可采用多个面向不同主题的事实表共享维度表的“星型”数据仓库模型。数据仓库的建立，有利于后期对数据的高效应用。

基于电子病历的医院信息平台的数据仓库建设框架如下图所示，采取“ODS库→数据仓库→展示平台”的三级架构。

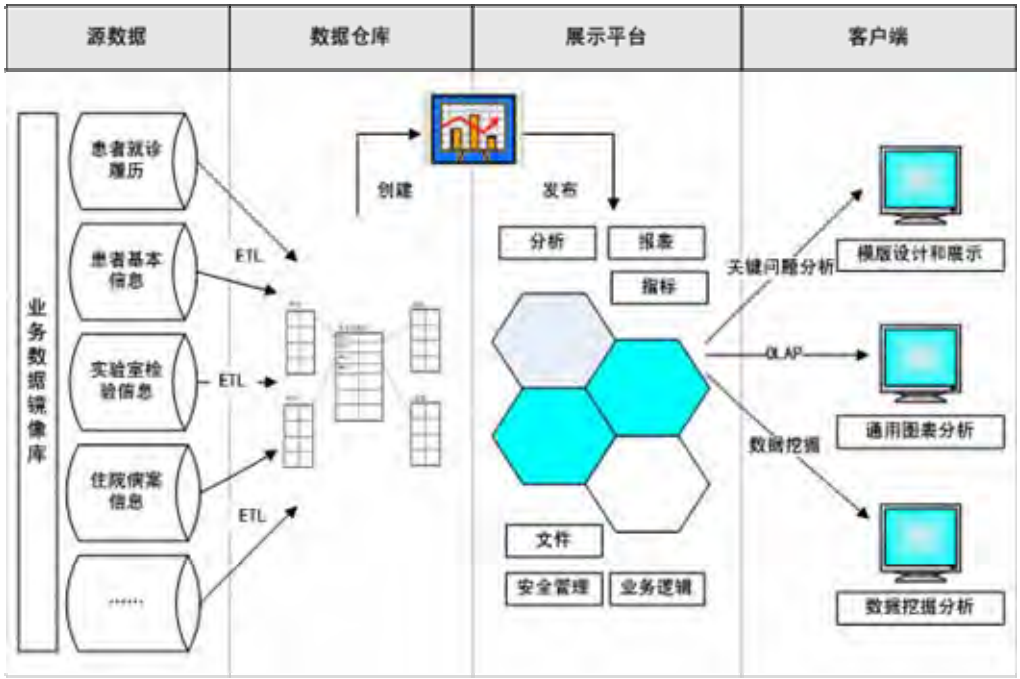

图 5-32 基于电子病历的医院信息平台的数据仓库建设框架

ODS库是医院医疗信息原始业务数据库的镜像库，定时与医疗信息业务数据库进行同步，为后面的数据转换、数据仓库建立提供稳定、可靠的数据源。ODS库的设置，缓解了ETL过程中频繁访问生产数据服务器产生的大批量数据交换对医院信息平台及网络造成的压力，并最大限度降低数据数据仓库对原有业务系统的影响。

数据仓库是数据整合汇总中心，以业务需求为基础创建ODS库数据的抽取整理规范及流程，抽象出满足业务分析主题的度量和维度，区分事实表与维度表，按照“星型模型”、“雪花模型”的方式建立事实表与维度表之间的关联关系，将原有的二维数据表转换成以分析主题为中心的多维表。数据仓库的建立，可以有效地管理业务数据，为数据展示、挖掘利用奠定基础。

数据仓库的数据主要供管理决策分析之用，所涉及的数据操作主要是数据查询，一般情况下并不进行修改操作。数据仓库的数据反映的是一段相当长的时间内历史数据的内容，是不同时点的数据库快照的集合，以及基于这些快照进行统计、综合和重组的导出数据，而不是联机处理的数据。因为数据仓库只进行数据查询操作，所以数据仓库管理系统相比数据库管理系统而言要简单得多。数据库管理系统中许多技术难点，如完整性保护、并发控制等等，在数据仓库的管理中几乎可以省去。但是由于数据仓库的查询数据量往往很大，所以就对数据查询提出了更高的要求，它要求采用各种复杂的索引技术；同时由于数据仓库面向的是高层管理者，他们会对数据查询的界面友好性和数据展示提出更高的要求。

5.3.8.9 对外服务信息库

医院需要对外提供各类形式的信息服务，同时，从系统安全性的角度考虑，在数据架构设计时，应根据具体的信息服务业务模式不同，设计相对独立的对外信息服务数据库，包括：

- ✧ **网站服务信息库**

建立独立的外WEB数据库，通过医院门户平台，为广大公众患者提供检验报告和检验履历查询、特色门诊网上预约、医疗咨询等服务。

- ✧ **呼叫中心信息库**

建立对应的呼叫中心信息库，以呼叫中心的方式，为患者提供医疗咨询、预约、检验检查结果报告查询、随访等服务。

5.3.8.10 智能化管理信息库

智能化管理信息库中存在几个相对独立的数据库，包括系统管理数据库、系统安全数据库、数据库管理数据库和灾难备份数据库。其中前三个数据库是出于

软件自身的功能需求，记录一些有关系统资源、数据库性能、监控等方面的系统信息、历史数据和日志；而灾难备份数据库则是从数据保护及最终应用切换的角度出发，提供对核心业务数据库、网站数据库、数据库等的异地备份。

异地备份的目标在于当信息中心的主服务器硬件失效、软件失效或系统运行环境失效（如电源失效、空调失效、大楼失火等等)导致计算机系统的失效时，能在较短的时间内进行系统恢复，并且最大限度地防止数据的丢失。

5.4 平台基础设施架构设计

信息基础设施层是支撑整个医院信息平台运行的基础设施资源、软硬件及网络等资源，主要包括各类系统软件、系统硬件、数据存储、网络设备、安全设备等。其中系统软件包括基础软件、数据库和数据仓库等。

5.4.1 基础软件

所谓基础软件是介于应用系统和数据库系统之间的系统软件。一般统称为中间件。具体包括应用服务器、门户服务器、内容管理和搜索引擎、企业服务总线、业务流程管理、业务规则引擎和事件驱动引擎。

5.4.1.1 应用服务器

应用服务器是Web应用拓扑结构的核心，是构造Web应用IT基础架构的基本支撑。大部分基于平台的应用将是Web应用，例如电子病历浏览器。应用服务器为Web应用提供了应用开发部署、数据存取和应用集成等服务。可以把一个Web应用看作一个客户与Web站点之间一系列的交互作用：整个交互过程从显示在Web浏览器中一个页面开始，通过用户单击该页面上的一个按钮或链接就产生一个请求，该请求被送到Web应用服务器，Web应用服务器对这个请求进行处理，产生新的页面，并送回到客户端，在Web浏览器中显示的新页面就是这一次请求的结果，可能也是下一次请求的开始。所以说，Web应用包含了一组交互或处理步骤，每一步必须产生一个页面形式的响应，这个页面作为后继交互作用的入口。

目前，国内医院在基于电子病历的医院信息系统建设中，主要有基于Java EE和.Net两种主流技术的应用服务器架构选择。

1) Java EE 应用服务器技术要求

- ✓ 通过Java EE兼容性认证,实现Java EE规范；
- ✓ 在支持WebServies方面：支持构建基于Web服务的分布式应用；
- ✓ 在跨平台方面：支持各种主流平台，如WINDOWS、Linux、UNIX等；
- ✓ 支持多种主流数据库，并对数据库的访问效率提供优化；
- ✓ 支持对两种以上异构数据库之间两阶段提交交易处理；
- ✓ 支持Connection Pool技术，Connection Pool可动态调整；
- ✓ 内置且支持主流的HTTP Server；
- ✓ 支持基于JMS的主流消息中间件；
- ✓ 支持Cache；
- ✓ 提供安全性方面：支持标准的安全协议SSL（Secure Socket Layer），支持Java5,JAAS,JSSE,JCE,CSIv2安全模式和技术，支持crypto card Eracom CSA8000；
- ✓ 支持XML；
- ✓ 基于Java Management Extensions(JMX)，提供图形化的管理工具，基于浏览的管理工具，可以方便的进行远程管理；
- ✓ 内置并提供对WEB应用服务器运行状态监测及统计分析功能，以便对系统进行有效的优化工作；
- ✓ 在提高开发效率方面：提供对应用开发的主流框架的支持。包括Spring Framework和Struts Framework等；支持嵌入集成化的应用开发工具，Eclipse、RAD、JDevelop等，支持JavaEE建模、开发、调试（支可视化环境中调试JSP、Servlet、EJB组件以及WebServices开发）、测试（集

成测试环境、单元测试、性能测试）到部署完整软件开发过程，提供开发效率。开发工具支持团队开发和主流的版本控制软件，如CVS等；

- ✓ 扩展能力方面：支持应用级负载均衡，能够管理多个应用服务器和组件的调度和运行。支持群集。支持单机环境下的应用级动态的负载平衡（多JVM进程）。支持多机环境下的应用级动态的负载平衡，说明负载均衡时支持的最多机器台数。支持异构Cluster，Web应用服务器支持异构Cluster技术。在原业务系统不停机的情况下，支持动态增加服务器，扩展系统性能；
- ✓ Cluster情况下，支持Session级故障恢复，单点登录的状态复制，容器的状态复制等等，从而确保了Web应用不会因为单点故障而导致用户数据丢失。支持应用服务器的亲和性、支持集中式管理，可以通过统一的管理器管理整个分布单元下位于多台机器上的多个应用服务器，并可以方便的进行图形化管理；
- ✓ 提供HTTPSession管理：在管理HTTPSession状态方面提供了多种不同的机制，支持HTTPSession存放在内存中、或固化到数据库中。支持Session级故障恢复。支持HTTPSession的亲和性；
- ✓ 提供并支持多种目录服务LDAP；
- ✓ 服务器端脚本支持方面：支持多种脚本语言，并满足Web2.0要求。比如可以部署php等多种脚本语言和动态语言应用程序；
- ✓ 监控能力方面：使得开发人员和系统管理员可以监控已部署的应用程序的运行情况。通过性能监控工具，收集应用程序运行时的各类信息，包括各类容器中消耗的时间，被调用的方法及其响应堆栈，关联的应用程序名和模块名，异常的出处等。可以利用收集的这些信息来进行性能调优和程序调试；
- ✓ .Net互操作性方面：能够提供Java和.NET互操作的能力。Java虚拟机JVM和.NET通用语言运行时CLR都提供了程序运行所需的功能服务，其中包括内存管理、线程管理、代码编译（或Java特有的即时编译JIT）等等。

由于这些特性的存在，在一个操作系统中，如果程序同时运行在JVM和CLR两种环境之上，由于任何一个进程都可以加载与之对应的任何共享类库，这使得相应的操作将变得非常繁琐。应用服务器应通过提供WebService和.Net互操作的框架，可方便的实现该应用服务器和.Net的互操作。

2) .Net 应用服务器技术要求

除了应具备上述JavaEE应用服务各方面共有功能之外，.Net应用服务器还有以下自身特点的技术要求：

- ✓ Web服务器支持方面：指应用服务器对Web服务器内置或集成的支持策略，Web服务器主要是IIS；
- ✓ 数据连接标准方面：支持的数据库ODBC连接标准；
- ✓ 对象模型支持方面：指对主要分布式对象模型的支持，包括CORBA、DCOM等；
- ✓ 提高开发效率方面：支持构建基于Web服务的分布式应用，协助程序开发人员更加容易建置及布署.Net应用程序。

5.4.1.2 门户服务器

基于平台的Web应用可以用门户的方式提供给用户使用。医院信息门户可以为医院的医务人员、医院管理者和患者等分别提供个性化的信息服务。门户服务器提供包括内容聚合、单点登录、个性化定制和安全管理等服务的基础Web平台，并能集成信息检索、知识库管理和协同工具等更高级的功能。

门户服务器（Portal Server，Portal）建立在HTTP Server之上。负责接收HTTP请求，调用Portlet，并将Portlet产生的内容聚集到Portal页面返回给用户。

门户逻辑分为门户容器和门户服务提供平台：

- ✓ 门户容器：提供了Portlets运行环境，使得实现JSR168/286规范的第三方应用可以将需要进入医务人员门户、或医院管理者门户、或患者门户的业务应用信息等集成。同时，门户容器为第三方应用提供单点登录、

用户授权、安全等服务。

- ✓ 门户服务提供平台：支撑门户容器的运行，提供核心业务服务和基础设施服务。并提供面向服务的体系架构，将异构平台上的应用系统的不同功能部件（服务），通过这些服务之间定义良好的接口和规范，按照松耦合方式整合在一起。使得第三方应用系统能够将门户所需要的业务信息、流程、文档和服务整合提供给终端用户使用。

根据基于电子病历的医院信息系统架构要求，需要的门户服务器技术能力要求如下：

- ✓ 跨越各个系统的用户集成统一管理能力，提供医院协同及面向区域医疗各类应用系统访问的单一登录能力，并且能够提供多种目录源及认证方式的接口；
- ✓ 能够方便地集成各类应用系统，通过数据集成，应用集成及展现集成方式实现医疗卫生网的入口；
- ✓ 实现个性化的界面展示和内容定制功能，用户可以配置完成个性化界面和展示内容的修改；
- ✓ 提供内容管理及发布能力，以模板化组件化的思路构建动态的管理发布体系，体现医院系统面向协同平台的信息发布能力；
- ✓ 具备支持用户的实时、异步的协同工作能力，支持个人信息服务能力；
- ✓ 提供与门户一体化的搜索引擎；
- ✓ 以上这些功能模块都必须一体化，能够集成进行管理，并且提供完善和方便的二次开发接口；
- ✓ 构建在Java EE架构应用服务器之上的门户服务器，要符合主流MVC框架为主的设计架构，并符合JSR168/268的Portal体系架构；
- ✓ 整个门户服务器软件的设计必须采用插件式的方式集成平台中的各个模块，并且提供集成平台的方便管理，保证各个模块的松散耦合，集中

统一管理；

- ✓ 门户服务器必须采用LDAP的目录认证方式，并可以选择和独立的认证服务器结合；
- ✓ 门户服务器既可以作为一个服务进行系统集成，也可以作为一个客户应用进行系统集成，必须支持WSRP的协议；
- ✓ 门户服务器中涉及的关键技术，如涉及到国际标准或国内标准相关的内容，应符合相关标准，保证系统的开放性；
- ✓ 门户必须提供良好的运行支撑框架，支持SOA架构，同时支持组件化的应用开发，保证各个组件的松散耦合，集中统一管理；
- ✓ 支持多种浏览器，支持多种手持终端等；
- ✓ 支持主流的操作系统，如Windows、Linux、UNIX等；
- ✓ 门户服务器能够支持选择多种主流的数据系统；
- ✓ 门户服务器必须提供符合WebService规范系列技术接口；
- ✓ 门户服务器需提供整合在一起的LDAP Server，同时能够与第三方的LDAP Server进行集成，提供灵活的安全身份管理解决方案；
- ✓ 支持多种标准技术，如XML、XSL、JavaScript、JSP、CSS等，用于门户页面的展现；
- ✓ 门户服务器具有良好的分布式功能和性能伸缩性，能够通过增加硬件设备实现系统性能的拓展和提高，应能够同时支持系统基于应用服务器的垂直扩展及水平扩展；
- ✓ 提供基于WEB的图形化的配置和发布工具，并且提供基本的系统性能图形化监测工具；
- ✓ 支持集成开发环境、门户组件开发工具和集成测试环境。

5.4.1.3 内容管理和搜索引擎

医院信息平台上不仅存储着结构化数据，也存储着大量的非结构化数据。对于非结构化数据一般采用内容管理系统来管理，使用搜索引擎来查询和使用。

1) 内容管理综合技术要求

- ✓ 组件化平台设计，分层架构，低耦合度，降低系统的复杂性，具有很高的扩展性和可维护性；
- ✓ 应具有良好的跨平台跨网段性能，支持Windows、Unix、Linux等平台，提供XML标准接口支持；
- ✓ 支持信息可选择动态发布和生成静态页面两种方式；
- ✓ 支持主流数据库；
- ✓ 支持主流应用服务器中间件。

2) 文档管理技术要求

- ✓ 支持单篇文档的录入、浏览、修改、删除、审阅等；
- ✓ 提供页面预览功能，文档录入到系统后，就可以预览发布成页面以后的效果；
- ✓ 支持多种文档类型，包括HTML文档、普通文档、外部连接、外部文件四种类型；
- ✓ 完整的文档操作功能按钮，便于用户选择操作，包括采集、发布、复制、引用、移动、删除、导入、导出、提交、版本管理等。

3) 模板管理技术要求

- ✓ 完整的模板操作功能按钮，便于用户操作选择，包括增删改、导入、导出、备份、恢复、预览、检索；
- ✓ 支持基于网页集成工具的模板可视化编辑；
- ✓ 可以支持任意风格的HTML模板，模板的内容置标和HTML、XML规范兼容；
- ✓ 模板的存储以及模板中所使用的图片、样式表、脚本等由数据库统一管

理，可以实现不同人员之间模板的统一。

4) 内容发布技术要求

- ✓ 提供静态发布为主的发布机制，系统要求以静态发布的方式提供主站的信息内容发布服务；
- ✓ 提供发布状态管理，用户可以方便的查看已发、正发和待发的任务；
- ✓ 可以分别指定主页、概览页面和细览页面的文件名和后缀，例如：可以让最终生成的页面为HTML、SHTML、ASP和JSP等，以便支持脚本等。

5) 内容审核技术要求

- ✓ 信息发布须支持可定制的多级审核流程，可以由各级管理员针对不同的栏目定制不同的审批流程，只有经过审核确认的内容才会最终发布；
- ✓ 所有编审的流程，都可以通过可视化的方式进行定义。流程的设置权限，可以由系统管理员统一分配,也可以由二级或三级管理员进行设置。

6) 搜索引擎技术要求

- ✓ 提供多种搜索策略，实现查全和查准目标的有机统一。针对中文特性，提供按字搜索、按词搜索、字词混合搜索等。按字搜索保证查全，按词搜索保证查准，并通过对分词词典的维护，逐步提高差准率，同时保证100%查全覆盖；
- ✓ 分词词典：系统支持设立主题词表、同义词/反义词典、禁用词典以及词典按需维护；
- ✓ 分词规则库：统计建立大量歧义排除规则，有效提高了分词准确性、提高查准率；
- ✓ 扩展检索：支持主题词典自动扩展检索、同义词/反义词自动扩展检索、全半角自动扩展检索、简繁体自动扩展检索等；
- ✓ 自然语言检索：对检索语串进行自然语言理解处理，根据关键词语在内容中的位置和频度等参数计算内容相关度，根据内容相关度从高到低输出检索结果；

- ✓ 支持搜索动态更新技术；
- ✓ 对数据库进行增删改操作时快速同步更新搜索，无需重建整个搜索也无需局部重建搜索，充分满足企业搜索应用的必备条件---信息的实时性要求；
- ✓ 支持全方位检索方式和多种结果展示方式，满足应用需要；
- ✓ 提供按字、词、句的简单检索方式，并支持多种检索运算符，按照位置检索、二次检索、渐进检索、词根检索等多种专业检索方式，满足科研等专业应用的要求；
- ✓ 支持运用多线程、高并发设计，海量数据即时响应；
- ✓ 要求采用多线程设计，支持SMP体系结构；采用完善的缓存（Cache）技术，支持数据库复制镜像，提高并发性能。同时，先进的搜索和查询算法、多库并行检索技术，使得G级数据库查询速度达到亚秒级；
- ✓ 要求支持以下三种字符集：GB2312/GBK/GB18030、BIG5、UTF8编码，方便多语言检索应用程序的开发，且支持中英文语种的混合检索。

5.4.1.4 企业服务总线（ESB）

医院信息平台中的医院信息交换层主要采用企业服务总线来构建。企业服务总线为实现医院内部各信息系统之间、和区域卫生信息平台之间，以及和上级卫生部门之间的数据、应用、流程整合提供服务。并提供SOA框架下，Web服务的集中管理和安全控制。

企业服务总线提供多种通讯协议的访问接入，不同通讯协议之间的转换，不同数据格式的加工和处理，基于数据内容的智能路由，基于主题的数据订阅/发布，应用整合异常处理。

对医院信息平台而言，ESB需要满足以下技术要求：

- ✓ SOA支持方面，遵循SOA设计原则和技术标准，能够构建标准的企业服务总线平台，提供松耦合模式，将业务逻辑和应用逻辑、数据逻辑等分离开，提供一个满足企业的应用集成和信息调解需求的解决方案；

- ✓ Web服务支持方面，支持最新WebServices标准，包括SOAP1.1/1.2、WSDL1.1、MTOM/XOP、WS-I Basic Profile 1.1等，支持WebServices自有的安全性WS-Security和寻址功能WS-Addressing，可以实现WebServices同步和异步不同形式的调用；
- ✓ 智能路由方面，灵活的消息路由方式，支持基于消息内容的处理和路由；而且还可以执行一系列方式的消息交互，包括了过滤、充实、监视、分发、关联、拆分（一对多）和合成（多对一）等；
- ✓ XML格式转换方面，标准XML数据的格式转换，并且可以通过图形化映射组件、XSLT、客户化Java程序、ESQL等多种方式实现转换功能；
- ✓ 非XML格式转换方面，非标准XML数据的格式转换，实现XML消息格式和其他数据格式之间的映射，包括了C Record、JMS、TDS分隔符、平文本、行业专有数据格式等多种格式，同时也要支持自定义数据格式；
- ✓ 发布/订阅方面，提供发布/订阅功能，支持队列和主题两种订阅模式，主题订阅模式支持树状结构，即支持多级主题模式，支持主题模糊的匹配方式，同时支持跨越多节点的发布订阅能力；
- ✓ 图形化开发工具方面，提供图形化界面开发工具，实现简单和复杂的数据流程设计，提供图形化界面的数据映射和拖拽方式，以及配置功能的开发。提供多种内置功能组件和节点，功能涵盖协议接入、路由、转换、监控、例外处理等，同时要支持自定义的处理节点，提供多种编程语言(C/C++,Java等)的实现接口；
- ✓ 通讯协议支持方面，提供可靠的数据或消息传输，确保消息传输的最简化连接方式，如支持MQ、TibcoEMS等标准消息中间件，支持JMS最新标准。支持灵活和开放的协议支持，包括HTTP/HTTPS、JMS、FTP/File、Socket、SMTP、SOAP/HTTP、SOAP/JMS等；
- ✓ 数据库支持方面，实现与关系数据库实现无缝的集成，同时支持JDBC和ODBC两种数据库连接方式，支持数据库要涵盖主流数据库；在数据交换和流转的过程中，支持业务逻辑中对不同数据库的存储操作，支持对不

同数据库实现不同的用户和密码支持。

- ✓ 管理方面，提供图形化性能监控工具，支持统计和分析的功能，同时支持Pub/Sub报告模式；
- ✓ 性能方面，具备高性能处理能力，尤其对于XML数据的校验和解析、XSLT解析、非XML报文的处理、路由和过滤、数据库操作、WebServices调用等都要满足高性能要求，提供动态的缓存机制，保证数据能够在内存中最快速的处理；
- ✓ 可用性方面，提供高可用性，保证平台7*24小时的运行；提供高稳定性，保证在数据量或应用连接数高峰运行时的系统运行正常，保障持久化的系统运行；
- ✓ 安全性方面，提供多种安全机制，用户级别的认证、授权，支持标准的LDAP服务器；访问级别的SSL传输机制；数据内容级别的数字签名等机制。

5.4.1.5 业务流程管理

为了支撑全院级的医院信息系统协同，可以在ESB的基础上增加业务流程管理系统。流程管理服务作为SOA架构的重要组件，为未来医疗信息系统的业务发展和业务创新，提供了灵活高效的技术平台。

流程管理服务主要提供开发灵活、按需业务流程的方法，提高了快速定义、创建和部署灵活的解决方案的能力，通过集成业务流程内部的服务、数据、规则、角色和规格来满足不断变化的客户需求。这个单一、简单的基于网络服务的平台提供了一个强劲的框架，可以通过将应用服务器与流程引擎和企业服务总线（由一个集成的开发环境（IDE）来支持）相结合，来构造、部署和管理合成的随需应变的应用流程。

流程管理工具的技术要求包括：

- ✓ 平台支持方面，应提供广阔的系统平台支持，能运行在包括Windows、Linux、UNIX等系统之上。流程协议支持支持BPEL4WS协议，并包括灵活

的人员活动的解决方案，支持多种人员任务节点，包括机器调人员，人员调机器和人员调人员；人员库可以与系统、客户和LDAP的用户信息集成；

- ✓ 流程机制方面，用户的工作项管理灵活多样，能声明、批准、拒绝或传递。支持多种方式的人员升级机制，对流程并不会造成太多影响；
- ✓ 管理方面，包含可客户化的图形操作界面，提供启动、管理和监视流程的功能，并能够很好的与门户服务器集成。提供整套API供用户或第三方开发管理界面；
- ✓ 开放性方面，必须是独立于应用，符合SOA标准。运行的应用服务器如果是使用获得Java EE1.5认证的Java应用服务器，支持EJB、JMS、JCA等规范；如果运行的是.Net应用服务器要支持组件对象模型COM；
- ✓ 平台支持方面，广阔的系统平台支持，能运行在包括Windows、Linux、UNIX等系统之上；
- ✓ 流程协议支持方面，支持BPEL4WS协议，并包括灵活的人员活动的解决方案，支持多种人员任务节点，包括机器调人员，人员调机器和人员调人员；人员库可以与系统、客户和LDAP的用户信息集成；
- ✓ 流程机制方面，用户的工作项管理灵活多样，能声明、批准、拒绝或传递。支持多种方式的人员升级机制，对流程并不会造成太多影响；
- ✓ 管理方面，包含可客户化的图形操作界面，提供启动、管理和监视流程的功能，并能够很好的与门户服务器集成。提供整套API供用户或第三方开发管理界面；
- ✓ 流程事务方面，必须支持单事务流程，即微流或短流程(Microprocess)和多事务流程，即宏流或长流程(Macroprocess)，并具有补偿功能。在长流程中，每一节点要求能调整事务方式，可以参与前一事务或独立事务；
- ✓ 选择器方面，支持选择器的使用，可以通过同一接口动态的选择和调用

不同服务，业务人员通过Web界面就可以修改条件，体现业务灵活性；

- ✓ 业务状态方面，支持业务状态机，可以非常方便地使用UML来描述随着业务变化的流程；
- ✓ 子流程方面，支持子流程的调用方式，切合实际业务，方便开发和管理，父子流程实现联动，甚至可以是同一事务，当父流程由于某些原因需要中止时，子流程自动中止；
- ✓ 扩展性方面，具有良好的可扩展性，支持多种方式的集群包括服务器级和硬件级的不停机扩展。工作流引擎所使用的消息中间件也应具备集群功能；
- ✓ 流程整合能力方面，能够将组件（Java Bean，EJB，JCA、COM）包装成服务供流程使用。流程创建之后能够直接部署到工作流引擎平台上使用；
- ✓ 良好的流程建模工具支持方面，不但要具有流程建模开发，并要求能够实现团队开发和仿真测试，最终结果能够导出为BPEL；
- ✓ 开发工具方面，具有图形化的可直接拖拉的开发界面，支持流程的动态调试，增加断点，单步执行，跳入，跳出，实时修改数据的图形化调试工具，支持业务流程模块单元测试。

5.4.1.6 业务规则引擎

医院信息系统有非常复杂的业务逻辑，其中最主要的体现在业务规则的复杂性。传统的做法是每个业务系统各自建立和维护各自的业务规则，这些规则有些还是硬编码的方式实现的。因此很难面对不断变化的业务需求，给开发和维护造成很大的挑战。从业务的角度看，业务规则是一种原则，包含在特定活动或范围内关于指导、操作、实践或过程的行为规范。从信息系统的角度看，业务规则是一个定义或限制业务某些方面的声明。

业务规则引擎是复杂逻辑的发源地，可以从医疗业务流程中以单独实体的形式提取业务规则，可更好地对医院信息系统进行分离，从而提高可维护性。

业务规则引擎技术要求包括：

- ✓ 要求能够将业务流程与业务规则分离，将规则公开为服务，能够使BPEL流程在到达决策点时通过查询该引擎来利用这些服务；
- ✓ 支持通过图形方式操作规则，而不是在编程语言中或在流程内部对规则进行编码。业务用户可以使用工具自行编写规则，并且无需IT人员的协助即可进行部署后的规则更改；
- ✓ 可以对规则集进行并行和按顺序的评估，支持使用并行执行进行高效的业务逻辑评估；
- ✓ 应包含基于多个业务规则评估构建的复杂返回结构；
- ✓ 允许将业务域逻辑转换为简单规则，实现高度易变的业务策略。

5.4.1.7 事件驱动引擎

事件驱动引擎用来支持事件驱动编程所需的构造和服务，它将为客户提供个性化事件处理概念和支持事件处理概念的能力，这些概念包括事件源、事件接收器、事件处理器和事件流。

事件驱动引擎技术使得复杂的医院信息系统能够高效发送、接受那些跨越层级结构的同步和异步事件，而不需要知道产生这些事件的系统方面的细节。一个事件驱动的交互模型，比通常的请求/响应机制对实时变化和刺激有着更好的响应效率。

事件驱动引擎技术要求包括：

- ✓ 支持主流的事件处理语言，用该语言指定事件处理规则（并且不使用私有规则语言）；
- ✓ 支持将第三方事件流处理(ESP)和复杂事件处理（CEP)引擎作为一个或多个处理引擎；
- ✓ 支持事件处理服务（比如线程调度、IO连接管理、计时器服务、监控服务等），并能够进行定制事件处理；

- ✓ 提供对基于标准的用于配置和元数据定义的语言的支持；
- ✓ 基于SOA，事件驱动能够作为服务组件化进行构建。

5.4.2 数据库

数据库是管理数据的基础。在医院信息平台架构下，除了常用的关系型数据库，还有对象型数据库、XML数据库等多种不同类型的数据库。此外对于知识库也需要专门的管理系统。对于扫描后的电子文档也要有专门的文档管理系统。

5.4.2.1 关系型数据库

基于电子病历的医院信息平台建设需要企业级的商业化关系数据库支持，具体技术要求包括：

1) 通用性技术要求

- ✓ 要求兼容多种硬件体系：可运行于X86服务器或UNIX服务器等硬件体系之上。数据库各种平台上的数据存储结构和消息通信结构完全一致，使得数据库各种组件可以跨不同的软、硬件平台与数据库服务器进行交互；
- ✓ 能对多种操作系统支持：支持Windows、Linux、UNIX等操作系统；
- ✓ 对标准高度兼容：提供对SQL92的完全支持以及SQL99的核心级别支持，与SQL标准高度兼容，使应用程序移植更简便；
- ✓ 对多种开发接口支持：支持多种数据库开发接口，包括ODBC2.X/3.X、JDBC3.0、OLE DB2.7、Unix ODBC、PHP、DB Express以及.Net Data Provider，以方便为开发人员提供自由的选择空间；
- ✓ 对主流开发工具支持：支持多种主流开发工具、持久层技术和中间件。支持的集成开发工具；支持的持久层技术有Hibernate、IBATIS sqlmap等；支持主流中间件；
- ✓ 对多语言支持：Unicode标准为全球商业领域中广泛使用的大部分字符定义了一个单一编码方案，保证了同一个位模式在所有的计算机上总是

转换成同一个字符，数据可以随意地从一个数据库或计算机传送到另一个数据库或计算机，而不用担心接收系统是否会错误地翻译位模式。支持Unicode、GBK等多种字符集。借助Unicode支持，可为应用程序提供国际化支持。

2) 安全性技术要求

为了保证系统的安全性，数据库系统应采用基于角色与权限的管理方法来实现基本的安全功能，并采用三权分立的安全机制，将审计和数据库管理分别处理，同时增强了强制访问控制的功能。另外，系统还应实现通信加密、存储加密以及资源限制等辅助安全功能：

- ✓ 三权分立的安全机制
- ✓ 多种身份验证方式
- ✓ 资源限制
- ✓ 自主访问控制
- ✓ 标记与强制访问控制
- ✓ 数据库审计
- ✓ 通信加密
- ✓ 存储加密
- ✓ 导出数据加密
- ✓ 独立的加密引擎
- ✓ 密钥自管理功能

3) 可靠性技术要求

任何一个系统都存在发生各种意外故障的可能性，数据库系统的高可靠性可以避免或降低系统的意外故障对用户带来的损失。要求需要通过提供以下功能实现系统的高可靠性：

- ✓ 故障恢复
- ✓ 多种备份与还原方式
- ✓ 基于时间点还原
- ✓ 备份压缩

- ✓ 数据复制
- ✓ 数据库集群

4) 高性能技术要求

要求通过以下机制实现了系统的高性能：

- ✓ 可配置的多工作线程处理功能
- ✓ 高效的并发控制机制
- ✓ 基于代价的查询优化技术
- ✓ 执行计划重用
- ✓ 视图查询合并
- ✓ 存储过程优化
- ✓ 数据分区
- ✓ 函数索引
- ✓ 大对象存取优化

5) 扩展性技术要求

要求具有良好的扩展性，主要表现在以下几个方面：

- ✓ 多处理器支持
- ✓ 64位全面支持及优化
- ✓ 海量数据存储和管理
- ✓ 存储设备支持
- ✓ 分布式支持
- ✓ 外部链接
- ✓ 外部过程/函数
- ✓ 全文检索

6) 易用性技术要求

要求对应的安装、配置要比较简单，尽可能多的配置、管理、优化工作交由系统自动完成。包括：

- ✓ 实用易操作的图形化/远程管理工具

- ✓ 实用的命令行工具
- ✓ 套丰富的示例库
- ✓ 动态缓存区管理
- ✓ 虚拟视图
- ✓ 类型别名
- ✓ 同义词
- ✓ 数据迁移
- ✓ 性能监视与分析
- ✓ 作业调度
- ✓ 自动升级
- ✓ 数据库重演
- ✓ 数据库快照

5.4.2.2 对象型数据库

关系型数据库不是建立基于电子病历的医院信息平台的唯一选择。目前对象型数据库也可以用于业务系统的开发和平台的建设。

对象型数据库是将面向对象技术引入数据库领域，通过对象访问，SQL访问，和多维存储的直接访问，提供对复杂数据的访问。因为引入面型对象概念，对象数据库附加了封装、继承和多态等面向对象的特性，通过对象-多维数据结构的存储映射，更好的描述了数据与数据的关系。

