# 第六章　招标项目需求及技术要求

**本项目核心产品：服务器、网闸**

## 第 1 章 需求分析

### 网络系统需求

一、系统用途

系统主要承载郑州市慢病管理服务信息平台数据中心网络传输。

二、功能需求

数据中心网络系统的需求涵盖了性能、可靠性、可扩展性、安全性、灵活性、可管理性、兼容性和节能性等多个方面，在设计和建设数据中心网络系统时，需要综合考虑这些需求，以构建一个高效、稳定、安全的网络环境。

1.安全性：数据中心存储和处理着大量的敏感数据，因此网络系统必须具备强大的安全性。这包括网络访问控制、数据加密、入侵检测和防范等措施。通过设置严格的访问控制策略，确保只有授权用户能够访问数据中心的资源。对传输的数据进行加密，防止数据在传输过程中被窃取或篡改。利用入侵检测系统实时监测网络攻击行为，并及时采取防范措施。

2.灵活性：数据中心需要支持多种应用和服务，不同的应用和服务对网络的要求可能不同。因此，网络系统需要具备灵活的配置和管理能力，能够根据应用的需求动态调整网络资源，如带宽分配、QoS（Quality of Service，服务质量）策略等。

3.可管理性：数据中心网络系统通常规模较大，设备众多，因此需要具备良好的可管理性。这包括集中管理、自动化管理和故障诊断等功能。通过集中管理平台，可以对网络设备进行统一的配置、监控和管理，提高管理效率。自动化管理功能可以实现网络设备的自动配置和部署，减少人工干预，降低管理成本。故障诊断功能可以快速定位和解决网络故障，提高网络的可用性。

4.兼容性：数据中心可能会使用来自不同厂商的网络设备和技术，因此网络系统需要具备良好的兼容性，能够确保不同设备和技术之间的互操作性。这有助于保护用户的投资，避免因设备不兼容而导致的问题。

5.节能性：随着数据中心规模的不断扩大，能源消耗成为一个重要的问题。因此，网络系统需要具备节能特性，采用节能型的网络设备和技术，降低能源消耗，减少运营成本。

三、性能需求

1.高性能：数据中心需要处理大量的数据流量，因此网络系统必须具备高带宽和低延迟的特性。高带宽可以确保数据能够快速传输，满足应用程序和用户的需求。例如，对于大数据分析、云计算等应用，需要网络能够支持每秒数 GB 甚至数 TB 的数据传输。低延迟则对于实时性要求高的应用至关重要，如在线交易、视频会议等，网络延迟应尽可能低，以保证用户体验。

2.高可靠性：数据中心的业务通常是 7x24 小时不间断运行的，因此网络系统必须具备高可靠性。这包括冗余设计，如冗余链路、冗余设备等，以防止单点故障导致整个网络系统的瘫痪。此外，还需要具备快速故障恢复能力，能够在出现故障时迅速切换到备用设备或链路，保证业务的连续性。

3.可扩展性：随着业务的发展，数据中心的规模和数据流量会不断增加，因此网络系统必须具备良好的可扩展性。这意味着网络系统能够方便地添加新的设备、链路和节点，以满足不断增长的需求。同时，网络系统的扩展不应影响现有业务的正常运行。

## 计算和存储系统需求

一、系统用途

计算和存储系统为郑州市慢病管理服务信息平台提供计算资源。它们是郑州市慢病管理服务信息平台的核心组件，支撑着郑州市慢病管理服务信息平台支撑环境服务、管理等多方面功能的顺利进行。

二、功能需求

计算和存储系统要满足郑州市慢病管理服务信息平台的需要，还需要支撑后期郑州市慢病管理服务信息平台的扩展应用，在满足平台建设需求的前提下，采用优化设计，使数据处理和存储资源能够满足用户的高性能、高安全可靠、可扩展、可管理等需求。

系统需要具备独立的数据库服务器，具有双机热备和负载均衡模式。

集成服务器、应用服务器、数据库服务器等采用了虚拟化、云计算技术；在虚拟化平台基础上为应用软件提供 CPU、内存、磁盘、操作系统等基础计算资源。相关应用可部署在弹性计算服务实例中以对外提供服务。虚拟机之间可以通过虚拟化技术做到隔离保护，其中每一个虚拟机发生故障都不会影响同一个物理机上的其他虚拟机运行，每个虚拟机上的用户权限只限于本虚拟机之内，可以保障系统平台的安全性。根据本项目中不同业务类型的典型负载情况，动态分配计算资源池。

通过在同一物理服务器上运行多个虚拟机，能够大幅度提高硬件资源的使用效率，减少

物理服务器数量，降低能耗和硬件维护成本。

数据处理系统采用虚拟化技术可快速部署新服务或应用，可以根据业务需求即时调整资源分配，快速扩展或缩减 IT 资源，加速服务响应速度。

虚拟环境中，不同服务或应用可以在相互隔离的虚拟机中运行，有效防止某个系统的问题蔓延到整个网络，增加了信息系统的安全性。

为软件开发和系统升级提供安全的沙盒环境，可以在不影响生产环境的情况下进行测试、调试和验证，加速新功能的部署周期。

三、性能需求

服务器是虚拟化数据中心的核心，其承担着数据中心“计算”功能。对于虚拟化数据中心中的服务器，通常都是将相同或者相似类型的服务器组合在一起，安装云操作系统，使其计算资源能以一种虚拟服务器的方式被不同的应用使用，即所谓的虚拟化资源池。这里所提到的虚拟服务器，是一种逻辑概念。对不同处理器架构的服务器以及不同的虚拟化平台软件，其实现的具体方式不同。

通过虚拟化技术，实现计算资源的虚拟化，构建虚拟数据中心，按需提供满足要求的运算处理资源。

1.计算条件

服务范围：郑州市全域慢性病人群，约 1047200 人。

服务频率：依据《国家基本公共卫生服务规范（第三版）》（国卫基层发〔2017〕13 号）慢性病管理服务一般包含诊疗服务（按照每年 5 次估算）、随访服务（国家要求每年 4 次）、体检服务（国家要求每年 1 次），即每年针对慢性病管理服务的次数为 10 次，每次开展慢性病管理服务需要操作慢性病管理服务平台 3 次计算。按照慢性病管理服务均发生在 1 年中 250 个工作日计算。

1.服务器运算量

按照慢性病管理服务业务集中在工作日上午 6:00-7:00 时，则系统并发用户数为=1047200（人）*10 次*3 次/250(工作日）/1(小时）/3600(秒）=1047200*10/250/1/3600≈35 次，按照实测，日常条件下系统并发用户数是平均值的 10 倍计算，则系统并发用户数为 350 人，按照同时在线数为同时并发数的 10 倍计算，则系统同时在线数 3500 人。

（1）数据库服务器

针对平台建设时服务器的选型做出分析，在本方案中主要是针对数据库服务器进行分析。

在进行平台数据服务器设备选型工作时，我们以国际上通用的 TPC 委员会发布的用于评测事务处理业务的 TPC—C 基准为依据，综合考虑业务系统交易复杂性、并发交易数、数据库读/写比例、数据库表等因素，推算出符合业务规模的配置方式，同时考虑到系统管理所需消耗的资源，对重要资源保留一定的升级和扩展空间。

为了方便计算数据库服务器的造型，我们约定：

平台同时在线用户数（U1,3500）；

平均每个用户每分钟发出业务请求（N1,8）；

平台发出的业务请求，更新、查询、统计各占 1/3，平均每次业务请求产生事务数 T1,8,12,18；

一天内忙时的处理量为平均值的倍数（G1,8）；

经验系数为（J1,1.6）（实际工程经验）；

考虑服务器保留 30%的冗余；

服务器需要的处理能力为：

TPC-C=U1*N1*T1*G1*J1/冗余系数=3500*8*（8+12+18）*8/3*1.6/0.7≈6485334

根据测试结果，本项目采用国产化服务器，对应 1CPU 的 tpmC 测试值至少可达 50000，选取 50000 作为选配服务器 CPU 数量的参考值，则系统数据库服务器所需计算资源为 130 核物理 CPU。同时考虑数据库高可靠性部署，则系统数据库服务器所需计算资源为 260 核物理 CPU。

