10 安全

10.1 前提假设

本章节的前提假设条件如下：

假设一：RHIN 系统不支持从 POS 到 POS 直接发起的点到点的 PHI 等信息传输。

假设二：当将 PHI 等信息从 RHIN 系统下载到 POS 点上后，POS 将负责该信息的安全性。

假设三：和 RHIN 系统相连的 POS 系统都将遵循 POS 站点安全建设规范。

假设四：RHIN 系统下直接接入 POS 系统。本章节不考虑 RHIN 系统上下级互连的情况。

假设五：已建立 RHIN 系统 CA 认证体系或直接利用第三方 CA 认证体系。

10.2 安全方案目标

本安全方案的目标是支撑和保障区域卫生信息平台的信息系统和业务的安全稳定运行，防止信息网络瘫痪、防止应用系统破坏、防止业务数据丢失、防止卫生信息泄密、防止终端病毒感染、防止有害信息传播、防止恶意渗透攻击，以确保信息系统安全稳定运行，确保业务数据安全。

10.3 安全等级需求

基于健康档案的区域卫生信息平台所涉及信息包括：病人的基本健康信息，病人的诊疗数据，卫生资源数据等等。这些业务信息遭到破坏后，所侵害的客体是公民、法人和其他组织的合法权益。一旦业务信息遭到非法入侵、修改、增加、删除等不明侵害（形式可以包括丢失、破坏、损坏等），会对公民、法人和其他组织的合法权益造成影响和损害。程度表现为严重损害，即工作职能收到严重影响，业务能力显著下降，出现较严重的法律问题，较大范围的不良影响等。根据以上描述

我们可以确定基于健康档案的区域卫生信息平台业务信息安全保护等级为第二级。

表 10-1 业务信息安全分析

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

基于健康档案的区域卫生信息平台属于为国计民生、经济建设等提供服务的信息系统，其服务范围为区域范围内的普通公民、医疗机构等。该系统服务遭到破坏后，所侵害的客体是公民、法人和其他组织的合法权益，同时也侵害社会秩序和公共利益但不损害国家安全。客观方面表现的侵害结果为：（1）可以对公民、法人和其他组织的合法权益造成侵害（影响正常工作的开展，导致业务能力下降，造成不良影响，引起法律纠纷等）；（2）可以对社会秩序公共利益造成侵害（造成社会不良影响，引起公共利益的损害等）。根据《定级指南》的要求，出现上述两个侵害客体时，优先考虑社会秩序和公共利益，另外一个不做考虑。上述结果的程度表现为：对社会秩序和公共利益造成一般损害，即会出现一定范围的社会不良影响和公共利益的损害等，则业务信息安全保护等级为第二级。

表 10-2 系统服务安全分析

系统服务被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

信息系统的安全保护等级由业务信息安全等级和系统服务安全务安等级的较高者决定。所以，基于健康档案的区域卫生信息平台安全保护等级为第二级。

表 10-3 RHIN 安全等级

信息系统名称	安全保护等级	业务信息安全等级	系统服务安全等级
基于健康档案的区域卫生信息平台	第二级	第二级	第二级

但是，从总体上考虑到某些基本业务信息系统（Point Of Service，POS）的信息系统，比如疾控中心，其系统服务遭受破坏后，可能会对社会秩序和公共利益造成严重损害，即会出现较大范围的社会不良影响和较大程度的公共利益的损害等，所以其安全保护等级建议定为三级。但是由于本章主要考虑区域卫生信息平台的安全保障，所以其它 POS 系统的安全保障方法不做论述。

10.4 系统风险分析

10.4.1 信息和信息系统分析

信息和信息系统构成了 RHIN 的信息资产。基于健康档案的区域卫生信息平台的使用对象主要是医疗卫生人员，最终的服务对象是居民和患者。医疗卫生人员为了更好的为居民和患者提供可靠的、可及的、连续的医疗卫生服务，需要依赖平台提供的众多服务。

RHIN 平台中的业务数据的类型主要包括文档数据、操作型数据、辅助决策型数据。文档数据是以文档形式存在于平台中的临床和预防保健业务数据，例如检验报告、处方，传染病报告卡等。这些数据是结果数据。操作型数据一般是指平台从业务系统中采集、汇总、供实时业务查询和统计使用的数据。辅助决策数据是指存储在数据仓库中，以主题方式组织，是经过二次加工的历史数据。这些信息是需要安全保护的重点对象，其可用性、机密性和完整性均需要进行一定程度的保障。

RHIN 平台网络基础设施平台由内、外两大网络部分组成。外部网络对外收集和提供信息(向下级部门采集与提供信息，向上级数据中心报送信息)，内部网进行信息管理和系统开发。其网络拓扑示意图如下：

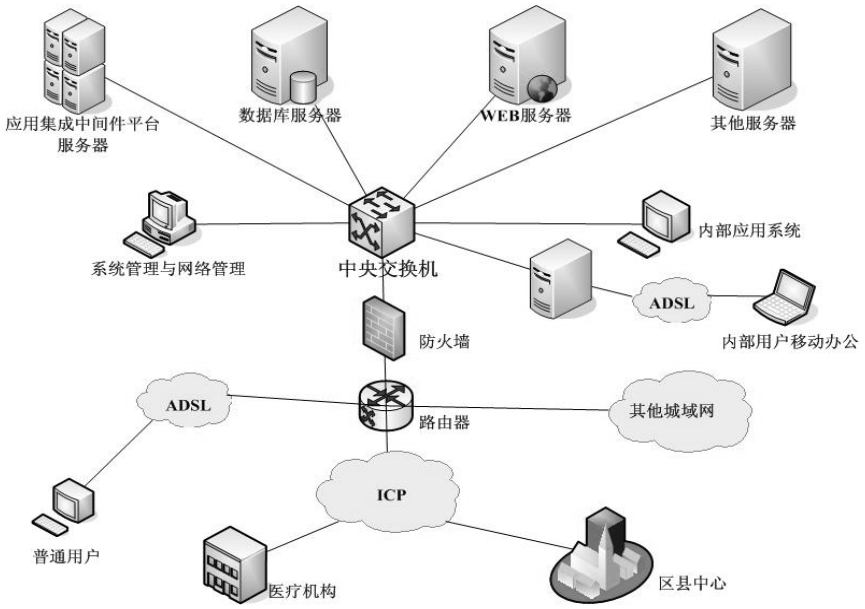

图 10-1 信息和信息系统分析

10.4.2 安全风险分析

我们之所以要解决安全问题，是因为信息网络存在被病毒、黑客攻击等各类安全威胁攻击的可能性，也就是说存在安全风险，并随时可能因此造成财产、时间、声誉上的损失，而根据安全风险的定义，安全风险的大小主要取决于以下四个方面：资产的价值、资产的脆弱性、面临的威胁程度，以及已经采取的防范措施。

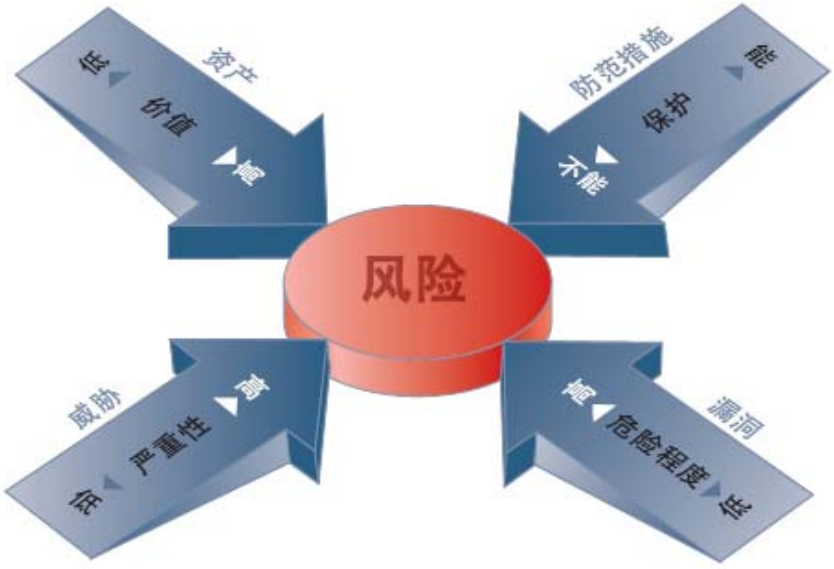

图 10-2 安全风险要素分析

也就是说，当一个系统具有了信息化的核心资产（有很重要的数据保存在服务器上，比如患者信息，），这些资产存在弱点和漏洞（比如承载这些信息的操作系统或数据库具有缓冲区溢出漏洞），又同时存在被安全威胁攻击的可能（比如黑客已经开发出了针对这种漏洞的蠕虫和攻击方法等），而且系统没有部署相应的防御手段（比如网络或主机入侵防御系统），那么就会导致安全风险，从而给系统造成损失。

因此，RHIN 平台的安全风险和这四个方面紧密相关，也只有同时解决好这四个方面的问题，才可能真正的确保 RHIN 平台的安全。

10.4.3 资产分析

在本网络中，数据中心数据库服务器、应用集成平台服务器和内部应用系统承载了关键的数据信息，需要进行重点的防护。此外，RHIN 数据交换系统也需要进行重点保护，以避免非授权访问和攻击等安全事故发生。

10.4.4 威胁分析

RHIN 平台面临的威胁主要来自于身份假冒、信息窃取、内容篡改、非法入侵、病毒侵袭等造成的破坏。

身份假冒、口令窃取威胁

身份鉴别是网络安全的基本要求，互联网拥有大量用户，系统很难分辨哪些是合法用户，哪些是非法用户，存在身份假冒等威胁。一旦医护人员或患者的身份被假冒，将影响到患者信息、医疗数据的安全性和隐私性。

信息窃取、数据泄漏、信息篡改威胁

RHIN 系统存在大量不宜公开的内部信息，如病人的健康信息、医疗记录等，互联网作为高度开放的网络，内部数据在传输过程中极易被窃取和监听，内部数据要面对高水平黑客和别有用心者，信息泄漏的威胁更大。而且由于 RHIN 担当了跨系统医疗健康数据交互的功能，一旦数据被篡改，其影响范围将会非常大。另外，随着便携式数据处理和存储设备，比如笔记本电脑、USB 存储介质的广泛应用，由于设备丢失而导致的 PHI 等数据泄漏途径也不可忽视。

恶意攻击和入侵威胁

RHIN 系统具有互联网连接，而且和多个区域卫生机构具有连接，其遭到恶意

攻击的风险更大，特别是为医疗机构和百姓服务的系统，允许从互联网上直接访问，虽然提高了服务范围，方便了大众，但是相对封闭的内部网络而言，也面临着更多来自互联网的威胁。若不能采用有效的入侵防御手段抵御恶意攻击和入侵，保持服务窗口的良好稳定运行，势必对系统的可用性造成威胁，影响政府形象。