根据基于电子病历的医院信息系统建设和整合的特点，选择的对象型数据库技术有如下要求：

- ✓ 具有面向对象特性，能支持复杂对象和复杂对象的复杂行为，支持已经被广泛使用的SQL，具有良好的通用性；
- ✓ 要求能较好地能够支持非常复杂的数据模型；
- ✓ 支持持久对象的程序设计语言，可以使它的数据成为持久的、可共享的，并使它的程序执行成为原子的；
- ✓ 在安全性、完整性、坚固性、可伸缩性、视图机制、模式演化等许多方

面有较好的特性。

5.4.2.3 XML 数据库

临床文档架构CDA是用来交换和存储电子病历最佳的方式。CDA是也是基于XML技术的。因此采用XML数据库可以直接存储以CDA格式的电子病历数据。

在基于电子病历的医院信息系统的建设中对于XML的数据服务器的选择，希望考虑以下技术要求：

- ✓ 支持层次型的XML Native存储，不需要使用大对象或者拆分映射的方法；
- ✓ 使用关系型和SQL相融合的技术；
- ✓ 支持基于XML树的检索，支持XML国际标准查询语言XQuery技术；
- ✓ 支持使用Schema等XML技术来保证输入数据的标准性，适应电子病历系统基于模板的标准化信息录入；
- ✓ 提供优秀的XML处理，能够将XML和关系型结合起来，支持混合型的数据存储；
- ✓ 支持定制，包括方便地对查询进行定制、方便地对展示进行定制、方便地对各种模板进行定制。

5.4.2.4 知识库管理系统

对于临床知识可以采用知识库管理系统来存储。知识库用来存放各种规划、专家的经验、有关知识和因果关系等，主要包括事实库、规则库和约束库三部分。事实库存放求解问题的说明性知识、构成信息实体的事实等；规则库中的主要内容是特定领域构规则、定理、定律等过程性知识及说明模型库中各个模型的使用范围、方法及关系的规则信息。约束库主要是说明知识的使用范围和使用条件。

知识库系统结构与知识的表示方法有关。常用的知识表示法有：产生式规则，语义网络、谓词逻辑、框架、黑板模型、面向对象的表示及几种方法混台使用的表示法。以产生式规则表示的知识库系统，由知识库、知识生成支持机构、推理机、工作存储器等部分组成。无论知库系统结构如何组成，知识库、推理机及工作存储器是知识库系统的主要组成要素。

知识库管理系统的主要功能是在决策过程中，通过人机交互作用，使系统能够模拟决策者的思维方法和思维过程，发挥专家的经验、推测和判断，从而使问题得到一个满意而又具有一定可信度的解答。

5.4.2.5 电子化文档管理系统

主要是对纸质文档扫描件、照片、医学影像等电子化文档的管理，相关的技术要求如下：

- ✓ 需要运用自动识别技术加速档案电子化的速度和精度。同时支持OCR文字识别和条码识别两大领域技术；
- ✓ 要求能高度抽象具备很好的系统通用性。支持多层的分布式计算环境；
- ✓ 对稳定性方面的要求，具体包括：
  - 归档服务--在设计时，要设计成可冗余的服务，如果要提高系统的稳定性和可靠性，系统中可配备多台归档服务，由于系统的良好调度，在所有归档服务器都正常运转的时候，可平均分担扫描控制台提交的影像文档，当有某台归档服务器由于故障不能运转时，系统会在剩余的归档服务器中均匀分担故障服务器的任务。保证系统的稳定性；
  - 应用逻辑服务器--同样可以采用前面所说的冗余技术，来保证系统的稳定性和可靠性；
  - 文档仓储服务器--数据在光盘刻录的过程中，要可以采用刻备份盘的策略来保证数据的可靠性，从而提高系统的稳定性。
- ✓ 在系统配置方式要提供高度可伸缩性的要求。包括：
  - 文档仓储服务层次，由于采用了分布式网络存储技术具有高度的可伸缩能力，随着系统数据的增长，要可以非常方便地添加文档服务器来适应这种数据的增长；
  - 应用逻辑服务器，在有大规模的用户访问的时候，要可以通过添加

新的应用逻辑服务器，来平衡系统的负载。以保证系统的响应能力；

- 归档服务器，同样采用了分布式计算和负载均衡技术以后，在扫描的数据量增长的情况下，要可以来通过多个归档分布和合作的方式来保证系统的数据处理能力。

✓ 在流程和结构设计上对保证系统的高效性的要求。包括两个方面：

- 保证人员的高效性要求--系统的业务流程的设计上采用高度分工协作的流水线模式，系统中的各个角色各司其职。从而使得系统处于最高效运行的状态，另外这种精确分工的流程设计原则，可以降低人员的培训成本和培训时间；

- 保证设备的高效性要求--系统采用分布式计算环境，在这个环境中彼此协作，可用通过有效的设备配置比例，来使得系统中的所有设备都处于高效运行状态，从而能最大限度地保护系统的投资。避免计算资源的浪费。

✓ 对提供的管理工具以用于提升系统可管理性方面的要求，包括：

- 通过系统日志体系、用户管理系统，来提供一个精确的角色分工和管理体系。要可以在随时管理和监控系统的运行情况和人员的操作情况。并可以及时发现问题及时纠正，从而提高系统的运行质量和效率；

- 通过提供比较友好的图形界面，用于维护系统。系统要支持高度可靠的分布式部署模型，用于保证系统的可维护性，同时要配备管理工具，通过采用图形化操作界面，以增强系统的可维护性。

5.4.3 数据仓库

除了用数据库来管理数据，对于决策性数据最好建立单独的数据仓库来管理。数据仓库是整合和利用业务系统产生的数据，为决策提供支持的一项技术。数据仓库系统专注于回答过去发生了什么，为管理层提供了及时、准确、全面的

信息，从而可以帮助医院的管理层做更好的、基于信息的决策。

因为业务系统主要是为即时更新的事务服务的，数据的历史也相对比较短，所以它无法满足战略决策的需要，因为后者需要基于海量历史数据的查询分析。所以我们需要创建数据仓库，从业务系统抽取数据，从而使数据脱离业务系统，可以自由组合，减少对业务系统性能的影响；整合数据，使数据转化为信息；优化数据，使数据易于查询，帮助决策。

5.4.3.1 数据仓库的特点

数据仓库是用以支持管理层决策的数据集合。它具有以下特性：

1) 面向主题的(Subject Oriented)

业务系统是基于应用的，按照业务操作的流程设计开发系统。而数据仓库是面向主题的，主题通常是业务上谈论的一些名词，比如患者、药物、财务等。面向主题的数据组织方式，符合人们数据分析的思维模式；它有利于为分析对象提供完整、一致的数据描述，破除各部门各自的理解，同时也能统一地梳理各个分析对象所涉及的数据之间的联系。

2) 集成的(Integrated)

数据仓库的集成包含两个层面：第一，分散在不同业务系统的同一主题的数据需要整合在一起；第二，对于字段的定义也要统一，如解决字段的同名异义、异名同义、单位不统一、字长不一致等等。

3) 非易失的(Nonvolatile)

数据载入到数据仓库后，主要进行的是查询的操作。所以说数据仓库中的数据是非易失的，它没有业务系统中传统意义上的修改。

4) 随时间变化的(Time Variant)

数据仓库中的数据是业务系统中不同时间的数据快照。因此数据仓库的数据都包含时间戳，以标明数据的历史时期。这个特点有利于展现各项数据指标的历史变化曲线、预测未来的趋势。

5.4.3.2 数据仓库架构

目前主流的数据仓库市场上有两类拓扑架构：基于数据集市的架构和企业级

数据仓库(Enterprise Data Warehouse,EDW)架构。对于前者，我们可以有针对性的快速实现某些数据集市，而且数据集市可以部署在不同的基础架构上，对软硬件的要求比较低，但是总体上开发比较复杂，同一个业务系统可能需要开发多套抽取程序，而且所有数据集市给用户呈现事实的唯一版本(Single Version of the Truth)也会有比较大的难度。对于企业级数据仓库架构，可以确保给用户呈现事实的唯一版本；当然在建设过程中，需要通盘的设计，对于软硬件的要求也会很高。

下图是数据仓库的架构。

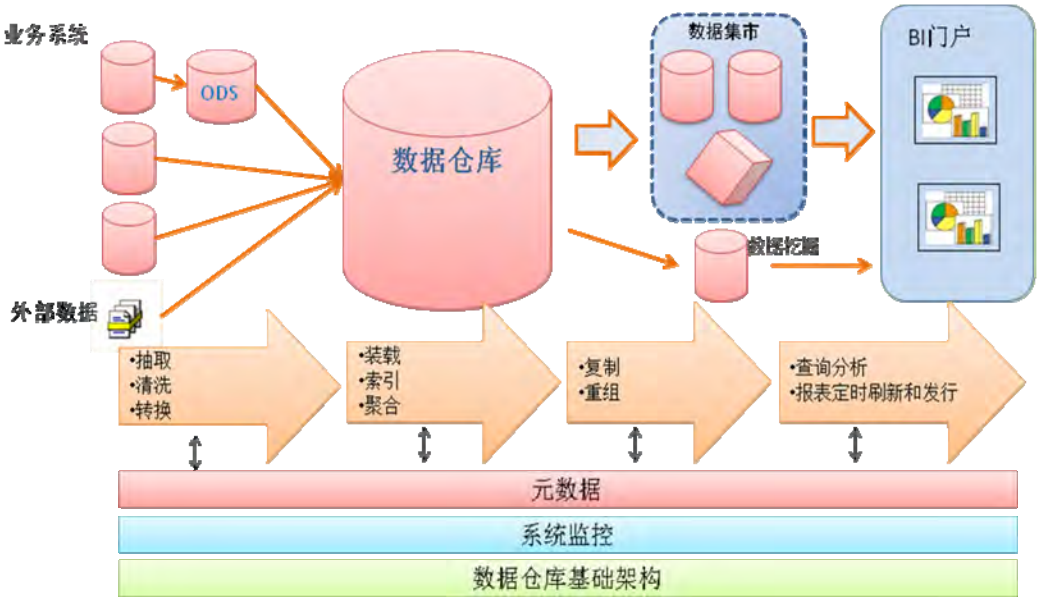

图 5-33 数据仓库架构

数据仓库的数据源包括业务系统、ODS(Operational Data Store)、购买的外部数据。数据仓库存储着从数据源获取的整合的数据。对于数据集市、数据挖掘，他们按照各自的需求从数据仓库获取、组织数据。数据挖掘可以从海量数据中，提取隐含在数据中的、人们事先不知道的但可能有用的信息和知识。在商业智能（Business Intelligence，BI）门户里，通过BI工具，按照业务上的语言，提供报表图表、自助分析等商业智能功能，和展现数据挖掘的成果。

数据仓库依赖于数据整合功能，抽取源数据，通过数据清洗、数据转换，装载到数据库中；同时按照数据集市和数据挖掘建设的要求，通过复制或重组，加载到数据集市或数据挖掘数据存储中。数据仓库通过BI工具，提供报表的定时刷

新和发行的功能。

在数据整合、展现、分析的过程中，通过与元数据管理模块的交互，掌握元数据的转换过程，以方便用户获取BI门户上展现的数据与业务系统的数据的关系。

5.4.3.3 数据存储

数据仓库中主要是基于海量数据的查询分析，这要求数据仓库需要有别于传统业务系统的数据库和数据建模方法。

目前为数据仓库提供的数据库有很多种类型。按存储结构分，除了传统的按行存储的关系型数据库（Relational DBMS），还有专门为数据仓库设计的按列存储的列式数据库(Columnar DBMS)，按值结构存储的相关性数据库(Correlation DBMS)，和多维联机分析处理(MOLAP)数据库。从联机分析处理的角度，前三类归为ROLAP（关系型联机分析处理）数据库。MOLAP因为将数据以多维结构存储在分析服务器上，而且预先聚合，所以查询速度相对较快，也限制它无法处理大数据量；而随着ROLAP数据库技术的发展，使得在ROLAP数据库中访问海量数据的性能得到了质的飞跃。

按存储介质分，除了磁盘，为了提升数据查询的速度，内存数据库应运而生。当然内存的存储量也是受到技术以及投资额的限制的。

按系统架构分，主要有对称式多重处理架构（Symmetric Multi-Processing）和大规模并行处理架构（Symmetric Multi-Processing），前者共享内存和存储，后者不共享内存和存储，所以它在数据量极大（T甚至P级）的情况下显示出了优势。

在数据建模上同样也是围绕提高海量数据的查询速度。数据仓库中的数据是按照星型、雪花模型来组织的。星型模型是最常用的数据仓库设计结构的实现模式，该模型的核心是事实表，围绕事实表的是维度表，通过事实表将各种不同的维度表连接起来。对于数据建模，一般采用维度建模（Dimensional Modeling）的方法。它可以分为四个步骤来实现：

1）选择业务流程；

2）确定数据的粒度；

3）选择维度表；

4）识别事实表。

5.4.3.4 数据整合

数据整合(Data Integration)是数据仓库中数据准备的部分。它从业务系统中抽取数据，然后通过数据清洗和转换，将数据加载到数据仓库中。也可从数据仓库的上一数据层，抽取转换加载到下一数据层。在数据整合过程中需要采取多种策略确保数据质量，比如缺省值策略、数据清洗策略、数据标准化策略等。数据质量管理也包含主数据管理(Master Data Management),比如如何判断两组患者的信息是否指的是同一个患者。

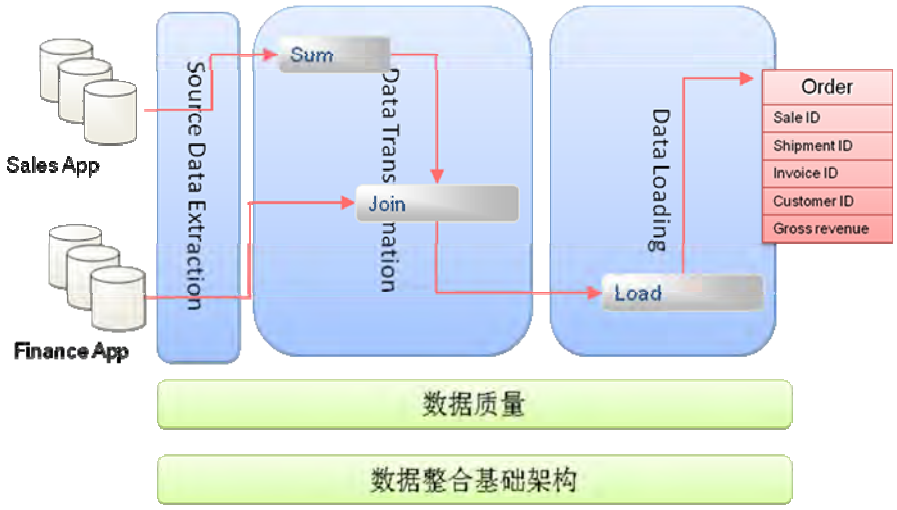

图 5-34 数据整合流程示意图

传统的数据整合流程是ETL（Extract-Transformation-Load），即抽取-转换-加载。为了充分利用数据库的性能，减少网络开销，提高数据整合的效率，可以选择在数据库上实现转换，所以流程就变成ELT(Extract-Load-Transformation）。

对于实时性要求很高的数据仓库系统，可以选择从业务系统推送（Push）数据到数据仓库，而不是传统的抽取（Extract）业务系统的数据。推送(Push)数据需要改造业务系统以支持这种模式。

5.4.3.5 商业智能

商业智能给用户提供了历史、现在和预测的视角去审视医院的运营。通过商业智能工具，业务分析人员和管理层可以知道本公司或本单位过去发生了什么，为什么会发生，和今后将发生什么。商业智能根据不同的业务需求，或者不同用户类型的需求，提供以下几种功能：

1) 固定格式报表

它可以满足中国式报表的需求。中国式报表通常有多层表头、斜线；交叉表；表格和图表混排。

2) 仪表盘报表

可以通过仪表盘、消息树、雷达图、模拟仿真分析等直观的方式可视化地呈现关键信息和关键绩效指标，便于对他们进行监控、分析、管理，并据此进行判断、决策。

3) 即时自助查询

通过一个简单的查询面板可以直接连上语义层，对关心的数据进行报表，随机查询和数据分析工作。语义层按照业务的语言进行呈现，屏蔽了数据库中的字段、表以及表与表之间的关系等技术术语。它提供了丰富的数据展现形式，如表、交叉表、图等；也提供了丰富的在线数据分析手段，如切片、切块、向下钻取、向上钻取、交叉表、旋转等。

4) 多维在线分析

主要是针对多维联机分析处理(MOLAP)数据库的数据分析。它提供多维视图和动态分析报表功能，支持客户对数据进行旋转、切片和分层钻取，并从各个角度对数据进行分析和比较。

5.4.3.6 数据挖掘

数据挖掘是从海量数据中，提取隐含在数据中的、人们事先不知道的但可能有用的信息和知识的过程。数据仓库为数据挖掘提供了很好的数据准备。基于数据仓库，人们可以根据不同的业务需求采用合适的数据挖掘算法分析数据，发现规则。

常用的数据挖掘算法包含决策树、关联规则、线性回归、聚类、贝叶斯、神经网络等。下面是对决策树和关联规则的简单介绍。

1) 决策树

决策树是根据数据源，找到决定预测目标的因素的重要关系等级以及程度。当根据一个或多个变量预测目标时，分析变量对目标的重要程度。比如可以用来分析医院的目标客户，即患者。

2) 关联规则

分析发现数据库中不同变量或个体间之间的关系程度。比如可以用来分析疾病与疾病之间的关系，研究是否存在并发症的可能。

5.4.4 服务器部署与虚拟化技术

5.4.4.1 服务器支撑架构

服务器支撑架构是基础设施中的重要组成部分，对基础软件、数据库、数据仓库等提供计算资源支撑。服务器支撑架构的设计，需要满足医院信息平台对于服务器处理能力、可靠性、可扩展性以及安全性的要求。

5.4.4.1.1 信息交换层

信息交换层是医院信息平台的重要组成部分之一，提供医院内部以及与外部的数据交换和共享。通过基础软件服务器的部署来提供服务，包括企业服务总线以及相关的通用服务等。

信息交换层对于服务器支撑架构的主要技术要求包括：

- XML 处理优化
- XML 负载处理
- XML 安全性
- SOA 优化

由于信息交换层的重要性，服务器支撑架构需要确保向信息交换层的适当服务提供适当数量的资源。同时它还将监视性能级别，以便将高需求的服务实例化到可用基础架构资源上，从而满足对处理优先级的要求。

5.4.4.1.2 基础软件服务器

基础软件服务器包括应用服务器、门户服务器、内容管理和搜索引擎、企业服务总线、业务流程管理、业务规则引擎和事件驱动引擎等。对于服务器支撑架构的技术要求主要包括：

- 网络带宽、数据吞吐量和 XML 处理优化
- 计算性能的要求
- 可扩展性
- 高可用性、高可靠性
- 安全性

服务器基础架构应具有良好的可扩展性，可以随基础设施资源的增加而提供更多的计算资源，以满足对基础软件服务器的支撑需求。可靠性通常意味着每个单独的平台上每个服务至少有一个实例正在运行，从而实现一定程度的故障切换和负载平衡。多个服务实例也可以实现负载平衡（通过基于软件/硬件的负载平衡程序来实现）。

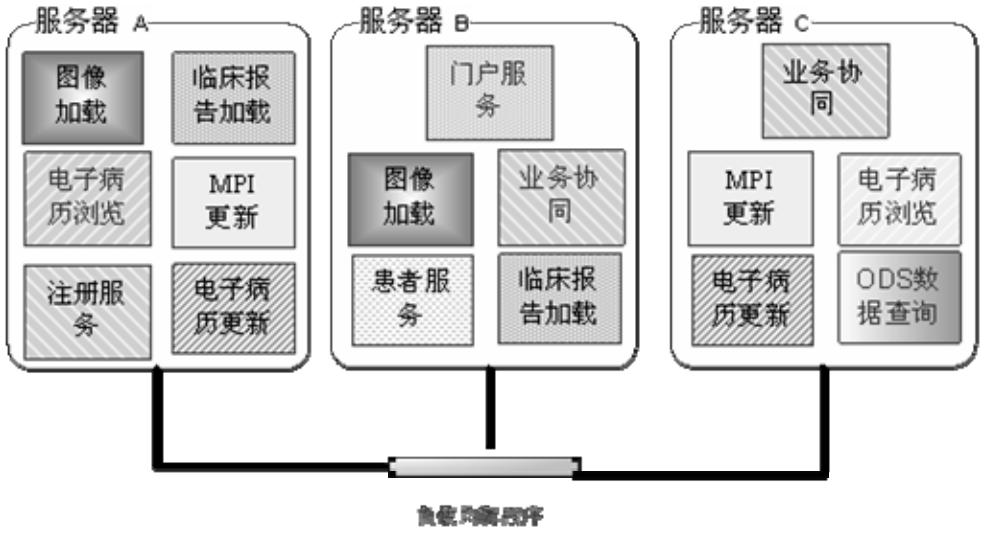

图 5-35 服务部署和负载平衡

在服务的部署过程中，需要重点区分不同服务对于服务器带宽、网络、存储的需求。同时根据服务类型和优先级的不同，在服务器资源分配上优先考虑优先级较高的服务。

应用虚拟化技术，可以更为方便的进行动态资源分配。结合硬件服务器对于虚拟化的支持，可以实现网络、IO、计算能力等资源的直接访问，优化虚拟化平台的性能。

5.4.4.1.3 数据库服务器(ODS、电子病历存储、电子化文档管理、知识库管理等）

在医院信息平台建设中，数据库的主要用途是安全恰当地提供及时、准确和相关的健康信息，该信息用于支持安全有效地向个人直接提供健康服务，为医院内部管理提供数据支撑，以及为区域卫生信息平台提供相关数据等。

医院信息平台的数据库系统，主要满足包括 ODS、电子病历存储、电子化文档管理、知识库管理等不同类型的数据存储要求。这些不同类型的数据，大部分源自医院内部各应用程序，通过数据转换后以结构化或者非结构化的形式存储在数据库或者文件系统中。

对数据的所有访问，都需要确保通过离散的、预定义的、受控的且主动审计的方式进行。这种保护应扩展到医院信息平台基础架构中的所有数据存储库。

数据存储库更新关系和及时性

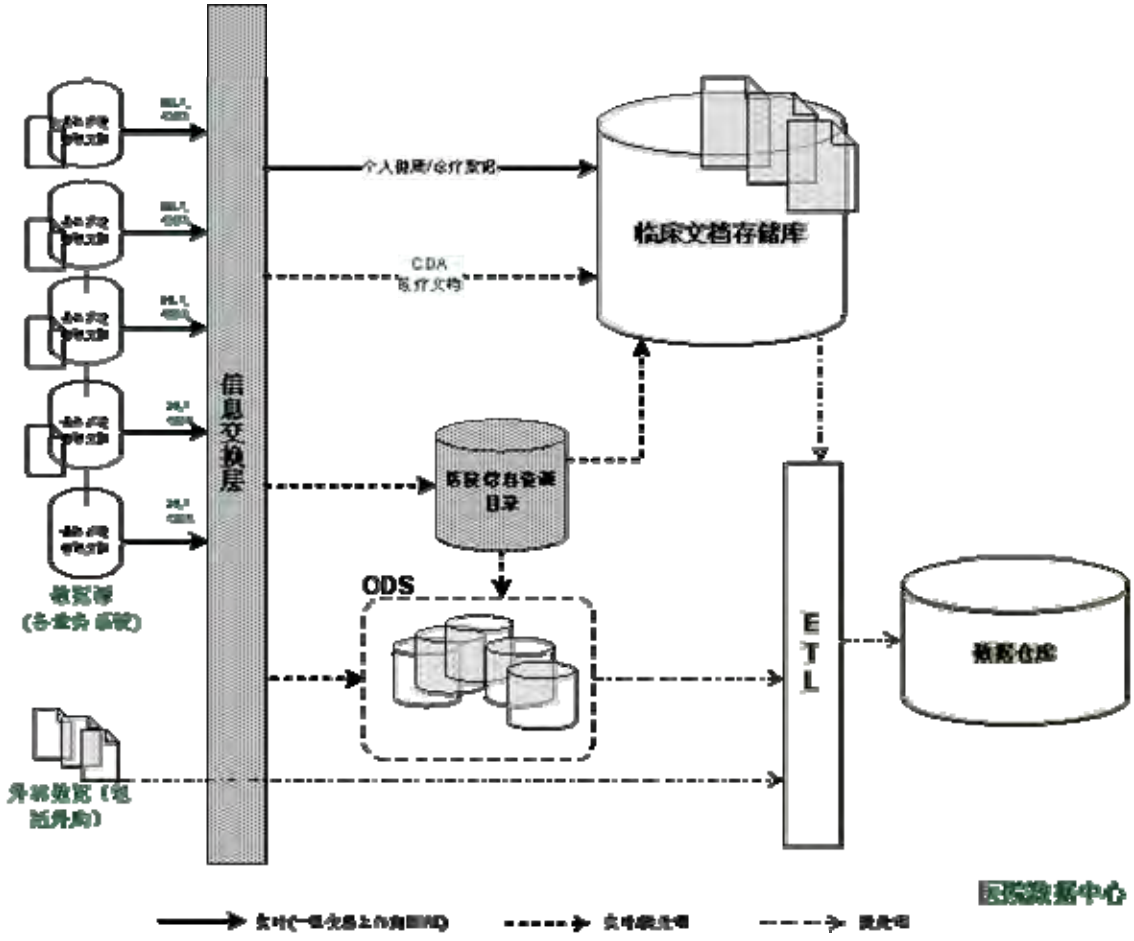

图 5-36 数据库和更新的及时性

如上图中所示，电子病历是集成平台中的关键信息，为保障医疗服务信息的及时有效，任何上传的个人健康/诊疗数据都会立即更新到电子病历存储库中。与事件关联的详细信息（包括任何相关文档）将被立即缓存/排队等待更新。数据仓库将以批处理方式更新，并在夜间进行。下面是每种数据类型的摘要及其在集成平台中的处理情况：

表 5-11 数据存储库更新频率

数据类别	来源	更新频率
个人健康/诊疗数据	各业务系统/外部系统发布的时间事件	从各业务系统/外部系统实时更新
电子病历文档数据	由各业务系统/外部系统提交的文档	文档的缓存/延迟更新。关系数据联机更新
ODS 数据	由各业务系统/外部系统提交的文档	实时//延迟更新
数据仓库	集成平台数据和医院各业务系统数据，以及外部数据（包括外购）	在非高峰时间执行的每日批处理更新
日志/审计	由任何数据更新/服务生成。	发生更新/服务时

数据库服务的技术考虑事项

电子病历数据访问的主要形式是更新和浏览。在数据库服务的设计中，要根据电子病历更新的客户端并发量进行考虑，同时还需要考虑联机收集各业务系统的信息以保持电子病历的及时性的需求。

大型文档可以用批处理模式上传。对于患者转诊很关键并且需要实时进行的情况，电子病历系统应提供实时的数据服务以完成业务请求。

集成平台数据库包括需要联机提供以供查询和快速处理对医院至关重要的变化信息，例如，完整的病历信息提取以及与特定疾病（像最近的猪流感疫情）相关的健康状况。这就需要联机汇总数据，而不是采用数据仓库的批处理模式。

ODS 数据的更新可以是实时的，也可以采取异步、延迟的方式进行。而对于 ODS 数据的访问则是通过联机汇总数据的方式进行的，与数据仓库的批处理方式不同。

电子化文档和知识库的自动更新同样可以是异步、延迟的方式，同时也应该支持人工实时更新。对于电子化文档和知识库的访问都是实时的，需要保证访问的及时性。

数据库部署方式

医院信息平台对于数据库的高可用性有较高的要求，通过数据冗余/镜像、主/备份数据库服务器或者数据库集群技术等方式，来满足医院信息平台对于数据库高可用性的需求。一般来说，目前主流的数据库部署方式有以下两种：

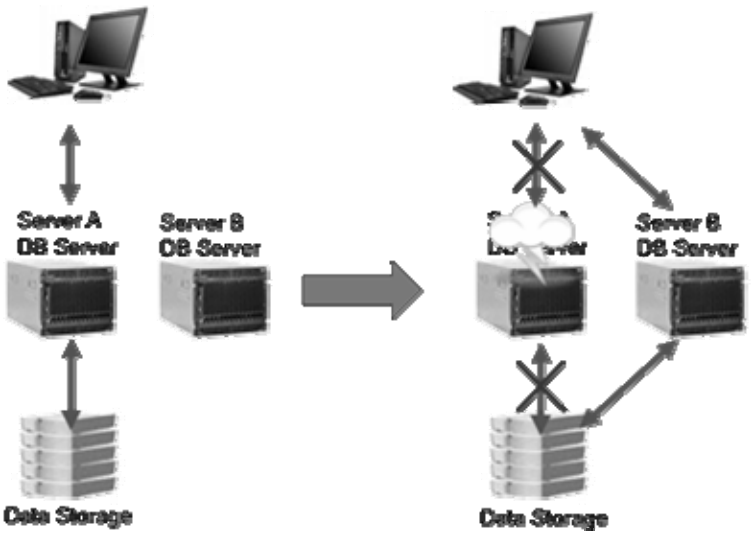

图 5-37 主/备份数据库（双机）

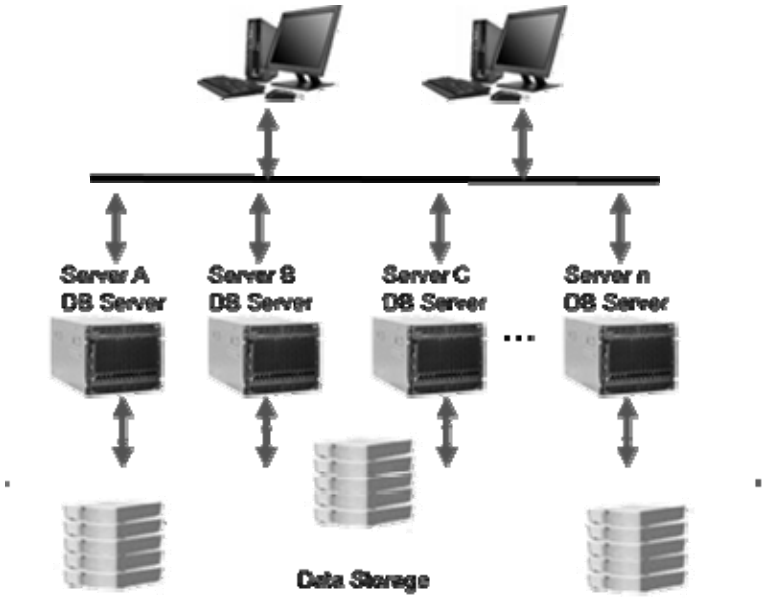

图 5-38 基于数据引擎的数据库集群技术

主流的数据库产品对于以上两种部署方式都提供了支持。在医院信息平台建设中，需要根据医院实际情况来进行选择。原则上来说，如果医院信息平台建设时，能够有效的对数据库所支撑的各应用系统的数据访问和更新进行细分，并且能够合理分配到多台数据库服务器上，则可以采取第二种方式进行部署。否则，由于数据库集群的实现机制限制，反而可能造成系统整体性能的下降。

5.4.4.1.4 数据仓库

数据仓库的主要用途是提供一个处理、搜索、分析和检索数据的独立环境，而不影响医院信息系统其他组件所需的重要性能服务级别。这对于支持医院信息系统中业务数据相关联的分析、研究和管理而言非常重要。

数据仓库的技术考虑事项

- ETL（抽取、转换和加载）是数据仓库的重要功能，因为它将涉及转换和规范化以确保临床数据在上下文中以及内容方面的呈现一致性；
- 数据及时性 - 数据仓库更新通常在以夜间批处理的方式进行。这样可以最大程度地减少高峰时间对重要临床支持的中断。它从集成平台数据库以及医院各业务系统提取数据，因此，它将依靠信息交换层与通信；
- 数据完整性和可靠性 - 数据仓库是医院内部关键信息的存储骨干，并且还作为医院及更高级别健康信息分析的信息主要来源；
- 数据同步 - 在医院内部有多种数据，数据仓库的目标不是合并每个单一片段的信息/数据。数据同步成了一个难题，它需要通过控制策略和管理来确保同步和分发。有关复制的内容将在“存储架构”章节讨论；
- 数据访问-通过门户访问商业智能工具(Business Intelligence Tool)是访问数据仓库的主要机制。只有医院内部用户才能访问数据仓库数据并对其进行分析。公众用户可以访问基于数据仓库数据形成的发布报告。数据集市/查询是访问数据仓库中数据的方式，可以将这些访问权提供给医院外部的医疗专业人员。数据访问服务将是确保数据访问方便、安全和及时的关键；
- 备份和恢复 - 详细信息将在“存储架构”章节介绍；
- 可扩展性 - 数据分布（集中式/分布式）将根据数据操作的位置和处理/存储数据的位置来确定最有效的实施模型；
- 可用性 - 数据仓库数据是医院信息化的关键资产之一，因此其可用性非常关键（对于大中型医院数据仓库需要提供97%的可用性）。可用性既指

数据的可用性，也指数据的可访问性。

数据仓库设计

从数据处理的角度来看，有多种物理架构适合数据仓库实施，具体取决于工作负载的规模和类型：

- SMP：对称多处理模型是共享环境中的多CPU单服务器模型。存储是分开进行，并且通常通过SAN交换机进行通信，因此网络带宽将是解决大规模数据处理的关键。扩展SMP需要将服务器升级为更高的处理能力。