根据工程经验，应用服务器的处理性能是数据库服务器处理性能的 0.8 倍，则系统应用服务器所需计算资源为 104 核物理 CPU。

即本项目所需服务器资源 364 核物理 CPU，同时考虑未来三年系统对计算资源的增量需求按照 20%计算，综合虚拟化平台对物理 CPU 消耗按照 20%计算，则系统合计需要 525 核 CPU。

2.存储资源需求

慢性病随访规模：覆盖全郑州市慢病人群约 104.72 万人，每年每人随访 4 次，严重病人按照 1 个月随访 1 次进行估算，预估每年慢性病随访规模 500 万人次。

慢性病复诊规模：覆盖全郑州市慢病人群约 104.72 万人，平均按照每人每 2 个月复诊 1 次计算，预估每年慢性病复诊规模 650 万人次。

健康管理规模：覆盖全郑州市慢病人群约 104.72 万人，平均按照每人每天应用 1 次估算，预估每年健康管理服务规模 40000 万人次。

慢性病随访每次产生的数据量暂估为 20KB（实测数据），慢性病复诊每次产生的数据

量暂估为50KB（实测数据），健康管理每次产生的数据量暂估为40KB（实测数据），数据存储量预测如下：

1年慢性病随访数据量所需存储量为：500*10000*20/1024/1024/1024≈0.1TB；

1年慢性病复诊数据量所需存储量为：650*10000*50/1024/1024/1024≈0.3TB；

1年慢性病健康管理数据量所需存储量为：40000*10000*20/1024/1024/1024≈7.5TB。

即1年慢性病健康管理服务数据量约8TB，考虑存储空间按照3年进行配置，按照每年业务数据量增长10%，则系统三年所需存储量为=8+8*1.1+8*1.1*1.1≈27TB。同时考虑系统在虚拟化平台中按照3副本存储进行配置，即平台未来三年所需可用存储空间为81TB。

## 备份系统需求

1.系统用途

业务生产过程中会产生大量的多样化的数据，对于应用系统而言数据就是根本，任何操作、分析、结算等都从数据库中提取。各应用系统在面对人为操作失误、病毒木马侵袭和黑客攻击、设备硬件故障、系统故障、管理疏忽、自然灾害等意外事件时，极易造成数据丢失。另外当操作系统发生重大故障时，需要先重新安装操作系统、重装所有应用程序，然后才能恢复数据，耗费相当长的时间才能够重新恢复应用。为保证数据系统的安全，确保在应急情况下的紧急处理，必须对业务数据库及操作系统制定备份和恢复机制。各数据中心的数据在本地或异地备份，在系统数据出现问题的时候，通过数据恢复系统，对损坏的数据进行恢复。

2.功能需求

（1）备份系统可以将郑州市慢病管理服务信息平台关键数据（如患者记录、诊断信息、治疗计划等）备份到独立的存储介质中，避免单点故障。同时，可以通过加密措施和访问权限控制等手段，确保数据的安全性，防止数据被非法获取或篡改。

（2）在数据损坏或丢失的情况下，备份系统可以根据需要恢复数据到某一特定时间点的状态，确保郑州市慢病管理服务信息平台能够迅速恢复正常工作。此外，还可以针对各种可能的故障场景进行备份策略的设定，保证数据能够及时恢复到最新状态。

（3）备份系统可以支持郑州市慢病管理服务信息平台在发生自然灾害、设备故障等突发事件时，通过快速恢复数据，确保郑州市慢病管理服务信息平台业务的连续性。

3.性能需求

为保障医疗信息化体系的安全，有效应对自然灾害、人为破坏造成的灾难，避免单点故障，确保各业务系统的高可用性和业务连续性。本项目同步考虑建设相应的灾备体系，本项

目将实现系统的应用级容灾，以确保灾难发生时，实现关键服务在允许的时间范围内恢复运行，数据不会丢失或者遭到破坏，应用级容灾的 RPO≤5 分钟，RTO≤15 分钟。

数据和应用恢复整体满足《信息安全技术信息系统灾难恢复规范》（GB/T20988-2007）的第 5 级要求。如果数据中心出现重大灾难性损失，可以达到信息系统数据基本不丢失。同时容灾中心建设在充分考虑可扩展性的条件下，与主数据中心设计能力相匹配，在主数据中心暂停服务期间，容灾中心能够提供基本的应用系统服务和数据查询工作。

备份一体机按照备份策略对全量业务进行全备和增备，根据数据量估算，各系统业务所需结构化数据备份总量为 10TB，考虑备份策略下的多备份副本需求，确定副本系数为 3；存储利用率按照 80%计算，则备份需求容量=10×3÷80%≈37.5TB。

## 安全系统需求

网络架构的安全是网络安全的前提和基础，选用主要网络设备时需要考虑业务处理能力的高峰数据流量，要考虑冗余空间满足业务高峰期需要；网络各个部分的带宽要保证接入网络和核心网络满足业务高峰期需要；按照业务系统服务的重要次序定义带宽分配的优先级，在网络拥堵时优先保障重要主机。

分区分域合理规划路由，业务终端与业务服务器之间建立安全路径。

根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的网段或 VLAN。保存有重要业务系统及数据的重要网段不能直接与外部系统连接，需要和其他网段隔离，单独划分区域。

重要区域与其他区域之间部署网闸或者防火墙等隔离设备，并启用 ACL 进行访问控制。

1.系统用途

实现对郑州市慢病管理服务信息平台网络安全防护，满足网络安全等级保护第三级要求。

本项目建设的郑州市慢病管理服务信息平台是关系郑州市慢病管理服务信息平台内众多企业的重要信息系统，面临的威胁来自各个方面，从国内外网络安全形势和发展趋势、主要的安全脆弱点和攻击类型，以及新技术发展引发的新的安全风险进行综合分析。具体包括以下几方面：

**表 1-1 网络安全面临威胁需求表**

| 序号 | 威胁源 | 威胁描述 | 威胁分类 | 威胁程度 |
|---|---|---|---|---|
| 1 | 基于政治目的来自敌对势力的黑客攻 | 国内外敌对势力基于政治目的，利用网络传播、宣传、违反法律和社会道德的信息， | 外部 | 高 |

| 序号 | 威胁源 | 威胁描述 | 威胁分类 | 威胁程度 |
|---|---|---|---|---|
| | 击 | 盗窃机密信息，并进行颠覆活动。 | | |
| 2 | APT 攻击威胁 | APT—高级持续性威胁作为以商业和政治为目的的一个网络犯罪类别，已经成为一种常见的攻击手法。APT 攻击行为首先具有极强的隐蔽能力，通常是利用企业或机构网络中受信的应用程序漏洞来形成攻击者所需 C&C 网络。 | 外部 | 中 |
| 3 | 虚拟化技术安全威胁 | 虚拟化软件各种底层应用程序的安全漏洞；虚拟机应用程序的安全漏洞；虚拟机流量交换的安全风险。 | 外部 | 高 |
| 4 | 对网站系统的攻击 | 黑客通过 SQL 注入攻击、跨站攻击、CSRF（跨站请求伪造）、网页篡改、网页挂马等攻击，造成网站系统可用性被破坏，敏感数据泄露，政府信誉受到损害。 | 外部 | 高 |
| 5 | 数据信息泄露 | “拖库”攻击及个人信息泄露等。黑客对目标网站进行扫描，查找其存在的漏洞，然后通过该漏洞在网站服务器上建立“后门（webshell）”，通过该后门获取服务器操作系统的权限。最后利用系统权限直接下载备份数据库，或查找数据库链接，将其导出到本地。 | 外部 | 高 |
| 6 | 木马病毒等恶意代码 | 恶意代码是通过执行发生作用为了实现恶意目的程序，包括木马，病毒工具，蠕虫，广告软件等，恶意代码的传播途径越来越多样，加壳等保护自身的手段也渐趋多样化。 | 外部 | 高 |
| 7 | 抗拒绝服务攻击 | 侧重于通过很多“僵尸主机”向受害主机发送大量看似合法的网络包，从而造成网络阻塞或服务器资源耗尽而导致拒绝服务，分布式拒绝服务攻击一旦被实施，攻击网络包就会犹如洪水般涌向受害主机，从而把合法用户的网络包淹没，导致合法用户无法正常访问服务器的网络资源。 | 外部 | 高 |
| 8 | 内部人员无意或突发的系统误操作 | 由于内部管理疏漏，内部人员操作失误造成敏感信息的外泄以及对信息系统的无意破坏。 | 内部 | 中 |
| 9 | 有组织的计算机犯罪 | 反政府组织、宗教极端组织、犯罪团伙或个人利用网络传播、宣传、搜索违反法律和社会道德的信息，进行颠覆活动或敲诈勒索；造谣、蛊惑民众，导致社会不稳定，也给国家安全带来严重的威胁。 | 外部 | 中 |
| 10 | 网络或安全防护设备被错误配置 | 网络或安全防护设备被非授权人员有意或无意错误配置，导致关键应用系统不可用。 | 内部 | 中 |
| 11 | 不安全的网络通信 | 网络通信过程中没有采取措施对敏感数据进行保护，有可能导致数据被泄露或被破坏。 | 外部 | 高 |
| 12 | 不及时地安全服务 | 安全服务不及时，有可能导致安全问题没有被及时解决，信息系统可用性被破坏，敏感数据被泄露、破坏或不可用，政府信 | 内部 | 中 |