病毒传播和扩散威胁

如今，病毒种类多、更新速度快，常常呈指数级的速度扩散，这将影响 RHIN 网络中的终端、服务器的正常运行。

结合RHIN应用的特点，下面总结出RHIN信息系统面临的主要具体威胁如下：

P, N, S, A, D

代码含义：P-1： P 代表威胁发生在物理层面；1 代表序号。

同样，N 代表威胁发生在网络层；S 代表威胁发生在系统层；A 代表威胁发生在应用层；D 代表威胁发生在数据层。

表 10-4 RHIN 信息和信息系统面临的主要威胁

标号	威胁描述	备注
P-1	雷击、地震和台风等自然灾难	
P-2	水患和火灾等灾害	
P-3	高温、低温、多雨等原因导致温度、湿度异常	
P-4	电压波动	
P-5	供电系统故障	
P-6	静电和外界电磁干扰	
P-7	通信线路因线缆老化等原因导致损坏或传输质量下降	
P-8	存储重要业务信息的介质老化或质量问题等导致不可用	
P-9	网络设备、系统设备及其他设备使用时间过长或质量问题等导致硬件故障	
P-10	攻击者利用非法手段进入机房内部盗窃、破坏等	
P-11	攻击者非法物理访问系统设备、网络设备或存储介质等	
P-12	攻击者采用在通信线缆上搭接或切断等导致线路不可用	
N-1	黑客通过 Internet 连接对 EHR 等信息进行破坏和非授权访问	
N-2	黑客或内部人员从 POS 点通过网络连接对 RHIN 平台进行攻击或非授权访问	
N-3	黑客或内部人员从和 RHIN 平台连接的第三方网络通	

	过网络连接对 RHIN 平台进行攻击或非授权访问	
N-4	RHIN 数据中心中的服务器感染蠕虫、或者被种植木马、后门程序而导致向外发起的非法网络连接	
N-5	攻击者利用分布式拒绝服务攻击等拒绝服务攻击工具，恶意地消耗网络、操作系统和应用系统资源，导致拒绝服务	
N-6	攻击者利用网络协议、操作系统、应用系统漏洞，越权访问文件、数据或其他资源	
N-7	攻击者利用网络结构设计缺陷旁路安全策略，未授权访问网络	
N-8	攻击者和内部人员利用网络扩散病毒	
N-9	攻击者截获、读取、破解通信线路中的信息	
N-10	蠕虫通过 POS 连接或第三方外部网络连接扩散到信息平台	
N-11	蠕虫通过内部网络连接扩散到信息平台	
N-12	利用网络设备、防火墙的漏洞的蠕虫和入侵攻击导致网络基础设施瘫痪	
S-1	内部人员下载、拷贝软件或文件，打开可疑邮件时引入病毒	
S-2	内部人员利用技术或管理漏洞，未授权修改 EHR 等系统数据或修改系统程序	
S-3	服务器或客户端计算机因为未能及时应用最新补丁程序而导致被入侵或感染蠕虫	
S-4	由于系统配置安全问题比如系统用户、数据库用户的口令质量和更改策略，对文件和资源共享没有进行适当安全保护，而可能导致的安全攻击	
S-5	对系统管理员和用户进行身份猜测和假冒攻击	
S-6	攻击者或内部人员对其进行过的非法系统访问行为抵赖	
A-1	内部人员，如区域卫生信息平台工作人员对电子病历等信息进行越权访问	
A-2	POS 机构、外部机构人员、外部攻击者对电子病历等信息进行越权访问	
A-3	内部人员，如区域卫生信息平台工作人员对电子病历等信息进行破坏	
A-4	POS 机构、外部机构人员、外部攻击者对电子病历等信息进行破坏	
A-5	攻击者通过中间人攻击、假冒等手段对上传到区域卫生信息平台的 EHR 等信息进行篡改和假冒攻击	
A-6	攻击者或其他越权访问或操作人员对自己的行为抵赖	
A-7	EHR 等等信息在 POS 到区域卫生信息平台传输过程中，或者在区域卫生信息平台内部网络传输过程中被窃听	
D-1	攻击者截获、读取、破解介质的信息或剩余信息，进行电子病历等敏感信息的窃取	
D-2	内部人员通过移动介质或移动计算设备存储电子病例等敏感信息，由于介质或设备丢失而导致信息泄漏	

D-3	内部人员或攻击者利用邮件、Web、打印、拷屏、拷贝等方式和手段将电子病历等敏感信息传输到 RHIN 平台外部。	
D-4	由于物理、恶意代码、攻击、误操作等各种原因导致的数据破坏和丢失	

10.5 安全需求

RHIN 中承载着重要的病人的基本健康信息，病人的诊疗数据，卫生资源数据等等。这些业务信息遭到破坏后会带来严重的后果，所以本方案的核心是保障 RHIN EHR 等相关数据信息免受各种形式的窃取、破坏、篡改。为了实现这个目标，我们需要从物理、网络、系统、应用、数据等多个层面部署安全保障措施，达到安全目标。同时，本安全建设还需要满足国家相关安全要求，比如等级保护的要求。

10.6 安全方案框架和安全风险管理

RHIN 信息安全保障体系覆盖信息系统安全所要求的各项内容，包含信息安全战略、信息安全规范和标准、信息安全管理、信息安全运作及信息安全技术五部分，符合区域卫生信息平台的业务特性和发展战略，满足信息安全要求。

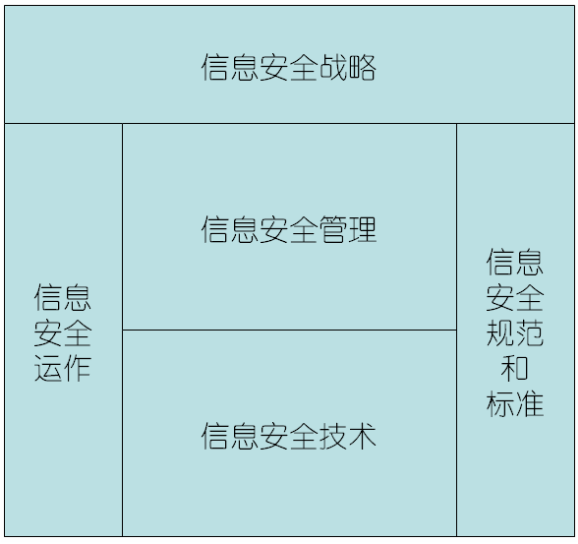

图 10-3 安全方案框架

1） 信息安全战略：信息安全战略以风险管理为核心理念，是 RHIN 信息安全保障体系的核心，是信息安全工作的原则、宗旨、指导，为信息安全工作指明了方向；

2） 信息安全规范和标准：信息安全规范与标准体系是是风险管理理念的逐层细化和落实，包含信息安全管理、运作、技术体系标准化、制度化后形成的一整套对信息安全的管理规定；

3） 信息安全管理：信息安全管理体系框架是从企业管理的层面出发，为实现信息安全战略而设置的组织架构、管理体系、宣传教育、审计制度等一系列相关管理措施；

4） 信息安全运作：是是基于风险管理理念的信息安全日常运作模式及其概念性流程在各个对象层次上的实现；

5） 信息安全技术：采用成熟先进的技术和控制手段，实现各技术层面的风险防范和控制。

从技术体系上，RHIN 需依托公钥基础设施所提供的数字证书等服务，实现网络安全、系统安全、应用安全、数据安全，并且基于关联分析技术建立集成的安全管理平台，实现网络、系统、数据等层次安全防护的数据交换和关联分析，并落实安全管理和运维策略，形成一体化的安全防护体系。同时，为 HIAL 层提供需要的安全和隐私保护服务。RHIN 安全支撑平台的总体系统结构如图所示。

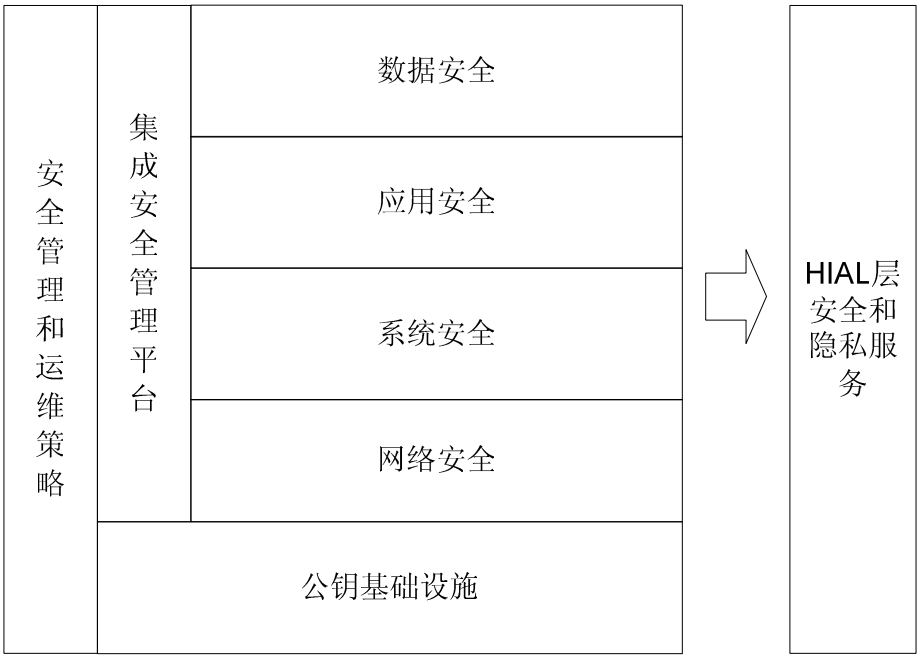

图 10-4 RHIN 安全方案总体结构

传统的安全保护方案往往是自成体系，缺乏整体的、优化的和分层的安全防护概念，缺乏整体安全风险的控制能力，在安全防护工作中的管理维护、安全事件处理效率和相关安全方案资源整合等方面都需要进一步的改进。比如在传统的安全防范体系建设中，往往片面地考虑对某类威胁的防御措施，比如防病毒、防入侵；或者仅考虑对某类脆弱性的保护，比如补丁管理，网络准入控制等等；这类安全建设的出发点是头痛医头，脚痛医脚，没有从安全风险管理的整体高度把握安全建设的核心，其结果是形成大量安全孤岛，各种防御措施片面、割裂，没有呼应关系，造成管理混乱、运维复杂，无法明确安全投入回报，无法明确安全管理绩效。

因此，我们需要从各种安全风险要素的关系上出发，明确资产、威胁、脆弱性之间的关系，并且基于三者之间的关联关系，在安全控制手段上实现有限的技术关联，并且通过一个集中的平台呈现出整体安全风险状况，从而实现安全风险管理方法论的落实，对安全风险实现合理控制和有效展现。