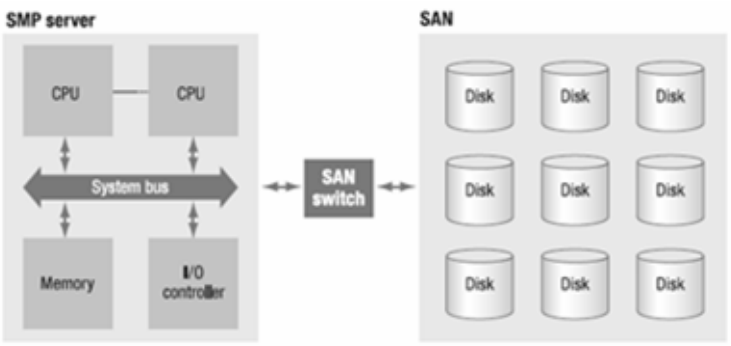

图 5-39 SMP 数据仓库架构

- **集群**：集群是统一到单个计算环境中的SMP服务器组。这也是一个共享一切的环境。集群扩展只是将更多资源添加到集群中（增加CPU、内存和I/O周期）。

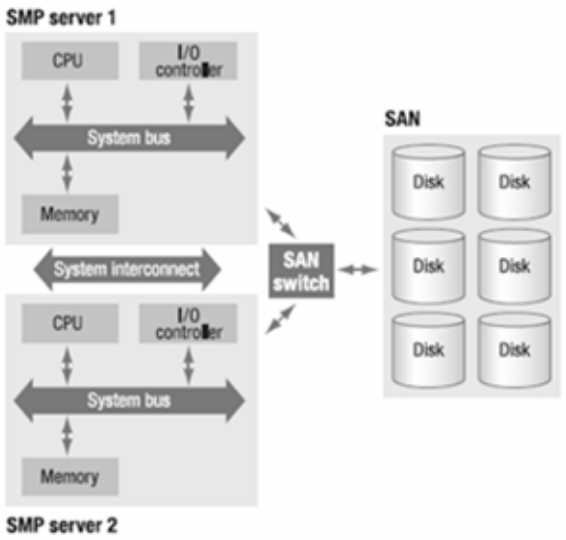

图 5-40 集群化 SMP 数据仓库架构

- **MPP**：海量并行处理(MPP)架构是由独立的SMP组件组成的。处理被拆分到整个架构中的并行组件中，这通常需要仔细设计数据的放置方式，以便尽可能以本地方式处理数据，然后将结果组合起来。

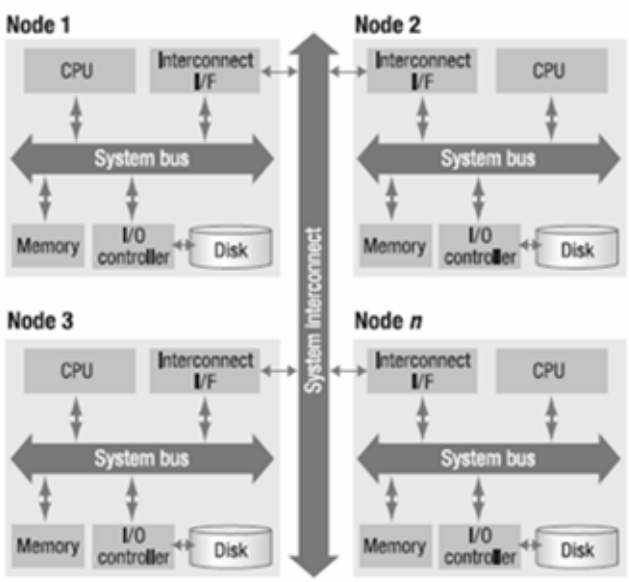

图 5-41 MPP 数据仓库架构

一般情况下，如何选择数据仓库架构取决于数据量、并发用户访问和数据访问/更新及时性属性。

数据操作量很大（当天更新很多，用户数>100）的大型数据集(>2TB)倾向于采用 MPP 架构。SMP 更适合小规模的数据仓库(例如，数据集<500GB，用户数<25)，其数据访问和数据量也相对稳定。

对于医院信息平台实施，对不同规模的数据仓库的技术要求意味着数据仓库实施也可以采用不同的架构：

表 5-12 数据仓库架构规模

	小型	中等	大中型
可用性	--	95%	97%
数据仓库架构	--	SMP/集群	集群/MPP
服务器等级	--	多路关键任务 x86 服务器(或相同等级)	高端多路关键任务服务器

5.4.4.2 虚拟化技术

传统的部署方式下，往往采用单独的物理服务器来部署基础软件、数据库、数据仓库等软件服务器。虚拟化技术的引入，可以实现资源的动态分配。在部署方式上，可以以虚拟机的方式来部署软件服务器。在实现灵活部署的同时，提供了更好的可扩展性和高可用性。

5.4.4.2.1 虚拟化技术及发展趋势

虚拟化是在 IT 基础设施领域最常被谈论的新技术之一，服务器虚拟化则逐渐成为构建系统中考虑的一个重要方面。依据 IDC 的报告，从广义上来定义，服务器虚拟化平台通常由以下四大部分组成：

- 虚拟化平台：包括虚拟化的核心软件和硬件平台。虚拟化软件构建于核心管理程序、基本资源控制和应用编程接口（API）之上。硬件平台指的是支持虚拟化的计算能力以及为虚拟化提供的硬件增强等；
- 虚拟机管理（VMM）：这其中包括主机级管理，以及跨虚拟服务器和数据中心的管理；
- 虚拟机基础设施（VMI）：虚拟机基础设施是当前促使大多数客户做出购买决策的增值特性。这其中包括实时迁移、自动重启，以及跨主机的虚拟机工作负载平衡；
- 虚拟化解决方案：虚拟化解决方案代表了上述技术与某些支持工作流以及流程自动化能力的捆绑，旨在满足特定的业务需求。包括VDI或灾难恢复等解决方案。

一些更高层次的应用，例如高可用性、灾难恢复、负载均衡以及自动化随着技术的发展得到了很好的推广。更多的企业正在向虚拟化 3.0 迈进，软硬件平台的能力将成为最基础的需求。面向服务的基础架构、基于策略的管理模式以及可变成本管理也受到了更多的关注。

5.4.4.2.2 物理服务器向虚拟服务器的迁移

由虚拟机系统软件厂商提供的集中式虚拟机和主机服务器管理软件拥有一系列广泛的功能，包括在虚拟化环境中进行虚拟机与主机配置、供应、监控、迁移以及资源管理等。虚拟机与主机管理架构的设计与部署可对整个虚拟化环境的效率产生极大影响。下面我们将针对虚拟化环境部署中的物理服务器向虚拟服务器的迁移进行阐述：

物理服务器到虚拟机（P2V）转换指的是从非虚拟化的环境，即物理服务器的部署向虚拟化环境迁移的解决方案。例如，医院已经拥有一些现有系统，采用的是物理服务器的部署方式。从医院信息平台建设的整体规划考虑，如果需要向虚拟化环境迁移，可以应用物理服务器到虚拟机的转换技术来进行迁移。

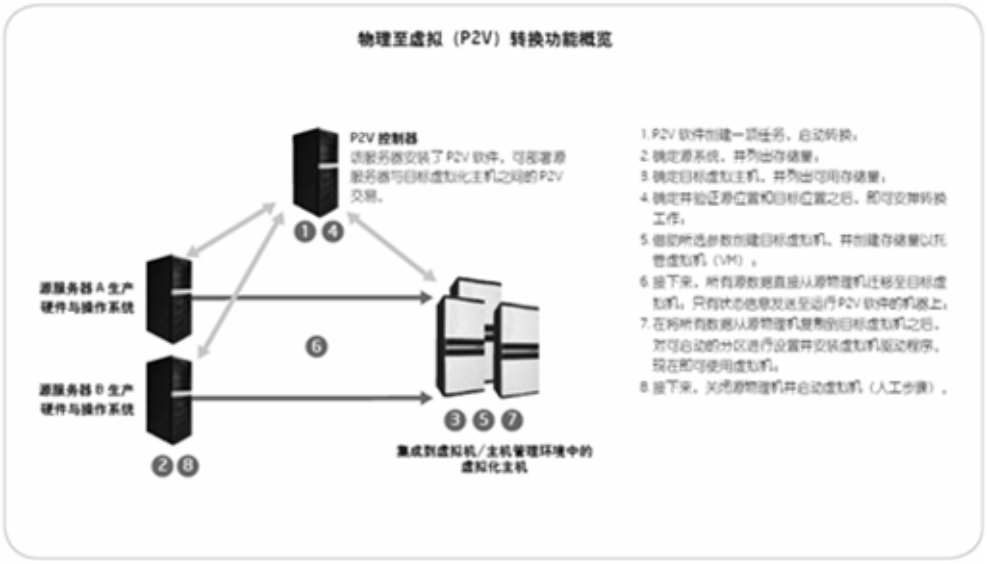

图 5-42 物理服务器到虚拟机的转换

物理服务器到虚拟机（P2V）转换需要定义一个明确的流程和架构，从而顺利将每台需要转换的物理服务器移植到虚拟化环境中。通过人工转换流程可以满足数据中心内大量不同物理服务器配置下转换的需求；通过批处理转换能够转换更多的系统，但同时也需要进行额外的规划和深入的沟通。

5.4.4.2.3 虚拟化平台的管理与监控

采用虚拟化技术，需要建立有效的虚拟化平台的管理和监控机制：

- 将所有应用系统、服务器系统的故障事件消息机制与虚拟化平台的监控程序结合起来。使用虚拟机/服务器管理软件来跟踪服务器的状态和性能；
- 使用虚拟化平台所提供的动态资源平衡功能来实现虚拟机的负载平衡，应用虚拟化平台的高可用性特性来实现服务器、网络等故障切换的自动化；
- 建立资产管理数据库来跟踪所有虚拟机和部署的主机信息。

5.4.4.3 服务器整合技术及方法

随着医院内部业务系统的逐步完善，部署的服务器数量和种类繁杂，部署架构和环境也更为复杂。无论是大中型医院还是小型医院，普遍都面临对于服务器资源的管理困难。随着各医院对于 IT 系统效率、可靠性和可扩展性的要求提升，服务器整合的需求也日益得到重视。

在本节，我们主要对目前市场上主流的一些服务器整合技术进行探讨：

5.4.4.3.1 刀片服务器技术

刀片服务器技术经过多年的发展，成为了服务器整合广泛采用的一种方式。我们在对医院现有服务器环境的调研中发现，一些医院已经采购和使用了刀片服务器。然而，大多数医院并没有提出一个整体的服务器部署架构，也没有把刀片服务器作为整合的工具来充分的利用。

刀片服务器的特点是以计算资源集成为主，强调高计算密集度，以数据中心或大企业应用为目标。目前市场上的刀片服务器并没有形成一个共同的标准，各厂商依据自己的设计来进行构建。

企业级刀片是面向大型企业的产品。中小企业级刀片则属于企业级刀片技术下移的产物，在产品特性、可扩展性、容量等方面较强。

不同规模医院，在选用刀片服务器时，应根据自身业务发展的需要，进行整体规划，将服务器资源进行有效整合。

5.4.4.3.2 模块化服务器技术

模块化服务器是在传统刀片服务器之上的进一步扩展，它把集成计算、存储、网络等 IT 设备于一体，采用集成化的管理，具有简单易用的特点。模块化服务器不单纯以提高计算密集度为目标，为中小企业应用提供集成可靠的服务器产品。它实现了部件模块化，支持开放的管理标准。

对于中等规模或小型医院的医院信息平台而言，IT 管理的人力和资源相对有限，模块化服务器为这些用户提供了更好的选择：

- 服务器、网络和存储集成一体化
- 统一、简单、易用的管理平台
- 强大的远程管理功能，主动故障报警
- 省电降耗
- 集中控制，集成存储，按需分配
- 静音组合，无需专门机房

图 5-43 全集成化的模块化服务器平台

从安装部署的角度来看，模块化服务器具有以下一些特点：

- 快速部署最大限度降低现场配置及安装工作
- 远程配置、软件更新，降低 TCO
- 实时系统健康监控，远程诊断、排查系统问题，降低现场成本

- 故障切换，当一个刀片上的应用出现故障，可迅速切换到另一个备份刀片上，提高可用性

5.4.4.3.3 基于虚拟化技术实现服务器资源整合和动态分配

虚拟化技术可借助信息基础设施更好地提供服务，从而帮助客户节省资金。与传统的物理服务器部署方式相比，虚拟化所带来的一些优势包括：

- 能够迅速保存、复制和供应虚拟机，从而实现零停机时间维护并支持全新的“go live（实时化）”方案；
- 动态共享服务器平台中的闲置资源，从而在消除烟囱式（stovepipe）部署的同时，进一步提高性能和利用率；与此同时也能为应用提供一个隔离性的操作环境；
- 可以实现更高的技术标准化水平和流通率，从而降低运营和维护成本；
- 可在虚拟服务器组件发生故障时进行无缝故障切换，从而提高系统可用性；
- 降低复杂性，从而改进逻辑和物理灾难恢复。

虚拟化技术的应用不仅可以实现动态管理和分配共享的计算资源，实现更高效和灵活的使用计算、存储以及网络，而且可以在以下几个方面对医院信息平台的建设提供帮助：

- 系统资源整合和隔离：对于中小型的平台建设，由于资源有限，可能需要在一台物理服务器上部署不同的应用。而传统的部署方式可能造成应用之间的相互影响和安全隐患。通过虚拟机可以实现在一台物理服务器上部署多种应用，同时实现不同应用系统之间的隔离，以获得更好的系统稳定性和安全性。
- 动态分配资源应对突发性事件：通过动态的资源分配，可以在突发性事件发生过程中将计算资源进行集中分配，从而更好的满足突发性事件中的骤增的计算需求。
- 虚拟化技术减少单点故障：除了物理的灾难恢复数据中心，建立共享的

虚拟执行环境可以减少单点故障，可以提高医院信息平台的系统可靠性；

- 虚拟机在灾难恢复中的使用：在灾难恢复中使用虚拟环境使虚拟机从一个执行环境中迁移到另外一个数据中心的备份介质上执行。由于当中牵涉大量的数据复制，I/O虚拟化与高网络带宽可确保平台的运作顺畅；
- 通过分离的虚拟网络提高安全性：除了物理网络分离，使用虚拟网络技术也可以在共享网络中建立足够的防护；
- 突破底层资源的物理配置约束：服务集群在医院信息平台中可以部署到兼容的虚拟机集群(而不是传统的划一服务器配置与型号)，提升应用与服务的扩展性。这种兼容性更可应用到灾备数据中心，以实现最大化的投资。

5.4.4.4 服务器及相关基础设施管理

服务器及相关基础设施管理要求其功能贴近用户需求，操作简单实用。

因医院信息系统涉及面广，分布较为分散，可以采用动态的多层网络架构，以满足不同用户的网络结构需求，对服务器节点状态进行实时监控和资源管理，为系统管理员提供一个统一的、集中的、可视化的和跨平台的管理。实现降低用户的管理成本，同时也提高用户的管理效率，降低系统维护 TCO。

服务器及相关基础设施管理，应支持跨平台（Windows、Linux、UNIX 等）管理，带外(Out of band)管理，远程故障报警，底层硬件监控、资产管理等。

弹性架构，动态部署

系统管理需要灵活的管理体系结构，用户可以根据管理网络的复杂程度选择不同的管理结构组成。如果管理网络比较简单，如只限于局域网和通过外网管理一个局域网，则可以选择简单网络管理架构；如果需要管理到比较复杂的网络，如多个不同网络的管理，则可以选择复杂网络管理架构。

整体管理，统一监控

管理员通过访问整合的管理平台，来完成对服务器的管理功能。系统管理者可通过专线或其他接入方式，在机房远端访问到管理平台，进行远程监控、管理服务器，包括 CPU、内存、硬盘使用率、风扇转速、操作系统、进程、网络流量及其它运作状态。与管理平台的数据交互需要经过加密。

系统管理平台可以监控所有服务器节点的状态，根据节点的不同状态，了解服务器正常运行、关机还是异常状态。系统管理员无需登录每一台服务器去查看服务器运行状态，整体掌握所有服务器资源及状态。

集中控制，分布管理

要求集中控制功能可以实现远程管理，而不用到机房中去实现电源操作等功能。

智能设计，多重警告

当系统出现异样当系统出现异常，如风扇转速减慢、系统温度过高、CPU 利用率、内存利用率过高、系统服务异常终止等，要求管理系统能够以多种方式通知系统管理者。此外，当保存所有重要资料的机箱被不正常开启时，系统应通报用户作实时的保全处理。

应具备多重警告提示功能，例如：SNMP Trap、拨号、电子邮件和手机短信等。

5.4.4.5 灾难恢复

5.4.4.5.1 灾难恢复的级别

灾难恢复指基础设施在发生服务故障时的弹性与恢复能力。灾难恢复（DR）在医院信息平台建设中的应用分为不同级别：

- 组件故障
- 服务失败（多个组件故障导致关键服务不可用）
- 数据中心物理访问失效（数据中心操作维持正常）
- 数据中心失效（数据中心系统不能正常运作）

在灾难备份方案的规划中，需要对各业务部门的需求进行分析，根据不同类型的业务/非业务应用系统的运行情况进行统一规划。只有认真、详尽地分析灾难恢复要求，才能够保证满足服务等级协议（Service Level Agreement,SLA）。

本节着重讨论有关服务器基础设施的灾难恢复。对于网络和存储有关的灾难恢复，请参阅相关章节。

下表描述了医院信息化内各个组件的灾难恢复要求：

表 5-13 灾难恢复级别

			医院规模		
灾难恢复等级	恢复时间(RTO)	可接受的数据丢失(RPO)	小型医院	中等	大中型医院
AAA	0.5 小时或更少	最大 0.5 小时	-	-	电子病历、ODS、数据仓库
AA	0.5-2 小时	2 小时	-	电子病历, ODS	
A	2-4 小时	4 小时	电子病历, ODS	数据仓库	
B	4-72 小时	24 小时	数据仓库		

组件故障与恢复

组件故障指的是导致平台停机和数据损坏的硬错误和软错误。稳定可靠的服务器平台，应该具有连续监控关键功能、检测各种硬错误和软错误、以及自动更正或解决多数问题的能力。所有的医院信息平台服务器均需要具备基本的可靠性，可用性和服务功能（RAS）：

- 恢复数据总线错误
- 缓存 ECC
- 内存单一设备纠错
- 发生双位错误时内存重试
- 内存备件

对于更高水平的可靠性和可用性（如 DR A 级及以上），服务器应该支持 IT 和管理系统以检测错误。对于重要的医院信息平台功能（如 DR AAA 级），服务器应支持在硬件、固件和操作系统一级处理错误。同时，它还应可以透过固件和操作系统来纠正复杂错误和实现恢复。

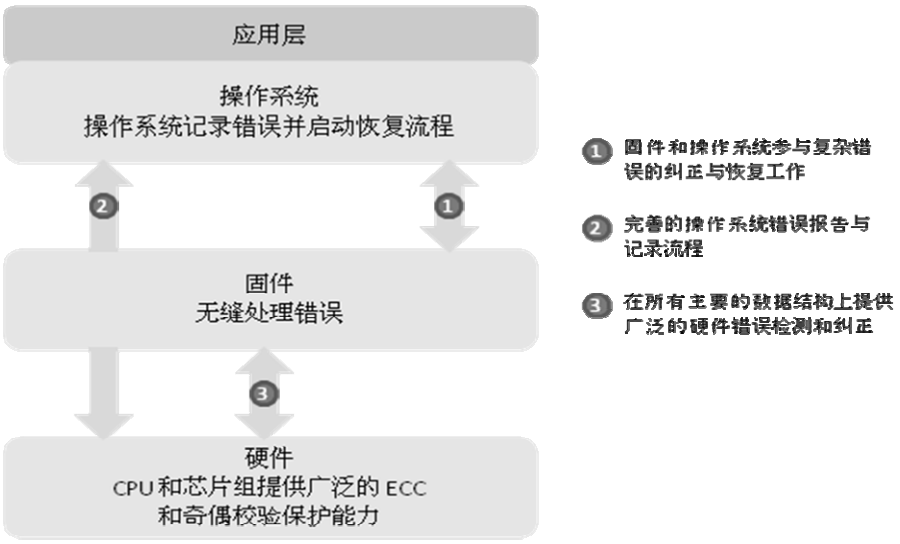

图 5-44 关键先进机器的架构检查实例

除了以上实例中的高级机器检查体系（Advanced Machine Check Architecture），对于 AAA 级功能，消除服务器内的单点故障也非常重要。这通常需要复制服务器内的组件和路径，满足高可用性要求的服务器类型最适合高级医院信息平台中的关键功能。

服务失败

服务失败，指的是多个组件故障导致关键服务不可用。通常来说，我们通过服务集群的方式来降低服务失败带来的威胁。通过将服务以分布式的方式部署在两台或多台物理主机上，可以消除因服务器单点故障导致的停机。

服务集群可以结合虚拟化技术，以经济高效地实现医院信息平台内的关键服务组件的高可用性。服务应用部署在虚拟机中，可以与其他服务共享服务器资源（特别是那些不能无法支持多 CPU 处理的服务）。将硬件服务器虚拟化之后，物理服务器并不需要在硬件配置方面完全一致。这也意味着，可以利用现有医院的服务器资源进行整合，提供更高效率的计算能力。

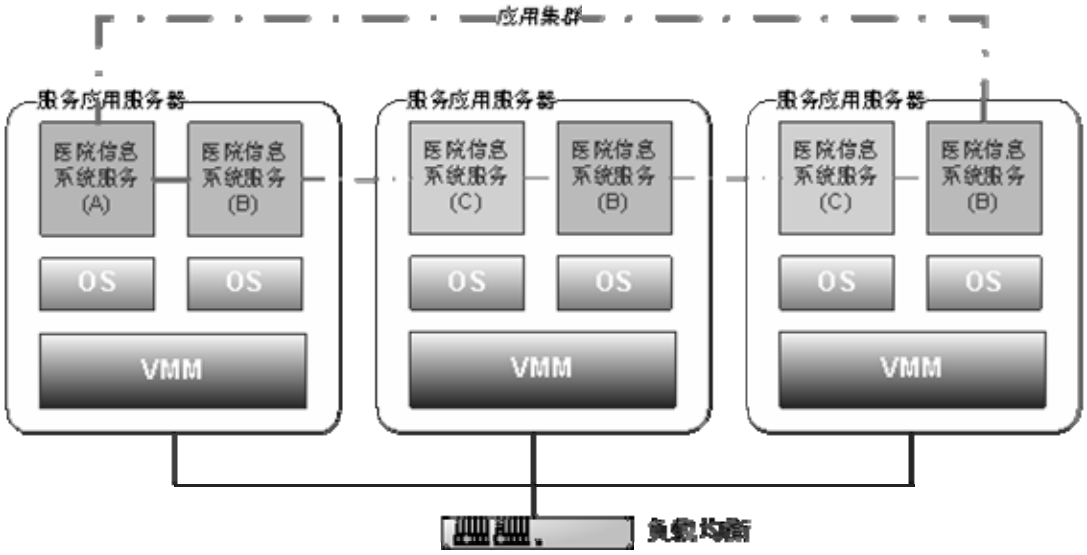

图 5-45 虚拟化应用服务集群

数据中心物理访问失效

数据中心访问失效是指主数据中心的运行正常，但物理无法访问该数据中心。如果主数据中心的运行全面正常，医院信息平台需要保障全面的远程连接与全面远程管理能力。医院内部/远程客户端需要具有远程的带外管理能力，并且具有较高的安全性。关于网络连接的高可用性，在“网络架构”章节中有单独描述。

数据中心失效

通常需要部署一个远程故障切换架构，允许在主数据中心遭遇灾难事件时，由备用数据中心接管关键任务运营。有很多技术可以用于实现远程故障切换架构，包括磁带，园区集群，以及数据库交易一级或磁盘 I/O 一级的广域网复制等。有关存储的灾难备份将在“存储架构”一章中讨论。

5.4.4.5.2 灾难恢复的部署

一些大中型医院，在建设医院信息系统的过程中，在一定程度上考虑到了灾难恢复的可行性。往往在医院内部的不同建筑内部署主数据中心和备份数据中心。这种部署方式往往是一种权宜之计，目的是减少主数据中心出现突发故障时

造成的损失。一些大型医院也可以考虑将备份数据中心建设在分支机构所在地，从而更好的规避风险。

在区域卫生平台的建设中考虑到了备份数据中心的建设，也使得医院信息平台借助区域卫生平台的主/备份数据中心实现异地灾难备份成为可能。

物理到虚拟的 HA 解决方案，是一种灵活的部署方式。主数据中心一些以物理服务器的方式部署的系统，在备份数据中心则可以采用虚拟机的方式来对应部署。这意味着，在备份数据中心可以将非关键服务部署在少量物理服务器上。当主数据中心发生故障时，非关键服务将会提供较低水平的服务，或者暂停。而关键服务可以部署在计算能力较强的物理服务器或者虚拟机上，从而保障关键服务的运行效率。这样，灾难备份规模较小，并且更为经济高效。

与集群技术和虚拟化技术相结合，可以更好的实现从主数据中心到备份数据中心的服务复制。一旦主数据中心发生故障，备份数据中心的集群节点将接管服务，从而实现灾难恢复。

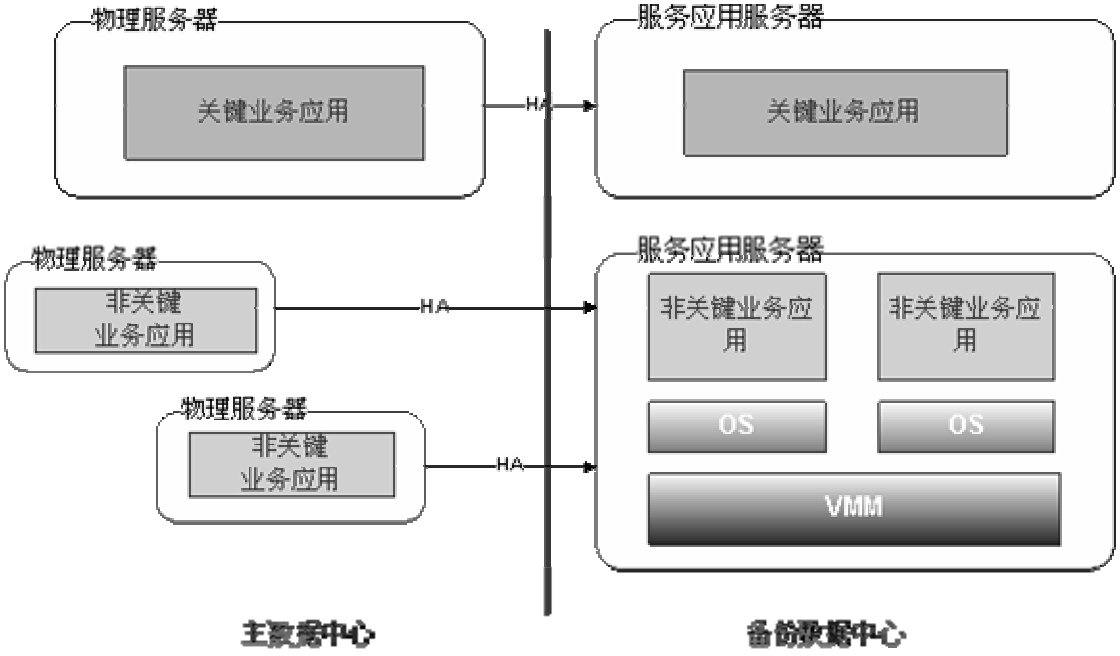

图 5-46 物理到虚拟的 HA 方案设计

在“存储架构”中将对数据复制、备份进行详细描述。

5.4.4.6 典型医院环境下服务器部署现状分析

为了更好的对基于电子病历的医院信息平台建设提供参考，我们对典型医院环境下的服务器部署现状做了分析。依照医院的不同规模，大致划分为大中型医院、中等规模医院和小型医院。

5.4.4.6.1 大中型医院服务器部署架构

1、部署架构示意图

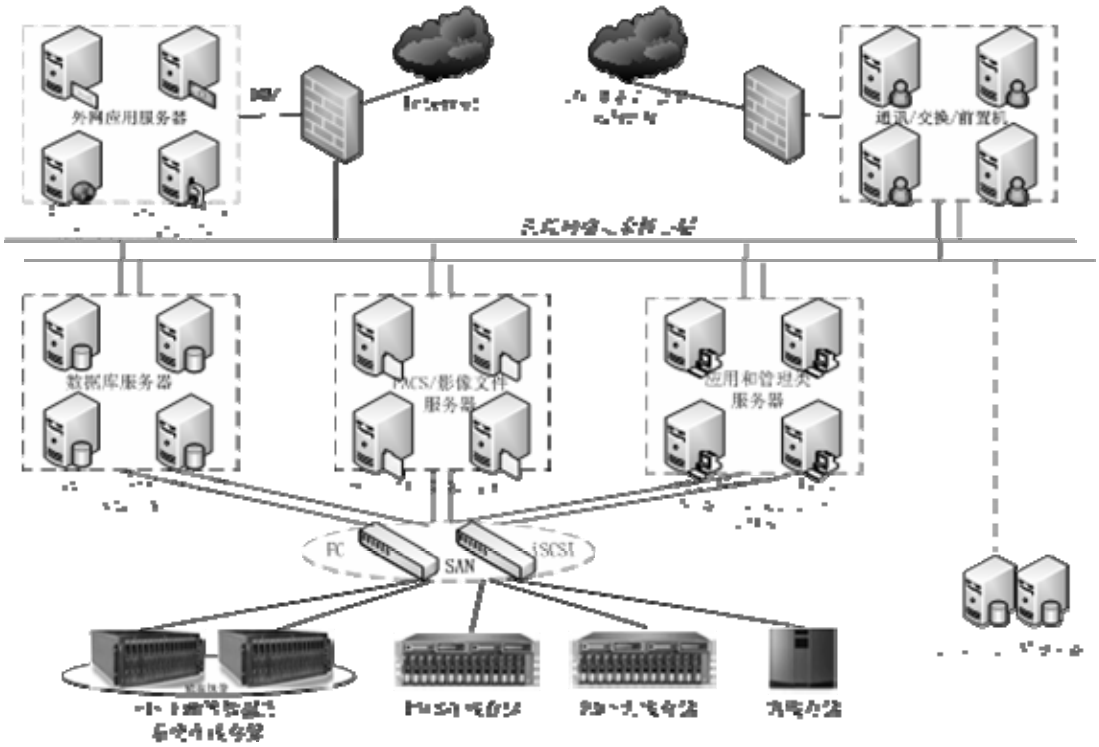

图 5-47 大中型医院信息系统服务器与存储系统部署方案

2、服务器系统部署说明

较多数量的大中型医院其信息系统建设已有较好的基础，特别是沿海发达地区的大中型医院更是普遍比较重视，但基本上都是逐年部署，相对缺乏统一规划，采用的技术平台也五花八门，不过也有很多医院已经在开始根据其医院信息化建设的统一规划来调整、整合数据中心，尤其是服务器的整合部署；医院信息系统的服务器基本上都是基于各种不同业务子系统来部署的，一般来说，大中型医院在服务器部署方面有以下共性：

1）HIS、EMR、LIS 等关键业务系统，多数的医院采用了 X86 架构的 PC 服务器，Windows Server 或 LINUX 平台为主，双机集群方案；采用 UNIX 服务器的医院也比较多，且大多数还采用了 UNIX 双机集群模式，主要是基于 UNIX 小型机本身的高可用角度考虑的；

2）PACS/RIS、以及超声、病理、心电等影像系统相对比较独立，通常来说，医院会单独进行部署，影像系统的服务器通常由数据库服务器、应用和归档服务器、RIS 服务器、临床浏览服务器等组成，其中 PACS 主数据库服务器一般双机模式；

3）其他各种应用和管理类服务器一般采用 X86 架构 PC 服务器，主要有中间件（双机）、集成平台（双机）、网络管理、备份管理、终端桌面管理、防病毒管理、域控制器等等；

4）由于 HIS 系统是支撑医院基本业务开展的基础应用系统，因此一般的大中型医院都部署有 HIS 门急诊业务应急系统，主要是采用每天从在线数据库下传公用数据，通过应用程序的设定，当在线系统故障时，临时启用应急系统；

5）大中型医院的信息系统与外部网络的连接也是相当广泛的，主要分为两部分：一是与医院业务紧密关联的区域系统，例如医保系统、新农合系统、社区卫生健康档案系统、远程医疗的接入等等，这些系统的接入一般都部署有前置服务器；二是医院本身基于改善医患关系、提高工作效率考虑基于 Internet 公网开展的一些外延应用，主要有短信平台、语音自助服务、OA 远程办公接入、医院门户网站、电子邮件系统等等；

大中型医院的信息化建设虽然面面俱到，也已经初具规模，有些医院在应用层面甚至还有一些非常有参考价值的特色（例如流程改造方面），但在服务器硬件平台的部署上，存在的比较普遍的问题主要有：

5）服务器资源使用率低下；大中型医院往往在给 HIS、EMR 等核心业务系统部署服务器硬件的时候，没有仔细分析和研究真正的需求，基本上

是根据预算来定设备配置和型号，这往往就导致购买了昂贵的设备，却只有 10%不到的资源使用率，同时，一般来说，又不愿意将其他业务系统部署、整合在一起，各个业务系统的服务器往往都是独立设备、独立运行；

6）各种技术平台混杂，给管理和维护带来较大的成本；大中型医院的数据中心机房内，往往可以看到各种五花八门的设备，小型机、PC 服务器（有机架式、台式、还有刀片系统等）、各种存储（有 FCSAN、IP-SAN、NAS、磁带机等）、各种安全设备，有 UNIX、LINUX、Windows，还有甚至各种数据库 Oracle、SQL、Cache’、Sybase；没有经过通过规划和部署的情况下，这些都是难免的，也无疑给医院 IT 维护工作带来空前的挑战，同时也将付出极高的代价。

3、典型服务器系统部署清单

表 5-14 典型服务器系统部署清单（大中型）

设备名称	机型	配置概述	数量	备注
HIS 服务器	高配 PC 服务器或中高端 UNIX 小型机	8 个或以上处理器，32G 或以上内存，2 块硬盘，4 个 1000M 网卡，2 个 HBA 卡，DVD，冗余电源，UNIX 或 Linux 或 Windows 操作	2	双机集群
EMR 服务器	中高配 PC 服务器或中端 UNIX 小型机	4 个或以上处理器，16G 或以上内存，2 块硬盘，4 个 1000M 网卡，2 个 HBA 卡，DVD，冗余电源，UNIX 或 Linux 或 Windows 操作	2	双机集群，或与 HIS 服务器部署在一起
LIS 服务器	PC 服务器	2 个或以上处理器，8G 或以上内存，2 块硬盘，4 个 1000M 网卡，2 个 HBA 卡，DVD，冗余电源，Linux 或 Windows 操作	2	双机集群，或与 HIS 服务器部署在一起
PACS 服务器	中配 PC 服务器或中低端 UNIX 小型机	4 个或以上处理器，16G 或以上内存，2 块硬盘，4 个 1000M 网卡，2 个 HBA 卡，DVD，冗余电源，UNIX 或 Linux 或 Windows 操作	2	双机集群
RIS 服务器	中端 PC 服务器	2 个或以上处理器，8G 或以上内存，2 块硬盘，2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1	
影像采集和归	中端 PC 服	2 个或以上处理器，8G 或以上内存，2	2-4	根据不同的