| 序号 | 威胁源 | 威胁描述 | 威胁分类 | 威胁程度 |
| --- | --- | --- | --- | --- |
| | | 誉受到损害。 | | |
| 13 | 零日漏洞攻击 | 即安全补丁于漏洞曝光的同一日内，相关的恶意程序就出现，并对漏洞进行攻击。它是利用以前未知的软件缺陷，缩短攻击时间，在安全产品发生作用之前攻击就已达到顶峰，这种攻击很少发生，但危险性也尤为严重。 | 外部 | 高 |

2.功能需求

（1）安全物理环境

机房采取全方位物理安全防护措施，形成纵深防御体系，机房的安全防护措施如下：

边界防护。建立围墙、安全门岗、门锁等安全边界来保护区域内的软硬件设施安全，只有经过授权的人员才能进入安全区域。

安全区域划分。根据区域的人员和区域所面临的相关风险来划分不同安全级别区域。每个区域都有一个必须的特定保护级别，以指明该区域必须设定的控制类型。部署智能安防系统（监控+门禁），门禁系统可设置不同等级权限，监控门的状态和告警。

电能供给安全。提供不间断供电系统、备用电源、发电机组等设备来防止电力中断和电力波动对系统造成的损害，降低电源故障风险。

自然灾害防护。部署探测设备（烟雾探测器等）以便在灾害发生的早期及时发现。设置报警自动应答机制，如切断电源、关闭设备等，降低发生自然灾害造成的损失。

（2）安全区域边界

《网络安全等级保护 2.0》的安全区域边界要求明确指出：

应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；

应对进出网络的数据流实现基于应用协议和应用内容的访问控制；

应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；

应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；

当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提前报警。

应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；

应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析；

应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。

（3）安全计算环境

《网络安全等级保护 2.0》的安全计算环境要求明确指出：

应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；

应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问；

应启用安全审计服务，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

应提供数据有效性检验服务，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警；

应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断；

应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

应禁止未授权访问和非法使用用户个人信息。

（4）安全管理中心

《网络安全等级保护 2.0》的安全管理中心要求明确指出：

应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；

应能够提供一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；

应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；

应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；

应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；

应能对网络中发生的各类安全事件进行识别、报警和分析；

应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；

应保证系统管理员通过管理工具或平台进行系统管理操作，并对这些操作进行审计；

应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

（5）应用与数据安全

对郑州市慢病管理服务信息平台来讲，运行在网络上的各种网络服务器和各种专有设备构成了最重要的信息资产之一，如何确保这些重要的网络服务器能够稳定、可靠、安全地运行，是保证各项业务正常开展的基础。一般来讲，网络服务器所面临的主要安全风险包括非法访问、合法用户误用、滥用、数据泄露、篡改等。在数据传输的过程中面临着以下问题：

在数据传输过程中，由于数据加密不严或者其他原因被第三方窃取或者篡改；

数据在存储时，如何通过合理的访问权限分配，保证用户访问的合法性，同时还需要保证能够随时对这些数据进行高效、安全地访问。

（6）安全测评要求

此外，在《信息安全技术网络安全等级保护测试评估技术指南》（GB/T36627-2018）中还提出，等级保护测评过程中将会采取三类测评技术，分别是：

检查技术：主要包括文档检查、日志检查、规则集检查、系统配置检查、文件完整性检查以及密码检查等；

识别和分析技术：主要包括网络嗅探、网络端口和服务识别、漏洞扫描、无线扫描等；

漏洞验证技术：主要包括口令破解、渗透测试、远程访问测试等；

安全体系首先应当能够满足等级保护基本要求中的相关指标，其次应当能够满足等级保护测评指南中相关测评技术的检测要求。

3.性能需求

提高基础资源利用率。通过虚拟化技术将原来占用物理机的业务整合到虚拟化云平台中，既满足了业务需求，节约了投资，又很好的提高了数据中心的利用率。

业务高可用性和可靠性。随着信息化应用系统的不断增多，应用服务器系统的高可靠性、高可用性和易管理性变得极为重要，对于应用系统来说，无论是硬件设备，还是软件系统出现问题，都会造成业务中断，恢复起来也耗时较长，少则 1、2 个小时，长则半天，严重影响业务的正常使用。

保障数据安全性的需求。目前，本系统承载郑州市慢病管理服务平台业务，一旦遭受损失，其价值是无法估量的，因此，必须建立数据灾难备份系统，来保障医疗数据的安全性。

## 密码应用需求

《中华人民共和国密码法》《网络安全等级保护条例（征求意见稿）》《河南省网络安全条例》《商用密码应用安全性评估管理办法（试行）》等相关文件要求：关键信息基础设施、网络安全等级保护第三级及以上信息系统，每年至少评估一次，测评机构可将商用密码应用安全性评估与关键信息基础设施网络安全测评、网络安全等级保护测评同步进行。其他信息系统定期开展检查和抽查。

郑州市慢病管理服务平台及其敏感数据（个人信息、电子处方、在线药方等数据）缺乏有效的密码保护，数据泄露、数据篡改和身份仿冒事件频繁发生。数据是否真实、完整有效直接影响到慢病服务工作能否有效地开展，同时，这些数据一旦被恶意篡改，将给医院及病人带来损失，使城市的形象受损，信任度降低。

许多密码技术被黑客滥用造成严重危害，例如使用加密文件来勒索病毒、比特币支付赎金和暗网通信等。信息系统应用开发商对密码技术使用不正确、不合理和不规范，导致很多密码技术被弃用、乱用和误用，导致很多安全问题发生。大量信息系统依旧采用非国密等安全性不高的密码算法或相关算法服务。

密码是网络安全的核心技术，密码应用是否合规、正确和有效，涉及算法、协议、产品、技术体系、密钥管理、密码应用等多个方面，有必要委托专业机构和专业人员，采用专业工具和手段对系统商用密码应用进行测试和评估，形成评估结果，对后续商用密码改造提供必要依据。

按照《信息安全技术 信息系统密码应用基本要求》以下简称“基本要求”，提出对数据中心从物理和环境安全、设备和计算安全、应用和数据安全、安全管理等层面进行风险分析和密码应用要求。

（1）物理和环境安全

●安全风险分析

物理和环境安全层面，涉及机房的进出人员的身份鉴别和进出记录，视频的安全性。身份鉴别方面，机房电子门禁系统需要使用密码技术保证进入机房人员身份鉴别信息的真实性。电子门禁记录数据完整性方面，机房电子门禁系统需要使用密码技术保证电子门禁系统进出记录的完整性，视频监控系统需要使用密码技术保证视频数据的完整性。本项目依托郑州市第七人民医院机房建设，物理和环境安全不涉及。

●密码应用需求

需要部署符合 GB/T 39786-2021 标准要求的电子门禁系统对进出机房人员进行身份鉴

别。需要采用符合密码相关国家、行业标准要求密码技术，实现对门禁进出记录和视频监控数据进行完整性保护。

（2）网络和通信安全

●安全风险分析

在网络和通信安全层面，通信前需要使用密码技术对通信双方进行身份鉴别；需要使用密码技术对访问控制信息进行完整性保护；数据传输过程需要使用密码技术进行通信数据完整性保护；通信需要使用密码技术进行通信数据机密性保护；运维人员通过堡垒机管理服务器、数据库，在郑州市慢病管理服务信息平台网络内直接管理安全设备、密码设备，需要建立集中管理通道。