根据 GB/T 18336:2001《 信息系统安全性评估准则》，风险各核心要素的关联关系如下：

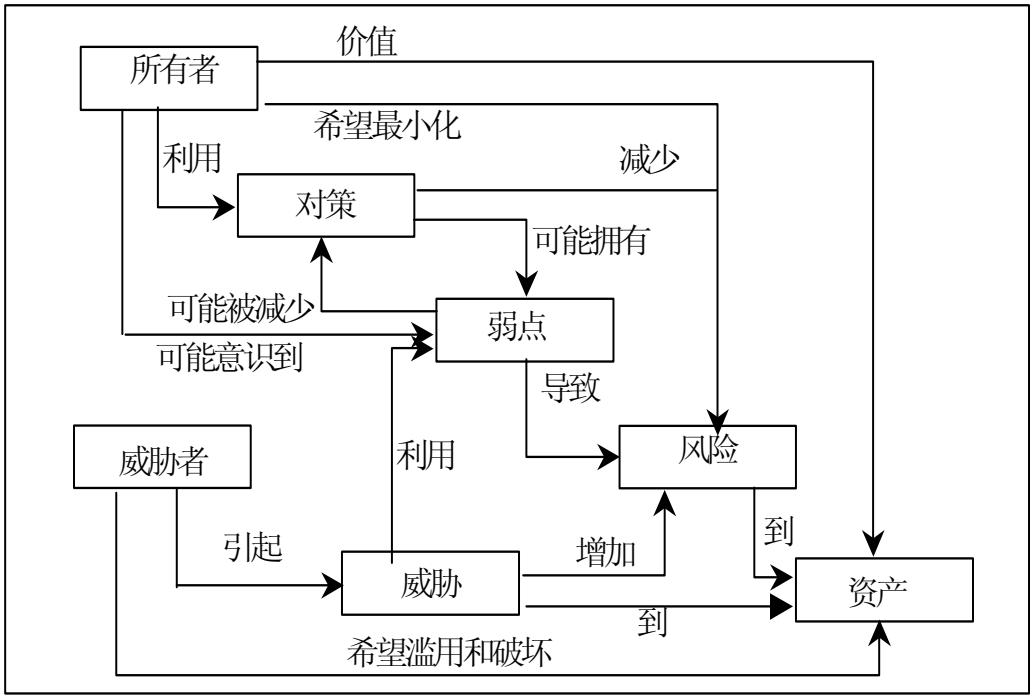

图 10-5 安全风险核心要素的关联关系

一个完整的信息安全保障体系需要明确资产目前面临的威胁，并且结合威胁

对弱点的利用情况，有针对性地进行威胁的防范和脆弱性的保护，从而达到有的放矢的防护目的，将关键资源投放到重点需要防护的资产上，增强安全性，同时能够大大简化管理和维护的复杂程度。

信息安全保障体系建设的生命周期如下图所示：

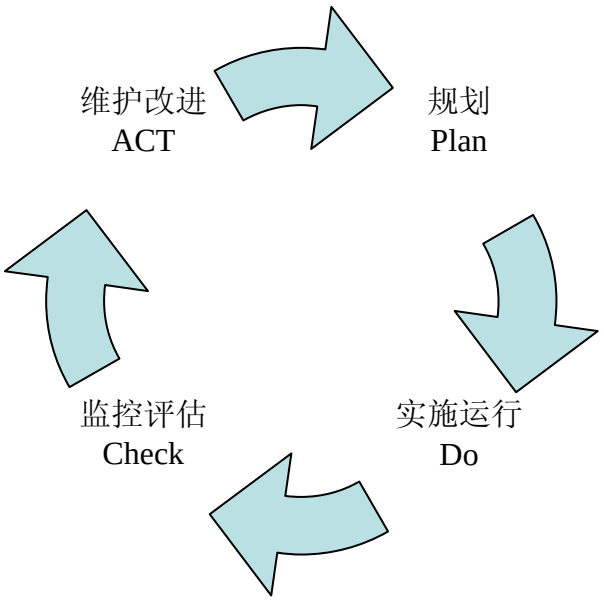

图 10-6 信息安全保障体系建设的生命周期

其中，规划（Plan）阶段定义信息安全保障体系的目标和范围，定义信息安全保障体系的战略和架构，识别主要的安全风险和控制措施，并制订信息安全保障体系的实施蓝图规划；

实施和运行（Do）阶段定义风险控制计划，针对相关的风险控制目标定义具体的控制措施，并加以实施；

监控和评估（Check）阶段对残留风险进行监控，并对信息安全保障体系的有效性进行周期性的评审；

维护和改进（Act）阶段对信息安全保障体系进行调整，并进行持续的改进。

为了更好的保障 RHIN 平台的安全性，全面地管理安全风险，形成统一的安全保护管理以及高效率的安全事件处理机制，我们需要形成统一的安全保护工作机制，建立整体的安全防护体系，将所需的人力、流程和设备有效地整合并组织在一起，为面向服务的 RHIN 平台提供了集中化的安全管理架构。该体系是根据 PDCA（Plan，Do，Check，Act）闭环管理理念，为了更好的满足安全的需求，建设一套符合自身发展特点的安全管理体系。

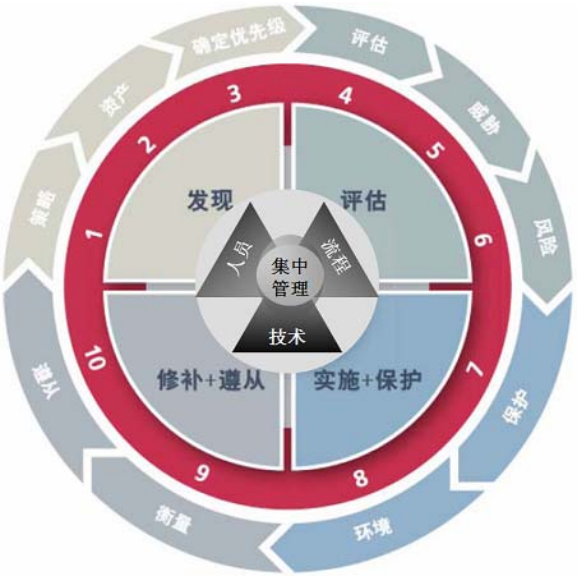

图 10-7 整体安全风险管理体系

该体系由以下的功能单元组成了一个整体的、可操作的、可衡量的、可考核的以及可持续保障的面向业务系统安全风险管理的体系架构。

该体系融入了人员、管理流程和安全技术三方面，其中人员可以通过这个管理体系实现简化的安全管理，提高人员的管理效率；在管理流程方面，集成业务系统安全流程和工作流程，更好的服务于业务系统。如某系统出现安全威胁时，通过我们的集中管理平台可以迅速发现该风险并根据风险优先级，将高优先级的风险通过工单系统发送工单到相关安全管理员，安全管理员在根据工单完成相关的修补工作后，管理系统可以自动验证工单修补状态，实现一个闭环的工单管理工作流程。在技术方面，通过采用集成的和开放的平台架构，可以通过安全产品间的集成发挥更大的安全防护能力和保护已有投资。

该体系是一个可持续的安全防护过程，原有系统发生改变或增加新的系统时都可以按照整体安全管理体系来实施安全保护方案，提高了整体的和各业务平台的安全防护能力。根据上述的流程对业务系统评定其优先级，确定可承受的风险，实施适当的保护措施，并衡量安全法规遵从情况，保障面向服务平台的安全性。

10.7 HIAL中提供的安全和隐私服务说明

区域卫生管理层和辖区卫生机构层之间通过区域卫生信息应用访问层（HIAL）来进行信息交互，以实现健康档案的互联互通性，信息访问层所提供的服务主要

包括两个方面：一方面提供通信总线服务，如消息传输服务、消息路由等；另一方面提供应用软件通用的系统管理功能，如安全管理、隐私管理、应用审计等。

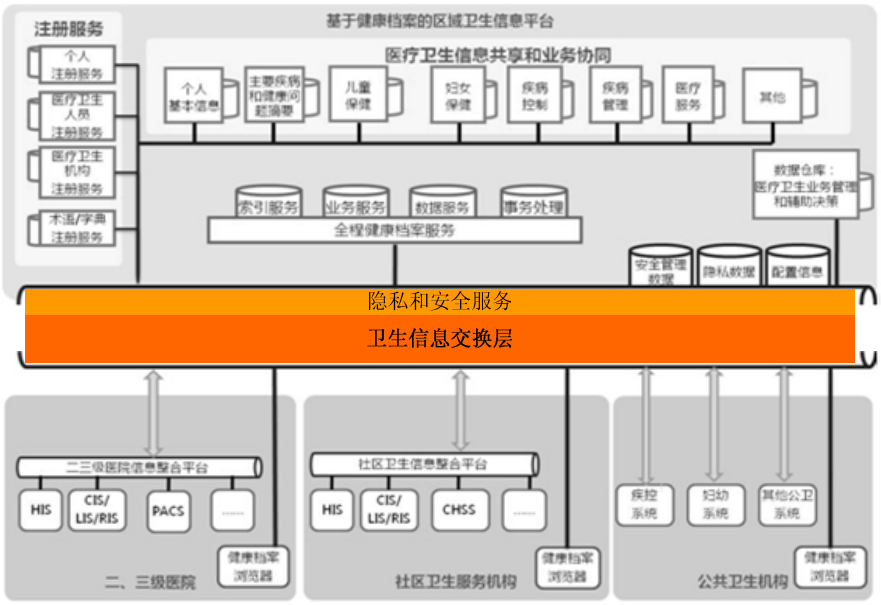

图 10-8 HIAL 层次示意

HIAL 中提供的隐私和安全服务如下所示：

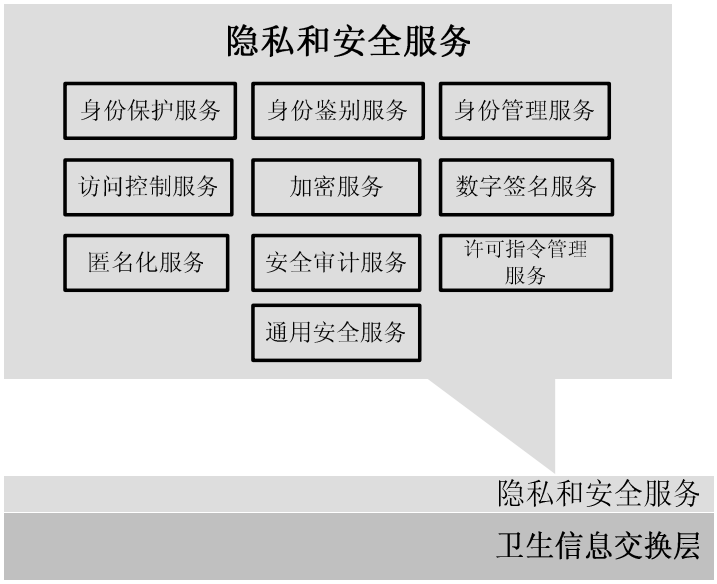

图 10-9 HIAL 提供的隐私和安全服务示意

隐私保护及信息安全是区域卫生信息平台所要重点解决的问题。主要体现在如下几个方面：

1).身份保护服务

这项服务将一个患者或居民的身份解释为一个健康档案标识符。患者或客户通常由一个如社保卡号码的通用标识码来标识，这样的卡号关联到每个包含健康档案标识域中的健康档案标识符。健康档案标识符是一个受保护信息，只有交换层之上平台系统才能知道。