档服务器	务器	块硬盘，2 个 1000M 网卡，2 个 HBA 卡，DVD，冗余电源，Linux 或 Windows 操作		PACS 决定
影像临床浏览服务器	中高端 PC 服务器	4 个或以上处理器，16G 或以上内存，6 块硬盘（本地大容量配置或连接到 SAN 上），2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1-2	
体检系统服务器	中高端 PC 服务器	4 个或以上处理器，16G 或以上内存，6 块硬盘（本地大容量配置或连接到 SAN 上），2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1-2	
其他应用服务器	中端 PC 服务器	2 个或以上处理器，8G 或以上内存，2 块硬盘，2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	2-4	根据不同应用需要配置，例如合理用药、手术麻醉、ICU 等等
中间件/集成平台服务器	中高端 PC 服务器	4 个或以上处理器，16G 或以上内存，6 块硬盘（本地大容量配置或连接到 SAN 上），2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1-2	根据医院信息系统的技术框架决定， B/S 、C/S/S 等
备份服务器	中端 PC 服务器	2 个或以上处理器，8G 或以上内存，2 块硬盘，2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1	
管理服务器	中低端 PC 服务器	1 个或以上处理器，4G 或以上内存，2 块硬盘，2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1-6	网管、防病毒、域、桌面管理等等
前置类服务器	中低端 PC 服务器	1 个或以上处理器，4G 或以上内存，2 块硬盘，2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1-4	医保、新农合、EHR、远程医疗等
外网应用服务器	中端 PC 服务器	2 个或以上处理器，8G 或以上内存，4 块硬盘，2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1-4	门户网站、电子邮件、OA 远程、短信平台、语音平台等

5.4.4.6.2 中等规模医院服务器部署架构

1、 部署架构示意图

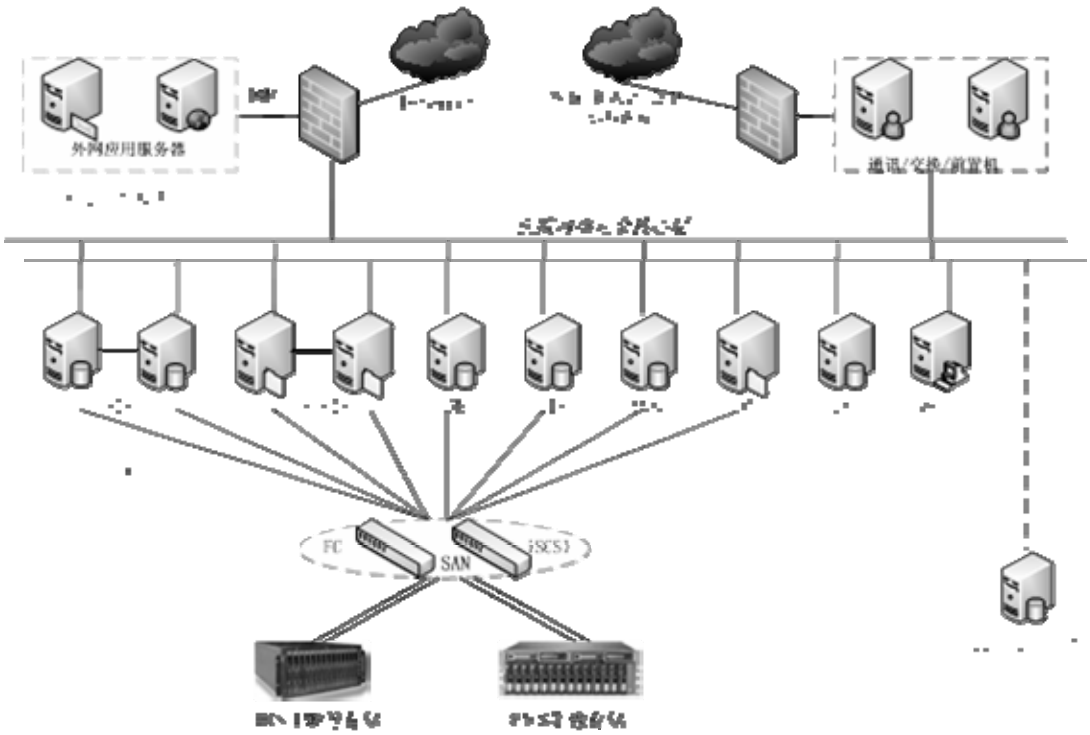

图 5-48 中等规模医院信息系统服务器与存储部署方案

2、 服务器系统部署说明

中等规模的医院实际上与大型医院在业务和功能需求方面大致类似，无非是应用系统的规模会相对小一些，目前情况来看，中等规模医院之间的信息化建设差异还是比较大的，有些医院的信息系统应用覆盖很广，除了 HIS、LIS 以外，也与大医院一样有 EMR、PACS/RIS 等系统，甚至也有门户网站、OA 系统等等，特别是县市级最大的医院，也是当地区域范围内信息化建设的标杆。由于中型医院的系统应用规模相对较小，但覆盖面仍然很全，所以具有以下特点：

1）根据各个业务系统的上线时间不同，采用搭积木形式，逐步增加服务器；例如 HIS 是最早上线的，一般都有双机热备，要上 EMR 时，再部署 2 台双机服务器，要上 LIS 时又部署服务器，如此类推横向扩展，与大医院一样也存在服务器资源浪费的问题；

2）中型医院也同样会部署有各类外部业务系统的接入，医保、新农合等，因此也需要前置机；

3）至于管理类、中间应用层、外网应用、应急备份等方面，中型医院也通常采用要用什么就部署什么的思路，很难找到共性；

4）中型医院的服务器大多数采用的是 X86 架构 PC 服务器，其中 HIS、EMR、PACS 等通常会采用中高端配置；

3、 典型服务器系统部署清单

表 5-15 典型服务器系统部署清单（中等规模）

设备名称	机型	配置概述	数量	备注
HIS 服务器	中高端 PC 服务器	4 个或以上处理器，16G 或以上内存，6 块硬盘（本地大容量配置或连接到 SAN 上），2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	2	双机集群
EMR 服务器	中端 PC 服务器	2 个或以上处理器，8G 或以上内存，2 块硬盘，2 个 1000M 网卡，2 个 HBA 卡，DVD，冗余电源，Linux 或 Windows 操作	2	双机集群，或与 HIS 服务器部署在一起
LIS 服务器	中端 PC 服务器	2 个或以上处理器，8G 或以上内存，2 块硬盘，2 个 1000M 网卡，2 个 HBA 卡，DVD，冗余电源，Linux 或 Windows 操作	2	双机集群，或与 HIS 服务器部署在一起
PACS 服务器	中端 PC 服务器	2 个或以上处理器，8G 或以上内存，2 块硬盘，2 个 1000M 网卡，2 个 HBA 卡，DVD，冗余电源，Linux 或 Windows 操作	2	双机集群
RIS 服务器	中端 PC 服务器	2 个或以上处理器，8G 或以上内存，2 块硬盘，2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1	
体检系统服务器	中高端 PC 服务器	4 个或以上处理器，16G 或以上内存，6 块硬盘（本地大容量配置或连接到 SAN 上），2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1-2	
其他应用服务器	中端 PC 服务器	2 个或以上处理器，8G 或以上内存，2 块硬盘，2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1-2	根据不同应用需要配置，例如合理用药等等
备份服务器	中端 PC 服务器	2 个或以上处理器，8G 或以上内存，2 块硬盘，2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1	
管理服务器	中低端 PC 服务器	1 个或以上处理器，4G 或以上内存，2 块硬盘，2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1-4	网管、防病毒、域、桌面管理等等
前置类服务器	中低端 PC 服务	1 个或以上处理器，4G 或以上内存，2 块硬盘，2 个 1000M 网卡，DVD，冗余电源，	1-4	医保、新农合、EHR、远程医疗

	器	Linux 或 Windows 操作		等
外网应用服务器	中端 PC 服务器	2 个或以上处理器，8G 或以上内存，4 块硬盘，2 个 1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1-2	门户网站、电子邮件等

5.4.4.6.3 小型医院服务器部署架构

1、 部署架构示意图

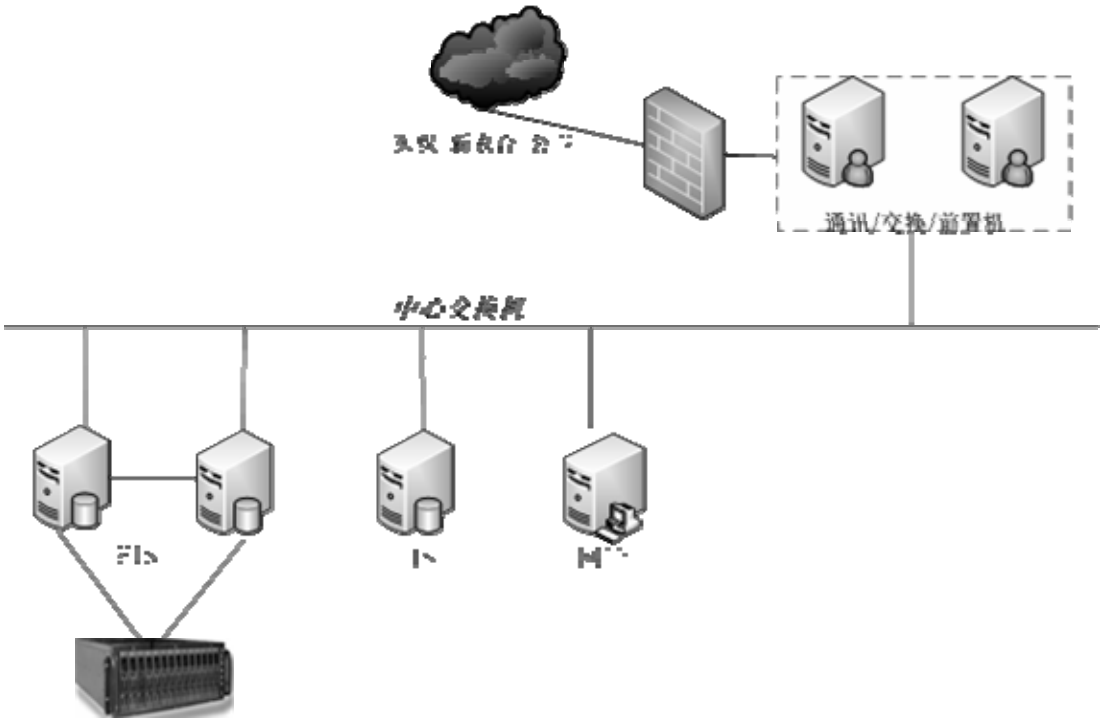

图 5-49 小型医院信息系统服务器和存储部署方案

2、 服务器系统部署说明

小型医院的信息系统基本上是为了满足医院基本业务运行需要即可，因此，大部分的小型医院如果要上信息系统，则通常出于两个方面的考虑：一是为了实现医保联网结算、EHR 联网；二是为了医院内部业务部分实现电脑化操作，便于财务管理；基于以上两点，大部分已经上了信息系统的小型医院在部署服务器时就比较简单：

1）HIS 服务器，有的是双机形式，有的就只用单机运行；

2）可能会有 LIS 系统，单独配置 1 台服务器；

3）根据需要会有一些前置服务器，比如社区 EHR 接入、医保、新农合等等；

4）小型医院的信息系统数据备份也比较简单，通常会在服务器本地做一下备份，然后定期在管理员的电脑上或做异地备份；

5）小型医院的信息系统安全性和稳定性较差，如果服务器出现故障，基本就让信息系统处于瘫痪状态，转为手工操作，直到服务器修复；且小型医院的 IT 维护力量非常薄弱，因此采用简单有效、低成本的服务器整合方案是非常有必要的；目前已有一些地区，在当地卫生主管部门的筹划下，将小型医院的服务器全部集中到区级平台的数据中心集中管理，本地不再部署服务器；

3、 典型服务器系统部署清单

表 5-16 典型服务器系统部署清单（小型）

设备名称	机型	配置概述	数量	备注
HIS 服务器	中低端 PC 服务器	1 个或以上处理器，4G 或以上内存，2 块硬盘，2 个 10/100/1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1-2	
LIS 服务器	中低端 PC 服务器	1 个或以上处理器，4G 或以上内存，2 块硬盘，2 个 10/100/1000M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1	
前置类服务器	中低端 PC 服务器	1 个或以上处理器，2G 或以上内存，2 块硬盘，2 个 100M 网卡，DVD，冗余电源，Linux 或 Windows 操作	1-3	医保、新农合、EHR 等

5.4.4.7 医院信息平台服务器整合思路

医院信息平台的建设，即要考虑集成平台本身的建设，也要考虑现有系统的现状。透过对典型医院服务器部署环境的现状分析，我们不难看出，随着医疗信息化系统需求不断增加，医院普遍面临着信息化管理难度越来越大的困境。

随着专业的不断细分，针对特定专业的系统不断涌现，医疗信息系统的复杂性和多样性更为明显。而传统的系统建设思路，往往是以项目为单位进行设计和采购的。

系统异构、数据量庞大、关联性强是医院信息系统数据的主要特征。如何提高数据的可管理性、可用性以及利用能力是医院信息化管理者需要重点考虑的问题。集中融合、提供服务是医院未来信息系统建设中的一条重要思路。

服务器资源的整合，不是简单的将旧有的系统迁移到高性能服务器、刀片服务器或者其他类型的高密度计算平台上。需要进行统一的规划，分析哪些系统可以进行整合，如何整合。再利用先进的技术方案和服务器平台来搭建医院服务器整合平台，将旧有的多台服务器进行整合，并实现服务器资源的合理调度分配。此外，我们还需要改变传统的按项目进行服务器资源设计和采购的方式，在新项目规划时进行统一考虑，与医院现有的服务器资源相结合来规划服务器配置。

服务器整合应遵循以下几个原则：

- 可管理性：可管理性是医院信息系统最迫切的需求，数据多样复杂性使得信息化管理的难度越来越大。
- 可靠性：医院是为患者提供医疗服务的机构，与患者的生命和健康息息相关。与普通企业相比，对于信息系统的可靠性要求更高。
- 可扩展性：服务器整合不是终点，而是一个不断演进的过程。服务器平台应具有良好的可扩展性。
- 安全性：系统整合可能带来一定的安全风险，在整合方案设计中应充分考虑安全性的要求。不仅要考虑被动的安全措施，也要考虑主动安全性。
- 开放性：服务器应采取开放式的架构，支持流行的开发框架和常用开发工具，对开发商提供较好的支持。应具有较好的可伸缩性、可靠性和经济性，人员培训成本较低。
- 满足计算性能：随着医院信息化的发展，数据量不断增加，系统复杂性也更高，计算能力的要求随之增长。服务器平台应该提供与之相匹配的计算性能来满足不断发展的要求。
- 绿色环保：随着医院部署的服务器数量不断增加，医院数据中心面临的能耗、散热的问题越来越突出，直接影响到了数据中心的可靠性和可用性。如何实现低能耗成为了未来几年医院数据中心建设必须要考虑的问

题。在服务器的选择中，应优先考虑符合国家有关规定的绿色节能产品。

从技术实现的角度，需要重点考虑以下一些问题：

- 虚拟化技术的应用。服务器虚拟化技术，与存储和网络虚拟化相结合，为服务器资源整合提供了经济、有效的技术手段。
- 应用系统对于计算能力、I/O和网络的需求。不同类型的应用系统，对于服务器资源要求是不同的。在服务器整合中，需要对这些应用系统进行调研和分析，并且通过硬件服务器相关的技术支持来获取更好的性能。
- 数据整合。医院信息系统数据包括结构化、文本、影像、动态影像等众多不同类型的数据，历史数据在线时间要求高，重复数据删除面临很大的挑战。数据整合的目的，是为医院管理者、医疗人员、患者提供完整视图，以满足诊疗和科研的要求。
- 异构系统的整合。一些医院信息化发展较早，部署了大量的PC服务器和UNIX小型机系统。对于异构系统而言，需要具体情况具体分析，从迁移的成本、对于医院业务的影响和未来系统发展等多方面进行综合考虑来做出决定。

5.4.4.8 典型医院信息平台服务器物理部署设计

医院信息平台服务器部署，应具有良好的可扩展性。以满足医院业务高峰期以及故障或灾难出现时的服务处理高峰。采取动态负载均衡是服务器部署的必要手段。所有服务器都应带有兼容的虚拟化硬件平台支持及并行多处理能力，以实施高效的资源管理与医院信息平台的处理能力最大化。

下图是服务器部署的典型物理设计：

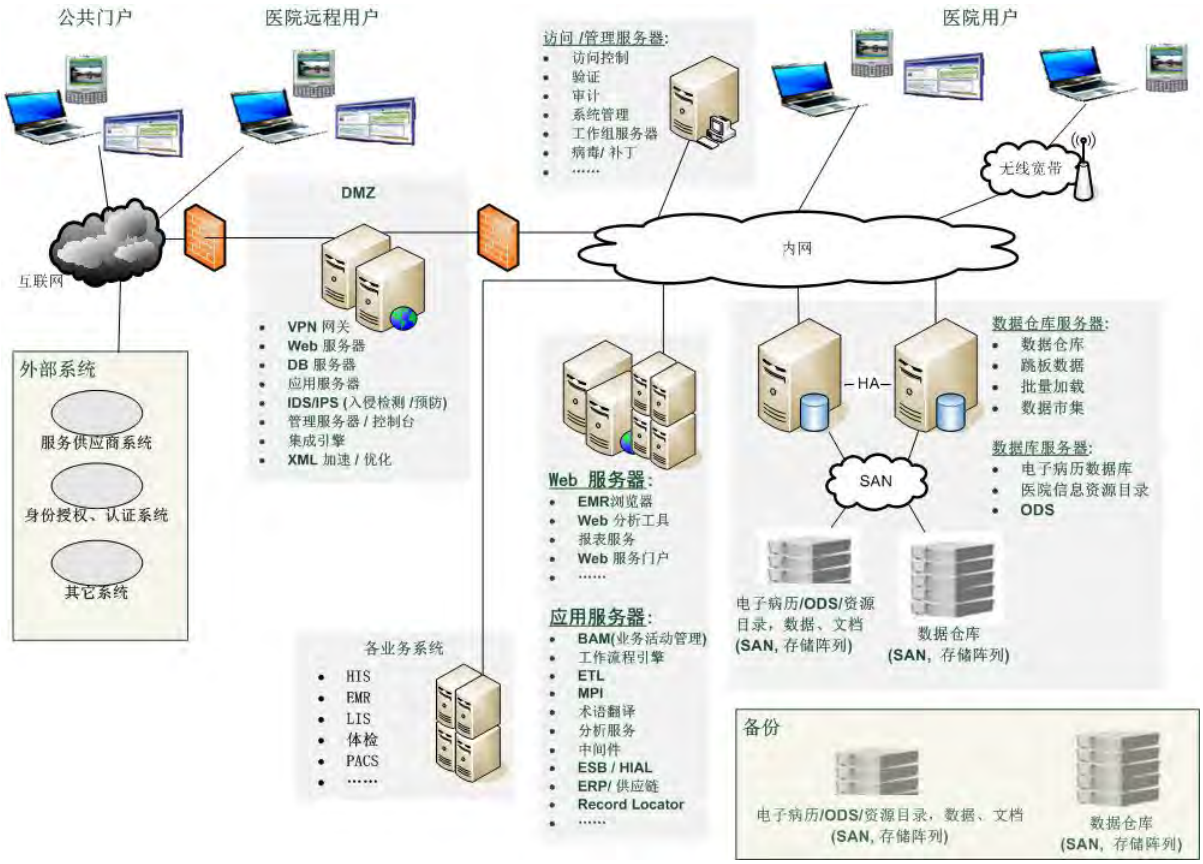

图 5-50 典型部署的服务器架构

下表列出了不同规模医院的基于电子病历的医院信息平台的服务器部署的参考配置，同时还概述了服务器和配置级别（注意：该服务器部署未包括各业务系统，也未包括与办公和生产服务相关的服务，如电子邮件和办公服务等）。详细规模将取决于具体要求，根据实际情况来实施。

列表中的部分服务器，可以采用虚拟化技术进行部署：

表 5-17 不同规模医院的典型服务器部署

	小型	中等	大中型	注释
数据存储服务器	双路多核 X86 服务器(或同级服务器)	集群多路多核 X86 关键任务服务器(或同级服务器)	集群关键任务服务器	详细配置取决于具体交易量而定
BI 服务器	多核 x86 服务器(或同级服务器)	双路多核 x86 服务器(或同级服务器)	多路多核 x86 服务器(或同级服务器)	详细配置取决于具体交易量而定

电子病历数据服务器	双路多核 x86 服务器(或同级服务器)	集群多路多核 x86 服务器(或同级服务器)	集群关键任务服务器	详细配置取决于具体交易量而定
Web 服务器	多核 x86 服务器(或同级服务器)(采用虚拟化技术)	多台双路多核 x86 服务器(或同级服务器)(采用虚拟化技术)	多台双路多核 x86 服务器(或同级服务器)(采用虚拟化技术)	虚拟机的数量取决于交易量而定
应用服务器	双路多核 x86 服务器(或同级服务器)(采用虚拟化和集群技术)	多台双路多核 x86 服务器(或同级服务器)(采用虚拟化和集群技术)	多台双路多核 x86 服务器(或同级服务器)(采用虚拟化和集群技术)	应用服务器详细配置取决于服务的数量和交易量。虚拟机的配置基于标准的 J2EE 或同级的性能标准。
访问/管理服务器	多核 x86 服务器(或同级服务器)	多核 x86 服务器(或同级服务器)	双路多核 x86 服务器(或同级服务器)	虚拟机不支持管理功能，必须推行独立的服务器。
数据访问层服务器	双路多核 x86 服务器(或同级服务器)	多台双路多核 x86 服务器集群(或同级服务器)	多台多路多核 x86 服务器集群(或同级服务器)	

5.4.5 存储架构

5.4.5.1 存储技术架构

存储技术的发展经历了三代，分别是直连式存储（Direct Attached Storage，DAS）、网络附加存储（Network Attached Storage，NAS）、存储区域网络（Storage Area Network，SAN）。

5.4.5.1.1 DAS

DAS是最先被采用的网络存储系统。在这种方式中，存储设备通过电缆（通常是SCSI接口电缆）直接到服务器。I/O（输入/输出）请求直接发送到存储设备。这种方式是连接单独的或两台小型集群的服务器。由于早期的网络十分简单，直连式存储得到发展。

DAS存储方式如下图所示：

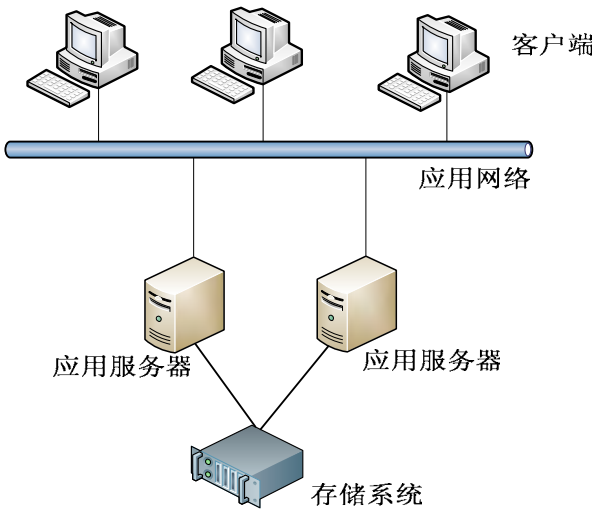

图 5-51 DAS 存储方式图

DAS存储方式的应用特点：易于部署，且经济实惠。但是它也有很多不足，如存储系统可共享性差，存储系统分散不易于管理等，比较适合应用简单、前端服务器较少、业务量小的环境，但随着业务的发展，会逐渐被替代。

5.4.5.1.2 NAS

NAS产品包括存储部件（例如磁盘阵列）和内嵌系统软件，能够支持多种应用协议（如NFS、CIFS、FTP、HTTP等），还能够支持各种操作系统，如Windows、Linux等，在不同的网络环境中使用也无需对网络环境进行任何的修改。NAS直接通过网络接口连接到网络上，简单地配置IP地址后，就可以被网络上的用户所共享使用。

NAS存储方式如下图所示：

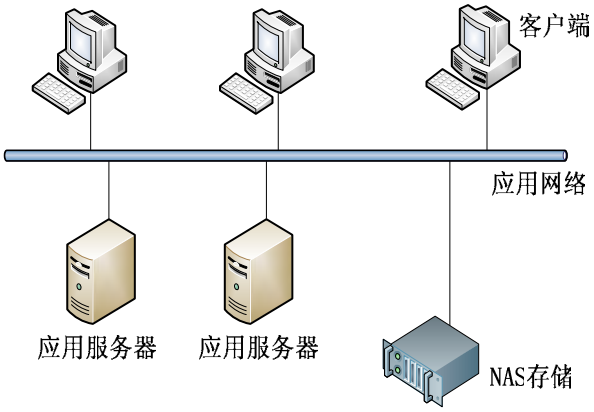

图 5-52 NAS 存储方式图

NAS存储方式的出现是局域网技术发展的直接产物，使得存储系统与服务器通过局域网通信成为可能。NAS的I/O访问是文件级的，通常采用TCP/IP或NetBIOS协议支持这种文件级的访问和存储。

主流IPSAN存储可以同时提供IPSAN和NAS两种方式，满足用户文件级和块级的访问。

NAS存储方式的应用特点：NAS存储方式通过以太网文件访问协议，提供不同操作系统的文件共享，由于依托现有的IP网络，易于部署。由于在IP网络部署，数据备份或者存储过程中会占用大量网络带宽，公用网络带宽限定了NAS存储的性能。

随着NAS存储的发展，出现了NAS和SAN融合的架构以及NAS集群模式，来解决NAS在以太网传输性能问题。

NAS和SAN存储架构的融合

SAN应用冗余架构和块级访问提供高安全性和高性能，NAS应用成熟的网络结构提供快速的文件存取。一个融合SAN和NAS技术的存储解决方案全面提供一套在以块(Block)和文件(File)I/O为基础的高效率平衡方案从而全面增强数据的可用性。

NAS和SAN可以满足用户不同的需求，越来越多的企业或部门开始采用NAS和SAN融合的解决方案。

NAS和SAN融合存储方式如下图所示：

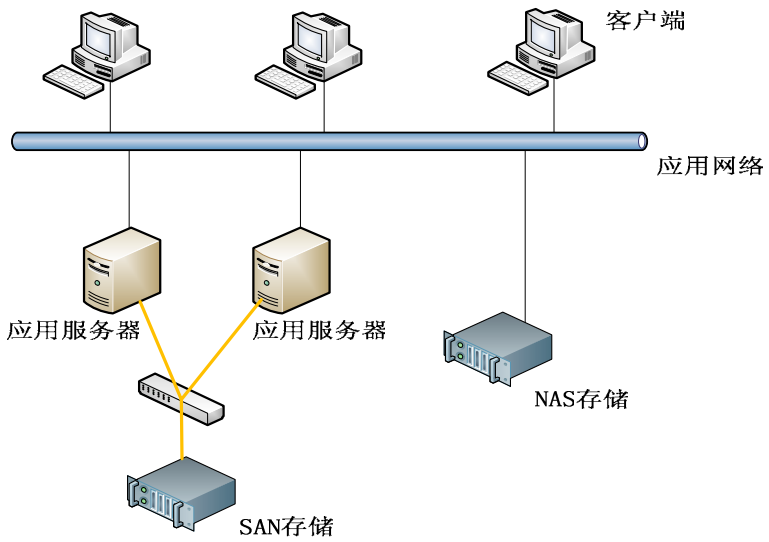

图 5-53 NAS 和 SAN 融合存储方式图

NAS 集群

非结构化数据（视频、图片、电子文档等）的快速增长，传统NAS遇到了性能、扩展性、管理等一系列的挑战，NAS集群的出现正好可以满足用户存储非结构化数据的需求。

NAS集群的存储方式如下图所示：

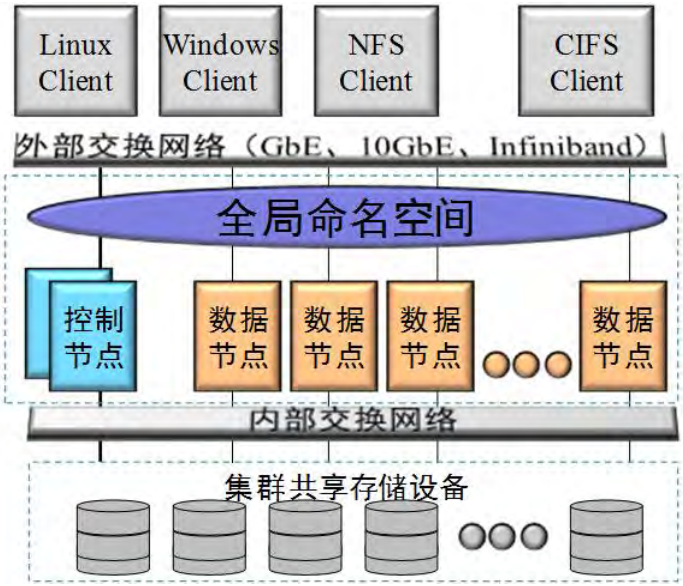

图 5-54 NAS 集群存储方式图

NAS集群的应用特点：

- 存储空间的海量性和扩展性。当企业数据的存储容量不足时，存储系统要能够实现在线容量的扩展而不中断前端主机业务的访问。
- 支持分层存储。后端存储单元支持SSD、FC、SATA等磁盘，并且后端存储单元支持不同磁盘类型的混插，满足了不同应用对性能的需求。
- 多用户访问的并发性和全共享性。NAS集群多节点之间采用集群模式，具有较高的计算能力和I/O带宽，并行对外提供访问服务。
- 集群设备的易用性和可用性。集群NAS设备采用专有的文件系统，提供全局命名空间，提供统一化的管理界面，方便用户管理。

5.4.5.1.3 IPSAN

IPSAN是基于TCP/IP的网络，将服务器和存储设备通过专用的网络连接起来，服务器通过“BlockI/O”发送数据存取请求到存储设备。最常用的是iSCSI技术，就是把SCSI命令包在TCP/IP包中传输，即SCSI over TCP/IP。

IPSAN存储方式如下图所示：

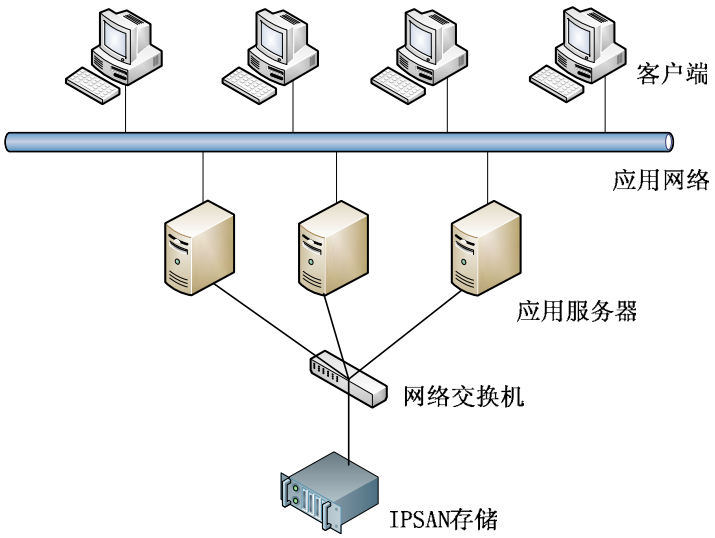

图 5-55 IPSAN 存储方式图

IPSAN 存储方式的应用特点：由于 IPSAN 存储方式是基于以太网，因此有容易部署、没有距离限制、成本低等优势，随着10Gbps以太网的应用，IPSAN存储方式得到相应的应用和发展。但以太网本身的安全性、稳定性等一些因素在制约着它的发展。

5.4.5.1.4 FC SAN

存储设备利用光纤连接，采用光纤通道协议（Fiber Channel，FC），将服务器和存储设备间连接起来，组成单独的网络，I/O请求直接发送到存储设备。光纤通道协议实际上解决了底层的传输协议，高层的协议仍然采用SCSI协议，所以光纤通道协议实际上可以看成是SCSI over FC。

FC-SAN的设计初衷是基于企业级的核心数据以及应用的高端用户设计的，发展到现在，已经非常成熟、稳定。FC-SAN使用高效的光纤通道协议，由于是基于核心数据和应用设计的，FC-SAN大部分功能都基于硬件来实现的，核心交换设备-光纤交换机均带具有高可靠性及高性能的ASIC芯片设计，在主机端通过带有ASIC芯片的专用光纤HBA来进行数据信息的处理。

FC SAN存储方式如下图所示：

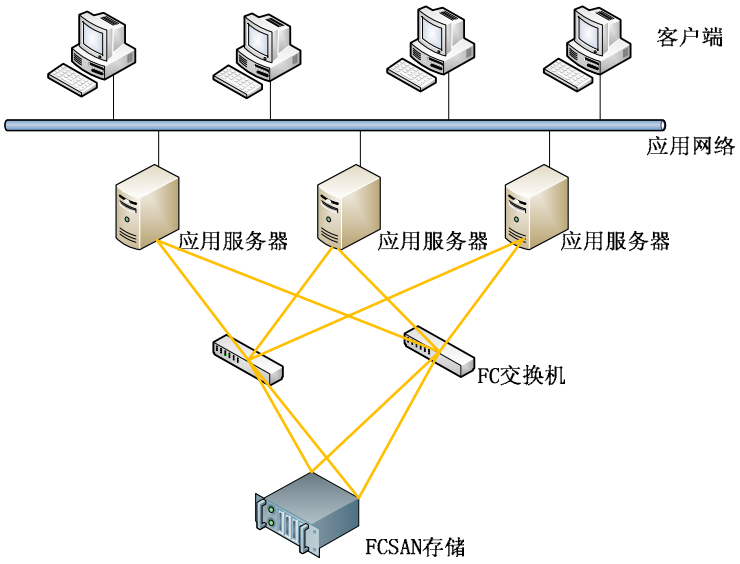

图 5-56 FC SAN 存储方式图

FC SAN存储方式的特点：

- 网络设备及传输介质

在链路中使用光纤介质，不仅完全可以避免因传输过程中各种电磁干扰，而且可以有效达到远距离的I/O通道连接；在FC-SAN中所使用的核心交换设备-光纤交换机均带具有高可靠性及高性能的ASIC（Application Specific Intergrated Circuits）芯片设计，使整个处理过程完全基于硬件级别的高效处理。在连接至主机的HBA设计中，绝大多数操作独立处理，完全不耗费主机处理资源。

- 并发操作能力

FC-SAN可以承接更多的并发访问用户数，当外接用户数呈大规模增长趋势时，FC-SAN就显示出其在稳定、安全、以及高性能传输率等方面的优势，比较适合电子病历平台等用户快速增长的业务需求。