在网络和通信安全层面，被测系统网络和通信过程中遇到的风险包括：链路可能会受到攻击，如 DDOS 攻击、流量攻击等，可能会导致业务系统全部瘫痪；链路发生故障导致资源和应用不可访问；非法设备从外部接入内部网络，或网络边界被破坏；通信传输过程中数据被非授权地截取、篡改，导致通信数据发生泄漏；关键节点存在恶意代码，导致对网络通信造成破坏等。

●密码应用需求

需要采用支持国密 SSL 功能的安全浏览器密码模块和安全认证网关实现通信实体身份鉴别保证通信实体身份的真实性，网络通信信道中数据的机密性和完整性；需要采用密码技术保障网络边界访问控制信息的完整性；需要采用密码技术保障对从外部连接到内部网络的接入设备身份的真实性。

（3）设备和计算安全

●安全风险分析

在设备和计算安全层面，主要包括服务器、数据库、安全设备。运维人员通过采用远程桌面的方式远程登录到服务器进行运维，例如：身份鉴别方式为“用户名+口令”，远程登录时采用 RDP 协议。

设备和计算操作过程中遇到的风险包括：设备被非法人员登录；用户口令遭到恶意破解，导致系统被入侵；系统遭到入侵后，删除账户、恶意分配账户权限、通过修改用户权限获取更高级别信息；对设备漏洞发动攻击；恶意调用系统资源，虚拟机逃逸；设备日志记录被非法篡改，以掩盖非法操作；远程登录设备时，身份鉴别数据被非法获取或非法使用；设备内重要程序和文件的来源不可信。

●密码应用需求

需要采用密码技术保障登录设备的用户身份的真实性；远程管理设备时，需要采用密码技术建立安全的信息传输通道；需要采用密码技术保障系统资源访问控制信息、设备中的重要信息资源安全标记、日志记录的完整性以及重要可执行程序的完整性，对其来源的真实性验证。

（4）应用和数据安全

●安全风险分析

在应用和数据层面，客户端与系统进行交互时，应用和数据面临的风险包括：业务系统被非法人员登录，导致业务系统被入侵；传输或存储的业务数据被其他应用获取、被外部攻击者非法获取；应用系统资源访问控制信息、应用日志记录被非法篡改，以掩盖非法操作；应用程序、重要应用配置等重要信息被非法修改；数据发送者或接收者不承认发送或接收到数据，或者否认所做的操作和交易。

●密码应用需求

身份鉴别。系统登录建议电脑终端用户使用智能密码钥匙、服务端部署身份认证系统，实现对电脑终端登录应用用户的身份鉴别，保证用户身份的真实性，防止非授权人员登录。移动终端用户使用移动终端智能密码模块，服务端部署移动端密码管理服务，实现移动端登录应用用户的身份鉴别，保证用户身份的真实性，防止非授权人员登录。

数据传输安全。建议在数据通讯过程中采取安全链路，客户端使用安全浏览器密码模块、服务端，部署安全认证网关，建立安全传输通道，保障通讯数据传输的机密性和完整性。

（5）高风险问题分析

●密码算法

该部分包括以下内容：

指标要求：信息系统中使用的密码算法应符合法律法规的规定和密码相关国家标准、行业标准的有关要求。

适用范围：所有级别信息系统。

安全问题：采用存在安全问题或安全强度不足的密码算法对重要数据进行保护，如 MD5、DES、SHA-1、RSA（不足 2048 比特）等密码算法使用安全性未知的密码算法，如自行设计的密码算法、未经安全性论证的密码算法等。

可能的缓解措施：无。

风险评价：上述安全问题一旦被威胁利用后，可能会导致信息系统面临高等级安全风险。

●密码技术

指标要求：信息系统中使用的密码技术应遵循密码相关国家标准和行业标准。

适用范围：所有级别信息系统。

安全问题：采用存在缺陷或有安全问题警示的密码技术，如 SSH 1.0、SSL 2.0、SSL 3.0、TLS 1.0 等；使用安全性未知的密码技术，如自行设计的密码通信协议、未经安全性论证的密码通信协议等。

可能的缓解措施：无。

风险评价：上述安全问题一旦被威胁利用后，可能会导致信息系统面临高等级安全风险。

●密码产品和密码服务

指标要求：信息系统中使用的密码产品、密码服务应符合法律法规的相关要求。

适用范围：所有级别信息系统。

安全问题：采用自实现且未提供安全性证据的密码产品；采用存在高危安全漏洞的密码产品；密码产品的使用不满足其安全运行的前提条件，如其安全策略或使用手册说明的部署条件；选用的密码服务提供商不具有相关资质；存在可能会对密钥管理造成严重安全隐患的安全问题。

可能的缓解措施：无。

风险评价：上述安全问题一旦被威胁利用后，可能会导致信息系统面临高等级安全风险。

# 第 2 章 项目建设方案

## 2.1 建设原则和策略

（1）统筹设计，兼顾未来

在设计方案过程中，统筹考虑郑州市慢病管理服务信息平台的系统、数据、网络等资源情况，以确保数据能够及时和充分交换共享。充分利用现有资源和设施，并兼顾未来扩展需要，结合项目建设内容，科学编制设计方案。

（2）需求主导，协调推进

从郑州市慢病管理服务信息平台的实际需求出发，保证郑州市慢病管理服务信息平台正常运转，兼顾扩展需求。在系统的开发与建设过程中，确保系统便于操作、易于扩展，从方案设计的各个方面充分以项目建设的实际需求为前提。

（3）采用成熟产品，确保系统稳定

方案中采用的技术架构，功能完善、性能成熟，具有强大的数据传输、处理、分析计算能力，具有效率高、安全性好、可扩展能力强等特性，遵循业界标准。

（4）保障安全，自主可控

按照项目建设要求，本项目所有采购的软硬件设备统一选用信息安全自主可控产品，核心硬件配置适当冗余，保证系统高可靠运行。系统设计严格按照国家计算机信息系统安全的有关规定和要求，建立有效的安全保障体系，运用先进技术，全面强化安全管理，建立健全防范机制，确保数据安全。

## 2.2 建设目标与建设内容

### 2.2.1 建设目标

为深入贯彻落实习近平新时代中国特色社会主义思想和党的二十大精神，按照深化医药卫生体制改革、全面推动健康中国建设、维护和增进人民群众身体健康要求，以健康需求和解决人民群众主要健康问题为导向，以控制慢性病危险因素为重点，以健康促进和健康管理为手段，建设郑州市市域一体化慢病管理服务信息平台，以信息化加大慢性病预防和医疗相互紧密连接性，实现对慢病患者进行全方位、全生命周期健康管理，有效降低疾病发生率、重症发病率，从而降低医疗费用，不断满足辖区居民对美好健康的需求。

本项目通过郑州市慢病管理服务信息平台支撑环境建设，建立安全可靠、性能稳定的包含网络资源、计算和存储资源、安全资源、密码资源、备份资源等在内的郑州市慢病服务数据中心，确保郑州市慢病管理服务信息平台安全、稳定运行。

**建设规模和内容**

按照郑州市慢病管理服务信息平台医卫专网与互联网应用系统建设需求，建设包含计算和存储系统、备份系统、网络系统、安全系统、密码系统等的数据中心，为郑州市慢病管理服务信息平台提供可靠数据中心支撑。

计算和存储系统，用于承载郑州市慢病管理服务信息平台数据计算和存储需求，采用云计算技术，配置服务器、虚拟化平台等 9 台（套）。

备份系统，根据郑州市慢病管理服务信息平台备份要求，在医卫专网配置备份一体机 1 台。

网络系统，用于承载郑州市慢病管理服务信息平台数据中心网络需求，主要配置核心交换机、业务交换机、安全交换机、管理交换机等 12 台。

安全系统，按照网络安全等级保护第三级要求，在医卫专网和互联网配置防火墙、堡垒机、数据库审计、上网行为管理等 10 台。

密码系统，按照商用密码应用安全性第三级要求，在医卫专网配置国密 VPN 安全网关、服务器密码机、签名验签服务器、智能密码钥匙、个人证书、SSL 证书等 48 台（套）。