2).身份鉴别服务

这项服务验证用户的身份。这项服务是在执行医疗卫生应用与区域卫生信息平台之间的事务的场景下被调用，以验证参与事务用户的合法性。

3).身份管理服务

这些是面向更高层次服务提供的基础服务，例如用户注册、认证、授权，其中包括用户的唯一标识、查找用户的标识、挂起/取消用户访问权。

4).访问控制服务

这些服务确定对信息平台应用功能的基于角色的访问权限。这些服务还提供配置和管理用户及角色访问功能和数据的授权，比如根据病种、角色等多维度授权。

5).加密服务

加密服务包括三个方面内容。一是密钥管理服务：创建和管理数据存储的加密密钥；二是数据库加密服务：加密和解密数据库表中的数据字段（列）和记录（行）以保护健康档案以及信息平台中处于使用状态的其它保密的关键系统数据；三是数据存储加密服务：加密和解密文件和其它数据块，用于保护在联机存储、备份或长期归档中的数据，以实现关键信息（字段级、记录级、文件级）加密存储。

6).数字签名服务

数字签名由医疗卫生应用程序的用户创建，以确保临床数据的不可否认性，这样的临床数据如：数据文件、报告、记录中的字段域、安全声明、XML 文档，包括被转换为 XML 文档的 HL7 消息或对象中的元素。这项服务在生成签名之前先验证数字证书没有被撤销。

7).匿名化服务

这些服务保护患者的隐私和安全，确保在信息平台中以及提供正常医疗服务以外的（例如医疗保险、管理以及某种形式的研究）传递中使用的患者资料不向

非授权用户透露患者的身份。

8).安全审计服务

这些服务提供对每个事务所涉及到的系统、用户、医护工作者、患者/居民、健康数据等等的报告功能。这些服务对于满足其他业务需求，如系统管理、事务监控、记录重要的与隐私和安全有关的事件等，也是至关重要的。

9).许可指令管理服务

许可指令管理服务转换由立法、政策和个人特定许可指令带来的隐私要求，并将这些需求应用到区域卫生信息平台环境中。在提供访问健康档案或经过区域卫生信息平台传输健康档案之前，这些服务应用于健康档案以确定患者或个人的许可指令是否允许或限制健康档案的公开。这些服务还允许信息平台用户管理患者/居民的特定许可指示，例如根据法律法规的需要和允许，阻止和屏蔽某一医疗服务提供者访问健康档案或者在紧急治疗情况下不经许可直接开放健康档案。

10). 通用服务

通用服务包括在网络安全、系统安全、数据安全，以及在网络设计和系统设计层次实现的各种安全和可用性服务，比如网络安全隔离、网络入侵防御和监测、网络恶意代码防护、数据安全存储、恢复和销毁等等。

10.8 安全技术建设方案

10.8.1 安全域划分

一般规划的卫生信息平台以卫生局为核心，各医院、社区卫生服务中心等卫生单位接入，逻辑分布如下：

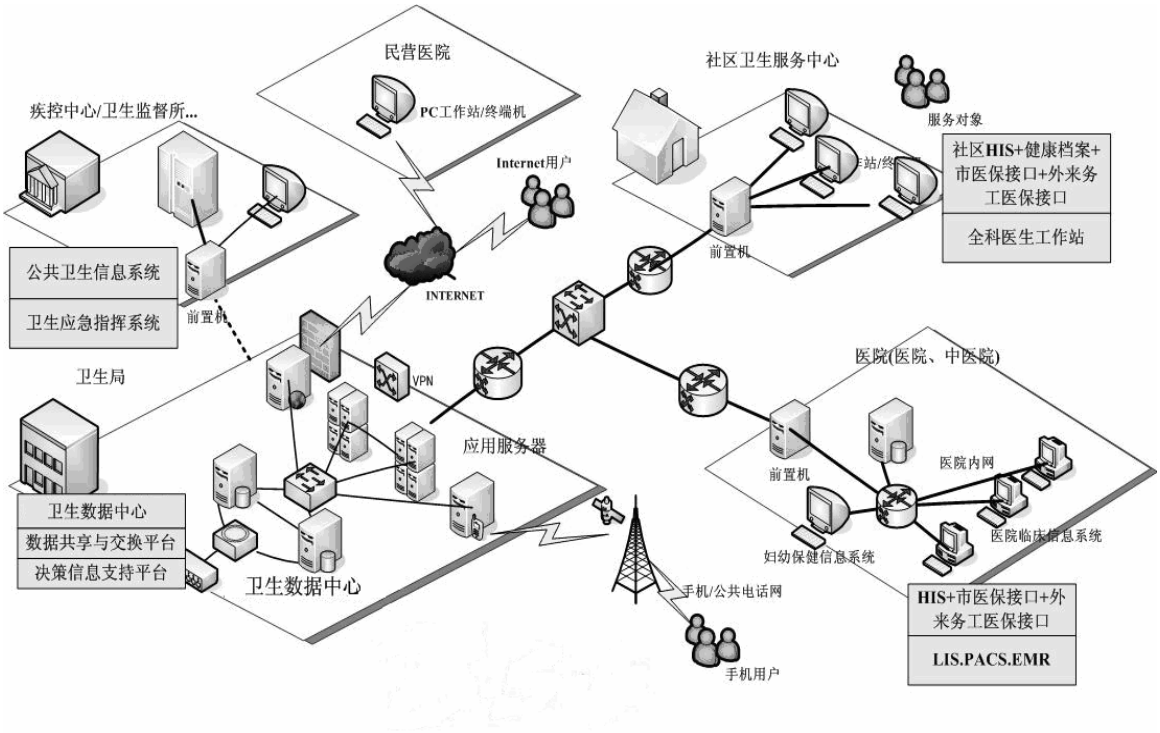

图 10-10 区域卫生信息平台逻辑分布图

通过网络分区，明确不同网络区域之间的安全关系，也可以对每一个区域进行安全的评估和实施，不必考虑对其他区域的影响，保障了网络的高扩展性、可管理性和弹性。达到了一定程度的物理安全性。

按照 RHIN 应用系统信息和应用分类的安全需求，可以将 RHIN 平台划分为外部服务区域、卫生机构信息交换区域、内部业务信息处理区域、行政办公区域、管理区域。对于涉及国家秘密的信息，RHIN 需要专门建设政务内网承载，并且与外部网络物理隔离。

RHIN 处理的信息中可能涉及到一部分涉密信息，需要建设专门的内网来处理，并且和外网以及 Internet 物理隔离。本章主要讨论 RHIN 在互连互通情况下的安全建设，内网安全建设可参照其中适用的部分。具体安全域划分如下图所示。

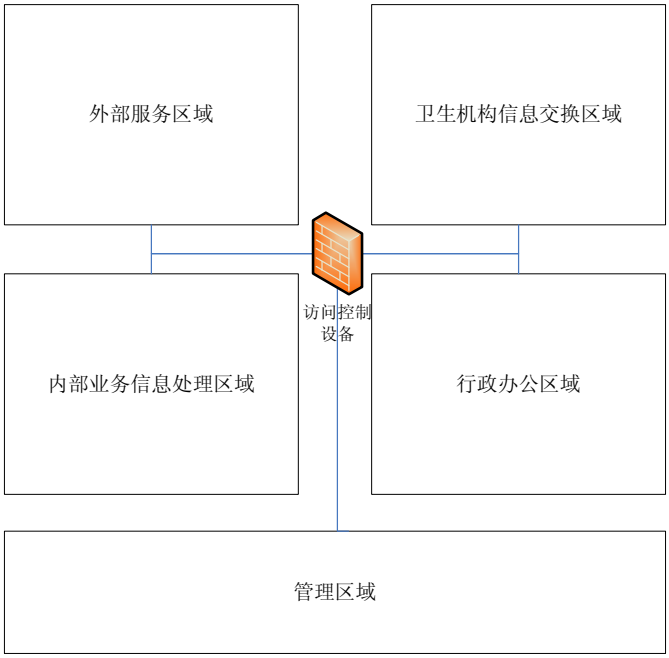

图 10-11 安全域划分图

1） 外部服务区域

外部服务区域包含了提供给公众的服务设施，比如提供健康信息查询的 Web 服务器、个人信息注册服务器等。其允许公众直接访问。

2） 卫生机构信息交换区域

该区域提供对各 POS，如医院、社区卫生机构、疾控、妇幼以及其它卫生系统的数据交换服务。根据和 POS 连接方式方式的不同，应当采取不同方式的数据安全和安全访问控制以及入侵防范、病毒隔离措施。仅允许经授权的 RHIN 系统使用人员和 POS 系统用户访问。

3） 内部业务信息处理区域

内部数据是仅允许 RHIN 系统内部人员访问的数据。内部数据处理区用来承载处理内部信息的 RHIN 应用系统及其数据库，处理内部的业务。仅允许经授权的 RHIN 系统使用人员访问。

4） 行政办公区域

行政办公区域主要是指 RHIN 内部办公系统区域，承载各种办公应用以及办公用客户端计算机，提供办公用邮件、工作流、内部 Portal 等。本章主要关注业务安全，对行政办公区域的安全防护不做深入讨论。

5） 管理区域

管理区域面向 RHIN 系统安全管理人员、承载网络和安全管理中心等，为全网的 RHIN 系统提供统一的资源管理、权限管理、策略管理、审计管理、入侵防范、恶意代码防范、数据安全和安全可视化管理等。为所有的 RHIN 系统用户，提供共性安全支撑服务，如防恶意代码库升级、入侵库升级、漏洞管理、统一身份鉴别和权限验证等。仅允许安全管理人员访问。

10.8.2 安全区域的等级划分

根据各区域承载的信息和信息系统的重要性不同，将各个区域的安全等级细化如下：

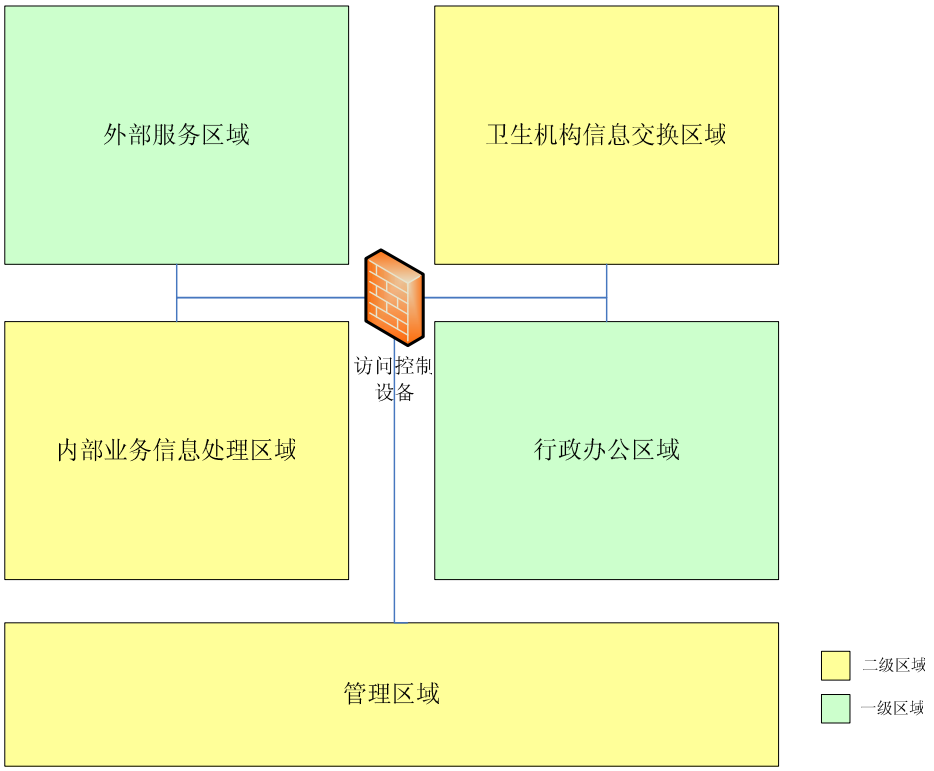

图 10-12 安全域等级划分图

10.8.3 物理安全

RHIN 信息系统在物理层面临的主要具体威胁见表 10－4。物理安全主要是指机房和办公场地的安全性，主要应考虑以下几个方面内容。

1). 物理位置的选择

- 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；

• 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。（未符合此要求项，则须符合防雷击和防水和防潮要求项）。