- 设备稳定性

FC-SAN由于使用高效的光纤通道协议，因此大部分功能都基于硬件来实现的，如后端存储子系统的存储虚拟通过带有高性能处理器的专用RAID控制器来实现，中间的数据交换层通过专用的高性能ASIC来进行基于硬件级的交换处理，在主机端通过带有ASIC（Application Specific Intergrated Circuits）芯片的专用HBA来进行数据信息的处理。因此在大量减少主机处理开销的同时，也大大提高了整个FC-SAN的稳定性。

- 可扩展性

在全交换（FC-SW Fibre Channel switch fabric）的FC-SAN中，各通信终端通过FC端口登陆后来进行数据的传输与处理，而每个端口会提供专用的24位的FC端口地址（WWN）来进行数据通信，根据其地址分配策略，在FC-SW中实际可用的地址值达到1550万，因此在实际的企业级应用中，完全可以满足任何规模的存储网络的建立。

- 可靠性

在整个系统中，除了本身系统即基于高靠的环境中外，所有设备均采用高可靠性的硬件及芯片来设计，并且系统的核心部件以及相关的所有链路等均可采用热插拔双冗余的设计，如存储子系统的冗余控制器、冗余电源等；链路可采用多路径冗余或者负载均衡等等。

- 可管理性

FC-SAN本身即一个开放式的独立系统，并存储和处理企业核心的数据信息，因此对其有和良好的管理与监控也至关重要。它可以提供各种方式的连接，如WEB、RS-232等；各种管理界面，如字符界面、命令行界面、GUI图形界面等；各种集中或独立的灵活管理方式，如C/S方式的集中管理、直接本地LED或者远程WEB单独监控、整个存储子系统设备的集中管理与配置或单个模块的特定监控等等。

FC SAN存储方式的不足：

FC SAN应用成本较高，需要配套的光纤交换机、每个服务器配光纤HBA卡，因此在做FC SAN规划时要充分考虑成本问题

5.4.5.2 医院存储需求分析

医院对存储系统的应用主要集中医院业务系统，医院业务主要分为医院内部业务和医院外部业务。

医院的内部业务以电子病历为核心，主要包括临床服务、医院管理、平台应用等业务域。医院电子病历信息是一个纵向不断增加的信息集合，随着业务的普及，信息量成指数增加。电子病历信息的高效存储和访问，成了医院提高工作效率的基础和保障。

医院的外部的业务主要集中在和社区卫生服务中心、区域卫生信息平台的协同，主要的业务包括远程医疗系统，双向转诊模式，病人自我服务等。针对公众患者提供各项医疗卫生业务并开展所涉及的信息服务，要求数据存储系统具有多用户并发访问能力和连续性读写能力。

随着医疗行业的信息化建设的推进，业务系统数据越来越多，数据的价值也越来越大，就面临着数据如何管理，尤其如何统一管理的问题。另外，数据安全也非常重要，数据的丢失或系统停机将给医院业务系统产生严重的后果，甚至变得不能接受。

医院信息平台涉及到的业务系统比较多，且在建设初期，每个业务系统都有自己的存储系统，数据比较分散，管理起来较为复杂，且没有统一的备份、容灾系统。急切需要一个统一化的管理平台，整合现有的存储设备到统一存储池，集中管理和存储信息化平台的数据。

“9.11”事件爆发以后，“容灾”这个词汇逐渐成为人们谈论最多的焦点之一。而随后的一系列自然灾害的发生，更推动了 IT 系统容灾的需求。医疗行业也不例外，今天许多医院管理者和就医者都十分关心医院的 IT 系统的高可用性。

医院信息系统是一个数据量大，数据类型复杂和事务并发多的实时系统，由于医院业务的特殊性，任何人为或自然因素所导致的应用或系统中断，都会造成医院巨大的经济和名誉损失及严重的法律后果。所以医院应用对 IT 系统的持续稳定运行提出了非常苛刻的要求。

随着医疗水平的日新月异，先进医疗设备和精确的医疗系统逐步增加，在以后的医院 IT 系统结构中添加不但增加新的成本，而且对结构也是一个冲击。所以，随着 IT 在医疗界标准越来越统一，我们需要一个更加开放的结构，更加富有兼容性的系统，更加安全的数据。

5.4.5.3 存储设计

5.4.5.3.1 概述

医院存储系统设计是结合医院的内部、外部业务总体需求特点来考虑的。内部业务涉及到医院业务水平、医院核心数据、医院未来的发展，要求存储系统不仅要具有较高扩展性、较高的性能、较高的带宽，还要考虑数据的安全性、数据存储的高效性、数据读写的稳定性，这样就需要存储系统具有较高的数据备份恢复能力、较高业务兼容性、较高的稳定性。外部业务主要是医院和外部的交互，主要要考虑到数据的连续性、数据访问的性能，这样就需要存储系统具有持续较大的带宽和较高的性能。

就数据结构层次来说，又分成结构化数据和非结构化数据。结构化数例如 HIS 系统主要业务系统的稳定性要求高，当系统硬件发生问题到业务恢复控制在 5-15 分钟之内，对存储系统稳定性要求较高；非结构化数据例如医疗影像数据由于每天都会有大量数据，并且电子病历系统需要对这部分数据尽显随时调阅，对数据保存周期要求较长，通常要求永久保留。

5.4.5.3.2 设计原则

- 先进性

在存储系统的设计过程中，充分依照国际上的规范、标准，存储及容灾设备采用标准的接口、规范和协议，借鉴国内外主流的网络存储备份体系结构，使用国际上成熟的模式和最新的存储及备份技术，以及业界领先的存储产品，才能使网络存储及容灾系统的建设不断地保持其技术与方案的先进性。

- 数据的安全性和系统的高可靠性

存储系统负责完成对医院业务系统的业务连续性支持，医院应用系统对可靠性有着很高的要求。作为该系统核心的存储平台的高可靠性则更是重中之重。由于医院应用系统的整合，势必会带来数据的整合，因此需要采用集中存储方式实现数据的统一存储，即所有的数据共享均集中存储于统一的 SAN 架构之上。数据存储在同一存储平台之上，存储平台的稳定性直接决定了业务的连续性。存储平台的任何故障会造成巨大的影响。因此存储平台的数据安全性和系统高可靠性尤为重要。为了保证数据安全，除了建立可靠的数据存储备份系统之外，可以采用先进的存储设计方案和先进的软、硬件产品。

- 系统的高性能

存储系统要存储大量的文档库、ODS、数据仓库等数据类型,需要支持更多医院信息系统的在线业务日常正常运行要求。医院通常每天产生的数据量会很大，如何在大量数据量情况下满足医生工作站的并发访问，整个存储系统的性能也是一个非常关键的要求。而且备份系统也要支持不断增加的数据流量和存储容量，以保证各种数据的及时处理和可靠的完成，这要求网络存储系统要具有足够的容量，为了及时、迅速地传送数据，网络存储设备还必须具备高速处理能力，提供

高速数据链路，保证系统高吞吐能力，满足各种医院各种应用系统对数据传输带宽的需求，系统的性能应能很好的适应未来的扩充和扩展的需要。

- 系统的可扩展性/可扩充性

医院业务系统集中数据存储的基本要求，存储系统应能支持巨大的存储容量，可以集中存储不同平台的业务系统数据，从而使医院业务系统实现数据的集中存储和集中管理。

随着时间的推移、技术的发展以及环境的变化，医院业务系统的数据量会飞速增长，许多新业务系统会不断产生，因此对医院建设数据存储和容灾系统的可扩展性有很高要求。需要充分考虑系统存储备份容量空间的预留，同时随着业务的发展，对存储系统的可扩展性要求仍将非常迫切。这主要表现在对存储和备份系统容量的平滑扩充以及对新的主机系统的平滑连接，以尽量减少对已有正常业务的影响。

- 灵活性和系统管理的简单性

由于存储及数据备份系统的数据量非常大，如何有效的管理大量的数据，包括数据备份/恢复，都对存储系统的管理提出了巨大的挑战。系统管理人员需要有高效的方法实现全面的存储系统监控，包括实时数据性能监视、错误监测、错误状态识别等等。另外作为医院数据集中的存储平台，由于前端需要连接的服务器数量很多，如何在多个服务器平台之间对容量进行灵活的划分和调度也是为存储系统的管理提出了巨大的挑战。

- 价格适中、投资合理

医院建立存储及数据备份系统的经济性也是网络建设中的一个重要方面。经济性需从两个方面来考虑，首先是建立数据集中存储、容灾系统过程中的费用，同时还有系统建成后的维护费用和对投资的保护能力。在考虑使存储、容灾系统具有高性能的同时，还必须考虑投资的合理性，不能一味追求不切实际的先进性。在建设的过程中还需要考虑未来的升级能力和提供商的服务水平。

另外，存储及数据备份方案除了要满足当前应用医院业务系统的需要外,还要为未来的的医院业务量发展和数据高速膨胀打下一个良好的基础，必须考虑未来整个系统应用级容灾的现实需求，方案必须可以和已经建设的信息基础架构完美结合，成为统一信息基础平台。

5.4.5.4 数据保护机制

5.4.5.4.1 本地保护

传统磁带备份方式

传统的医院 HIS/PACS 系统数据备份方式通常采用物理磁带库/磁带机与备份软件相结合，通过设定某种备份恢复策略实现数据备份和恢复的自动化。这种方式适合文件以及数据库类型数据备份，例如：PACS/LIS 等业务系统数据备份恢复保障。很难满足目前医院 HIS 系统 RPO/RTO 需求，采用备份方式进行数据保护通常备份周期以 24 小时为单位，而门诊系统对系统宕机到恢复业务时间在分钟级，因此该种方式适用于医院除门诊以外其他系统数据和恢复基本要求。

传统磁带备份系统架构如下：

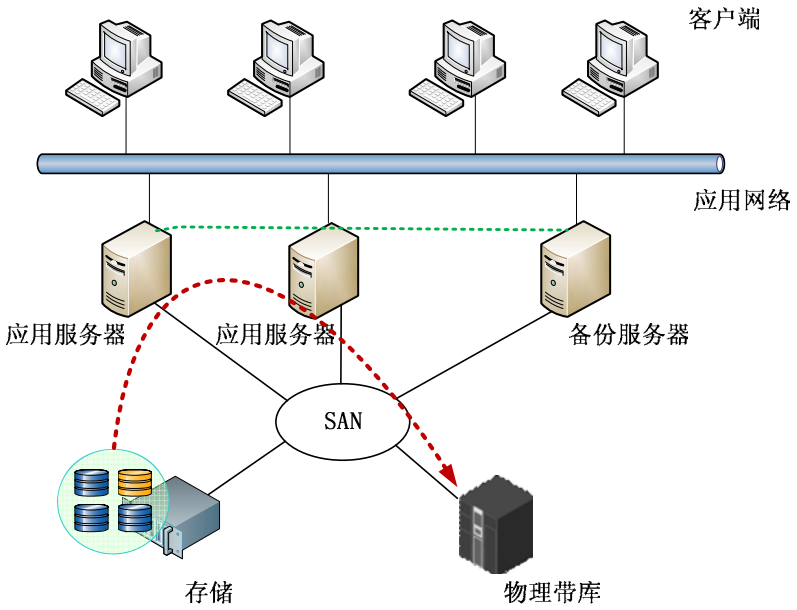

图 5-57 传统磁带备份系统架构图

虚拟磁带库备份方式

虚拟磁带库（Virtual Tape Library，VTL），VTL 采用磁盘作为备份介质，将磁盘仿真为一种或者多种磁带库和磁带。仿真后的磁带/磁带机在备份服务器上显示为真实的物理磁带/磁带机，整个备份和恢复的过程和物理磁带库完全一致。VTL 采用了磁盘备份介质，具备了磁盘备份/恢复的高性能和高可靠性，有效缩短了备份时间，提高了数据的安全性。

虚拟磁带库备份方式采用磁盘技术来模拟磁带备份，实现了磁带技术和磁盘技术的最佳融合。虚拟磁带库方式提升了备份效率，在大型医院数据相对较多的情况下，采用虚拟磁带库技术可以提升备份系统数据备份的效率。

虚拟磁带库备份方式系统架构如下：

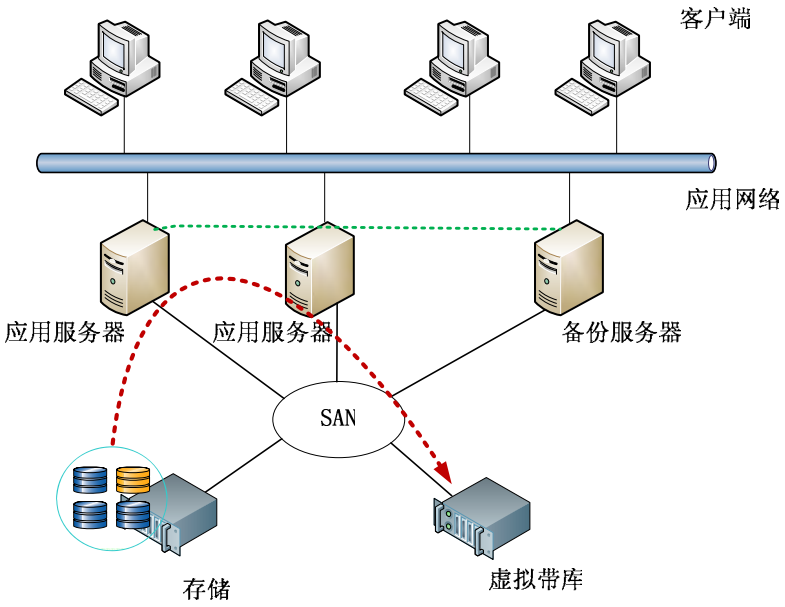

图 5-58 虚拟磁带库备份架构图

存储快照保护方式

存储快照是基于存储的高级软件功能来实现的，它是数据集合的一个完全可用拷贝，该拷贝包括相应数据在某个时间点（拷贝开始的时间点）的映像。

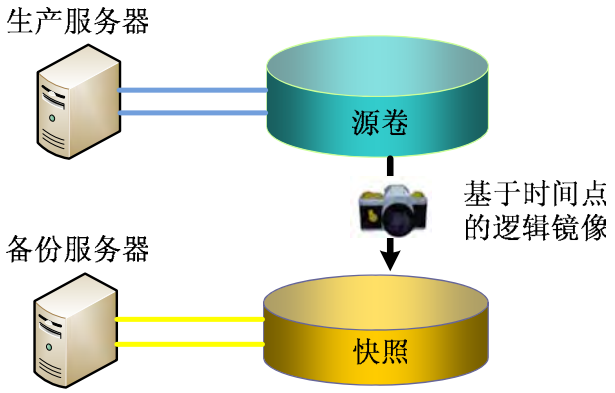

图 5-59 存储快照保护方式

快照的主要功能：能够进行在线 数据备份与 恢复，也可用于实现数据测试、查询等。当存储设备发生应用故障或者文件损坏时可以进行快速的数据恢复，将

数据恢复某个可用的时间点的状态。快照的另一个作用是为存储用户提供了另外一个数据访问通道，当原数据进行在线应用处理时，用户可以访问快照数据，还可以利用快照进行测试等工作。

表 5-18 数据保护比较

比较项	传统磁带备份	VTL 备份	存储快照
备份介质	磁带	磁盘（SAS、SATA）	磁盘（FC、SATA）
备份速度	低	高	与存储性能有关
备份窗口	8-12 小时	低于 8 小时	可实现数据的定期备份
数据恢复速度	极低	高	高
可靠性、部件故障率	磁带机、机械手均为非封闭电控转动、移动机械部件，故障率高	磁盘为封闭精密部件，故障率低；磁盘阵列并有 RAID 保护	磁盘为封闭精密部件，故障率低；磁盘阵列并有 RAID 保护
环境影响	受湿度、粉尘影响大	受湿度、粉尘影响小	受湿度、粉尘影响小
可维护性	低，需要专业维护人员	较低，一般 IT 人员就可维护	高，自动化过程，一般 IT 人员可维护
存储设备部署类型	离线存储设备	近线存储设备	近线存储设备
适用场合	数据需要归档存储	数据更新比较频繁，需要提高备份频率和速度	关键应用的数据，需要定期备份，数据恢复时间要求高

5.4.5.4.2 异地容灾

容灾的定义：在两相隔较远的异地，建立一套或多套功能相同的 IT 系统，互相之间可以进行健康状态监视和功能切换，在主站点发生故障时 IT 系统继续正常对外提供服务。

容灾在具体实现方式上分成两类：数据级容灾和应用级容灾。

数据级容灾

数据级容灾实现方式有如下几种：

- 基于数据库的运程数据复制
- 基于服务器逻辑卷的远程复制
- 基于存储系统的远程数据复制

前 2 种模式在数据复制时会对生产系统服务器产生很大的负载，对生产服务器产生很大影响，一般数据级容灾选用基于存储系统的远程复制。

下面是基于存储系统数据级容灾架构图：

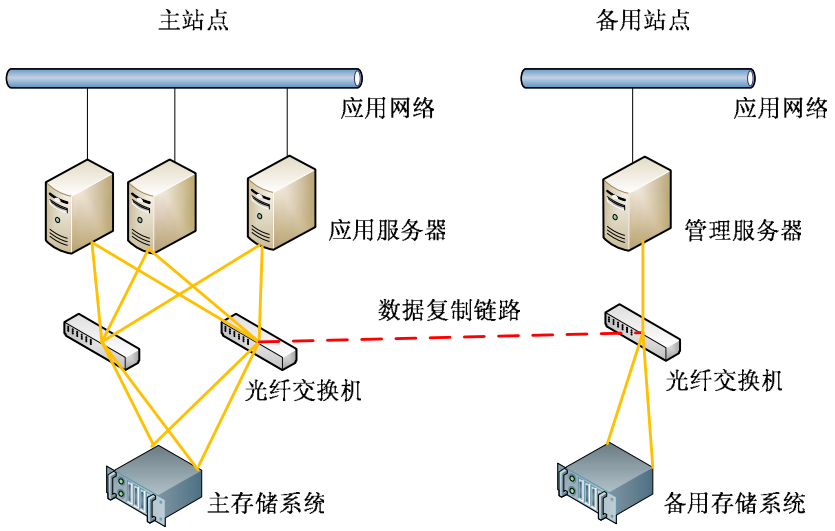

图 5-60 数据级容灾架构图

基于存储系统的数据级容灾有很多方式，常见的有同步或异步数据复制：

同步方式：服务器向存储写数据，数据同时写入灾备中心存储，远程存储系统确认本次 IO 结束，才进行下一次的数据写入。

对数据一致性要求比较高的应用一般采用同步方式。

异步方式：存储系统接受本地服务器的一个写 IO，通知主机 IO 完成，再传送数据到远程磁盘阵列。

对于距离比较远、对性能要求比较高、允许有小部分数据丢失的数据级容灾一般采用异步方式。

应用级容灾

HIS、EMR、LIS 等业务系统支撑医院基本业务开展的关键系统，当在线系统故障时必须有相应应急系统，应用级容灾将存储的软件功能和应用软件结合起来。在存储层通过专有光纤网络或者以太网络实现数据的实时复制，在服务器应用层通过高可用软件实现应用的异地容灾。

下面是应用级容灾的架构图：

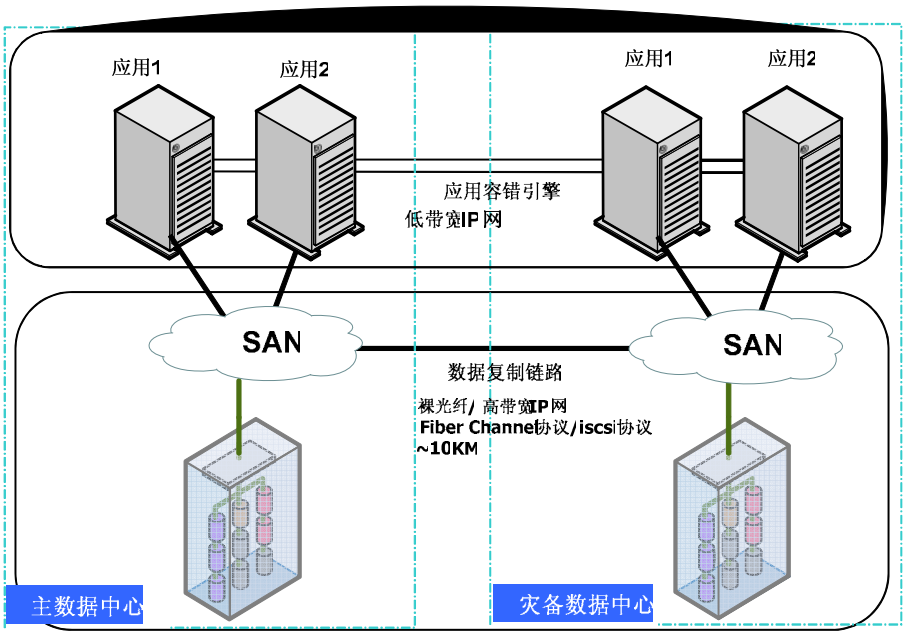

图 5-61 应用级容灾架构图

应用级容灾的特点：

- 通过安装在服务器端的应用高可用软件可实现应用系统业务连续性、服务器的零宕机。
- 通过主存储系统端通过专有链路的数据复制，可以实现两地数据实时同步，释放了前端应用网络的带宽。
- 应用级容灾通过存储的高级软件功能和应用软件的结合，可以为应用提供全方位、多层次的数据保护方案。

5.4.5.5 部署模型

5.4.5.5.1 小型规模的医院存储规划方案

小型规模医院存储部署通常是满足医院信息系统的数据实现基本的数据集中存储和备份需求，服务器端通过与存储网络的连接，把数据存储到磁盘阵列之上；数据安全保障通过备份服务器对业务系统数据按照指定的周期进行数据保护，通常在周一至周五夜间进行增量或者差异数据保护，周 6 至周日进行一周数据的完全数据保护，并把最终备份数据备份到磁带库中。

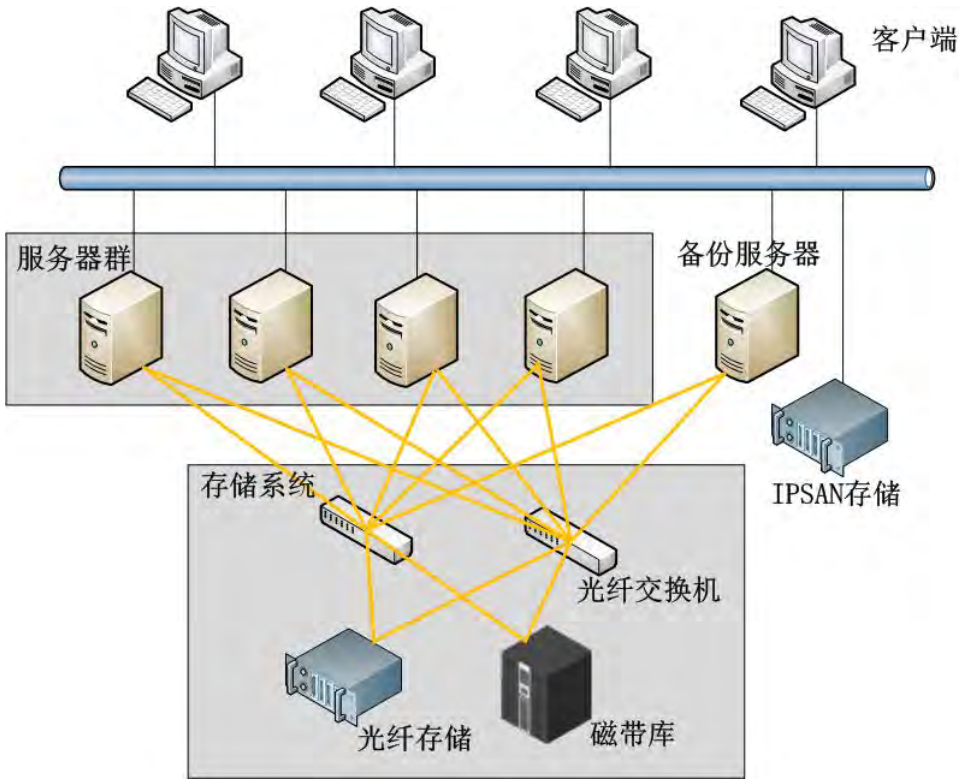

图 5-62 小型规模的医院存储规划方案

方案描述：

- 根据小型医院信息平台应用和数据的安全以及性能的要求，小型规模的医院存储系统采用中端光纤架构存储和低端 IP SAN 存储，结合磁带库（物理或虚拟），构建存储局域网络；
- 前端信息化应用平台服务器通过光纤 SAN 网络将数据存放到光纤存储系统上，实现了平台数据的集中存储；
- IPSAN 存储设备可以通过 NAS 文件共享方式，将一些医院信息平台文档集中存放和共享；
- 存储系统支持分层存储，支持 SSD、FC、SATA 磁盘，满足医院信息平台不同应用性能和容量需求；
- 整个光纤网络所有设备冗余，防止单点故障的发生，保证业务连续性；
- 磁带库采用虚拟磁带库或者物理带库方式，通过 LAN-BASE 或者 LAN-FREE 的模式，对信息化应用平台数据做定期的备份和归档。

5.4.5.5.2 中型规模的医院存储规划方案

中型规模的医院已经实现了最基本的数据集中存储和备份，需要加强业务系统业务连续性方面因素，在本地建设近线存储，通过连续数据保护方式把在线阵列的数据备份到近线阵列之上，当数据发生灾难时，可以通过近线阵列进行恢复或直接把业务切换到近线阵列，通过这种方式提升了存储系统整体的可靠性，中型规模医院已经具备一定规模的医疗影像设备数量，影像数据的长期备份和归档可以采用物理/虚拟带库来实现。

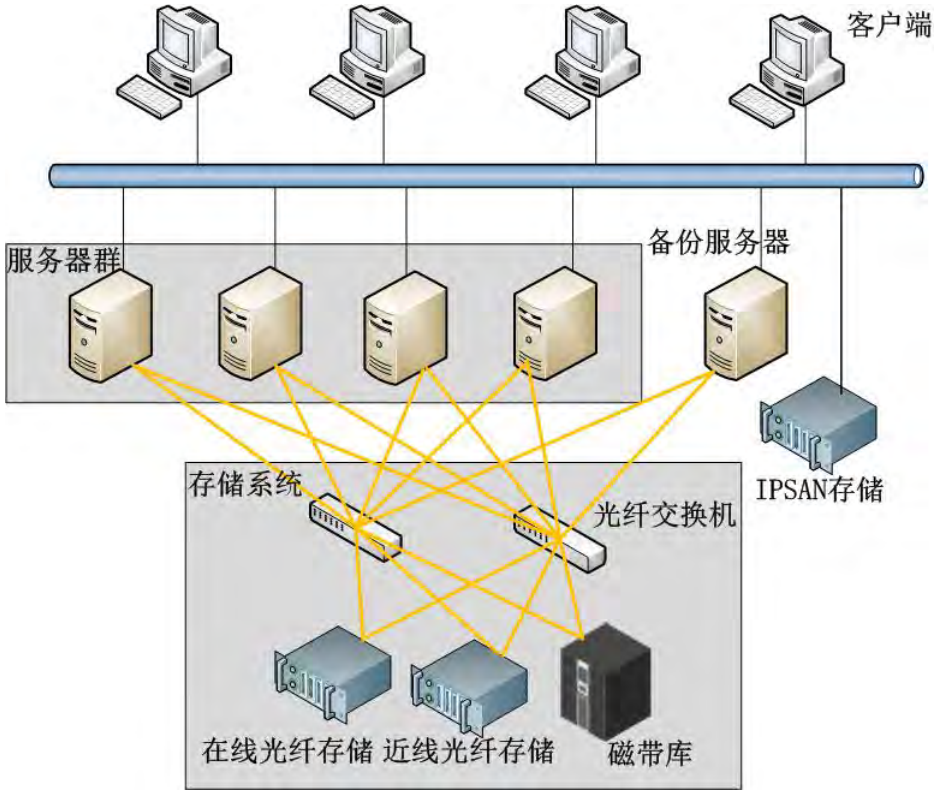

图 5-63 中型规模的医院存储规划方案

方案描述：

- 根据中型规模医院信息平台应用和数据特点，存储系统采用高端全光纤存储和中端 IP SAN 存储，结合磁带库，构建光纤存储局域网络；
- 平台应用服务器通过冗余光纤 SAN 网络连接到存储系统，实现平台数据的集中存储；
- IP SAN 存储设备可以通过 NAS 文件共享方式，将一些医院信息平台文档集中存放和共享；

- 在线存储系统和近线存储系统通过 IP 或 FC 网络做适时同步，将数据适时的备份到近线存储上，当在线存储系统发生故障或者灾难时，将业务切换到近线存储系统，保证业务的连续性；
- 存储系统支持分层存储，支持 SSD、FC、SATA 磁盘，满足不同应用性能和容量需求；
- 整个光纤网络所有设备冗余，防止单点故障的发生，保证业务连续性；
- 磁带库采用虚拟磁带库或者物理带库方式，通过 LAN-BASE 或者 LAN-FREE 的模式，对信息化应用平台数据做定期的备份和归档。

5.4.5.5.3 大型规模的医院存储规划方案

大型医院规模的医院对业务连续性要求更加苛刻，在要求本地数据中型有完善业务连续性保障和数据安全的同时，需要在远程建立灾备中心，通过灾备中心防止一些自然、人为等灾难因素。

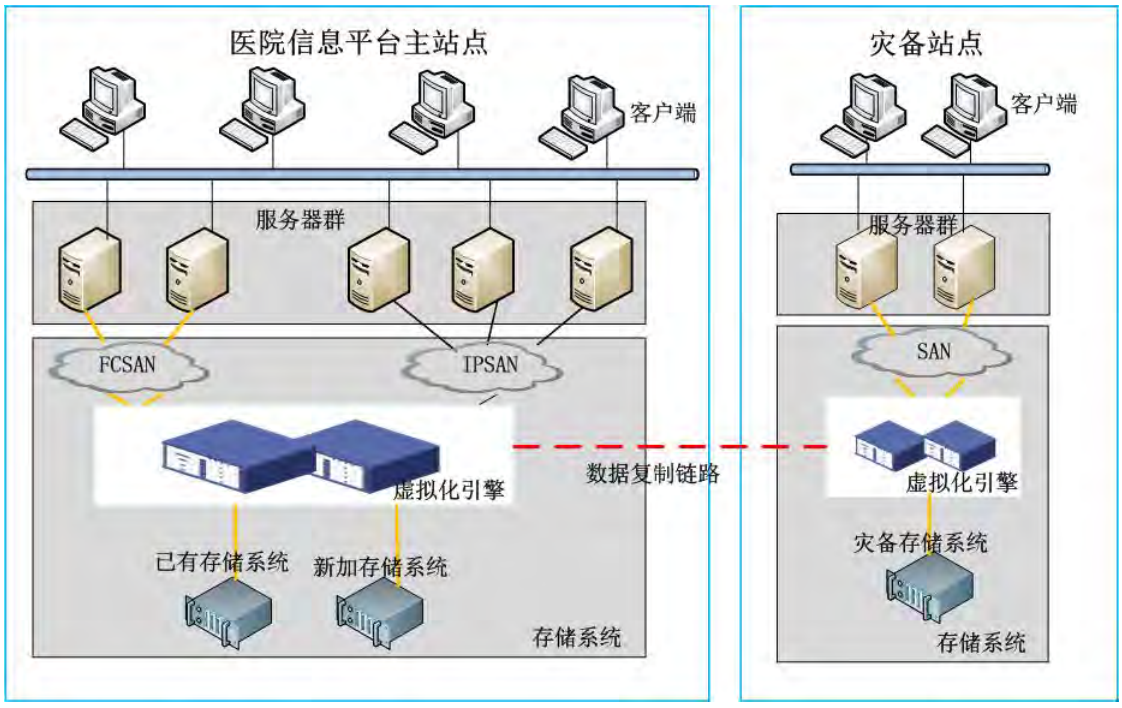

图 5-64 大型规模的医院存储规划方案

方案描述：

- 根据大型规模医院信息平台应用和数据特点，存储系统采用高端虚拟化存储架构，对现有存储设备提供统一化的管理；

- 平台应用服务器通过冗余 FC SAN 网络和 IP 网络连接到存储系统，实现平台数据的集中存储；
- 数据中心存储系统和灾备中心存储系统通过 IP 或 FC 网络做适时同步，将数据适时同步到灾备中心上；
- 应用服务器通过虚拟化存储高级软件，可以实现数据应用级的容灾，当数据中心发生故障或者灾难时，应用业务可以自动切换到容灾中心，保证业务的连续性；
- 存储系统支持分层存储，支持 SSD、FC、SATA 磁盘，满足不同应用性能和容量需求；
- 整个光纤网络所有设备冗余，防止单点故障的发生，保证业务连续性；
- 虚拟化存储的备份引擎，通过 LAN-BASE 或者 LAN-FREE 的模式，对信息化应用平台数据做定期的备份和归档。

5.4.5.6 存储管理

由于医院信息平台设计的应用、设备较多，对存储管理要求比较苛刻，以下是存储信息平台要求：

直观的管理界面：

直观的阵列管理窗口图形化显示：存储系统的逻辑组件（存储器卷和卷组）、物理组件（控制器和驱动器）、拓扑元素（主机组、主机、主机端口）以及卷到 LUN（Logical Unit Number）之间的映射。

配置的灵活性：

所有卷的设置都是单独配置，保证能够满足某个特殊卷准确需要的特性。

在线管理：

存储系统允许增加新的驱动器模块、配置卷、创建卷，而不会打断对现有数据的存取操作；

可以允许使用现有卷组中的空闲容量来对现有卷的容量进行扩展；

可以改变一个卷组的 RAID 级别；

可以允许改变某个指定卷的分段大小；

可以动态碎片整，合并卷组内的空闲容量，给现有的卷和新创建的卷带来了最优化的存取模式；

非中断式的控制器固件升级（不中断数据的存取）；

极高的可用性：

支持自动通道故障切换功能、在线存储器管理功能以及热备磁盘功能。

直观的诊断和恢复：

提供故障诊断帮助，能对存储系统出现的问题进行诊断并确定出恰当的恢复步骤。

5.4.6 网络与通讯基础架构

随着医院信息化进程的深入，共享与交换已经成为医院信息化建设的主题。这意味着，医院信息平台的运行将越来越依赖基础网络的建设。网络上承载的流量从最初的单一流量，逐渐过渡到非常复杂的流量，各种涉及公民隐私、医院关键数据的信息在网络上进行交互和传递，一旦发生故障，将对医院造成巨大的经济、信誉以及名誉损失，甚至可能会导致医疗事故及医患纠纷的产生。医院的信息化对网络的可靠性也提出了新的要求，在医院平台的建设过程中，需考虑网络架构的冗余性设计。近年来，新的医院业务系统不断上线，医学影像系统不断普及，医院网络流量呈加速递增趋势，这对网络的性能也提出了更高的要求。个人电脑的普及，以及医院网络上涉及个人及医院秘密的信息越来越多，网络信息安全问题也成为了在建设医院信息平台过程中非常重要的一环，需要特别关注。随着新应用（如无线查房、无线巡诊、无线监护等）的发展以及以 802.11n 为代表的新一代无线网络标准的产生，使得无线网络的建设成为医院信息化建设的一个重要的方面，在构建医院信息平台的时候应充分考虑到网络的无线扩展性。