## 2.3 总体架构设计

本期项目总体网络拓扑结构如下图所示：

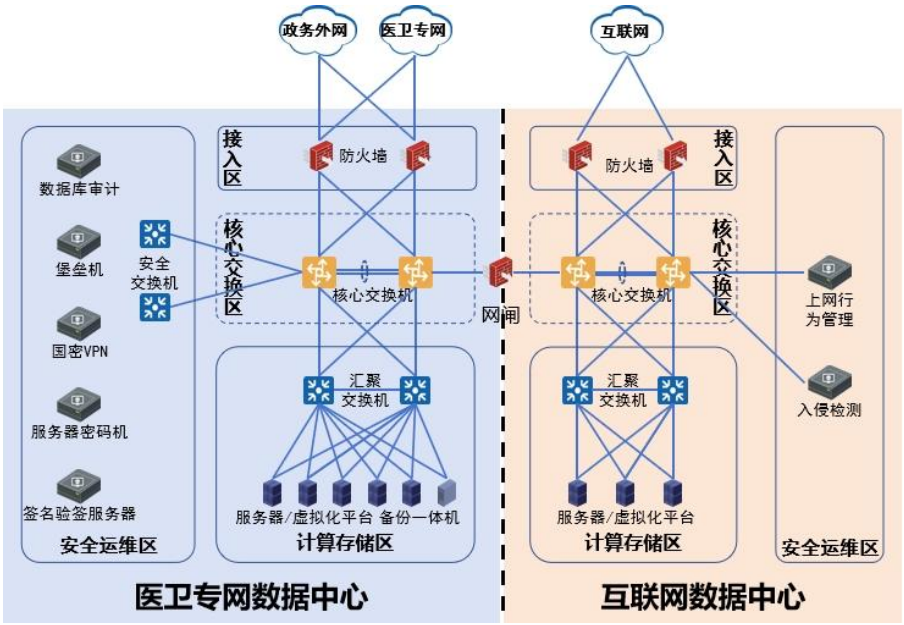


**图 2-1 总体网络架构图**

本项目总体网络拓扑如上图，主要分为医卫专网和互联网两部分。

医卫专网区和互联网主要分为计算存储区、核心交换区、安全运维区和接入区。

## 2.4 应用系统及信息资源规划建设

本项目不涉及应用系统及信息资源规划建设内容。

## 网络系统设计

### 建设原则

在数据中心网络系统建设过程中，需要综合考虑以上原则，根据实际需求和业务特点，制定合理的建设方案，以构建一个先进、可靠、安全、灵活、可管理的网络系统。

1.先进性原则：采用先进成熟的网络技术和设备，以满足当前及未来一段时间内数据中心对高性能、高带宽的需求。例如，选择支持万兆甚至更高带宽的以太网技术，以及具备先进交换架构和处理能力的网络设备，保证数据的快速传输和处理。

2.可靠性原则：构建冗余的网络架构，包括冗余链路、冗余设备等，消除单点故障。如采用双核心交换机、链路聚合等技术，当某一设备或链路出现故障时，系统能够自动切换到备用设备或链路，确保业务的连续性。同时，选择可靠性高的网络设备，具备良好的硬件质量和软件稳定性。

3.可扩展性原则：网络系统应具备良好的扩展性，能够方便地添加新的设备、链路和节点，以适应数据中心规模的扩大和业务的增长。例如，采用模块化的网络设备，便于增加端口数量和功能模块；设计网络架构时预留足够的扩展空间，如 IP 地址、VLAN 等资源。

4.安全性原则：建立多层次的安全防护体系，包括网络访问控制、数据加密、入侵检测与防范、病毒防护等。通过防火墙对进出数据中心的流量进行过滤和控制，采用 VPN 技术对远程访问进行加密，部署入侵检测系统实时监测网络攻击行为。同时，加强对网络设备和服务器的安全配置管理，防止安全漏洞被利用。

5.灵活性与可管理性原则：提供灵活的网络配置和管理功能，能够根据业务需求快速调整网络策略。例如，支持 VLAN 划分、QoS（服务质量）控制等功能，实现对不同业务流量的分类管理和带宽分配。采用集中式的网络管理系统，对网络设备进行统一的配置、监控和维护，提高管理效率，降低管理成本。

6.兼容性原则：确保网络系统中不同厂商的设备和技术之间具有良好的兼容性和互操作性。在选择网络设备时，优先考虑支持标准协议和接口的产品，避免因设备不兼容而导致的网络故障和性能下降。

7.经济性原则：在满足网络系统性能和功能需求的前提下，合理控制建设成本。选择性价比高的网络设备和技术，避免过度投资。同时，考虑网络系统的运营成本，如能源消耗、维护费用等，选择节能型设备和易于维护的网络架构。

8.绿色节能原则：采用节能型的网络设备和技术，降低能源消耗。例如，选择具有节能功能的交换机，支持端口自动休眠、动态功率调整等技术；优化网络架构，减少设备数量和链路长度，降低整体能耗。

9.标准性原则：遵循国际和国内相关的网络标准和规范进行建设，确保网络系统的开放性和标准化。采用标准的网络协议和接口，便于与其他网络系统进行集成和互连。

**架构设计**

整体网络架构采用核心层、汇聚层和接入层三层网络架构，各种网络分别使用一套网络设备，采用物理隔离的方式，保证每套网络数据的安全性。整套系统可实现万兆主干链路，千兆接入到桌面。

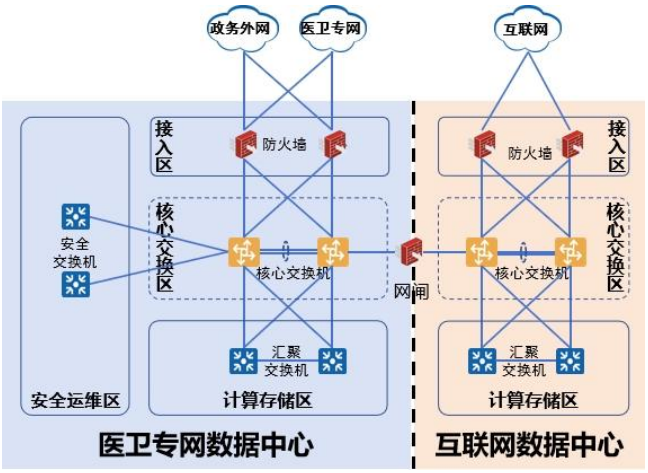


**图 2-2 网络拓扑架构图**

医卫专网采用三层网络架构，接入医卫专网和政务外网采用千兆电口，核心交换机 10Gbps 堆叠设计。

互联网采用三层网络架构，接入互联网，互联网出口按照 1000Mbps 设计，核心交换机 10Gbps 堆叠设计。

**配置方案**

**表 2-1 网络系统配置表**

| 序号 | 设备名称 | 主要技术（性能）指标 | 单位 | 数量 |
|---|---|---|---|---|
| 1 | 核心交换机 | 交换容量≥500Tbps；包转发率≥100000Mpps；双主控，双电源，≥48 个万兆光口，≥8 个万兆多模光模块，≥8 个千兆多模光模块；≥2 个交换插槽，≥6 个业务插槽；支持 IPv4/IPv6 双栈协议；支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；支持横向虚拟化功能；支持纵向虚拟化技术，含项目所需线缆等组件。 | 台 | 2 |
| 2 | 业务交换机 | 交换容量≥2.8Tbps，转发性能≥2000Mpps；10GE 光口数量≥48 个（含光模块），≥2 个 40GE QSFP+口（含光模块），≥4 个 100GE 光接口（含光模块）；≥1 根≥40G 堆叠线缆；≥4 个风扇，冗余电源；支持 IPv4/IPv6 双栈协议；支持集群或堆叠多虚一技术，支持纵向虚拟化技术。 | 台 | 2 |
| 3 | 安全交换机 | 交换容量≥2.8Tbps；包转发率≥1200Mpps；≥24 个千兆电口，≥4 个万兆 SFP+，≥1 个扩展插槽；双电源；≥2 个万兆多模光模块；≥1 根万兆堆叠线缆；支持静态路由、RIP V1/2、RIPng、OSPF、OSPFv3 等；支持 IPv4/IPv6 双栈协议；支持 Telemetry 技术，支持 SNMP 协议。 | 台 | 2 |
| 4 | 核心交换机 | 交换容量≥500Tbps；包转发率≥100000Mpps；双主控，双电源，≥48 个万兆光口，≥4 个万兆多模光模块，≥4 个千兆多模光模块；≥2 个交换插槽，≥4 个业务插槽；支持 IPv4/IPv6 双栈协议；支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；支持横向虚拟化功能；支持纵向虚拟化技术，含项目所需线缆等组件。 | 台 | 2 |
| 5 | 业务交换机 | 交换容量≥2.8Tbps，转发性能≥2000Mpps；≥48 个万兆光口，≥2 个 40GE QSFP+口，≥4 个 100GE 光接口；≥40 个万兆多模光模块，≥1 根≥40G 堆叠线缆；≥4 个风扇，冗余电源；支持 IPv4/IPv6 双栈协议；支持集群或堆叠多虚一技术，支 | 台 | 2 |