2). 物理访问控制

• 机房出入口应有身份鉴别机制（人工或电子方式），鉴别进入的人员身份并登记在案；

• 进入机房的来访人员应有有关方面的授权并由专人陪同，限制和监控其活动范围。

3). 防盗窃和防破坏

• 应将主要设备放置在机房等物理受限的范围内；

• 应注意对机房、线缆等重要区域做防鼠措施；

• 应对服务器、网络设备等关键设施进行固定，并设置明显的标记；

• 应将通信线缆铺设在隐蔽处，如铺设在地下或管道中等；

• 应对使用的介质（诸如：存有信息的光盘、软盘、移动硬盘、纸质文档等）分类标识，存储在介质库或档案室中；

• 应安装必要的防盗报警设施，以防进入机房的盗窃和破坏行为；

• 存有重要信息的设备或存储介质携带出工作环境时，应指定专人负责和内容加密。

4). 防雷击

• 机房建筑应设置避雷装置；

• 应设置交流电源地线。

5). 防火

• 应设置灭火设备和火灾自动报警系统，并保持灭火设备和火灾自动报警系统的良好状态；

• 机房内不应使用或堆放易燃物品或材料；

• 有条件的区域应使用机房专用自动灭火装置。

6). 防水和防潮

• 水管安装，不得穿过屋顶和活动地板下；

• 应对穿过墙壁和楼板的水管增加必要的保护措施，如设置套管；

• 应采取措施防止雨水通过屋顶和墙壁渗透；

• 应采取措施防止室内水蒸气结露和地下积水的转移与渗透。

7). 防静电

- 应采用必要的接地防静电措施；
- 机房地板铺设应采用机房专用防静电活动地板。

8). 温湿度控制

- 应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内；
- 温、湿度自动调节设施宜具备断续电自动重启机制；
- 应于关键场所配备温湿度监控设施；
- 有条件的地区应对温、湿度自动调节设施做冗余备份；
- 有条件的地区可采用关键场所的整体环境监控系统。

9). 电力供应

- 计算机系统供电应与其他供电分开；
- 应设置稳压器和过电压防护设备；
- 应提供备用电力供应（如：UPS设备、发电机等）；
- 应对UPS等设备做定期维护并保证此类设备的负载在合理范围内；
- UPS设备应能够于特定状态下（如启动、中断、故障等）向管理人员发出告警（如短信、声音方式）；
- 关键设备（如：核心服务器、核心交换机等）应保证电力供应来源的冗余，如：由不同供电途径作为电源输入。

10). 电磁防护

- 电源线和通信线缆应隔离，避免互相干扰；
- 机房区域应远离强电磁和辐射源。

10.8.4 网络安全

结合RHIN网络的特点，总结出RHIN信息系统在网络层面临的主要具体威胁。（见表10－4）：

在HIAL层次，该部分实现的隐私和安全服务主要包括：通用安全服务、访问控制服务、加密服务、安全审计服务。

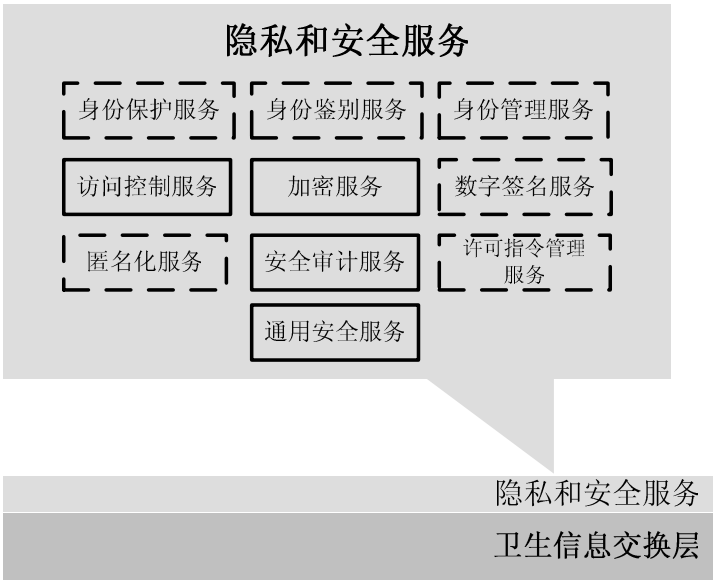

图 10-13 HIAL 在网络层次提供的隐私和安全服务

在网络安全建设中，应该考虑如下几个方面的安全保护措施：

1). 网络基础架构安全

该部分包括网络结构的设计和容量，网络设备和关键设施的安全保护和使用审计等。网络结构设计和容量考虑主要应对网络按照重要性进行合理分区，并且确保关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要，以及保证接入网络和核心网络的带宽满足业务高峰期需要；以上内容在网络建设章节已经有所考虑，此处不再赘述。网络设备安全主要应考虑对网络设备访问的安全性控制以及网络设备本身的安全考虑，比如及时发现网络设备存在的安全漏洞，并且防范攻击等等。尤其是当网络中存在无线接入设备的时候，一定要对无线接入设备的安全性进行评估和控制。

2). 网络安全控制

该部分包括网络访问控制，网络入侵防御等主要控制措施，即首先保证网络访问行为合理可控，然后再对网络中的一些非法行为进行识别和阻挡。

网络访问行为合理可控包括：能够根据用户、网络会话状态对通过网络对 RHIN 资源的访问行为进行明确的允许和拒绝；能够对内部用户未经允许私自连接到外部网络的行为进行识别等。能够对内部服务器和计算机由于感染蠕虫、或被种植木马后门程序而导致的向外非法连接进行识别和阻断。

网络非法行为识别和阻拦包括对针对 RHIN 网络和系统的蠕虫木马攻击、拒绝

服务攻击、入侵行为等进行识别和拦截，保障 RHIN 业务的安全稳定运行。

结合上述要求，在 RHIN 的网络中需要进行如下安全控制措施的部署：

1). 防火墙以及其它访问控制措施：

本类产品在边界上针对信息系统的网络数据流入/流出提供过滤和保护，目的是阻止安全域外部连接的非授权进入内部，以及通过网络手段阻断特定的内外连接。

在 RHIN 和外部网络的边界处应部署防火墙设备，能够根据会话状态信息、应用层协议、访问发起用户、被访问资源等进行访问控制规则设置，保证通过网络边界的会话是得到一定控制的。同时，为了保证整体安全性，防火墙设备自身应具备高度的安全性。同时，在 RHIN 和各个 POS 之间，以及存在不同安全等级的系统之间互联的边界处也应该考虑采用防火墙、VLAN 划分等安全访问控制措施。

2). 网络入侵防御和网络入侵检测设备：

网络入侵防御设备（Intrusion Prevention System，IPS）在网络入侵行为进入被保护网络之前通过报警、阻断等措施为信息系统提供防护，目的是对网络入侵行为进行阻止。同时，在某些网段需要采用网络入侵检测系统(Intrusion Detection System，IDS)，即针对网络入侵进行监测，它可以自动识别各种入侵模式，在对网络数据进行分析时与这些模式进行匹配，一旦发现某些入侵的企图，就会进行报警。目的是通过对网络入侵的检测，弥补防火墙等边界安全产品的不足，及时发现网络中违反安全策略的行为和被攻击的迹象。

网络入侵防御设备对蠕虫木马攻击、拒绝服务攻击、入侵行为进行识别，并且进行实时拦截。在 RHIN 和外部网络、POS 的边界部署网络入侵防御设备能够对进入 RHIN 的网络请求进行预先阻断，避免进入内部网络。在 RHIN 数据中心区域前部署网络入侵防御设备，保证不论攻击源于何方，包括外部网络和内部网络，均能够对核心资源进行有效保护。在 RHIN 数据中心等高数据并发的区域，为了保障不对关键业务的访问造成影响，网络入侵防御设备应采用专用硬件芯片架构，具有高处理能力。另外，网络入侵防御设备还需要对出入被保护区域的数据都进行检测，达到双向防范的目的。

为了简化部署，节约投资，建议在各区域卫生信息平台采用高端口密度的入侵防御设备同时实现入侵防御和入侵检测的功能，即对于关键链路实现串行接入对入侵实现实时阻断，同时采用同一台设备的其它端口对于其它网络采用端口镜像

的方式接入进行实时入侵检测。

另外，为了对网络设备的安全性进行保障，RHIN 应部署漏洞管理系统统一对 RHIN 中的安全漏洞进行发现、报告和处理跟踪。在网络安全方面，RHIN 需要采用漏洞管理系统对网络设备的配置安全如口令复杂度，安全漏洞状况等进行评估，并出具报告。可以和后续的主机系统漏洞管理集成在一个产品中实现。