本章节主要从医院的信息网络应用需求入手，分析医院的各类业务对基础承载网络提出的要求，在此基础之上，分析医院信息平台的数据流走向以及对基础网络的压力，综合得出在医院信息平台建设过程中，需要怎样的网络来进行承载。在理论分析的基础上，介绍医院信息平台建设的两种典型的网络架构——内外网融合的网络架构以及内外网分离的网络架构，在这两种架构之下分别分析了三层和二层网络子架构，并对各自的特点进行了分析。对于新业务需求驱动的无线网络，在本章节中也有相关的内容，通过对无线新应用的分析介绍了两种无线网络的部署方式——融合无线网络部署以及独立无线网络部署，以及在进行无线部署

过程中对一些新技术及新理念的采用。在本章的结尾，主要介绍在各种网络架构和规模下如何进行网络实现及设备选型，并对基本的网络管理和 IP 地址规划作了简要的介绍。

5.4.6.1 医院信息网络应用需求分析

5.4.6.1.1 医院业务应用分析

✧ **临床业务应用分析**

医院临床业务系统是以病人为核心，围绕医疗救治过程展开的系统，覆盖医院临床业务的各个环节。各子系统相互配合，共同完成医院临床业务需求。

医院临床业务具有如下特点：

- 数据流向的单一性：医院信息系统主要部署模式为 C/S 或 B/S 架构，医院各前置终端均需要通过对医院信息平台数据中心服务器的访问来实现相关功能。如:包括 HIS、LIS、PACS 等。
- 网络占用高。医院信息平台的建设过程中，整合资源共享数据是建设的主题，网络上交互的流量越来越复杂，部分系统具有数据量大，并发访问带宽要求高等。
- 业务数据实时交互，可靠传输。医院中部分业务系统涉及医院关键业务，数据流具有实时交互，要求进行可靠传输。如门诊区相关系统，医保结算相关系统等。
- 网络出口高带宽：医学文献检索系统的使用，使得医院可以利用互联网的海量医学资源，这一需求对医院互联网出口也提出了高带宽的要求。
- 无线传输数据量大，并发占用带宽高：无线查房系统的使用，主要为通过无线网络向手持 PDA 或平板电脑，传输文本信息、表单或 PACS 图像，这些应用对无线网络带宽也提出了更高的要求。
- 数据 7*24 不间断传输：ICU 监护仪信息系统对整网的稳定性、连续性、容灾性都提出了高要求，因此在网络架构设计过程中应充分考虑冗余架构。

✧ **医院管理业务应用分析**

医院管理业务是指以医院管理流程为中心，围绕医院管理中的各个环节展开

的业务系统。

医院管理业务具有如下特点

- 数据流单一，数据压力集中：数据流流向较为单一，主要为医院管理业务终端到数据中心相关服务器，各区域对服务器的访问数据在服务器区聚集，对网络带宽要求较高。
- 数据流量不规则，突发性强：该区域大部分数据是以文本类数据和表单数据为主，具有数据流量小，突发性强等特点。
- 可靠交付：电子邮件系统，由于其业务自身特点，对网络的时延特性要求较低但对可靠性要求较高。
- 对时延非常敏感：电子传真系统，及时通信系统，具有数据量不大，但突发性强，且对时延非常敏感的特点。
- 高综合传输质量：视频会议系统，由于其传输的是多媒体视频流，对网络带宽、时延、抖动都提出了新的需求。
- 传输信息敏感：管理业务数据包含医院很多关键信息，应注意信息安全的保护。

✧ **外部共享与交换业务应用分析**

外部共享与交换业务是以对外共享和域间交换为核心的业务，整个业务围绕交互过程展开。

平台应用具有如下特点

- 数据的敏感性与重要性：需要与多个机构进行专网互联，同时需要提供对外服务的互联网接口，需更加重视网络安全。
- 数据要求网络高可靠：该区域的交换数据数据量小，但要求网络可靠性高。
- 数据对网络服务质量的要求：部分业务存在多媒体数据传输，对网络带宽、时延等有一定要求。

5.4.6.1.2 医院信息网络数据流分析

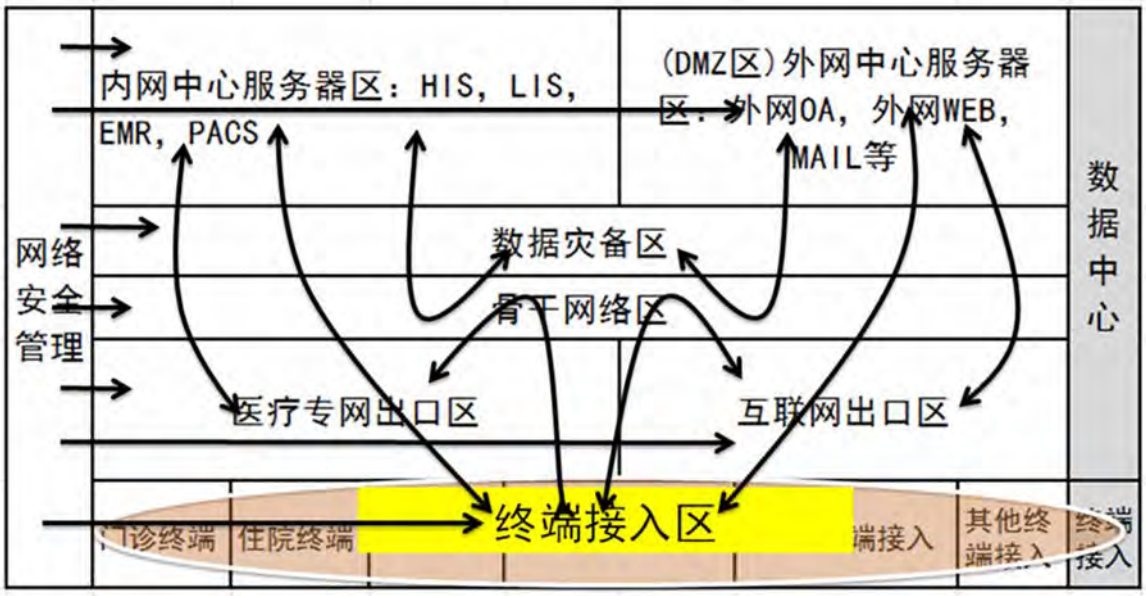

图 5-65 整体网络架构设计-医院信息平台网络数据流分析模型

通过上述分析，医院信息平台数据流具有以下特点：

- 各区域数据交互均需要进过骨干区域
- 主要数据流交互为接入区到服务器，符合 C/S 架构特点
- 数据中心区域中，大流量主要集中在业务服务器区以及数据灾备区
- 内网服务器会与医疗专网出口进行信息共享和交互
- 外网服务器会通过互联网出口区对外提供服务
- 网络安全管理区需管理各个区域流量

5.4.6.1.3 应用需求总结

✧ **内网业务需求小结**

内网主要为围绕医院医疗、救治等主营业务展开的网络。内网上承载着医院核心数据。需求小结如下：

- 内网服务器区会要承载内网所有接入终端的访问流量，有高带宽要求
- 数据灾备区需要进行大量备份数据的传输，对带宽要求较高
- 内网医学影像接入设备，化验系统接入设备由于其传输信息量较大，有高带宽要求

- 内网门急诊区域，对网络的冗余及实时性要求较高。
- 内网安全管理区需要监控网络所有区域，对网络带宽要求较高。
- 内网由于业务的关键性，对网络设备自身的稳定性及冗余性，以及网络架构的冗余性提出了很高要求，需保证 7*24*365 不间断运行。

✧ **外网业务需求小结**

- 门户网站系统，是对内对外的门户窗口，会聚集来自互联网以及医院局域网的访问流量，有高带宽需求。
- 邮件系统，电子传真系统，对网络可靠性有较高要求。
- 核心层设备需要承担整个外网的压力，需具备冗余性和抗攻击能力。
- 由于外网提供了互联网出口，需要更加注意保护医院信息安全。

✧ **网络出口业务需求小结**

- 广域网链路多样，出口设备需提供丰富的接口支持
- 广域网链路不稳定，可考虑多出口冗余备份
- 出口处是域内域间的分割点也是局域网广域网的分割点，有网络安全需求
- 网络出口易受攻击，设备需具备一定的抗攻击能力
- 移动办公对 VPN 接入提出了需求
- 规范员工上网行为的需求
- 对网络流量进行精细化管理的需求，防止带宽被垃圾流量占用，从而使关键业务得不到保障。

5.4.6.2 网络基础设施平台架构设计

在各种医疗设备 IP 化的今天，网络作为承载医院内外网业务的基础平台，其建设的质量将对医院信息化建设后续产生深远的影响。而网络在设计之初架构是否合理，是否具备高可用性，高扩展性，高稳定性以及高安全性，都将是网络基础设计平台设计的重点。医院的网络基础架构发展至今，主要分为三种架构，分别是内外网融合的网络架构、内外网分离的网络架构、以及最近几年刚刚兴起的基于业务的无线网络平台架构，这是和医疗信息化的发展阶段分不开的。所谓内外网融合的物理架构，就是医院的内网业务以及办公业务都在一张基础网络上运行，在这一网络架构之上，无论是数据的类型、重要程度，还是对网络的要求，

以及数据流方向都不尽相同，使得网络数据复杂度提高而可控性下降。但是随着一些网络新技术的应用，使得内外网融合的物理架构也具备了内外网分离的特点，典型应用是通过 MPLS（Multi-Protocol Label Switching） VPN 技术以及安全控制域的划分，在逻辑上将一张物理网络虚拟化成几张逻辑网络，逻辑网络之间通过 VPN 技术进行隔离，逻辑网络内通过安全域控制不同级别用户的访问权限，在保证网络安全，稳定，高效，可控的同时，最大限度的保护投资，降低医院信息化建设的门槛。内外网分离的网络架构，就是将医院的内网业务，如 HIS，LIS,PACS 等业务放在一张单独建立的网络上来运行，而办公业务，如 OA，邮件，WEB 等放在另一张网络上来运行，两网物理隔离，最大限度的保障内网业务及数据的安全。而近几年随着无线技术的发展，无线网络传输速率以及稳定性和可靠性都有了很大的提高，以 802.11n 为主的新一代无线网络标准以其高速，安全，使得无线网络作为全面移动医疗的基础支撑体系成为可能，在新一轮的医疗信息化背景下，更是被提高到了一个新的高度，基于业务的无线网络平台设计，既要保证与现有有线网络和现有业务的充分融合，又要保证其架构的独立性，目前主要包含两种无线网络架构，一种是基于现有有线网络的架构，这种架构对医院有线网络建设质量以及医疗信息化都有较高要求；另一种架构是独立的无线网络架构，新建无线网络与有线网络之间，通过核心交换机实现互联互通。

在三种类型的网络架构背景下，通过有线网络与无线网络的协调配合，为医院的全面信息化打下了良好的基础，使得诸如无线查房，无线会诊，RFID 病人药品识别，关键物品定位，无线医学影像传输，病人电子病历调阅等新的应用成为可能。

5.4.6.2.1 设计原则

- 标准化原则

标准化是医院信息平台网络建设的基本保障，是实现信息平台域内以及域间规范化互联互通的基础，应用服务系统建设必须在业务流程化、安全体系和安全技术、信息表示和信息交换、网络协议、软件结构、软件平台等标准方面遵循统一的技术标准，才能达到各医院域内和域间“互连、互通、互操作”要求，实现“信息交换、资源共享”。

■ 可靠性原则

医院信息平台网络建设时必须重点考虑业务系统能否有效的避免单点故障，在网络基础架构设计时，应充分考虑设备自身的稳定性，设备级的冗余备份以及链路级的冗余备份，保障在任何环境下，不因单设备或链路问题，导致服务中断，实现业务系统的 7×24 小时不间断工作。

■ 模块化设计原则

医院信息平台网络建设时采用模块化、分区化、分层次设计，将整体网络基础设施平台划分为若干个功能区块，便于安全域的隔离控制和后续扩展时对其他功能区的影响。

■ 安全保密性原则

医院信息平台承载着医院的医疗数据信息，病人的电子病历，医院的办公和财务数据等，涉居民的个人隐私、医疗保密数据以及医院财务信息等关键数据。因此在网络架构设计时需充分保障数据在提交、传输、存储、调用时的数据安全。

■ 高性能原则

随着医院信息平台业务的不断完善、增加。医疗数据传输与调用、远程协同医疗、PACS 影像等系统和资源将对网络性能提出更高的要求。因此医院信息平台整体网络架架构应具备高速转发性能，以保证各项业务的顺利开展。

■ 可管理性原则

医院信息平台的网络设备必须支持标准的 SNMP 协议，使其易于管理、维护，操作简单，便于配置，在安全性、数据流量、性能等方面能得到很好的监视和控制，可以进行远程管理和故障诊断。

■ 可扩展性原则

医院信息平台的网络设备不但满足当前需要，将来业务系统的业务量增加、以及更多的业务系统融入信息平台时能够提供有利保障。对于现有架构及设备应该尽可能通过扩展已有的功能或模块来实现，而无需更换已有资源，保护投资。

■ 技术成熟性原则

在网络建设方面，充分考虑采用国内通用的，成熟的软硬件产品，保证信息平台业务运行的高效稳定。

5.4.6.2.2 医院网络分层、功能分区设计

医院网络主要分为两层机构，包括数据中心层和终端接入层。而数据中心层主要包括骨干网络区，内网中心服务器区，外网中心服务器区，数据灾备区，安全管理区，医疗专网出口区，互联网出口区等区域，而终端接入区则包含门诊终端接入区，住院终端接入区，医技设备接入区，无线终端接入区，行政终端接入区等区域。

■ 网络分层概述

基于电子病历的医院信息平台业务模式具有扁平化特点，所有接入区终端点直接与数据中心的的业务系统进行交互。进行网络架构设计时应充分考虑此特点，设计信息平台主要由两大部分组成，医院数据中心层和终端接入层。终端接入层主要负责将门诊、住院、医技、行政终端等接入网络，实现业务数据的提交和电子病历资源以及医疗信息的调用，并且为网上办公提供网络基础；医院数据中心主要负责各业务系统的运行、管理，EMR 信息的存储、调用，办公系统的业务支撑，医疗影像信息的存储，以及信息平台的外联。

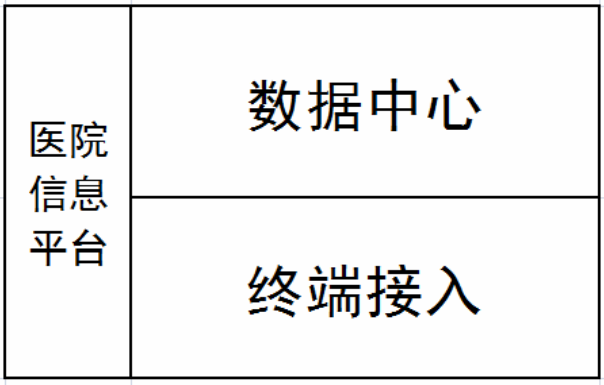

图 5-66 整体网络架构设计-网络架构分层模型

进行整体网络架构设计时充分考虑此特点，将网络架构分为二层：终端接入、数据中心。同时根据各自其特点进行进一步细化。

■ 网络分区概述

在阐述网络分区之前，先来明晰两个概念，本文中在介绍网络分区过程中所提到的内网外网的概念为逻辑上的划分，两种实际的物理架构中，逻辑上均包含内网和外网两部分。划分主要根据业务系统的对内对外服务属性，医疗核心业务

相关度等特性来进行，在实际实施过程中，需根据医院自身的实际情况，确定自身是否需要构建物理上内外网分离的网络。

网络基础设施平台根据其功能特点逻辑上划分 13 大模块：内网中心服务器区、外网中心服务器区（DMZ 区）、数据灾备区、骨干网络区、医疗专网出口区、互联网出口区、网络安全管理区、门诊终端接入区、住院终端接入区、医技终端接入区、无线终端接入区、行政终端接入区、其他终端接入区等。数据中心的各区域模块间通过独立的防火墙设备或者防火墙板卡进行安全隔离。

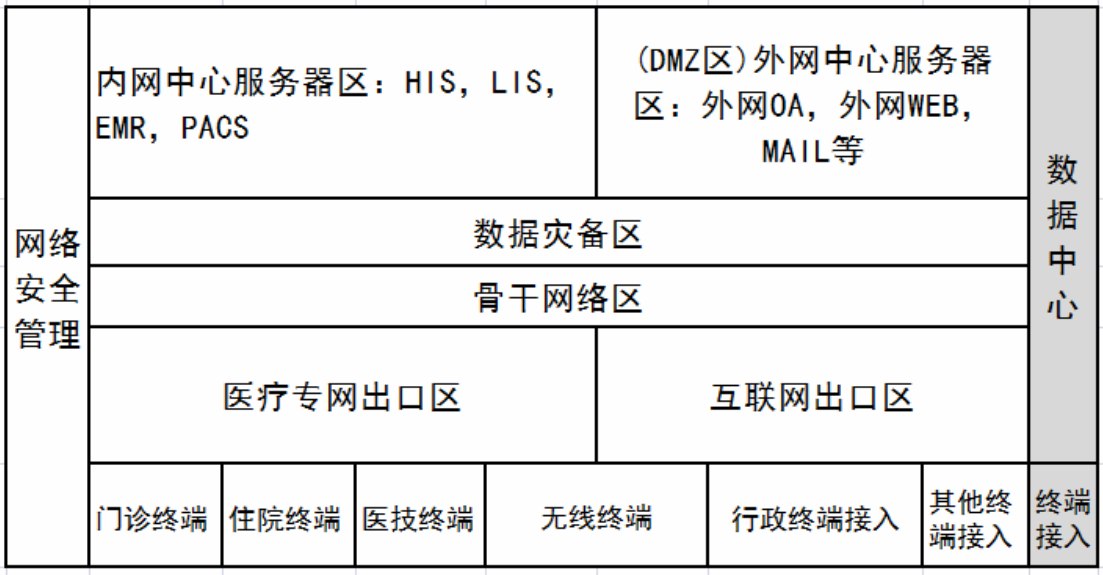

图 5-67 整体网络架构设计-网络架构分区模型

医院信息平台建议实际包含或功能上包含以下功能模块，方便针对不同的区域运用不同的控制策略：

- ✧ 内网中心服务器区
- ✧ 外网中心服务器区(DMZ)
- ✧ 数据灾备区
- ✧ 骨干网络区
- ✧ 医疗专网出口区
- ✧ 互联网出口区
- ✧ 网络安全管理区
- ✧ 门诊终端接入区
- ✧ 住院终端接入区

✧ 医技终端接入区

✧ 无线终端接入区

✧ 行政终端接入区

✧ 其他终端接入区

各区域的界限以及作用范围如下：

✧ **内网中心服务器区**

医院信息平台上内网所有的应用服务器、数据库服务器、中间件服务器、数据存储设备等一切内网业务系统相关设备的集中连接区域，是整个医院业务的核心。例如，内网中心服务器区域是 HIS 系统、LIS 系统，PACS 系统，EMR 系统，等所在的区域。

✧ **外网中心服务器区（DMZ 区）**

医院信息平台上外网所有的应用服务器、数据库服务器、中间件服务器、数据存储设备等一切外网业务系统相关设备的集中连接区域。例如，外网中心服务器区是医院外网 OA 服务器，外网 WEB 服务器，MAIL 服务器等所在的区域。

✧ **数据灾备区**

该区域是 HIS、电子病历、医学影像系统，等数据中心子系统的灾备区域，一般该区域为院内灾备区域，通过高速链路直接与核心交换机相连，实现业务系统与灾备区域数据实时的同步。

✧ **骨干网络区**

主要负责医院信息平台上数据中心区域内各服务器区之间的互联，以及数据中心区与终端接入区之间的互联或汇聚互联，该区域的主要功能为实现局域网内数据的高速处理和转发。远程链路汇聚主要采用高性能的路由器、VPN 网关服务器。HIS 系统、LIS 系统、EMR 系统、PACS 系统、网络安全管理系统等模块主要通过万兆平台及其以上的高性能三层交换机进行连接。

✧ **医疗专网出口区**

该区域主要功能为为医疗信息平台提供医疗专网的接入服务，医疗专网包含的主要内容包括：医疗行业上级单位，疾控直报网络，公共卫生突发预警系统，公安局，区域医疗卫生信息平台等。医疗专网出口为医院信息平台提供了与其他医疗信息平台及上级主管机构信息交互的安全高效的通道，是连接医院信息孤

岛，整合医疗信息网络的重要部分。这部分出口主要通过专线连接，最好能够提供冗余的出口线路。

✧ **互联网出口区**

该区域是为下载医学相关资料，获取互联网海量信息而提供的安全的 Internet 出口，也是医院门户网站，对外服务系统对公众社会提供服务的出口区域，该区域由于与广域网链路相连，外部网络环境较为复杂，存在较大的风险隐患，所以是安全防护的重点区域。该区域主要由高性能路由器、防毒墙、防火墙、流控设备、VPN 设备、上网行为管理设备，网站保护系统等组成。

✧ **网络安全管理区**

医院信息平台数据中心内保障整体信息平台安全、稳定运行的安全管理运维系统的连接区域。如证书服务器、身份认证、漏洞扫描、入侵检测、网络管理等。

✧ **门诊终端接入区**

该区域主要是将医院门诊部医疗相关的核心业务终端接入医院基础网络，主要包括门诊部门的医生工作站，护士工作站，计价终端系统等医疗相关终端系统接入网络，提供门诊部医疗终端与数据中心之间的互联互通性，使其能够快速，稳定与数据中心进行信息交互。

✧ **住院终端接入区**

该区域主要是将医院住院部医疗相关的核心业务终端接入医院基础网络，主要包括住院部门的医生工作站，护士工作站，住院部计价终端系统等医疗相关终端系统接入网络，提供住院部医疗终端与数据中心之间的互联互通性，使其能够快速，稳定与数据中心进行信息交互。

✧ **医技终端接入区**

该区域主要是将医院医技终端接入医院基础网络，主要包括医学影像系统，医疗化验系统，医疗监护系统等。由于医疗检测相关信息的私密性以及重要性，并且部分医技子系统将产生大流量的数据文件，因此本区域需要保证医技终端与数据中心相关服务器之间的高速数据交互。

✧ **无线终端接入区**

该区域主要是将无线查房系统，医疗手持终端，无线监护系统等依赖无线网络的系统通过高速可靠的无线接入点，连入医院的基础网络，保证其连接的稳定

性以及与数据中心信息交互的高速可靠性，为无线医疗，无线查房，无线监护提供基础支撑环境。

✧ **行政终端接入区**

将医院的非医疗事务类行政终端接入网络的区域，该区域包含丰富的办公应用，比如 OA、邮件、局域网及时通信等。该区域需要与医疗终端接入区域进行物理隔离或是逻辑隔离，以确保内网数据安全。

✧ **其他终端接入区**

该区域主要是将，除上述终端以外的一些其他医生所用终端接入网络的区域，这部分终端同时有办公和访问互联网的需求。如互联网医学资料查询需求等。

内外网融合与内外网分离的网络架构，都应该包含上述功能区域。只是在定位上，内外网融合的网络架构，将所有功能区域都放到一张网络上，通过二层隔离，三层隔离，安全域划分，MPLS VPN 技术等来逻辑隔离网络，保证网络安全。而内外网分离的物理架构，则是将内网中心服务器区，安全网络管理区，数据灾备区，外联接口区，门诊终端接入区，住院终端接入区，医技终端接入区放在了内网，而将互联网出口区，外网中心服务器区，行政终端区和其他终端区放在了外网，内外网之间物理隔离。两张网络拥有各自的核心层设备，无共用设备和线路，互不干扰。

5.4.6.2.3 内外融合的网络架构设计

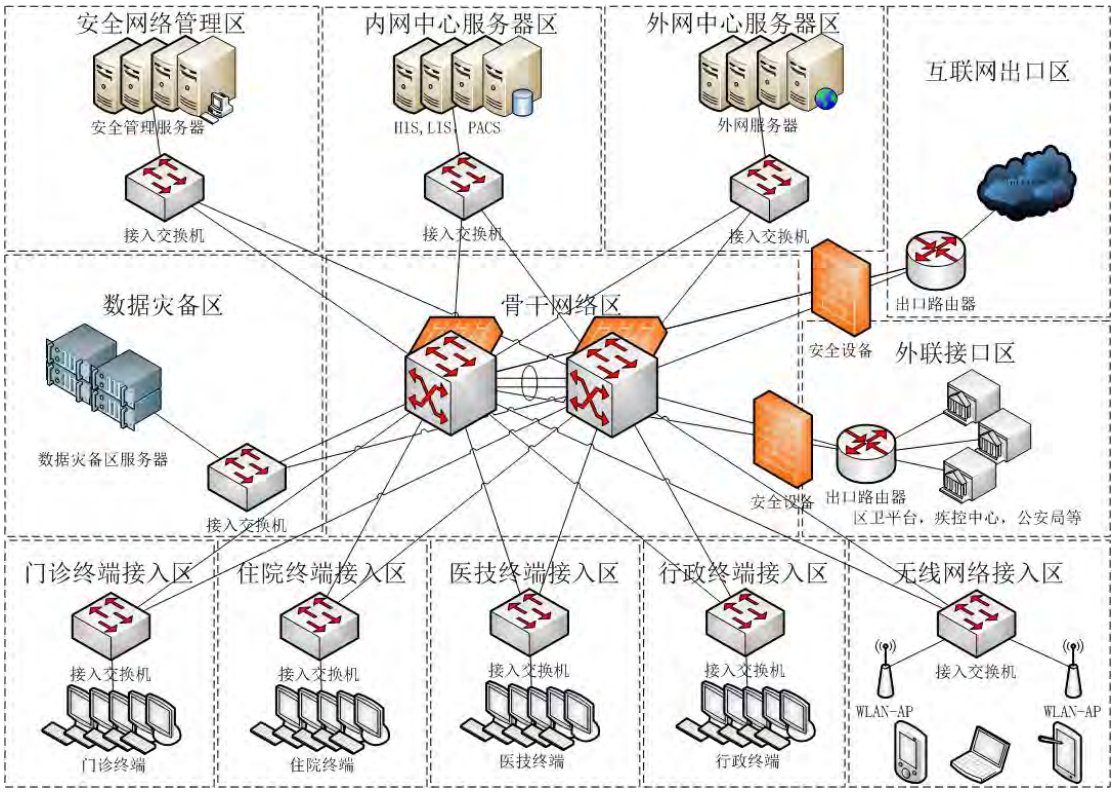

图 5-68 内外网融合的二层网络架构设计

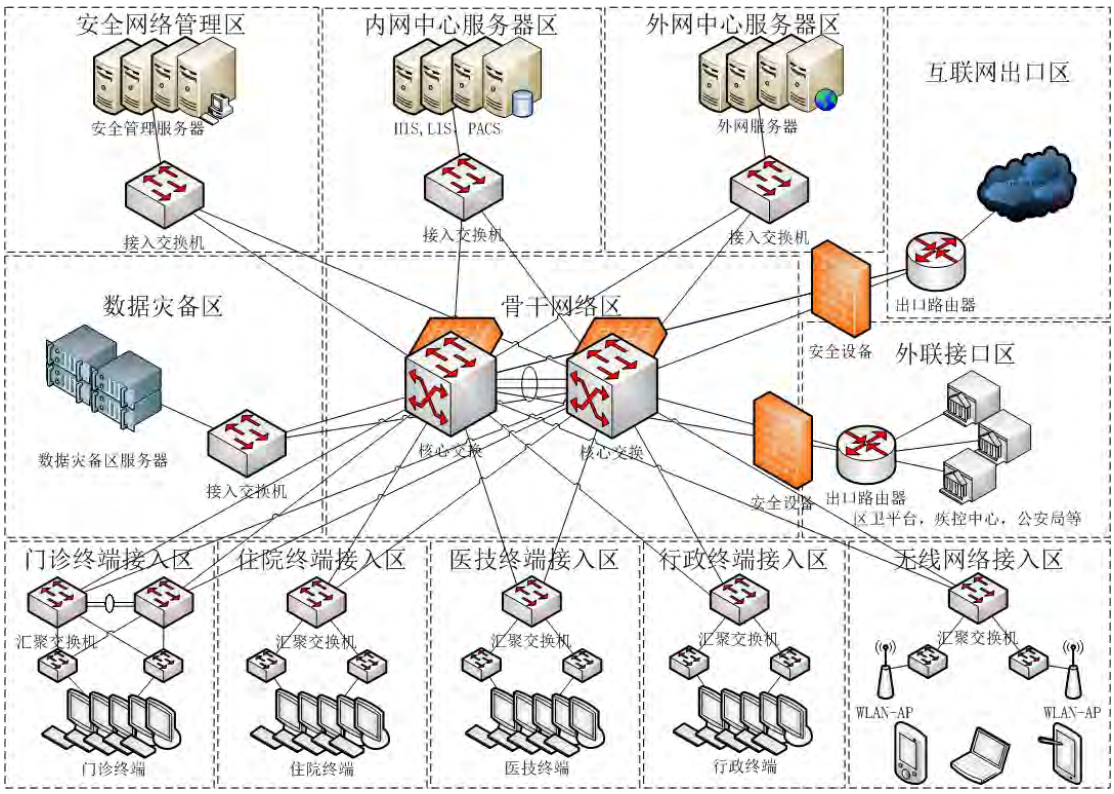

图 5-69 内外网融合的三层网络架构设计

内外网融合的架构设计，就是指医院将医疗内网与办公外网通过一张网络进行互联，逻辑上进行隔离，但物理上联通，通过防火墙，三层设备访问控制列表，二层设备 VLAN 划分，来达到两网逻辑隔离，网络服务互不影响的目的。他的优点是，可以保护投资，并且可以根据需要让某部分终端可以同时访问两个区域；缺点是，两网仅逻辑隔离，外网对设备的攻击可能引起内外网络全面瘫痪。但随着技术的发展，出现了一些新的技术，例如 MPLS VPN 等，可以使得两网虽在一张网上，但运行于各自不同的逻辑通道中，彼此之间互不可见；同时可以通过安全控制域的划分，让主机在接入时动态选择要进入的安全域，保证域内访问安全；就设备而言，通过设备本身的一些抗攻击机制，如中央处理器保护机制，网络基础设计保护机制来达到合理分配交换机硬件资源，满足不同场合应用的目的。

内外网融合架构下区域划分：

- ✧ 内网核心区
- ✧ 内网中心服务器区
- ✧ 安全网络管理区
- ✧ 数据灾备区
- ✧ 外联接口区
- ✧ 外网核心区
- ✧ 互联网出口区
- ✧ 外网中心服务器区
- ✧ 门诊终端接入区
- ✧ 住院终端接入区
- ✧ 医技终端接入区
- ✧ 行政终端接入区
- ✧ 其他终端接入区

在内外网融合的架构中，又包含两种子架构，分别是内外网融合二层网络架构和内外网融合三层网络架构。这两种架构有其各自的区别及特点。

二层网络架构，即全网接入层直接连接到核心或经过一个二层设备中转连接至核心。其特点是：全网拓扑简单，所有终端的网管位于核心交换机上，核心交

换机通过 MSTP（Multi-Service Transfer Platform）+VRRP（Virtual Router Redundancy Protocol）、环网技术或者硬件虚拟化技术进行部署，增加冗余性和鲁棒性，但容易造成核心交换机压力较大，易受到到来自各个区域终端的攻击，导致网络动荡，网络稳定性下降。

三层网络架构，即全网严格分为核心、汇聚、接入三层，接入层主要负责接入控制、VLAN 划分以及二层网络的隔离与互通等功能；汇聚层设备作为各汇聚区域的网关，进行三层网络访问控制，减轻核心交换压力，分割网络动荡区域，使得局部的问题不影响全局，汇聚层之上通过三层接口与核心交换机进行互联，运行动态或静态路由协议，提高网络自愈能力；核心层交换机主要负责高速的三层转发，由于已在汇聚层上进行控制域划分，此时核心层启用的策略更少，性能更高，风险降低。两种架构可以针对不同区域共同使用，形成二三层混合架构。例如将医技终端接入区与核心共同组成二层架构，而行政接入区则通过核心-汇聚-接入形成三成架构，将其网关下移至汇聚交换机，降低该区域对骨干网络的影响。

网络中，各层网络架构设计特点如下：

✧ **接入层设计**

接入层是医院信息平台上所有设备的边缘接入网络，是将终端接入网络的边缘，也是对终端用户进行访问控制和隔离的边缘。在网络的控制上，接入层扮演着越来越重要的角色，是网络安全边缘前移和全局网络安全的基础。

接入层网络设备主要由二层以太网交换机和无线接入点等设备组成，其中二层以太网交换机主要是为有线设备提供网络控制和接入，无线接入点则为无线终端提供无线网络接入，无线接入点可以通过电源供电也可以通过 POE（Power Over Ethernet）进行以太网供电，以太网供电时需要支持连接无线接入点的交换机支持作为 POE 供电设备，或是提供 POE 适配器。

作为医院信息平台的安全接入设备，接入层交换机应选用智能网管型交换机，具备 VLAN 划分，端口隔离，安全地址绑定，抗攻击，QoS，防雷击等功能，支持标准的 802.1x 访问控制，支持标准的 SNMP 简单网络管理协议，支持 DHCP-Snooping 等功能，支持标准的 RSTP（Rapid Spaning Tree Protocol），MSTP（Multi-Service Transfer Platform）生成树协议。

接入层的设计需要充分考虑设备的稳定性、安全性、冗余性和高性能，上联至数据中心的链路尽量使用双链路上联，通过生成树协议生成无环拓扑，避免广播风暴，保证终端设备稳定，安全，高速的接入医院信息网络平台。