| | | | | |
|---|---|---|---|---|
| | | 持纵向虚拟化技术。 | | |
| 6 | 管理交换机 | 交换容量≥1.30Tbps，转发性能≥550Mpps，千兆电口端口数量≥48 个，万兆 SFP+端口≥6 个；≥4 个 SFP+万兆多模光模块，≥1 根≥万兆堆叠线缆；支持 IPv4/IPv6 双栈协议；支持 RIPv1/RIPv2/RIPng，OSPF v1/v2/v3。 | 台 | 2 |

## 计算和存储系统设计

### 建设原则

服务器设备应满足本项目建设需求，在满足平台建设需求的前提下，尽量采用优化设计，使服务器资源能够满足用户的高性能、高安全可靠、可扩展、可管理等需求。服务器设备应满足以下配置原则：

（1）高性能原则

本项目拟采用的服务器设备，应达到当前服务器设备主流高端性能标准、技术先进，在运行速度、磁盘读写、容错能力、稳定性、监测功能及电源能效等方面具有较高的性能指标。

（2）安全可靠性原则

本项目落实国家深化安全可靠应用替代工作要求，基于医疗行业信息系统国产化适配情况，本项目的网络交换设备、集中式存储（全闪存）、虚拟化集中式存储、分布式存储、网络安全设备、备份设备采用国产自主可控产品；本项目其他有关软硬件设备的采购选用国产自主可控产品。

（3）可扩展性原则

本项目拟采用的服务器设备，应具有优秀的可扩展性原则。能及时调整配置来适应业务的发展，使服务器随负荷的增加而平稳升级，保证服务器工作的稳定性和连续性。

（4）可管理性原则

本项目拟采用的服务器设备，应易于操作和管理，对支持标准的管理系统进行有效地管理，实现较低的维护成本。

### 架构设计

计算和存储系统，主要在医卫专网和互联网配置服务器、虚拟化平台，具体架构如下图：

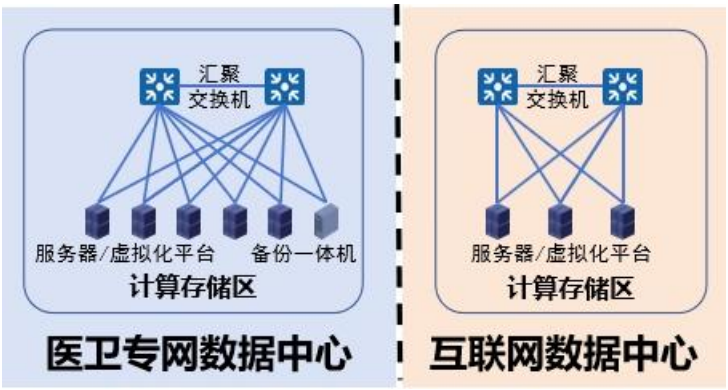


**图 2-3 计算和存储系统架构图**

**配置方案**

服务器作为业务系统的核心，承担着业务数据的存储和处理，具有业务量大、存储量大的特点，特别是关键业务服务器的选择尤为重要。服务器的可靠性和可用性是首要的需求，其次是数据处理能力和安全性，然后是可扩展性和可管理性。为保证信息系统持续稳定高效地运行，须保证服务器存储系统具有较高的可靠性、可扩展性和灾难恢复能力。数据库对于服务器的性能要求也不一样，对于大型数据库来说，服务器往往仅用来运行数据库，或仅运行单一的应用，需要有较高的 CPU 处理能力，大容量内存为数据缓存服务，并需要很好的 I/O 性能，使用这类应用时，通常需要有较高的 CPU 主频，基于中高端主机系统是适用于数据库服务器的选择。根据实际业务和功能需求，数据库服务器需要高可靠性、高性能、架构领先以及可维护性高的服务器产品来支撑信息系统的稳定与高效运行，满足郑州市慢病管理服务信息平台运行环境与配置，同时满足郑州市慢病管理服务信息平台 3～5 年运行需求。各类设备应具有良好的扩展性，方便灵活升级。

另外为了充分利用服务器硬件资源，应用服务器也可采用服务器虚拟化技术提供数据中心算力服务，服务器虚拟化技术可以使一个物理服务器虚拟成若干个服务器使用。服务器虚拟化需要具备以下功能和技术：

多实例：在一个物理服务器上可以运行多个虚拟服务器。

隔离性：在多实例的服务器虚拟化中，一个虚拟机与其他虚拟机完全隔离，以保证良好的可靠性及安全性。

CPU 虚拟化：把物理 CPU 抽象成虚拟 CPU，无论任何时间一个物理 CPU 只能运行一个虚拟 CPU 的指令。而多个虚拟机同时提供服务将会大大提高物理 CPU 的利用率。

内存虚拟化：统一管理物理内存，将其包装成多个虚拟的物理内存分别供给若干个虚拟机使用，使得每个虚拟机拥有各自独立的内存空间，互不干扰。

设备与 I/O 虚拟化：统一管理物理机的真实设备，将其包装成多个虚拟设备给若干个虚

拟机使用，响应每个虚拟机的设备访问请求和 I/O 请求。

无知觉故障恢复：运用虚拟机之间的快速热迁移技术（LiveMigration），可以使一个故障虚拟机上的用户在没有明显感觉的情况下迅速转移到另一个新开的正常虚拟机上。

负载均衡：利用调度和分配技术，平衡各个虚拟机和物理机之间的利用率。

统一管理：由多个物理服务器支持的多个虚拟机的动态实时生成、启动、停止、迁移、调度、负荷、监控等应当有一个方便易用的统一管理界面。

快速部署：整个系统要有一套快速部署机制，对多个虚拟机及上面的不同操作系统和应用进行高效部署、更新和升级。

通过服务器虚拟化技术将操作系统从运行它的底层硬件中抽离出来，并为操作系统及其应用程序提供标准化的虚拟硬件，从而使多个虚拟机能够同时在一台或多台共享处理器上独立地运行。借助虚拟化技术，可以轻松将多个不同服务器的工作负载整合到更为可靠并且性能更高的硬件上。

借助虚拟化技术将服务器的处理器、内存、磁盘和网络连接一起转换到了一个逻辑计算资源池中。操作系统及其应用程序被隔离到安全、可移植的虚拟机中。随后，基础架构会根据每个虚拟机的需要和优先级，将系统资源动态地分配给它们，从而实现主机级容量利用率以及对服务器资源的控制。由于虚拟机可以在资源池中的任一物理服务器上运行，并且无需宕机便可在这些服务器之间无缝地转移。因此，虚拟机可动态、自动地分配给资源池中最合适的主机，从而确保软件应用程序的服务级别。通过将硬件资源聚合到资源池，IT 环境可得到优化，从而动态支持不断变化的业务需求，同时确保灵活有效地利用硬件资源。

结合以上分析，本项目拟采用服务器虚拟化方式，资源池通过采用软件定义计算、软件定义存储、软件定义网络等技术将高性能物理服务器进行池化，将应用程序对底层系统和硬件的依赖抽象出来，解耦应用和操作系统与硬件，使物理设备的差异性、兼容性与上层应用透明，实现业务运行环境的快速部署、运行资源大小的及时动态调整，达到高可靠、自动化运维的目标。