上述安全控制措施在 RHIN 中的部署方式如下图所示：

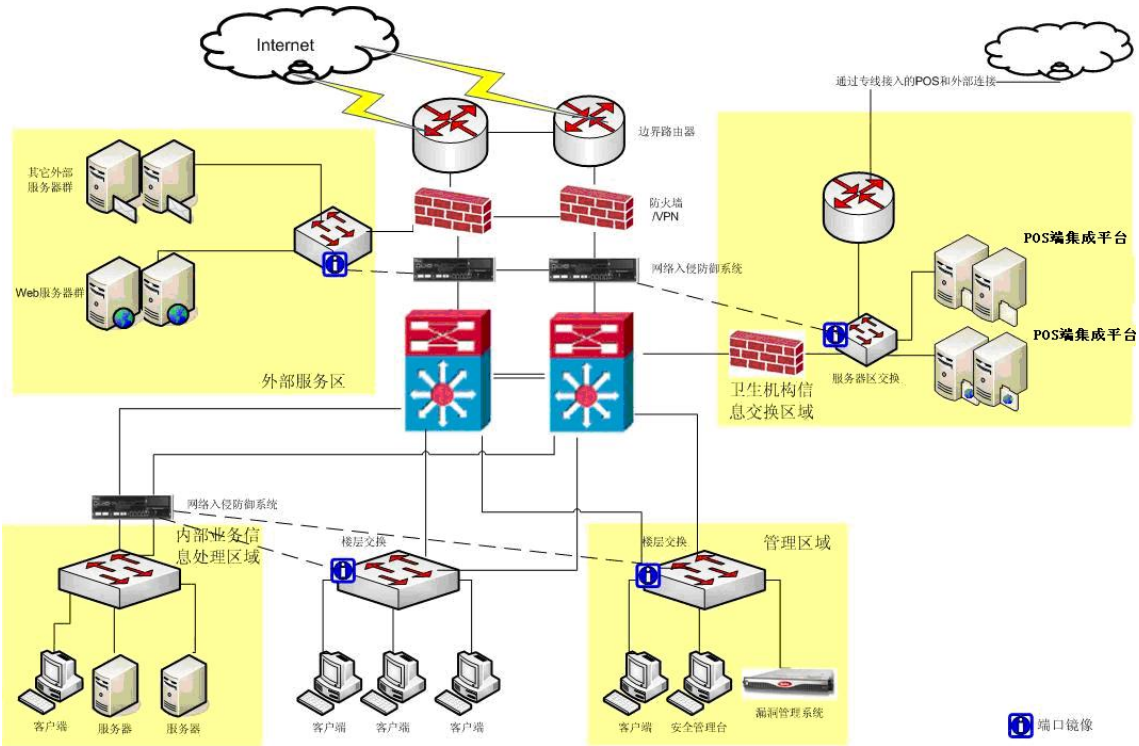

图 10-14 RHIN 网络层次安全部署示意图

首先，在 Internet 接入区域，部署防火墙和网络入侵防御设备。在大规模的数据中心，当有冗余性要求的时候可以部署双机进行 Active-Active 模式的负载均衡和备份。

其次，在通过专线接入的 POS 和外部连接区域和内部网络连接中间，部署防火墙，进行访问控制保护。同时，可以根据需要和物理位置条件，采用 Internet 接入区域部署的网络入侵防御设备的额外端口对本区域进行串行的网络入侵防御，或者仅通过端口镜像等方式实现对该区域的网络入侵检测分析。

第三，在为外部用户提供服务的外部服务区前段，可以根据需要和物理位置条件，采用 Internet 接入区域部署的网络入侵防御设备的额外端口对本区域进行串行的网络入侵防御，或者仅通过端口镜像等方式实现对该区域的网络入侵检测分

析。

第四，在存储和处理核心关键数据的数据中心服务器前段，单独部署网络入侵防御系统，避免通过各种途径进行的入侵和蠕虫传播。同时，该网络入侵防御系统同样可以利用额外的端口进行其它网段的入侵防御或入侵检测。

第五，在管理区域部署漏洞管理系统，对网络设备、主机和桌面计算机进行漏洞扫描和风险分析。为了便于管理，漏洞管理系统基于 RHIN 管理架构对资产进行分组并分配相关责任人，一旦发现某信息资产存在安全漏洞，即给相关责任人下发工单并对处理结果进行跟踪，保证问题得到及时处理。

3). 可用性保护的考虑

为了保障网络的可用性，接入网络进行安全保护的防火墙和网络入侵防御设备必须具有失效开放、失效关闭、断电保护等机制。同时，在非对称路由环境下，安全设备需要支持对网络会话的安全检测和入侵阻断。

10.8.5 系统安全

结合RHIN系统的特点，总结出RHIN信息系统在系统层面临的主要具体威胁。（见表 10－4）

在 HIAL 层次，该部分实现的隐私和安全服务主要包括：通用安全服务、身份鉴别服务、访问控制服务、安全审计服务。

在系统安全建设中，应该考虑如下几个方面的安全保护措施：

- 系统漏洞管理

系统漏洞管理和本文网络安全部分中所述的漏洞管理的目的相同，重点在于 IT 资产的发现和管理、漏洞评估、补救管理和策略评估结果。发现资产并评估资产的重要性，并且能够前瞻性地处理和识别漏洞；并实施基于资产的补救措施，评估并报告安全策略的符合性。

- 系统安全保护

系统安全保护重点在于通过附加于被保护系统之上的安全软件或补丁程序，对系统已知及未知的弱点进行保护，对蠕虫、病毒、木马等恶意代码进行防范。当由于某些关键系统之上应用软件兼容性或变更管理的原因导致无法应用补丁程序的时候，也需要考虑对关键系统的安全保障措施。

• 身份鉴别和安全审计

应对登录系统的用户进行身份标识和鉴别，并且其身份标识应具有不易被冒用的特点。登录失败时，可采取结束会话、限制非法登录次数和自动退出等措施；同时应该对系统操作进行审计，内容包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；应保护审计记录，避免受到未预期的删除、修改或覆盖等。

结合上述要求，在 RHIN 中需要进行如下系统安全控制措施的部署：

1). 漏洞管理系统

根据 Gartner 调查报告，安全漏洞一般可以分为两类：配置漏洞和系统漏洞。配置漏洞是指由于默认配置、误配置等导致的安全隐患；而系统漏洞则是指由于系统及其依赖的子系统在产品开发中的代码问题而导致的安全隐患。这两类漏洞都需要进行及时发现和完善的管理，避免系统成为黑客、蠕虫等攻击的目标。

漏洞管理系统可以进行资产分组、分类和优先级划分，模仿黑客的行为模式，协助 RHIN 找出网络中每一台主机、网络服务，以及相关信息与弱点，以了解整个网络架构的变动状况，是否影响或威胁 RHIN 的安全。并且通过定义工作流模版规则，它能自动从发现的弱点产生修补问题票单，通过邮件自动发送给相关的安全管理员，并且跟踪管理员的修补过程，若管理员及时修复，它能够进行确认并自动关闭该问题票单；若该弱点没有在规定时间内修补，则会发出报警，提醒管理员需要及时修补该弱点。

2). 主机安全软件

主机安全软件能够对包括客户端计算机和服务器在内的系统进行安全加固和威胁防范，包括防恶意代码，防入侵等等。防病毒类产品提供对计算机病毒的防治，防护侧重于防护本地计算机资源。计算机病毒防治产品是通过对内容或行为的判断建立系统保护机制，目的是预防、检测和消除计算机病毒。

由于新的病毒层出不穷，尤其是在 Windows 平台上的恶意代码更是泛滥肆虐，所以主机安全软件应当对于新病毒具有一定的主动防御机制，比如对系统目录的保护、防止蠕虫经常利用的溢出类型的攻击等等，即具有主机防入侵功能。主机防入侵类产品对已经抵达主机的数据进行监测，从主机或服务器上采集包括操作系统日志、系统进程、文件访问和注册表访问等信息数据，并根据事先设定的策

略判断数据是否异常，从而决定采取报警、控制等措施，目的是对入侵主机行为进行发现和阻止。

此外，主机安全软件应当具有自动更新机制，以便于应对随时出现的新的威胁。

3). 系统信息审计软件

安全审计类产品针对信息系统的活动信息进行审计记录及分析，目的是通过安全审计挖掘安全事件，并加以分析，得到相关信息。

在整个应用信任体系中，安全信息来自各种系统，对安全信息的收集在整个安全管理的体系中占有重要的作用。各类系统的运行日志和管理日志是安全信息的重要来源。日志不仅可以帮助管理人员对各种安全事件和安全操作进行审计，分析系统存在的薄弱环节，发现潜在的危险，而且大量的入侵行为直接与系统日志相关，如何快速准确的收集日志信息并将这些信息加以分析保存是安全管理工作中重要的一环。

4). 系统安全策略审计软件

应考虑对系统安全策略配置状况进行审计。系统配置问题是安全问题的重要源头，比如不安全的共享、弱口令等等往往会导致严重的蠕虫病毒传播、信息泄密或入侵行为。通过采用系统安全策略审计软件对 RHIN 范围内的主机进行安全策略审计和集中汇总，能够使得管理员能够对安全问题及时发现，并得以及时解决。

上述安全控制措施在 RHIN 中的部署方式如下图所示。

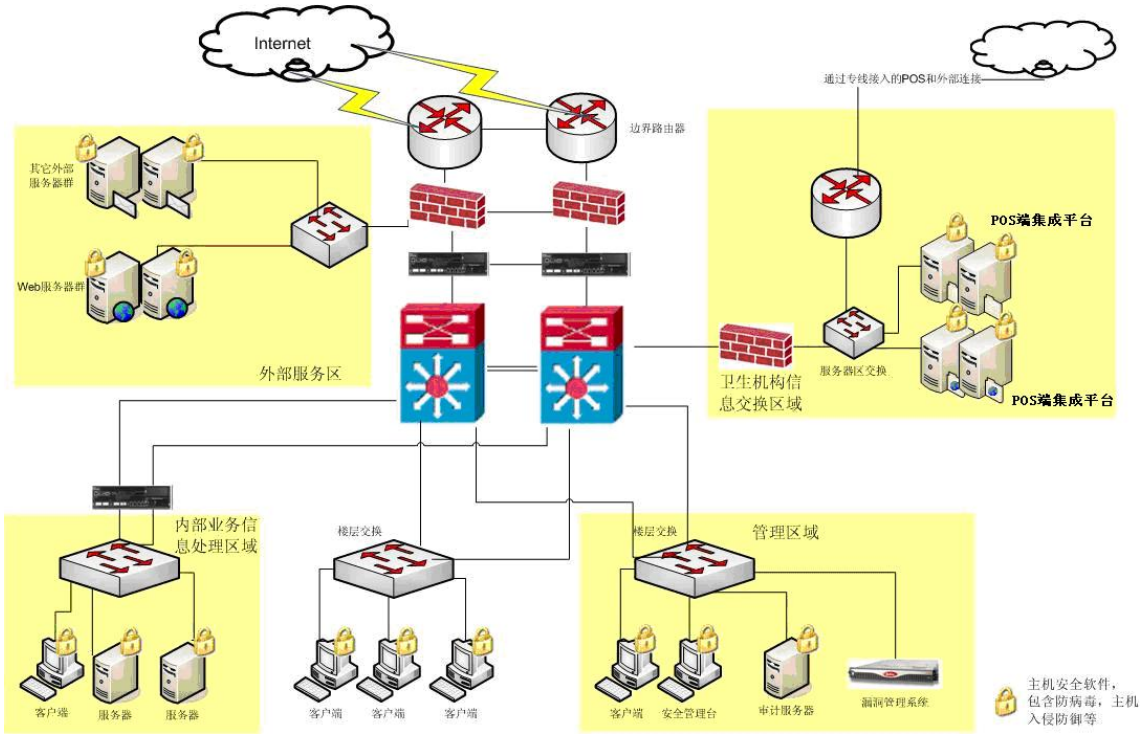

图 10-15 系统安全控制措施示意图

首先，在 RHIN 网络上的每台主机系统，包括服务器、客户端计算机、笔记本电脑等上面安装主机安全软件，包括防病毒软件，主机入侵防御，安全审计等等，实现对病毒、蠕虫、木马以及入侵行为的防御。