接入层功能点：

- ◆ 自身管理地址，管理口令，远程登录，受信任管理列表的，SNMP 控制字的设置
- ◆ VLAN 的划分与修剪
- ◆ 生成树协议（MSTP、RSTP）
- ◆ 二层网络访问控制策略设置
- ◆ 接口下安全地址的生成
- ◆ 802.1x 认证功能的开启以及与认证服务器的联动

✧ **汇聚层设计**

汇聚层是连接接入层与核心层之间的网络层，为接入层提供数据的汇聚\传输\管理\分发处理，集中接入层流量，再转发至核心层的功能，是局域网中隔离动荡的控制点，也是区域网络流量上收的关键点。汇聚层为接入层提供基于策略的连接,如地址合并，协议过滤,路由服务,认证管理等。通过网段划分(如 VLAN)与网络隔离可以防止某些网段的问题蔓延和影响到核心层。汇聚层同时也可以提供接入层虚拟网之间的互连，控制和限制接入层对核心层的访问，保证核心层的安全和稳定。汇聚层设计为连接本地的逻辑中心，仍需要较高的性能和比较丰富的功能。

汇聚层设备一般采用可管理的三层交换机或堆叠式交换机以达到带宽和传输性能的要求。其设备性能较好，但价格高于接入层设备，而且对环境的要求也较高，对电磁辐射、温度、湿度和空气洁净度等都有一定的要求。汇聚层设备之间以及汇聚层设备与核心层设备之间多采用光纤互联,以提高系统的传输性能和吞吐量。

用户访问控制一般会安排在接入层，但也可以安排在汇聚层进行。在汇聚层实现安全控制和身份认证时，采用的是集中式的管理模式。当网络规模较大时，可以设计综合安全管理策略，例如在接入层实现身份认证和 MAC 地址绑定，在汇聚层实现流量控制和访问权限约束。

汇聚层功能点：

- 自身管理地址，管理口令，远程登录，受信任管理列表的，SNMP 控制字的设置
- VLAN
- 生成树协议（MSTP、RSTP）
- VRRP
- 三层网络访问控制列表
- 静态或动态路由协议
- 路由汇总

✧ **核心层设计**

网络核心层是医院信息平台网络数据的骨干交换区域，各接入层数据经汇聚层汇聚后集中转发至核心层进行高速交换。核心层的主要职责为负责整个医院信息平台数据的高速转发，相关的策略应该尽量较少。核心层由于是整个网络的核心，从设备上来讲，需要在考虑高性能，高稳定性的同时，充分考虑设备引擎、业务线卡、电源、风扇等的冗余，同时需要具备的一定的抗攻击能力，如中央处理器保护能力，基础网络保护能力；从架构上来讲，需要充分考虑核心层设备间的冗余备份和负载均衡，利用 MSTP/RSTP+VRRP 技术，自愈环网技术，或者是通过更好的核心层设备的硬件虚拟化技术，实现设备级的冗余备份，同时，在设计时还应充分考虑网络链路的冗余性和可靠性，提高网络防灾能力。

二层网络架构下技术要点：

- 自身管理地址，管理口令，远程登录，受信任管理列表的，SNMP 控制字的设置
- VLAN
- 高速的三层转发
- MSTP+VRRP
- 三层访问控制列表
- 三层网络架构下技术要点：
- 自身管理地址，管理口令，远程登录，受信任管理列表的，SNMP 控制字的设置

◆ 高速的三层转发

◆ 路由协议

✧ **出口**

网络出口是医院信息平台与行政管理机构，区域卫生信息平台，互联网的分割点以及连接节点，是划分医院信息平台域内与域间，医院局域网与互联网的的标志。网络流量经出口与医院信息平台交互，因此，网络出口也是控制内外网交互安全的关键。而由于域外网络风险的不确定性，不加控制的交互会给医院信息平台带来巨大的风险，诸如病毒、攻击等等，都会对医院信息平台带来安全隐患。而作为医院互联网的出口，需具备控制和规范员工的行为，提高网络的使用效率，保证关键流量的访问速度，确保关键业务的正常运行，限制非必要流量访问，实时监控出口带宽和利用率，防止病毒攻击，进行网络的访问控制，提供网络访问日志，图形化的管理等功能。同时，由于出口设备在网络互联中的关键地位，应尽量支持硬件 BYPASS 功能。就出口链路而言，由于运营商线路的稳定性较差，需考虑配置多运营商线路作为网络出口，提供出口链路的备份。

目前随着医院信息化的进行，医院门户网站作用正日益增强，网上预约，网上挂号，对外信息发布平台日益完善。因此，医院信息平台应该具备对医院网站的保护与修复能力，能够及时阻止网络攻击，主动防止网页篡改。

出口设备主要包含：出口路由器，防火墙，VPN，IDS，流量控制设备，上网行为管理设备，网站综合保护系统等系统及其子系统。出口链路则包括连接行政管理机构和区域医疗卫生平台的 MSTP，SDH 等专用线路，也包括像 3G，ADSL，PSTN，ISDN 等备份线路，同时还需具备足够的互联网出口。

技术要点：

◆ 出口链路类型选择

◆ 多出口负载均衡

◆ 出口 NAT 转换规则

◆ 出口防火墙访问控制规则

◆ 出口 VPN 设置

通过对网络各层次的设计与利用，在保证内外网融合的同时，充分保证内网安全，杜绝非法的服务器访问，避免信息被偷窃、篡改。

5.4.6.2.4 内外网分离的网络架构设计

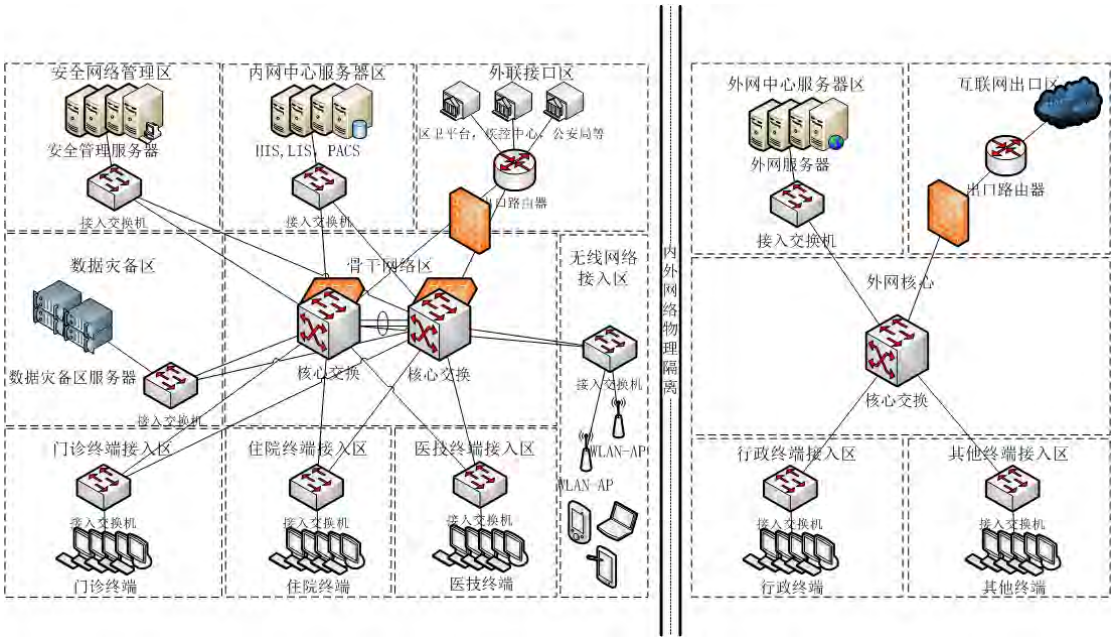

图 5-70 内外网分离二层网络架构设计

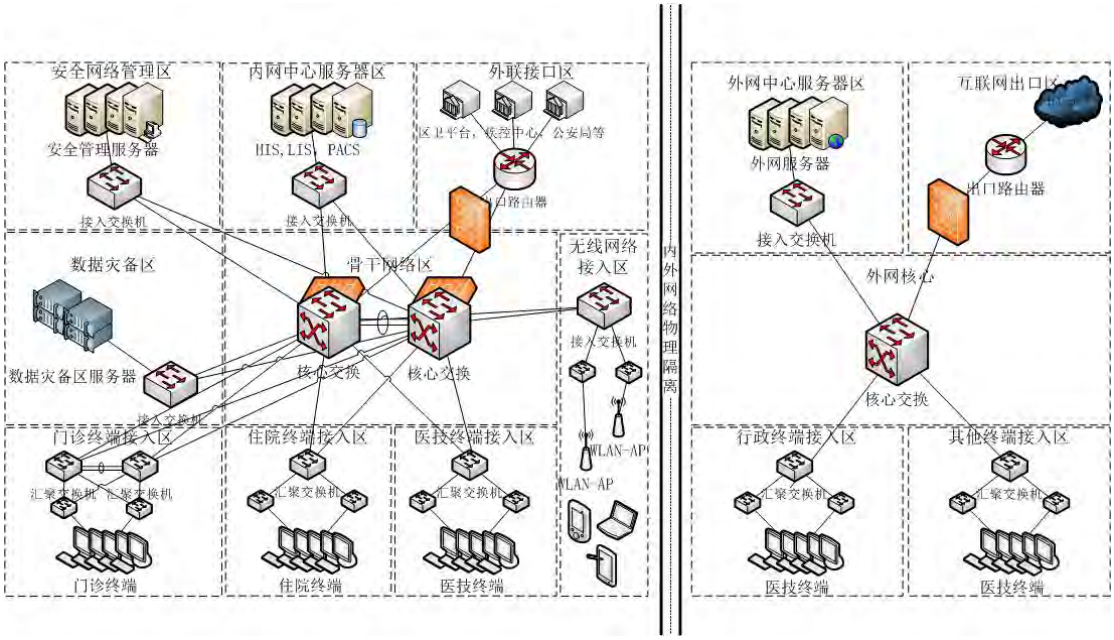

图 5-71 内外网分离的三层网络架构设计

严格意义上的内外网分离的网络架构设计，就是指将医院的内外网分别建设，两网物理隔离。内网主要承载医疗核心业务，如 HIS、LIS、PACS 和等。外网作为行政办公、对外发布、互联网医学资料查询的主要平台，对于稳定性和保

密的性的要求低于内网，并且接入终端及数据流特点也更为复杂。内外网无共用设备和链路，两网之间互不影响。此种网络架构设计，能够最大程度保证内网安全。但由于内外网完全物理隔离，医院对外服务器需要的数据需要通过手动或半自动的方式来进行同步，在实际系统的运行过程之中，在此种模式下，数据的实时同步能力将大大降低，对于一些实时业务的支持可能出现问题。

在目前医院信息平台建设的过程中，基本没有严格意义上的内外网完全隔离的网络架构，我们称之为广义上的内外网隔离架构。这是因为在当前医院信息平台的建设过程中，由于业务需要，双网架构均通过一定的手段和机制将医院的内外网联系起来，可通过多种方式（如 VPN，专线，数据库内部同步等）实施医疗协同，使得数据实时同步，对外医疗信息的传递等得以执行。本小节所述内外网分离的物理架构采用了广义上定义。

医院信息平台内外网分界如下：

- ✧ 内网：
  - ◆ 内网核心区
  - ◆ 内网中心服务器区
  - ◆ 安全网络管理区
  - ◆ 数据灾备区
  - ◆ 外联接口区
  - ◆ 门诊终端接入区
  - ◆ 住院终端接入区
  - ◆ 医技终端接入区
- ✧ 外网：
  - ◆ 外网核心区
  - ◆ 互联网出口区
  - ◆ 外网中心服务器区
  - ◆ 行政终端接入区
  - ◆ 其他终端接入区

同样内外网分离架构下也分为两种子架构，他们分别是内外网分离二层架构和内外网分离三层架构。同样二层架构为核心-接入架构，三层架构为核心-汇聚

-接入架构。在三层设计架构下，推荐门诊区域采用双汇聚架构，充分保证门诊区域 7*24*356 不间断运行。各层次设计原则和技术要点和内外网融合的方式是相同的。二三层架构可针对不同区域混合使用，例如将医技终端接入区与核心共同组成二层架构，而行政接入区则通过核心-汇聚-接入形成三成架构，将其网关下移至汇聚交换机，降低该区域对骨干网络的影响。

✧ 内外网分离架构的优缺点如下：

优点

◆ 两网并行运行，互不干扰。

◆ 充分保证内网网络稳定和业务系统安全。

缺点

◆ 两张网络单独建设，投资规模增大

◆ 灵活性稍弱，一台终端只属于一张网，不能同时对两网资源进行访问，也不能自由切换

◆ 需要管理两张网络，增加管理成本

是否需要进行两网隔离的医院信息平台建设，需要综合考虑医院的规模，业务系统的复杂度，以及实际的网络需要。需根据情况，灵活把握。

5.4.6.2.5 基于业务的无线网络平台架构

无线局域网指的是采用无线传输媒介的计算机网络，结合了最新的计算机网络技术和无线通信技术。首先，无线局域网是有线局域网的延伸。使用无线技术来发送和接收数据，减少了用户的连线需求。

在有线世界里，以太网已经成为主流的 LAN 技术，其发展不仅与无线 LAN 标准的发展并行，而且也确实预示了后者的发展方向。通过电气和电子研究所（IEEE）802.3 标准的定义，以太网提供了一个不断发展、高速、应用广泛且具备互操作特性的网络标准。这一标准还在继续发展，以跟上现代 LAN 在数据传输速率和吞吐量方面要求。以太网标准最初仅能提供 10 兆位/秒（Mbps）的数据传输速率，现在已经发展成为可以提供网络主干和带宽密集型应用所要求的 100 兆位/秒的数据传输速率。IEEE 802.3 标准是开放性的，减少了市场进入的障碍，并导致了大量可供以太网用户选择的供应商、产品和价值点的产生。最重要的是，

只要符合以太网标准就可以实现到操作性，从而使用户能够选择多个供应商提供的一种产品，同时确保这些产品能够共同使用。

第一代无线 LAN 技术是低速的（1-2 兆位/秒）专有产品提供。尽管有这些缺点，无线所带来的自由性和灵活性还是在纵向市场上为这些早期产品占据了一席之地，如零售业和仓储业，这些行业的移动工人使用手持设备进行存货管理和数据采集。随后，医院使用无线技术将病人的信息直接传送到病床边。随着计算机进入课堂，学校和大学开始安装无线网络，以避免布线成本和共享 Internet 接入。打头阵的无线供应商不久就认识到，为使这一技术获得市场的广泛接受，需要建立一种类似以太网的标准。供应商们在 1991 年联合到一起，第一次建议并随后建立了一个基于各自技术的标准。1997 年 6 月，IEEE 发布了用于无线局域网的 802.11 标准。

正象 802.3 标准允许数据通过双绞线和同轴电缆进行传输一样，802.11 WLAN 标准允许通过不同的介质进行数据传输。可以使用的介质包括红外线和两种在无需获得许可的 2.4 千兆赫频段上的无线电传输：跳频扩频（FHSS）和直序扩频（DSSS）。传播频谱是 40 年代开发的一种调制技术，可以在一个很宽的无线电频率波段内传播信号。这一技术是数据通信的理想选择，因为它对无线电干扰不很敏感，而且几乎不产生干扰。FHSS 受限于 2 兆位/秒的数据传输速率，仅推荐在非常特殊的应用如某些类型的水运工具中使用。对于其它所有的无线 LAN 应用，DSSS 是更好的选择。最近发布的 IEEE 演化版本 802.11b 可以通过 DSSS 提供与以太网相当的 11 兆位/秒的数据传输速率。FHSS 不支持 2 兆位/秒以上的数据传输速率。

Aironet/IEEE 的多级安全保密措施，极大地增强无线网络的安全可靠性，而且用户还可增加一些附属功能以达到更高的保密性，无线网络则已具有同有线局域网络甚至更高级别的保密特性。

与有线局域网相比较，无线局域网具有开发运营成本低、时间短，投资回报快，易扩展，受自然环境、地形及灾害影响小，组网灵活快捷等优点。可实现“任何人在任何时间，任何地点以任何方式与任何人通信”，弥补了传统有线局域网的不足。随着 IEEE802.11 标准的制定和推行，无线局域网的产品将更加丰富，不同产品的兼容性将得到加强。现在无线网络的传输率已达到和超过了 10Mbps，

并且还在不断变快。目前无线局域网除能传输语音信息外，还能顺利地进行图形、图像及数字影像等多种媒体的传输。

众所周知有线网络是通过网线将各个网络设备连接到一起，不管是路由器，交换机还是计算机，网络通讯都需要网线和网卡；而无线网络则大大不同，目前我们广泛应用的 802.11 标准无线网络是通过 2.4GHz 无线信号进行通讯的，由于采用无线信号通讯，在网络接入方面就更加灵活了，只要有信号就可以通过无线网卡完成网络接入的目的；同时网络管理者也不用再担心交换机或路由器端口数量不足而无法完成扩容工作了。总的来说中小企业无线网络相比传统有线网络的特点主要体现在以下两个方面。

✧ 无线网络组网更加灵活：

无线网络使用无线信号通讯，网络接入更加灵活，只要有信号的地方都可以随时随地将网络设备接入到企业 内网。因此在企业内网应用需要移动办公或即时演示时无线网络优势更加明显。

✧ 无线网络规模升级更加方便：

无线网络终端设备接入数量限制更少，相比有线网络一个接口对应一个设备，无线路由器容许多个无线终端设备同时接入到无线网络，因此在企业网络规模升级时无线网络优势更加明显。

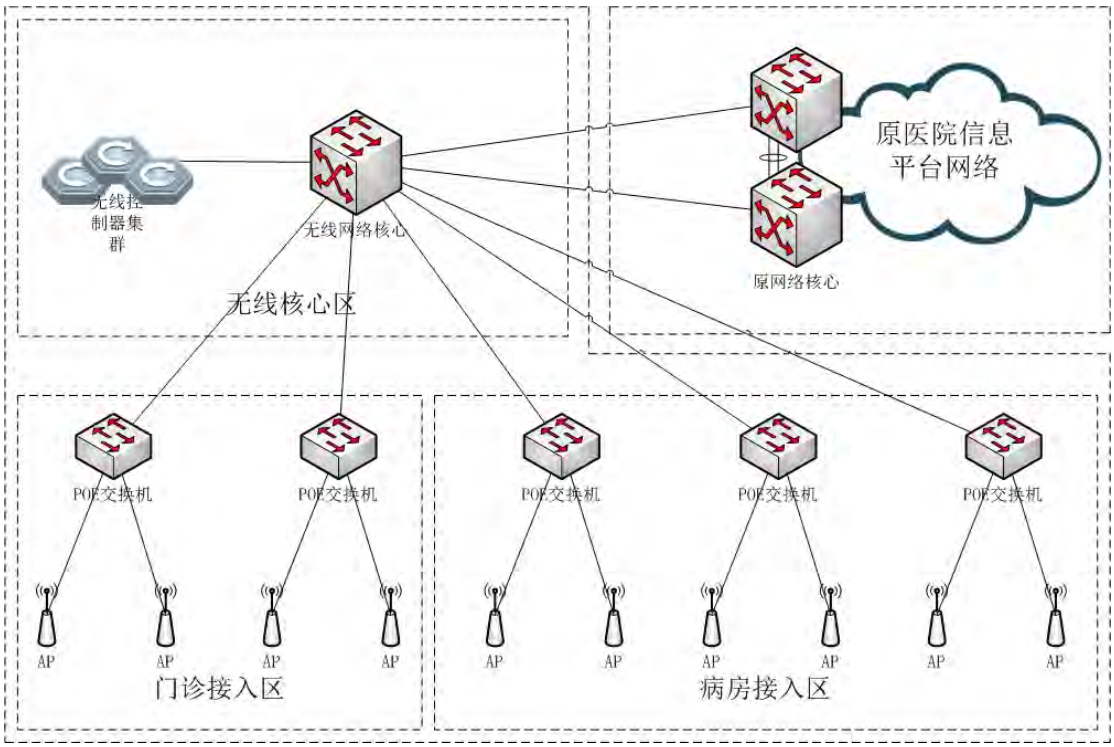

图 5-72 基于业务的独立无线网络平台架构

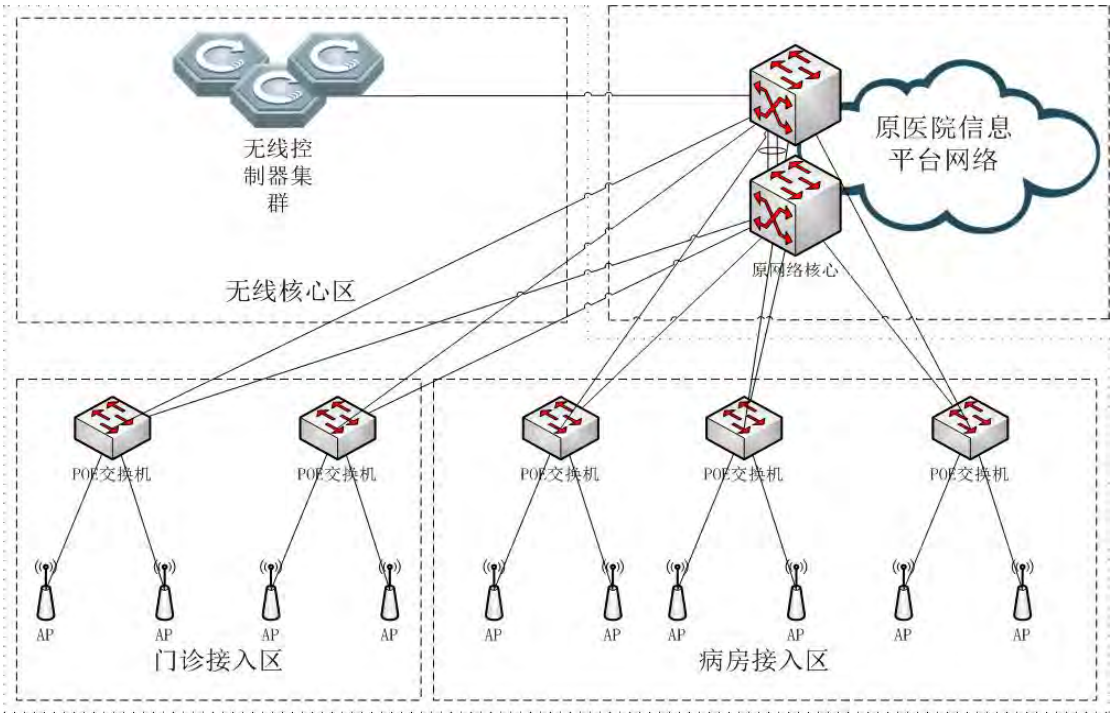

图 5-73 基于业务的融合无线网络架构

医院信息平台由于其业务特点，在无线网络建设时需要考虑如下问题：

- ◆ 由于医学影像资料的传输数据较大，应采用高速的无线网络连接，并且具备良好的技术后向兼容性
- ◆ 避免和医疗设备形成干扰。
- ◆ 良好的信号覆盖性能
- ◆ 安全的无线网络接入
- ◆ 简单方便集中的管理方式
- ◆ 支持市电供电和 POE 供电两种模式

基于以上需求，无线网络架构设计主要包含两种模式：独立无线网络架构和融合无线网络架构。独立无线网络架构，在网络建设时，独立建设无线传输网络，无线网络核心与有线网络核心互联，从而保证无线网络与有线网络的互联互通。而融合的无线网络架构，是将无线网络直接扩展到现有的有线网络架构之上，通过扩展 POE 交换机或 POE 适配器来实现无线网络的搭建，有线无线充分分融合。

✧ 基于业务的独立无线网络平台架构

优点：

◆ 无线网络流量通过无线网络运行，不对有线网络流量这造成影响，不增加原有设备转发压力

◆ 无线网络独立架构，可为像门诊区域这样的关键区域提供独立的备份链路

◆ 无线网络核心与有线网络核心直接相连，可支持数据的高速转发

◆ 部署简单，不影响现有网络拓扑结构

缺点：

◆ 无线网络初次建设成本较高

✧ 基于业务的融合无线网络平台架构

优点：

◆ 保护投资，降低无线网络初次建设成本

◆ 无线有线完全融合，充分利用现有网络资源

缺点：

◆ 部署时需要改动现有网络结构，对原网络进行调整，增加初次部署复杂度

◆ 随着无线网络带宽以及传输数据的增加，无线网络可能会给有线网络设备造成额外的压力

除此之外，还应充分考虑采用的无线网络技术的先进性，是否可以满足医学影像资料传输的需求，以及是否满足后向兼容和后续扩展的需要。推荐采用支持802.11n 标准无线设备来搭建医院的无线网络平台。802.11n 是高速无线网络的最新标准，能够兼容 802.11a/b/g，同时理论传输带宽达到 300Mbps，是之前802.11g 标准的近 5 倍，能够很好的满足医院对无线网络的需求。

在自治型 AP 和智能型 AP 的选择上，推荐采用智能型 AP 组网。智能无线是目前无线网络发展的方向，通过对全网 AP 的集中控制，达到简化网络管理，增强控制力度的目的。有条件的医院可以直接选择智能无线组网，也可通过采用胖瘦一体化 AP，进行分步无线网络部署。

5.4.6.3 基础网络设施平台实现

5.4.6.3.1 内外融合的平台实现

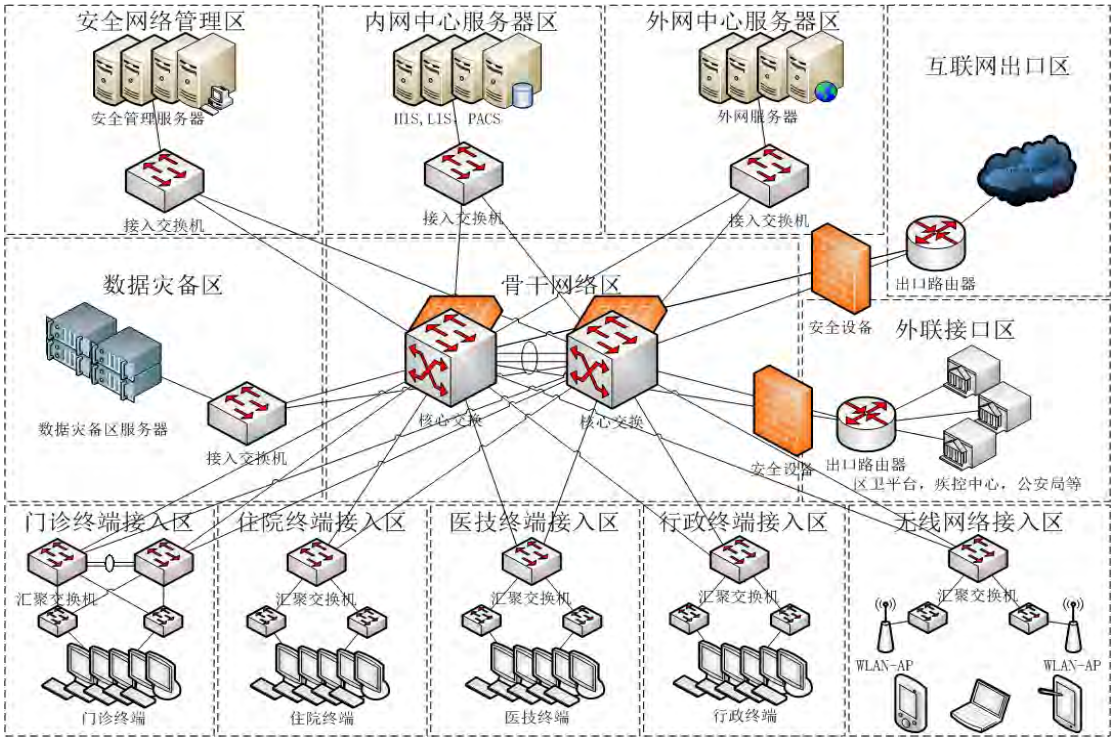

图 5-74 内外网融合的网络架构

设备选型

✧ **核心层**

核心层设备承担的主要流量如下

◆ 门诊终端接入区至内网中心服务器区流量

◆ 住院终端接入区至内网中心服务器区流量

◆ 医技终端接入区至内网中心服务器区流量

◆ 无线终端接入区至内网中心服务器区流量

◆ 行政终端接入区至外网中心服务器区流量

◆ 内外网中心服务器至数据灾备区流量

◆ 专网出口区至内网中心服务器区流量

◆ 互联网出口区至其他终端接入区流量

◆ 安全网络管理区至其他各区域流量

核心层设备承担的功能如下：

◆ 医院信息平台数据的三层高速转发

◆ 各区域间三层访问控制策略的执行

◆ 充当各接入设备的网关

基于以上原因，核心层设备建议选用高性能的万兆三层交换机，通过千兆链路与汇聚层设备相连，通过万兆链路进行核心层互联。在设备选择上，应充分考虑设备自身的冗余性，如电源冗余、引擎冗余、业务线卡冗余、所有线卡及电源支持热拔插，同时应具备一定的自我保护机制，如中央处理器保护机制，基础网络保护机制等。在网络规划时，应充分考虑网络架构的冗余性设计，建议采用两台或两台以上组成双核心或多核心环网，核心之间可进行冗余互备以及负载分担，减小由于单核心造成的设备压力及单点故障。

✧ **汇聚层**

汇聚层设备，汇聚层设备未区域网络流量的集中点，也是各种针对区域的访问控制策略的执行点，可以看做是小区域网络的核心。该层设备应具备较为丰富的三层安全功能，例如三层访问控制列表，QoS，VLAN 划分，VLAN 修剪，MSTP，RSTP，BPDU GUARD，ROOT GUARD 等功能。同时设备应具备一定的自我保护能力，如中央处理器保护，基础网络保护等，使得在单设备情况下，充分保证网络稳定。

汇聚层设备主要承担的流量如下（各汇聚设备由于在网络中位置不同，分别负担以下流量）

◆ 门诊终端接入区至内网中心服务器区流量（门诊部汇聚设备）

◆ 住院终端接入区至内网中心服务器区流量（住院部汇聚设备）

◆ 医技终端接入区至内网中心服务器区流量（医技部汇聚设备）

◆ 无线终端接入区至内网中心服务器区流量（无线区汇聚设备）

◆ 行政终端接入区至外网中心服务器区流量（办公区汇聚设备）

汇聚层主要承担的功能是

◆ 汇聚各自接入区域流量，集中转发至核心交换

◆ 进行区域间三层访问控制策略的执行

基于以上原因，汇聚层设备建议选用性能较高，且具备丰富安全功能的全千兆三层交换机，通过千兆与接入交换机以及核心交换机相连，同时汇聚交换机建议具备万兆扩展能力，方便后续网络升级。汇聚层设备需具备一定的稳定性，门

诊区域建议采用双汇聚设备，保证网络高可靠。

✧ **接入层**

接入层设备是各区域流量的接入节点，是网络安全到边缘思想的执行点，也是网络准入控制的实施点。该层设备应具备较为丰富的二层安全控制功能，例如VLAN 划分，二层访问控制列表，MSTP，RSTP，BPDU GUARD，BPDU FILTER，DHCP Snooping，安全地址绑定，802.1x 等功能。同时设备应具备一定的自我保护能力，如中央处理器保护，基础网络保护等，使得在单设备情况下，充分保证网络稳定。

接入层设备主要承担的流量如下（根据各接入设备位置不同，分别承担以下流量）

- ◆ 内网中心服务器接入流量（内网中心服务器接入）
- ◆ 外网中心服务器接入流量（外网中心服务器接入）
- ◆ 安全网络控制区接入流量（安全网络控制区接入）
- ◆ 数据灾备区接入流量（数据灾备区接入）
- ◆ 门诊终端接入流量（门诊终端区接入）
- ◆ 住院终端接入流量（住院终端区接入）
- ◆ 医技终端接入流量（医技终端区接入）
- ◆ 无线终端接入流量（无线终端区接入）
- ◆ 行政终端接入区流量（行政终端区接入）
- ◆ 其他终端区接入（其他终端区接入）

接入层主要承担的功能是

- ◆ 汇聚各接入终端流量集中转发至汇聚层或核心层
- ◆ 信息平台网络准入控制
- ◆ VLAN 划分与 VLAN 修剪
- ◆ 二层网络访问控制策略执行
- ◆ 同 VLAN 二层流量转发

基于以上原因，建议内网中心服务器区、外网中心服务器区、安全网络控制区、数据灾备区、医技终端接入区、无线终端接入区采用全千兆二层交换机作为接入设备，其他接入区域采用百兆二层交换机，千兆上联。接入层交换机应选用

智能网管型交换机，具备 VLAN 划分，二层访问控制列表，MSTP，RSTP，BPDU GUARD，BPDU FILTER，DHCP Snooping，安全地址绑定，802.1x 等功能。接入层交换机还应具备良好的防雷击特性，由于医院信息平台对网络稳定性要求的特殊性，建议以太网接口具备高于国家标准的防雷击能力。同时能在一定程度上抵抗网络攻击，如中央处理器保护，基础网络保护等。

✧ **网络出口**

网络出口是医院信息平台对外连接的关键区域，该区域主要由两部分组成：专网出口区域和互联网出口区域。两出口区域分两台设备设置，是为了避免由于互联网上对外网出口的攻击对专网出口造成影响，最大程度保证专网的互联互通性。

专网出口设备

专网出口设备主要承担流量如下（包括但不限于）

◆ 上级主管部门管理流量

◆ 平级部门调用相关数据流量

◆ 上传和调用区域卫生信息平台数据流量

专网出口设备主要承担功能

◆ 出口路由功能

◆ 多链路选择功能

◆ 类型丰富的专网接口

◆ 地址转换（NAT/PAT）功能

基于以上原因，出口设备应选择高性能路由器或专用出口设备作为网络出口，并添加防火墙进行域间网络访问控制。路由器应具备大容量、高性能的 NAT 转换能力，能够进行智能选路，并提供丰富的广域网接口。除此之外，路由器还应具备较高的冗余性和抗网络攻击能力。防火墙作为域间网络隔离点，需支持多种访问控制策略的制定，以及高性能的数据转发能力，避免成为网络性能瓶颈。