根据估算及实际业务部署需求，本项目对服务器计算资源需求 CPU 总核数为 572 核，医卫专网的计算资源占比为 65%，约为 372 核，互联网的计算资源占比为 35%，约为 200 核。

按照服务器 2 颗 CPU，单 CPU 物理核数 24，CPU 计算资源需要服务器计算如下：

1.医卫专网计算资源

372÷（2×2×24）≈4 台（按单个物理核心虚拟 2 个虚拟核心进行规划）。

2.互联网计算资源

200÷（2×2×24）≈3 台（按单个物理核心虚拟 2 个虚拟核心进行规划）。

虚拟化计算资源在医卫专网区域需要配置 4 台服务器，单台服务器配置 2 颗 24 核心 CPU，512GB 内存；虚拟化计算资源在互联网区域需要配置 3 台服务器，单台服务器配置 2 颗 24 核心 CPU，512GB 内存；

**表 2-2 计算和存储系统配置表**

| 序号 | 设备及软件名称 | 主要技术（性能）指标 | 单位 | 数量 |
|---|---|---|---|---|
| 1 | 服务器 | 标准机架式服务器；国产芯片、国产处理器；≥2 颗 24 核 X86 架构 CPU 或 2 颗 48 核 ARM 架构 CPU，主频≥2.2GHz；≥512GB 内存；≥2 块 960GB SSD 硬盘；≥4 个 10G 光口（含光模块），≥4 个千兆电口；≥1 块独立 RAID 卡（≥4GB 缓存）；冗余电源；≥4 块 4TB SATA HDD 硬盘，≥2 块 1.92TB SSD 硬盘。 | 台 | 4 |
| 2 | 服务器 | 标准机架式服务器；国产芯片、国产处理器；≥2 颗 24 核 X86 架构 CPU 或 2 颗 48 核 ARM 架构 CPU，主频≥2.2GHz；≥256GB 内存；≥2 块 960GB SSD 硬盘；≥4 个 10G 光口（含光模块），≥4 个千兆电口；≥1 块独立 RAID 卡（≥4GB 缓存）；冗余电源；≥2 块 4TB SATA HDD 硬盘，≥2 块 1.92TB SSD 硬盘。 | 台 | 3 |
| 3 | 虚拟化软件 | 支持 CPU 虚拟化，将物理服务器的 CPU 虚拟成虚拟 CPU（vCPU），供虚拟机运行时使用。当多个 vCPU 运行时，会在各 vCPU 间动态调度物理 CPU 的能力。支持主流的操作系统虚拟化。支持虚拟机管理，包含虚拟机资源管理、虚拟机生命周期管理、虚拟机模板管理、CPU QoS、虚拟资源动态复用、虚拟机资源动态调整、虚拟网卡、网络 I/O 控制、迁移网络、内置负载服务、分布式虚拟交换机、跨主机热迁移、跨存储热迁移、虚拟机高可用性（HA）、虚拟机回收站、动态资源调度（DRS&DPM）、虚拟机资源 QoS、网络安全组、VMware 虚拟机模板导入等功能。支持支持虚拟机和其他物理服务器统一管理。支持对系统环境检测，支持常见的虚拟资源和物理资源报警，支持虚拟服务器自助申请、自助缴费功能，支持虚拟使用报表导出，支持其他虚拟化平台统一纳管，提供 B/S 和 C/S 两种虚拟机控制台使用方式，支持网络流量优化、宿主机自治、迁移工具、虚拟机迁移工具等功能。满足本项目配置服务器虚拟化需要，具有扩展至≥10 台服务器虚拟化能力。 | 套 | 2 |

## 安全系统建设

### 安全技术体系

# 安全物理环境

机房建设参照等级保护三级物理环境安全控制项的要求，结合《数据中心设计规范》（GB50174-2017）标准进行建设，主要涉及的范畴包括环境安全（防火、防水、防雷击等）、设备和介质的防盗窃防破坏等方面。具体包括：物理位置选择、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、电力供应和电磁防护等控制点。

本项目利旧郑州市第七人民医院滨河院区机房进行建设，郑州市第七人民医院滨河院区机房符合《数据中心设计规范》（GB50174-2017）B 级机房建设标准，能够满足项目建设需求。

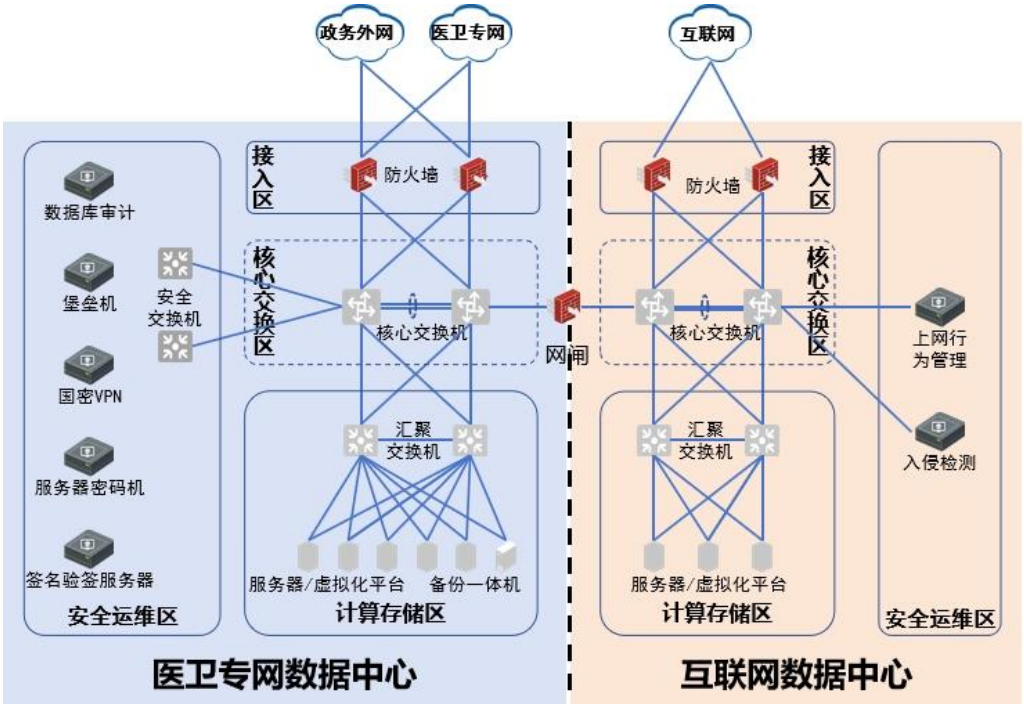


**图 2-4 网络安全架构图**

# 安全通信网络

依据等级保护要求第三级中网络和通信安全相关安全控制项，结合安全通信网络对通信安全审计、通信数据完整性/保密性传输、远程安全接入防护等安全设计要求，安全通信网络防护建设主要通过通信网络安全传输、通信网络安全接入，以及通信网络安全审计等机制实现。

（1）网络层架构保障

网络系统采用包括设备冗余、链路冗余的网络架构，满足租户业务连续性需求；提供的共享网络带宽能满足业务高峰期的需求，保证各业务系统正常运行。

本项目在数据中心出口通过防火墙配置 QoS 功能，实现对重要业务应用的带宽保障，并限制每个应用的带宽使用上限，避免个别用户占用过多带宽资源，提高网络资源利用率。

（2）区域边界隔离

网络边界隔离：在数据中心医卫专网与互联网之间部署网闸设备，利用其协议隔离和转换的功能对医卫专网、互联网进行安全隔离，避免医卫专网直接暴露在互联网上，医卫专网与互联网之间的所有通信和数据交换行为均需要通过网闸进行控制和转换。