其次，在管理区域设置审计服务器，对系统级别的行为进行分析和审计，并对记录进行存储留存。

另外，在管理区域设置安全管理台，对网络中的系统安全组件进行统一管理。

10.8.6 应用安全

结合RHIN应用的特点，总结出RHIN信息系统在应用层面临的主要具体威胁。（见表 10－4）

健康档案的区域卫生信息平台中要实现应用安全功能，具体在整体架构中信息交换层（HIAL）中建立相应的应用安全服务。

健康档案的区域卫生信息平台应用级安全要实现身份鉴别、身份管理、访问控制服务、加密服务、数字签名及安全审计等安全服务。此外，身份保护、匿名化、许可指令管理服务需要结合 RHIN 应用系统在应用层实现。

利用 PKI/CA 技术，为健康档案的区域卫生信息平台提供全面的数字证书服

务，实现统一的用户信息管理。基于 CA 认证体系，建立健康档案的区域卫生信息平台应用安全支撑平台，将安全支撑平台与信息平台应用系统相结合实现安全身份鉴别、访问控制，为应用系统的数据传输提供加密机制，为数据的完整性提供数字签名及验证功能，为应用系统提供安全审计服务。

1). 应用安全业务描述

利用 CA 认证体系，建立健康档案的区域卫生信息平台认证系统及应用安全支撑平台后。可在信息平台中为病人、医师、机构签发代表其身份标识的数字证书。

医院的医生通过区域卫生数据中心平台，就可持有数字证书安全登录信息平台，进行授权下的病历业务应用操作，处理完成后的病历数据由信息平台采用数字签名验证服务器进行数字签名，并通过的安全加密通道将电子病历上载到卫生数据中心中共享。

卫生数据中心可对电子病历信息资源共享的机制进行设置与管理,其他医院医生则通过安全认证身份后(数字证书)，访问其有权限的信息数据，对电子病历进行调阅。

病人也可通过卫生服务网站进行安全身份认证(数字证书)后，访问安全控制下的电子病历，进行远程查询，从而实现区域内电子病历的安全共享和访问。

在信息平台安全体系中，基于 CA 认证系统，综合运用了安全认证网关、签名验证服务器和行为审计管理系统，为电子病历信息化奠定安全技术保障。

卫生信息平台业务应用安全业务逻辑示意如下：

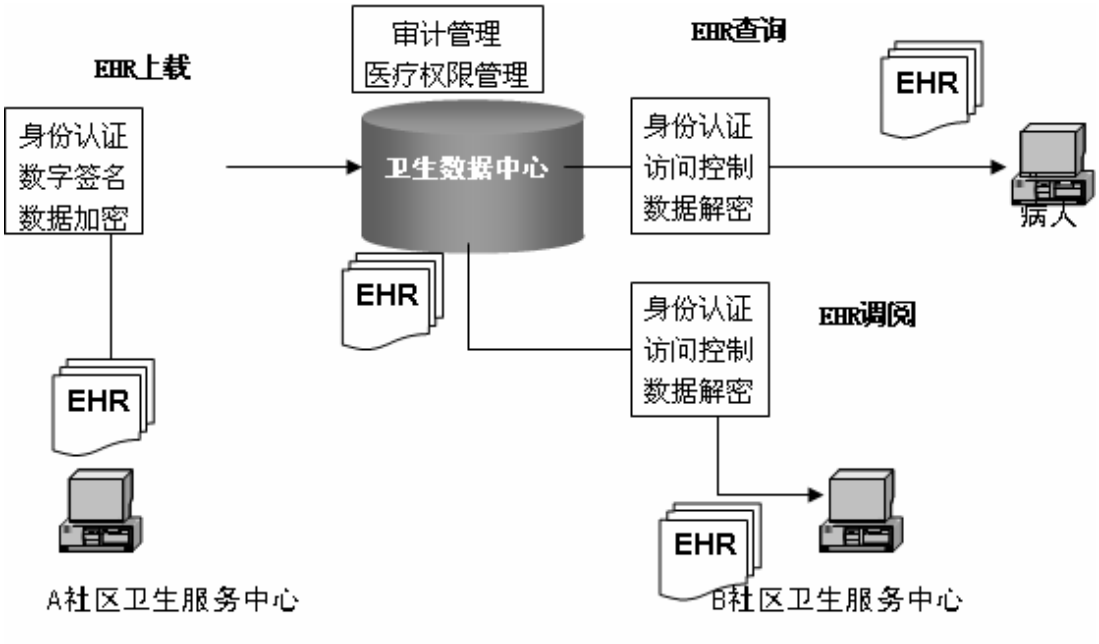

图 10-16 卫生信息平台业务应用示意图

2). 应用安全架构设计

健康档案的区域卫生信息平台应用安全保障体系的架构如下图所示：

图 10-17 应用安全架构设计图

如上图所示，卫生信息平台应用安全服务保障体系由认证系统和应用安全支撑系统组成。其中，证书注册中心 RA 系统是卫生信息平台应用安全的基础，为基于健康档案的区域卫生信息平台应用提供统一的用户信息供应及管理，并提供实现安全支撑服务所需的密钥。

应用安全支撑平台基于数字证书，由安全认证网关、签名验证服务器及安全审计系统组成。利用安全认证网关实现统一的安全身份认证和统一的权限管理，当用户身份认证通过后，安全认证网关根据用户的身份信息及所要访问的目标资源，进行访问控制判断；签名验证服务器为信息平台应用中的数据提供完整性保

障，实现应用操作过程中的抗抵赖功能，确保信息平台应用中关键业务操作的安全性；审计系统对信息平台用户的访问及系统间的交互等过程进行审计，为信息平台应用安全管理提供有效的审计管理服务。

应用安全支撑平台基于数字证书，将医疗卫生安全保障功能以独立服务的方式提供给医院、社区等医疗卫生信息系统使用，从而完成统一的电子健康信息网络安全应用平台的构建。基于数字证书的用户信息管理模式实现对涉及区域医疗卫生安全要素的统一管理，包括统一身份管理、医疗卫生角色管理、卫生信息资源管理、医疗卫生授权管理等。安全支撑平台中的安全认证网关、签名验证服务器等系统可实现包括身份认证服务、数据安全传输服务、行为审计服务。

3). 证书注册中心 RA 系统

证书注册中心 RA 系统负责为健康档案的区域卫生信息平台所有用户及服务系统提供数字证书业务服务。

数字证书被广泛应用于各类业务应用系统的安全建设中，作为系统中身份标识。数字证书由 CA 认证系统产生、分配及管理，并最终通过 CA 认证系统的信任链追溯到 CA 认证中心。

信息平台中的各个实体都必须拥有合法的身份，即由 CA 中心签发的数字证书，在信息平台的各个环节，进入信息平台的各个实体都需通过检验各自的数字证书，来验证与之交互的人员或服务系统身份的真实性，从而解决信息平台的信任问题。

在卫生信息平台安全服务建设中，根据健康档案的区域卫生信息平台的部署建设情况，在信息平台的业务服务窗口建立相应的 RA 系统，并将证书业务服务功能与相应的信息平台注册功能相结合，为用户、医师、机构签发代表其身份标识的数字证书，同时提供为服务系统、主机设备等签发数字证书功能。形成集中管理、分布式证书服务模式。

4). 安全支撑平台

在健康档案的区域卫生信息平台中，应用安全支撑平台由安全认证网关、签名验证服务器及安全审计系统组成。其中，安全认证网关基于数字证书，为信息平台提供安全的用户身份鉴别和权限控制机制，并在此基础上建立加密通道确保信息平台数据在传输过程中的机密性安全；签名验证服务器在信息平台的业务运行过程中，提供数字签名/验证功能，确保关键业务数据的完整性，实现相关业务

操作的抗抵赖；安全审计系统为信息平台提供全面的审计服务，为信息平台的管理提供方便、快捷、有效的审计数据。

安全认证网关

安全认证网关在数字证书认证系统的基础上，使用数字证书鉴别用户身份，为信息平台提供安全的用户身份鉴别服务。同时，安全认证网关基于用户的身份提供统一的权限管理及访问控制功能，并通过与信息平台应用相结合实现不同权限粒度权限控制，并将涉及业务的细节权限管理，转交应用系统自身来控制。安全认证网关支持建立加密通道，可以为信息平台提供数据传输安全保障。

安全认证网关部署在应用客户端与应用服务器之间，使用数字证书完成双方的身份认证，在服务器端和用户客户端建立高强度的 SSL 加密连接，实现客户端和服务器之间身份的有效认证和数据传输安全。采用安全认证网关为 RHIN 信息平台提供如下安全服务：

- 基于数字证书的高强度身份认证；
- 拒绝任何未授权用户对应用系统的访问尝试；
- 为应用系统提供用户在该应用系统中的身份信息；
- 为不同应用提供基于单一证书的单点登录服务。

安全认证网关要求部署方便，具体部署方式要随着信息平台部署方式的不同而配合进行，可采用串联、并联、双机热备和负载均衡等多种部署方式，适用不同的网络环境和应用需求，以有效支持实际的信息平台应用环境。

签名验证系统

在基于健康档案的区域卫生信息平台建设过程中涉及到电子健康档案和电子病历的传输和共享，因此需要采用数字签名技术来保证电子健康档案系统的安全性和不可抵赖性。

数字签名验证系统是提供数字签名服务以及对数据验证其数字签名的真实性和有效性的服务平台，系统通过对数据签名的验证保障数据本身的完整性。数字签名验证服务器主要是为了满足信息平台对数据完整性、抗抵赖的安全要求，通过提供身份认证、数字签名、数字信封、证书解析等安全功能，保障信息平台数据完整性、防篡改、抗抵赖的安全目标。

行为审计系统

行为审计系统通过查询、接收身份安全认证系统、安全认证网关、签名验证

系统的日志等数据信息，通过采集、分析、识别，实时动态监测用户证书的签发、使用情况；用户对应用系统的访问内容、访问行为和访问结果，发现和捕获各种用户访问应用操作行为、违规行为，全面记录应用系统中的各种用户访问会话和事件，实现对应用系统访问信息进行关联分析，为整体应用系统安全策略的制定提供权威可靠的支持。

其一，安全支撑系统状态监测

根据管理员制定的监测策略，安全监管平台可以实现对用户及安全系统的运行状况进行实时监控，监测结果以图表的形式直观反应。状态监测可以对多个设备同时进行，监测结果的集中显示使系统管理员可以方便地了解整个信任体系的运行状况。

行为审计系统负责将安全管理员和安全系统紧密的结合在一起，充分的发挥安全管理的作用。安全监控管理将延伸到整个信任体系中去，确保了整个信任体系中有关信息安全系统的数据能够及时的通知安全管理员，来维护安全保障体系的正常运转。状态监测不仅仅对用户访问应用系统的安全认证网关、签名验证系统的状态进行监控，还包括对身份安全认证系统中用户证书状态信息进行综合监控。

其二，安全信息统计分析

针对搜集到的系统日志，行为审计系统提供种类齐全的统计分析策略，并据此生成多类详尽的安全报告，如日报表、月报表、年报表、阶段报表、比较报表等，便于用户从各个角度了解日志数据。