互联网出口设备

互联网出口设备主要承担流量如下

◆ 各区域对互联网资源的访问流量

◆ VPN 远程办公流量

◆ 其他互联网访问流量

◆ 外部对外网 WEB 服务器的访问流量

互联网出口设备主要承担的功能如下

◆ 出口路由功能

◆ 多链路选择功能

◆ 类型丰富广域网接口

◆ 地址转换（NAT/PAT）功能

◆ 局域网广域网分割功能

◆ 网络访问控制功能

◆ VPN 功能

◆ 流量控制功能

◆ 上网行为管理功能

基于以上要素出口设备应包含整合出口路由，防火墙，VPN，流控设备，上网行为管理的单一设备，或部分整合设备。出口设备也可以使路由器，防火墙，VPN，流控设备，上网行为管理设备的组合。出口路由应高性能路由器，保证院内终端对互联网的高速访问，同时为外网访问内网 WEB 服务器提供高速链路通道。防火墙设备作为局域网和广域网的分割点，其访问控制功能至关重要，故防火墙需支持类型丰富的网络访问控制策略设置。VPN 设备应选用可支持 IPSECVPN 和 SSLVPN 的设备，保证 VPN 接入方式的灵活性。流控设备应具备较高且较为精细的流量识别功能，可基于流量识别对网络流量进行控制，保证网络带宽充分有效的利用。上网行为管理设备，主要是通过 URL 过滤库的设置，规范员工上网行为，保证网络安全，提升工作效率。

网络技术策略规划

✧ **核心层技术策略规划**

◆ 为设备和接口进行规范化命名及密码设置

◆ 为直连接入层的 VLAN 配置网关

◆ 通过访问控制列表，配置网络三层访问控制策略

◆ 与汇聚层设备运行 OSPF 路由协议或静态路由协议，并将直连路由发布进 OSPF 路由进程，完成各区域的互联互通

✧ **汇聚层技术策略规划**

◆ 为设备和接口进行规范化命名及密码设置

◆ 进行 VLAN 划分和修剪

◆ 对于双汇聚网络，采用 MSTP+VRRP 进行虚拟网关部署和多生成树实例配置

◆ 通过访问控制列表，配置网络三层访问控制策略

◆ 与核心层设备运行 OSPF 或静态路由协议

◆ 如果需要跨网段进行 DHCP，则配置 DHCP Relay

✧ **接入层技术策略规划**

◆ 双链路或单链路上联至汇聚或核心交换机

◆ 为设备和接口进行规范化的命名和密码设置

◆ 设置接入层设备管理 VLAN 并配置远程登录

◆ 通过 VLAN 划分与修剪区分不同的网络区域

◆ 通过运行生成树协议消除网络环路

◆ 部署 BPDU GUARD 消除接入层下私接设备对网络带来的环路隐患

◆ 部署 BPDU FILTER 防止对不运行生成树协议的设备的干扰

◆ 分别添加 SNMP 只读和读写控制字为网络管理打下基础

◆ 按需要在采用一定方式在接入层设备接口下生成安全地址，保证网络安全

✧ **出口区技术策略规划**

◆ 出口链路选择

◆ 多出口智能选路

◆ IP 映射设置

◆ NAT 规则设置

◆ 只能 DNS 设置

◆ 域内/域间，局域网/广域网网络访问策略设置

◆ VPN 建立和试运行

◆ 网络流量精细化控制规则设置

◆ 内容审计设置

- ◆ 网络日志服务器设置
- ◆ 网站访问黑名单设置
- ◆ 网络入侵检测系统 IDS 设置

5.4.6.3.2 内外网分离的平台实现

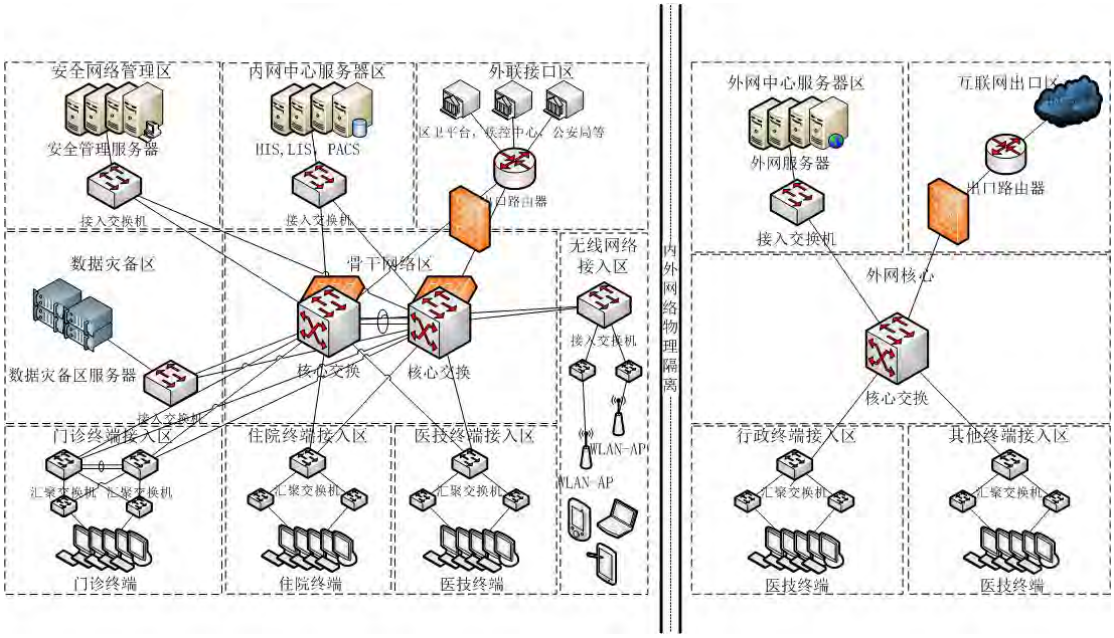

图 5-75 内外网融合的网络架构

设备选型

✧ **核心层**

医院信息平台核心层主要由两部分组成，分别为外网核心层和内网核心层

内网核心层

内网核心层设备承担的主要流量如下

- ◆ 门诊终端接入区至内网中心服务器区流量
- ◆ 住院终端接入区至内网中心服务器区流量
- ◆ 医技终端接入区至内网中心服务器区流量
- ◆ 无线终端接入区至内网中心服务器区流量
- ◆ 内外网中心服务器至数据灾备区流量
- ◆ 专网出口区至内网中心服务器区流量
- ◆ 安全网络管理区至其他各区域流量

内网核心层设备承担的功能如下：

◆ 医院信息平台数据的三层高速转发

◆ 各区域间三层访问控制策略的执行

◆ 充当各接入设备的网关

基于以上原因，核心层设备建议选用高性能的万兆三层交换机，通过千兆链路与汇聚层设备相连，通过万兆链路进行核心层互联。在设备选择上，应充分考虑设备自身的冗余性，如电源冗余、引擎冗余、业务线卡冗余、所有线卡及电源支持热拔插，同时应具备一定的自我保护机制，如中央处理器保护机制，基础网络保护机制等。在网络规划时，应充分考虑网络架构的冗余性设计，建议采用两台或两台以上组成双核心或多核心环网，核心之间可进行冗余互备以及负载分担，减小由于单核心造成的设备压力及单点故障。

外网核心层

网核心层设备承担的主要流量如下

◆ 行政终端接入区至外网中心服务器区流量

◆ 互联网出口区至其他终端接入区流量

◆ 互联网出口区至外网中心服务器区流量

外网核心层设备承担的主要功能如下：

◆ 外网流量的高速三层转发

◆ 域间三层访问控制策略的执行

◆ 充当外网各区域接入终端的网关

基于以上原因，外网核心设备建议采用高性能三层以太网交换机，通过千兆链路与汇聚交换机互联。网络采用单核心架构的同时，充分考虑设备自身模块的冗余性和稳定性。

✧ **汇聚层**

汇聚层设备，汇聚层设备未区域网络流量的集中点，也是各种针对区域的访问控制策略的执行点，可以看作是小区域网络的核心。该层设备应具备较为丰富的三层安全功能，例如三层访问控制列表，QoS，VLAN 划分，VLAN 修剪，MSTP，RSTP，BPDU GUARD，ROOT GUARD 等功能。同时设备应具备一定的自我保护能力，如中央处理器保护，基础网络保护等，使得在单设备情况下，充分保证网络稳定。

在内外网分离网络架构下，分为内网汇聚层和外网汇聚层设计。

内网汇聚层

内网汇聚层设备主要承担的流量如下（各汇聚设备由于在网络中位置不同，分别负担以下流量）

◆ 门诊终端接入区至内网中心服务器区流量（门诊部汇聚设备）

◆ 住院终端接入区至内网中心服务器区流量（住院部汇聚设备）

◆ 医技终端接入区至内网中心服务器区流量（医技部汇聚设备）

◆ 无线终端接入区至内网中心服务器区流量（无线区汇聚设备）

内网汇聚层主要承担的功能是

◆ 汇聚各自接入区域流量，集中转发至核心交换

◆ 进行区域间三层访问控制策略的执行

基于以上原因，汇聚层设备建议选用性能较高，且具备丰富安全功能的全千兆三层交换机，通过千兆与接入交换机以及核心交换机相连，同时汇聚交换机建议具备万兆扩展能力，方便后续网络升级。汇聚层设备需具备一定的稳定性，门诊区域建议采用双汇聚设备，保证网络高可靠。

外网汇聚层

外网汇聚层设备主要承担的流量如下

◆ 行政终端接入区至外网中心服务器区流量（办公区汇聚设备）

◆ 天塔终端接入区至互联网出口区流量

◆ 外网汇聚层主要承担的功能是

◆ 汇聚各自接入区域流量，集中转发至核心交换

◆ 进行区域间三层访问控制策略的执行

基于以上原因，汇聚层设备建议选用性能较高，且具备丰富安全功能的全千兆三层交换机，通过千兆链路与接入交换机以及核心交换机相连。汇聚层设备需具备一定的稳定性，保证网络高可靠。

✧ 接入层

接入层设备是各区域流量的接入节点，是网络安全到边缘思想的执行点，也是网络准入控制的实施点。该层设备应具备较为丰富的二层安全控制功能，例如VLAN 划分，二层访问控制列表，MSTP，RSTP，BPDU GUARD，BPDU FILTER，DHCP

Snooping，安全地址绑定，802.1x 等功能。同时设备应具备一定的自我保护能力，如中央处理器保护，基础网络保护等，使得在单设备情况下，充分保证网络稳定。

在内外网分离架构下，接入层设备主要分为内网接入层和外网接入层。

内网接入层

接入层设备主要承担的流量如下（根据各接入设备位置不同，分别承担以下流量）

- 内网中心服务器接入流量（内网中心服务器接入）
- 安全网络控制区接入流量（安全网络控制区接入）
- 数据灾备区接入流量（数据灾备区接入）
- 门诊终端接入流量（门诊终端区接入）
- 住院终端接入流量（住院终端区接入）
- 医技终端接入流量（医技终端区接入）
- 无线终端接入流量（无线终端区接入）

接入层主要承担的功能是

- 汇聚各接入终端流量集中转发至汇聚层或核心层
- 信息平台网络准入控制
- VLAN 划分与 VLAN 修剪
- 二层网络访问控制策略执行
- 同 VLAN 二层流量转发

基于以上原因，建议内网中心服务器区、安全网络控制区、数据灾备区、医技终端接入区、无线终端接入区采用全千兆二层交换机作为接入设备，其他接入区域采用百兆二层交换机，千兆上联。接入层交换机应选用智能网管型交换机，具备 VLAN 划分，二层访问控制列表，MSTP，RSTP，BPDU GUARD，BPDU FILTER，DHCP Snooping，安全地址绑定，802.1x 等功能。接入层交换机还应具备良好的防雷击特性，由于医院信息平台对网络稳定性要求的特殊性，建议以太网接口具备高于国家标准的防雷击能力。同时能在一定程度上抵抗网络攻击，如中央处理器保护，基础网络保护等。

外网接入层

接入层设备主要承担的流量如下（根据各接入设备位置不同，分别承担以下流量）

◆ 外网中心服务器接入流量（外网中心服务器接入）

◆ 行政终端接入区流量（行政终端区接入）

◆ 其他终端区接入（其他终端区接入）

接入层主要承担的功能是

◆ 汇聚各接入终端流量集中转发至汇聚层或核心层

◆ 信息平台网络准入控制

◆ VLAN 划分与 VLAN 修剪

◆ 二层网络访问控制策略执行

◆ 同 VLAN 二层流量转发

基于以上原因，建议外网中心服务器区采用全千兆二层交换机作为接入设备，行政终端接入区采用百兆二层交换机，千兆上联。接入层交换机应选用智能网管型交换机并具备良好的防雷击特性。同时能在一定程度上抵抗网络攻击。

✧ **网络出口**

网络出口是医院信息平台对外连接的关键区域，该区域主要由两部分组成：专网出口区域和互联网出口区域。两出口区域分两台设备设置，是为了避免由于互联网上对外网出口的攻击对专网出口造成影响，最大程度保证专网的互联互通性。

专网出口设备

专网出口设备主要承担流量如下（包括但不限于）

◆ 上级主管部门管理流量

◆ 平级部门调用相关数据流量

◆ 上传和调用区域卫生信息平台数据流量

专网出口设备主要承担功能

◆ 出口路由功能

◆ 多链路选择功能

◆ 类型丰富的专网接口

◆ 地址转换（NAT/PAT）功能

基于以上原因，出口设备应选择高性能路由器或专用出口设备作为网络出口，并添加防火墙进行域间网络访问控制。路由器应具备大容量、高性能的 NAT 转换能力，能够进行智能选路，并提供丰富的广域网接口。除此之外，路由器还应具备较高的冗余性和抗网络攻击能力。防火墙作为域间网络隔离点，需支持多种访问控制策略的制定，以及高性能的数据转发能力，避免成为网络性能瓶颈。

互联网出口设备

互联网出口设备主要承担流量如下

- 各区域对互联网资源的访问流量
- VPN 远程办公流量
- 其他互联网访问流量
- 外部对外网 WEB 服务器的访问流量

互联网出口设备主要承担的功能如下

- 出口路由功能
- 多链路选择功能
- 类型丰富广域网接口
- 地址转换（NAT/PAT）功能
- 局域网广域网分割功能
- 网络访问控制功能
- VPN 功能
- 流量控制功能
- 上网行为管理功能

基于以上要素出口设备应包含整合出口路由，防火墙，VPN，流控设备，上网行为管理的单一设备，或部分整合设备。出口设备也可以使路由器，防火墙，VPN，流控设备，上网行为管理设备的组合。出口路由应高性能路由器，保证院内终端对互联网的高速访问，同时为外网访问内网 WEB 服务器提供高速链路通道。防火墙设备作为局域网和广域网的分割点，其访问控制功能至关重要，故防火墙需支持类型丰富的网络访问控制策略设置。VPN 设备应选用可支持 IPSECVPN 和 SSLVPN 的设备，保证 VPN 接入方式的灵活性。流控设备应具备较高且较为精细的流量识别功能，可基于流量识别对网络流量进行控制，保证网络带宽充分有

效的利用。上网行为管理设备，主要是通过 url 过滤库的设置，规范员工上网行为，保证网络安全，提升工作效率。

网络技术策略规划

内外网分离架构网络技术策略规划与内外融合的网络策略各层次规划相同，只是两网分别执行，单独实施。具体如下：

✧ **核心层技术策略规划**

◆ 为设备和接口进行规范化命名及密码设置

◆ 为直连接入层的 VLAN 配置网关

◆ 通过访问控制列表，配置网络三层访问控制策略

◆ 与汇聚层设备运行 OSPF 路由协议或静态路由协议，并将直连路由发布进 OSPF 路由进程，完成各区域的互联互通

✧ **汇聚层技术策略规划**

◆ 为设备和接口进行规范化命名及密码设置

◆ 进行 VLAN 划分与隔离

◆ 对于双汇聚网络，采用 MSTP+VRRP 进行虚拟网关部署和多生成树实例配置

◆ 通过访问控制列表，配置网络三层访问控制策略

◆ 与核心层设备运行 OSPF 或静态路由协议

◆ 如果需要跨网段进行 DHCP，则配置 DHCP Relay

✧ **接入层技术策略规划**

◆ 双链路或单链路上联至汇聚或核心交换机

◆ 为设备和接口进行规范化的命名和密码设置

◆ 设置接入层设备管理 VLAN 并配置远程登录

◆ 通过 VLAN 划分与修剪区分不同的网络区域

◆ 通过运行生成树协议消除网络环路

◆ 部署 BPDU GUARD 消除接入层下私接设备对网络带来的环路隐患

◆ 部署 BPDU FILTER 防止对不运行生成树协议的设备的干扰

◆ 分别添加 SNMP 只读和读写控制字为网络管理打下基础

◆ 按需要在采用一定方式在接入层设备接口下生成安全地址，保证网络安

全

✧ **出口区技术策略规划**

◆ 出口链路选择

◆ 多出口智能选路

◆ IP 映射设置

◆ NAT 规则设置

◆ 只能 DNS 设置

◆ 域内/域间，局域网/广域网网络访问策略设置

◆ VPN 建立和试运行

◆ 网络流量精细化控制规则设置

◆ 内容审计设置

◆ 网络日志服务器设置

◆ 网站访问黑名单设置

◆ 网络入侵检测系统 IDS 设置

5.4.6.3.3 无线网络的平台实现

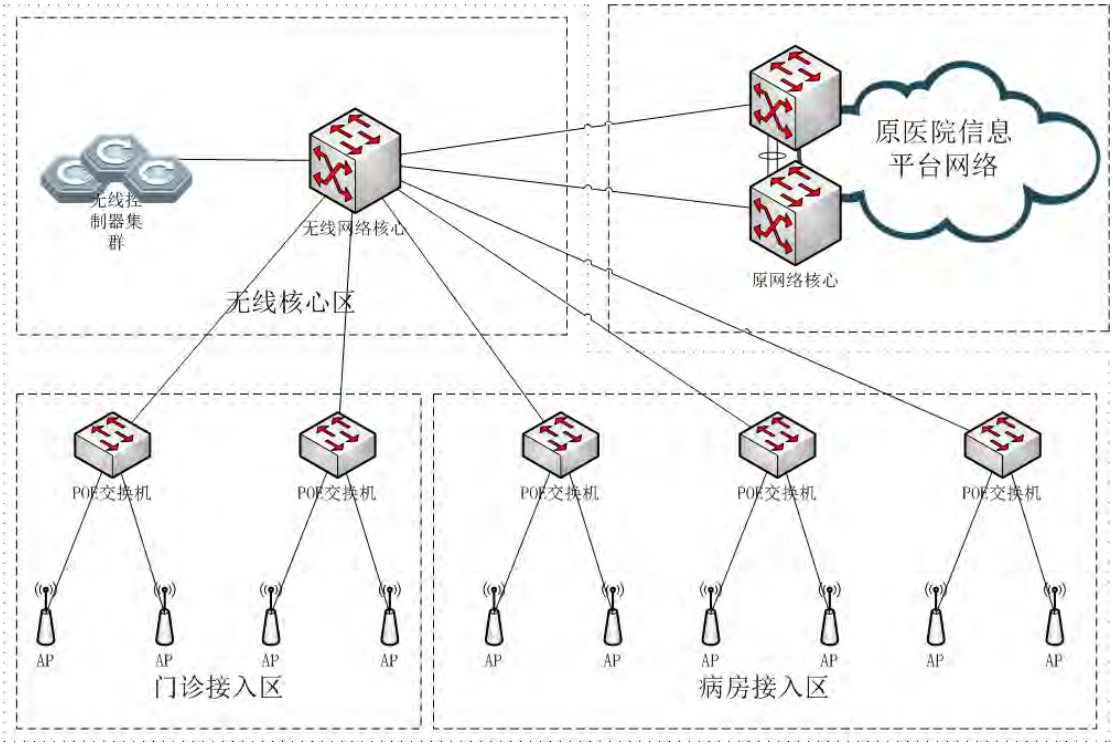

图 5-76 内外网融合的网络架构

设备选型

✧ **无线网络核心交换机**

无线网络核心交换机，承载着整个无线网络的流量，并需要将这些流量与医院原有线网络进行互联互通。故无线网络核心设备建议采用高性能三层以太网交换机，通过千兆链路与无线接入或汇聚交换机互联。网络采用单核心架构，为保证网路偶稳定，应充分考虑设备自身模块的冗余性和稳定性。如电源冗余、引擎冗余、业务线卡冗余、所有线卡及电源支持热拔插，同时应具备一定的抗攻击保护机制。

✧ **无线网络接入交换机**

无线网络接入交换机基本要求同其他各区域交换机相同，但考虑到采用高速无线的特殊性，无线网络接入交换机建议采用全千兆或百兆接入千兆上联交换机。无线网络设备供电具有特殊性，要求接入设备须支持 POE 供电，在 802.11n AP 部署区域，推荐千兆 POE 交换。

✧ **无线设备**

医院由于传输医学影像资料，无线语音呼叫，无线数据传输等的需要，对无线网络提出了一下要求。

◆ 高速的无线网络连接，低延时的数据转发

◆ 技术的先进性以及后向兼容性

◆ 简单的控制以及集中管理

◆ 丰富的安全特性

◆ 具备一定的容灾、抗灾能力

◆ 更大的信号覆盖区域

基于以上要求，推荐采用集中控制的 802.11n 智能型无线产品作为无线网络设备。802.11n 带宽是前一代无线标准 802.11g 的近 5 倍，并且全面支持 802.11a/b/g，充分满足高速，先进以及后向兼容。同时，智能网管型设备具有很好的集中控制力，方便进行网络控制和部署，集中控制也带来更高的安全性。无线控制器具有热备份能力，保证短时间内可进行切换。802.11n 的多输入天线设计，也大大提升了无线网络覆盖范围。

网络技术策略规划

✧ **核心层技术策略规划**

◆ 为设备和接口进行规范化命名及密码设置

◆ 为直连接入层的 VLAN 配置网关

◆ 通过访问控制列表，配置网络三层访问控制策略

◆ 无线网络核心层通过动态或静态路由协议与原有限网络实现互联互通

✧ **接入层技术策略规划**

◆ 单链路上联至汇聚或核心交换机

◆ 为设备和接口进行规范化的命名和密码设置

◆ 设置接入层设备管理 VLAN 并配置远程登录

◆ VLAN 划分

◆ 分别添加 SNMP 只读和读写控制字为网络管理打下基础

◆ 按需要在采用一定方式在接入层设备接口下生成安全地址，保证网络安全

✧ **无线网络技术策略规划**

通过无线控制器集中控制无线 AP，进行相关无线参数设置，并添加部分集中控制的安全策略。

5.4.6.4 网络管理

基于电子病历的医院信息平台是一个综合性的局域网信息平台，且最大的特点是内外网接入环境复杂。同时该信息平台对于核心业务的依赖性很强，因此在日常的运维管理过程中一方面要能够清晰掌握当前信息平台的整体运行情况，另一方面当发生一些问题时能够借用网络管理系统及时告警，协助运维人员快速定位故障和解决问题。

5.4.6.4.1 IP 地址规划

IP 地址规划原则

IP 地址规划应该是医院信息平台网络建设整体规划的一部分，即 IP 地址规划要和网络层次规划、路由协议规划、流量规划等统一。通过合理的 IP 地址规划和划分到达提升网络性能、简化网络的管理和维护的目的。

医院信息平台 IP 地址原则主要包括：

- ✧ 在 Internet IP 地址紧张的情况下，尽可能采用私有 IP 地址进行网络的地址规划，保证足够的网络地址可用空间；
- ✧ 地址分配是由业务驱动，按照接入单位的网络规模和业务量的大小分配各地的地址空间；
- ✧ IP 地址的规划与划分应该考虑到网络的后续规模和业务上的发展，能够满足未来发展的需要；
- ✧ IP 地址的分配需要有足够的灵活性，能够满足各种用户接入需要；
- ✧ IP 地址的分配必须采用 VLSM(变长掩码)技术，保证 IP 地址的利用效率；
- ✧ 采用 CIDR 技术，这样可以减小路由器路由表的大小，加快路由器路由的收敛速度，也可以减小网络中广播的路由信息的大小；

依据和参照的标准和规范

RFC 1366　《Guidelines For Management of IP Address Space》

RFC 1466　《Guidelines For Management of IP Address Space》

RFC 1597　《Address Allocation for Private Internets》

RFC 1918　《Address Allocation for Private Internets》

RFC 0793　《Transmission Control Protocol》

RF C0791　《Internet Protocol》

IP 地址规划与设计

IP 地址规划应该是医院信息平台网络建设的一部分，接入的区域数量众多，且各区域中需要接入平台的终端数亦较多，因此建议每个医院信息平台网络地址的使用范围采用 172.16.0.0/16 的私有地址范围，确保充足的地址空间现在需求和未来网络的扩展性需求；同时根据网络分区的设计原则来划分子网，各区域之间通过三层路由协议互访；在每个区内部根据接入终端的数量和规模进一步划分子网。

结合医院信息平台网络建设的整体模型以及各功能分区的对网络需求特点，现对 IP 的详细规划与设计做如下阐述：

- ✧ **骨干网络区**

此区域主要各分区之间的互连，网络运行时做路由的处理进而完成分区之间的数据转发，IP 地址主要是用来做三层设备的互联。因此，分配一个 B 类的地

址空间 172.16.254.0/24，两个三层设备之间的互连地址的子网掩码为 30。

✧ **内网中心服务器区**

此区域主要是医院信息平台内内网所有的应用服务器、数据库服务器、中间件服务器、数据存储设备等一切业务系统相关的设备的集中连接区域。因此，分配一个 B 类的地址空间 172.16.1.0/24，根据提供业务系统的用途和关联性在进一步划分子网。如：

表 5-19 业务系统地址规划

业务系统种类	IP 地址
注册管理服务器	172.16.1.0/24
HIS 服务器	
EMR 的管理与服务器	
…	…

✧ **安全管理区**

此区域主要是数据中心内保障整体信息平台安全、稳定运行的安全管理运维系统的连接区域。因此，分配一个 B 类的地址空间 172.16.2.0/24，根据管理的功能性需求进一步划分子网。如：

表 5-20 安全管理系统地址规划

安全管理种类	IP 地址
网络管理类服务器	172.16.2.0/24
网络安全类服务器	
身份认证、证书类服务器	
…	…

✧ **数据灾备区**

此区域主要是业务系统及健康档案数据的灾备区域，因此，分配一个 B 类的地址空间 172.16.3.0/24，根据功能性需求进一步划分子网。如：

表 5-21 灾备系统地址规划

灾备应用种类	IP 地址
灾备中心办公区	172.16.3.0/24
灾备中心服务器	
灾备存储设备	
…	…

✧ **专网出口区**

此区域主要负责连接外联单位，如社保中心、新农合，卫生局，疾控中心等。因此，分配一个 B 类的地址空间 172.16.4.0/24，根据部门数量和规模进一步划分子网。如：

表 5-22 专网出口地址规划

外联单位	IP 地址
社保中心	172.16.4.0/24
新农合	
卫生局	
…	…

✧ **终端接入区：**

分配一个或多个连续的 B 类地址范围，每个接入区域的子网掩码为 24（每个 B 类地址范围最大可以满足 255 个内网终端接入区域，每个终端接入区域可以最大满足 253 台主机接入医院信息平台），子网掩码也可以结合终端接入区域特点调整，在对应的上连骨干网络区的设备处作 IP 地址汇总和路由发布。如：

表 5-23 终端接入区地址规划

	接入单位	IP 地址
终端接入区	门诊终端接入区	172.16.50.0/24 172.16.60.0/24 …
	住院终端接入区	172.16.150.0/24 172.16.160.0/24 …
	医技终端接入区	172.16.150.0/24 172.16.160.0/24 …
	…	…

5.4.6.4.2 网络设备管理

医院信息平台的网络 IT 资源主要包括：

信息平台可能涉及 IT 资源：三层交换机、二层交换机、VPN 网关、路由器、防火墙、IDS/IPS、Windows/Unix 服务器、数据库、中间件等 IT 资源。

网络 IT 资源的管理主要包括四个层面：

◆ 网络规划管理

◆ 网络监控

◆ 故障管理

◆ 报表管理

✧ **网络规划管理**

网络规划管理主要是指医院信息平台中的网络 IT 资源能够实现在统一的界面进行直观的查看、管理。简化网管人员的管理难度。

◆ 网络 IT 资源发现

网络管理软件能够管理所有支持标准 SNMP 网管协议的网络设备，为多厂商设备共存的网络提供了统一的管理方式。

➢ 拓扑图自动发现多厂商设备；

利用网络管理软件能够自动发现平台中的 IT 资源，并自动生成相关联的拓扑图。并且网管人员能够在此基础上进行手工的添加、删除、修改，并标记资源的描述。

➢ 自动识别不同类型的设备

针对网络中的 IT 资源能够进行准确的识别和添加。主要包括：三层交换机、二层交换机、VPN 网关、路由器、防火墙、IDS/IPS、Windows/Unix 服务器、数据库、中间件等 IT 资源、防火墙、路由器、VPN 网关等

➢ 可以对设备进行性能监视，包括接口的流量监视，利用率监视等；

能够根据不同类型的设备，定义其监控的主要参数。下表列出重点资源的监控参数描述，实际管理过程中可进行必要性选择。

表 5-24 网络管理监控参数指导

资源类型	部件	指标中文描述
网络设备	接口	包含错误的输出包数
		接口丢弃的总包数
		接口包含的错误的总包数
		接口输入错误百分率
		接口输出错误百分率
		接口总流速
		接口流入速率
		接口流出速率
		接口输入丢包率
		接口输出丢包率

		带宽利用率
		该接口带宽
		接口流入量
		接口流出量
		接口总流量
		接收的字节数
		发送的字节数
		输入单播包数
		输出单播包数
		输入的非单播包数
		输出的非单播包数
		丢失的输入包数
		丢失的输出包数
		包含错误的输入包数
		由于定向到未知协议而被丢弃的包数
		输出队列中所有包数
主机（服务器）	CPU	CPU 利用率
	存储器	总空间
		利用率
		已用空间
		请求失败次数
	进程	CPU 占用率
		内存占用大小
	硬盘	设备发生的错误数
		磁盘容量
数据库	库信息	数据库日志使用率
		数据库日志缓冲命中率
		数据库数据文件的大小
	服务器信息	缓冲区池保留的页的数目
		发生的网络数据包错误数
		锁的动态内存总量
		当前动态内存总量
		动态内存总量
		SqlServer 数据库活动事务数
		SGA 缓冲池大小
		CPU 使用率
		缓存命中率
		支持的最大连接数
		执行输入和输出操作的时间
		Cpu 的工作时间
		每秒的探测扫描数
		每秒索引搜索数

		所有可用列表页总数
		每秒所发出的物理数据库页写入的数目
		每秒发出的物理数据库页读取数
		写到网络上的输出数据包数
		每秒大容量复制的行数
		每秒要求调用者等待的锁请求数
		每秒导致死锁的锁请求数
		当前用户连接数
		读取磁盘的次数
		写入磁盘的次数
		数据库闲置时间
		从网络上读取的输入数据包数目
IIS		当前连接数
		HTTP404 总错误连接数
		服务的 I/O 带宽
中间件	服务端口信息	当前线程数
		请求命中率
	应用程序信息	活动会话数
		平均会话在线时间
	JVM	内存利用率

- 可以接收设备告警，并进行告警信息显示。

在监控设备的同时，根据设备的运行状态进行有效评估，设定合理的告警阀值，当设备故障或某参数达到指定阀值后，能够自动进行告警，使网管人员及时掌握告警信息。告警方式主要有：终端显示告警、日志告警、邮件告警、短信平台告警。

◆ 网络拓扑管理

网络管理软件提供统一拓扑发现功能，实现本项目全网监控，可以实时监控所有网络和安全设备的运行状况，并根据网络运行环境变化提供合适的方式对网络参数进行配置修改，保证网络以最优性能正常运行。

- 全网设备的统一拓扑视图，拓扑自动发现，拓扑结构动态刷新；
- 可视化操作方式：拓扑视图节点直接点击进入设备操作面板；
- 在网络、设备状态改变时，改变节点颜色，提示用户；
- 对网络设备进行定时（轮询间隔时间可配置）的轮循监视和状态刷新并表现在网络视图上；

- 拓扑过滤，让用户关注所关心的网络设备情况；
- 快速查找拓扑对象，并在导航树和拓扑视图中定位该拓扑对象。

✧ **网络监控**

◆ 网络流量与带宽管理

网管系统应提供丰富的性能管理功能，同时以直观的方式显示给用户。通过性能任务的配置，可自动获得网络的各种当前性能数据，并支持设置性能的门限，当性能超过门限时，可以以告警的方式通知网管系统。通过统计不同线路、不同资源的利用情况，为优化或扩充网络提供依据。

◆ 服务器性能监控

服务器是基于电子病历的医院信息平台中的重要组成部分，通过服务器监视管理系统，实现对服务器与设备的统一管理。

- 支持对 CPU、内存资源消耗的监视；
- 支持对硬盘使用情况的监视；
- 支持运行进程的资源监视；
- 支持对服务的资源监视；

✧ **故障管理**

故障管理主要功能是对全网设备的告警信息和运行信息进行实时监控，查询和统计设备的告警信息。

◆ 告警实时监视，提供告警声光提示；

◆ 支持告警转到 Email 或手机短信；

◆ 支持告警过滤，让用户关注重要的告警，查询结果可生成报表；

◆ 支持告警拓扑定位，将显示的焦点定位到选定告警的拓扑对象；

◆ 支持告警相关性分析，包括屏蔽重复告警、屏蔽闪断告警等；

✧ **报表管理**

网络管理系统够针对 IT 资源的监控参数，根据管理人员的要求制定周期性的参数监控并产生相应的报表。从而使网管人员能够根据报表数据进行有效的分析，优化 IT 资源的使用、更新、维护。

报表主要包括二种类型：

◆ 实时性报表：当前设备的运行状态下，针对特定参数生成相应的报表清

单。如当前网络平台所有在线的 IT 资源列表。

- ◆ 周期性报表：针对某类或某类特定设备或资源参数，按照一定的时间周期进行参数变化跟踪，从而进行有效分析，以便于排除故障或优化资源。如，将核心交换机 1 天内的 CPU 占用率走势图产生报表进行分析能够准确判断出每天业务繁忙程度的时间规律。

✧ **网络设备配置、更新**

因为医院信息平台规模庞大，设备繁多，网络管理员的配置文件管理工作将十分繁重，如果没有好的配置文件维护工具，网络管理员就只能手动备份配置文件。这样就给网络管理员管理、维护网络带来一定的困难。

网络配置中心支持对设备配置文件的集中管理，包括配置文件的备份、恢复以及批量更新等操作，同时还实现了配置文件的基线化管理，可以对配置文件的变化进行比较跟踪。

5.5 平台安全体系设计

医院信息平台的安全体系设计，不仅要考虑平台本身，更应从整个医院信息化来全面进行考虑。在第 7 章安全保障体系中，将展开详细分析和描述。