行为审计系统收集到各个系统的日志信息后并不是简单的堆积数据，而是将各个系统的日志通过用户关联起来，进行有效的关联分析。

5). 应用安全服务部署

基于健康档案的区域卫生信息平台应用安全体系建设部署示意如下：

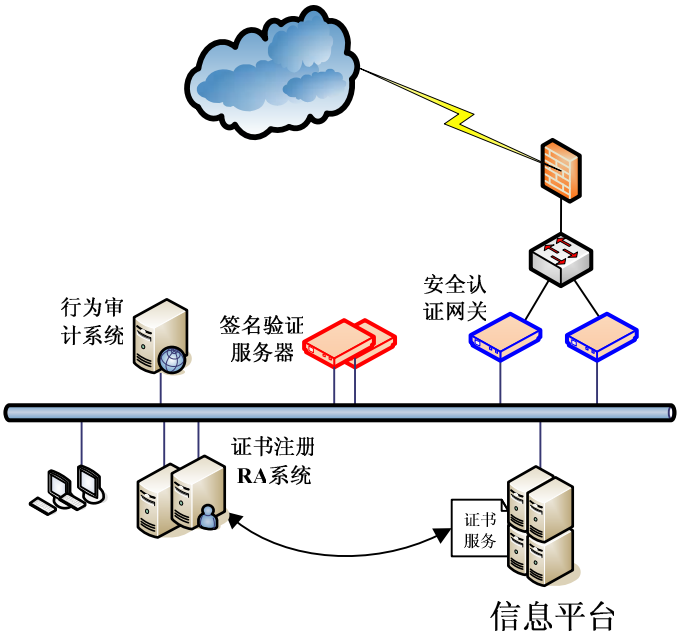

图 10-18 应用安全服务器部署

应用安全建设分区域部署认证系统的业务服务窗口证书注册 RA 系统，RA 系统包括主机、网络设备、安全设备、数据库等各种软、硬件系统。应用系统处部署安全认证网关签名验证服务器和行为审计等安全系统，为信息系统提供基础的安全服务。

10.8.7 数据安全

结合 RHIN 应用的特点，总结出 RHIN 信息系统在数据层面临的主要具体威胁（见表 10－4）

在 HIAL 层次，该部分实现的隐私和安全服务主要包括：通用安全服务、访问控制服务、加密服务、安全审计服务。

在数据安全层面，主要需要考虑数据丢失和数据泄漏两个方面的威胁。数据丢失防范主要依靠数据备份等机制完成，在本文其它章节有详细描述。

数据泄漏造成的根源来自外部黑客攻击和内部数据泄漏，据 FBI 的统计，70%的数据泄漏是由于内部人员造成的，而这些内部人员大都是有权限访问这些数据，然后窃取滥用这些数据。

无论是黑客攻击、还是内部故意泄漏，数据泄漏有以下三个途径造成：

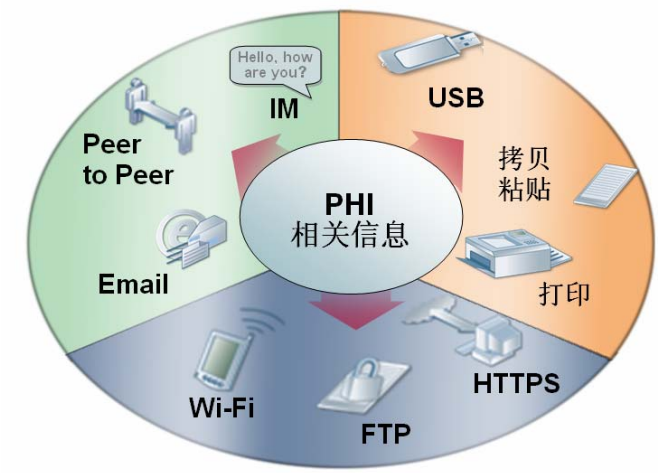

图 10-19 数据泄露途径分析

1) **物理途径**——从桌面计算机、便捷计算机和服务器拷贝数据到 USB、CD/DVD 和移动硬盘等移动存储介质上；通过打印机打印带出公司或者通过传真机发送。
2) **网络途径**——通局域网、无线网络、FTP、HTTP、HTTPS 发送数据，这种方式可以是黑客攻击“穿透”计算机后造成，也可能是内部员工从计算机上发送。
3) **应用途径**——通过电子邮件、IM 即时信息、屏幕拷贝，P2P 应用或者“特洛伊木马”窃取信息。

因此，RHIN 需要部署数据防泄漏技术措施，主要包括如下方面：

首先，防信息泄漏

防信息泄漏技术通过对安全域内部敏感信息输出的各种方式进行控制，目的是为了防止安全域内部敏感信息被有意或无意外漏。

通过部署防信息泄漏类技术在所有的客户端实现数据保护，并完成统一管理；通过数据保护客户端对用户的网络行为进行检测，阻断数据泄漏行为；通过数据保护客户端对具体应用进行检测，阻断数据泄漏行为；通过客户端程序，有效的审计各类数据调用行为，并记录全部用户行为；

其次，设备控制

对接入计算机的各类外置设备进行控制，防止机密信息通过这类外接设备发生泄漏；针对网络打印机、U 盘等各类高危外设的使用进行审计并记录；一旦发现

非法使用，可以第一时间阻断数据泄漏行为；

第三，磁盘和数据加密

包括文件加密、整盘加密以及移动介质加密等。

文件加密类技术用于防御攻击者窃取存储于文件中的数据，目的是保障文件中存储数据的安全。整盘加密类技术通过对整盘数据进行整体加密来实现数据保密，目的是在数据整盘存储层面保障数据安全。移动介质加密类技术通过对 U 盘等移动介质进行加密处理，防止意外丢失造成的数据泄漏。

通过以上技术手段，对移动终端和笔记本电脑的磁盘进行加密，保证移动数据终端的全面安全，就算笔记本丢失，也不会造成数据泄漏；能够对特定的文件进行加密和控制，并通过管理平台设定统一的管理策略，就算数据由于无意的合法行为造成泄漏，非授权用户也无法进行访问；

上述技术手段在区域卫生信息平台的部署方式如下：

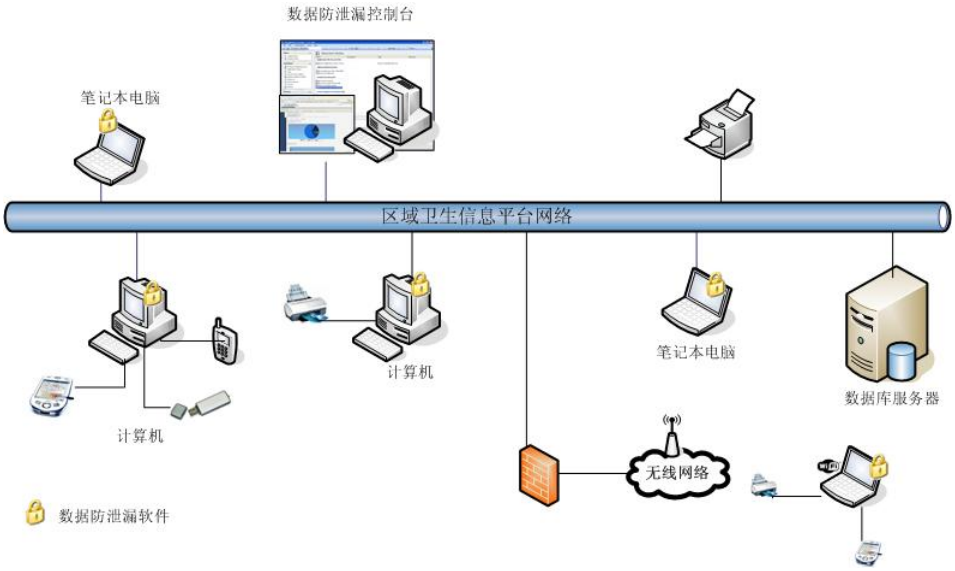

图 10-20 磁盘和数据加密图

10.8.8 安全层次关联和全面风险管理

主动防御不是简单地依靠单点的防范技术手段就可以实现的，而是需要依靠一个基于风险管理思想设计的整体防御体系。传统的安全防范体系往往是割裂的单点、条块式防御，而面对新的威胁，我们需要一个有机的可动态调整的风险管理体系。因此，我们需要在安全控制层次实现关联，以提供更高效的防御控制。

安全控制层次关联示例一：入侵防御设备和入侵检测设备能够获取漏洞管理系

统提供的被保护系统的漏洞信息，这样就可以通过被攻击系统是否具备相应的漏洞判断正在发生的入侵事件的相关性，给管理人员以明确的信息，节约管理人员负担，提高工作效率。

安全控制层次关联示例二：漏洞管理系统识别被保护系统存在的安全漏洞后，能够获取主机保护系统提供的信息，确认主机上是否已经部署相应的防御措施，从而判断实际风险程度。

通过资产分类和优先级定义，通过在后台的自动评估和计算，得出量化的信息系统的安全风险等级，帮助 RHIN 监控信息系统的真实存在的安全风险，并且进行自动的、持续的风险监控，呈现安全风险上升或下降的详细原因。

通过安全控制层次的关联， RHIN 能够得到一个全网整体的风险分布状况，而不是需要分析和处理多个不相关的安全产品的日志和报警之后才能够得出相关结论。

10.9 安全技术实现

RHIN 具体的安全系统配置，应根据当地实际业务需求、网络覆盖范围和规模以及经济条件，本着经济、实用、高效和分步实施的原则，选择适当的建设方案。以下按初级、中级、高级分别列出安全建设系统配置的三种安全配置参照表。在本参照表中，尽可能列举了实现安全需求所需要的工具和技术，符合国家安全等级保护二级要求。在此基础上，结合 RHIN 需求，在某些方面有所增强。

表 10-5 高、中、基本三个级别安全配置参照表

要求	基本配置	中级配置	高级配置
物理安全			
物理位置的选择	√	√	√
物理访问控制	√	√	√
防盗窃和防破坏	√	√	√
防雷击	√	√	√
防火	√	√	√
防水和防潮	√	√	√
防静电	√	√	√
温湿度控制	√	√	√
电力供应	√	√	√
电磁防护	√	√	√

网络安全			
网络结构安全	√	√	√
防火墙	√	√	√
安全审计	√	√	√
边界完整性检查		√	√
网络入侵防御及检测	√	√	√
防病毒网关			√
网络设备防护	√	√	√
漏洞管理系统		√	√
系统安全			
身份鉴别	√	√	√
安全策略控制	√	√	√
安全策略审计		√	√
安全事件审计	√	√	√
补丁分发软件	√	√	√
主机入侵防御		√	√
防病毒软件	√	√	√
漏洞管理系统		√	√
应用安全			
RA 注册中心		√	√
安全认证网关	√	√	√
签名验证服务器	√	√	√
加密主机服务器	√	√	√
访问控制	√	√	√
安全审计	√	√	√
通信完整性	√	√	√
网络传输加密	√	√	√
抗抵赖	√	√	√
软件容错	√	√	√
资源控制	√	√	√
数据安全			
数字签名	√	√	√
数据存储加密	√	√	√
设备控制	√	√	√
数据防泄漏	√	√	√
备份和恢复	√	√	√