内部重要区域边界隔离：在安全域划分的基础上，按照用户实际需求，对内部网络不同

安全域划分不同逻辑子网（VLAN），并在 VLAN 之间定义安全策略或访问控制规则（ACL），实现网络内部不同安全域之间的基本隔离。

高可用性设计：单线路、单设备的结构很容易发生单点故障导致业务中断，因此对于提供关键业务服务的信息系统，应用访问路径上的任何一条通信链路、任何一台网关设备和交换设备，都应当采用可靠的冗余备份机制，以最大化保障数据访问的可用性和业务的连续性。本项目在数据中心出口接入链路应采用多运营商链路互备、关键业务系统应采用多服务器互备外，对于数据中心骨干核心链路和安全网关设备等均采用冗余热备的部署方式，以提升网络系统的整体容错能力，防止出现单点故障。

（3）远程安全接入

本项目采用堡垒机来满足远程访问或远程运维的安全通信要求，保证敏感/关键的数据、鉴别信息不被非法窃听、暴露、篡改或损坏。

根据市域一体化慢病管理服务信息平台网络现状、业务特点及安全需求，对其网络区域划分进行如下设计，将网络划分为医卫专网、互联网两个部分；其中，医卫专网 4 个安全域：网络接入区、核心交换区、安全运维区、计算存储区；互联网划分 3 个安全域：网络接入区、核心交换区、计算存储区。

在医卫专网安全运维区部署国密 VPN 系统实现对通信数据的安全加密，对通信过程中的整个报文或会话过程进行加密，实现用户接入信息的加密传输，保证重要、敏感信息在通信传输过程中的完整性和保密性。

为了保障外部人员安全接入政务网络，同时又能提供灵活的接入方式，需要 VPN 设备符合国密局制定的《IPSEC VPN 技术规范》和《IPSEC VPN 技术规范》，支持国家商用密码算法 SM1、SM2、SM3、SM4；并且支持用户名口令、数字证书等多种组合捆绑的认证方式，以确保用户身份的可信。

VPN 系统具备以下基本功能：

安全接入管理：通过结合使用数字证书与专用 VPN 客户端软件，实现接入身份以及设备的准确识别、对接入终端的安全管理，保证系统接入过程的安全可靠。

传输过程安全：借助 IPSEC 或 SSL VPN 技术的隧道加密技术实现网络通信过程及数据传输过程的安全，并且可根据不同人员的角色确认应用的访问权限，实现随时随地，按需接入及受限访问，最大程度保证传输过程安全。

接入及传输过程管理：通过接入管理端对接入人员及接入设备进行统一管理，可实现人员的角色及权限的统一管理，实现不同角色访问不同的访问咨询。针对接入设备的安全性问

题，通过对设备进行合规性检查，确保设备接入后不会给网络带来风险。通过对接入过程进行安全审计，实时掌握接入及传输过程的状态并对网络接入及传输行为进行审计。

# 安全区域边界

依据等级保护要求第三级中网络和通信安全相关控制项，结合安全区域边界对于区域边界访问控制、区域边界包过滤、区域边界安全审计、区域边界完整性保护等安全设计要求，安全区域边界防护建设主要通过网络架构设计、安全区域划分，基于地址、协议、服务端口的访问控制策略；通过安全机制来实现区域边界的综合安全防护。具体如下：

（1）边界防护

网络安全系统为租户划分安全区域，在划分的不同区域之间部署相应的边界防护设备进行防护。通过部署边界安全网关配置细颗粒度的基于地址、协议和端口级的访问控制策略，实现对区域边界信息内容的过滤和访问控制，对非授权设备私自联到内部网络的行为进行检查或限制，来自内部用户非授权连到外部网络的行为进行检查或限制。

同时本项目在医卫专网和互联网的核心区分别部署两台下一代防火墙实现计算存储区与其他区域之间的边界安全防护。本项目在医卫专网和互联网之间配置网闸区域边界安全防护。

下一代防火墙具备以下基本功能：

安全隔离：防火墙串接部署实现内外网安全隔离和内部不同网络区域之间的安全隔离。

网络访问控制：防火墙工作在网络出口及不同网络区域之间，对内外网络之间及内部各个网络区域之间流转的数据进行深度分析，依据数据包的源地址、目的地址、通信协议、端口、流量、用户、通信时间等信息进行判断，确定是否存在非法或违规的操作，对不符合允许转发策略的流量进行阻断，从而有效保障网络安全。

会话监控：在防火墙配置会话监控策略，当会话处于非活跃一定时间或会话结束后，防火墙自动将会话丢弃，访问来源必须重新建立会话才能继续访问资源。

防范带宽滥用：可基于应用内容而非协议端口识别包括传统协议、P2P 下载、股票交易、即时通讯、流媒体、网络游戏、网络视频等常见网络应用，并能够详细统计每一种应用的流量、连接数和累积传输字节数，判断网络中的各种带宽滥用行为，继而采取包括阻断、限制连接数、限制流量等各种控制手段对网络应用访问流量进行精细化管理，确保关键应用或重要用户的带宽使用，确保网络业务通畅，满足业务高峰期带宽需要。

网闸具备以下基本功能：

内外网之间部署网闸，对 TCP/IP 数据包进行协议剥离，通过基于专用硬件和专有协议

的数据摆渡机制实现内外网之间安全的信息交换，阻断一切基于 TCP/IP 网络协议包头的未知攻击。网闸设备采用“2+1”系统架构，即内、外双主机系统加专用隔离硬件，其信息交换功能通过内、外端机来实现，信息交换的安全性通过隔离系统来保证。根据信息交换的发起源所在位置，支持从内端机向外端机和从外端机向内端机两个方向的数据交换，并对两方的数据交换进行访问控制。网闸支持基于通用的应用协议（如 HTTP、FTP、Telnet、SMTP、POP3、数据库访问、数据库同步、文件同步等）和用户自定义协议（TCP、UDP）的信息交换。

（2）区域边界入侵防护

网络安全系统部署的网络入侵防护主要在网络区域边界/重要节点检测和阻止针对内部的恶意攻击和探测，诸如对网络蠕虫、间谍软件、木马软件、溢出攻击、高级威胁攻击等多种深层攻击行为，进行及时检测、阻止和报警。

本项目在互联网和医卫专网配置的下一代防火墙具备入侵防护功能，实时发现和阻止从外部网络发起的网络攻击行为；阻止来自其他网络区域的攻击流量。

下一代防火墙可实现以下入侵防御功能：

防范网络攻击：综合采用模式匹配、协议分析、统计分析、流量异常检测、会话关联分析以及防逃逸等技术手段准确识别入侵攻击行为，为用户提供 2~7 层深度入侵检测能力。支持发现并阻断包括溢出攻击类、RPC 攻击类、WEBCGI 攻击类、拒绝服务类、木马类、蠕虫类、扫描类、网络访问类、HTTP 攻击类、系统漏洞类等在内的各种网络恶意攻击。

防范拒绝服务攻击：通过构建统计性攻击模型和异常包攻击模型，可以全面防御 SYN flood、ICMP flood、UDP flood、ARP Flood、DNS Flood、DHCP flood、Winnuke、TcpScan 以及 CC 等常见 DOS/DDOS 攻击行为。

防范带宽滥用行为：可根据数据内容而非端口智能识别包括传统协议、P2P 下载、股票交易、即时通讯、流媒体、网络游戏、网络视频等常见网络应用，并能够详细统计每一种应用的流量、连接数和累积传输字节数，判断网络中的各种带宽滥用行为，继而采取包括阻断、限制连接数、限制流量等各种控制手段，确保网络业务通畅。

通过在互联网部署上网行为管理，提供多种身份验证方式，完善实名制准入机制，并对入网终端进行多样化的入网要素校验与审核，对全网接入终端进行可信接入认证与检测，确保接入终端的安全性、唯一性、可控性，为医院构建可信终端入网体系，防止非授权终端接入内部网络。同时保存至少 6 个月的访问日志，以便协助公安调查取证。具体实现功能：

URL 过滤：上网行为管理设备中内置千万级 URL 列表，将 URL 按照一定的标准进行预分类，然后依据策略对内部用户访问的各种类别网页进行过滤。在过滤 URL 记录的同时，可以

对网络中所访问的 URL 进行记录和统计排名，以实现对 URL 访问的监控和控制。员工依然可以上网浏览网页，但其访问时间和内容将受到一定监控。

关键字过滤：上网行为管理设备提供对发帖的内容启用关键词过滤，对含有攻击国家领导人、分裂国家言论、下流词汇，或者伤害公司利益的帖子进行审计和过滤处理，并能对所有成功上传的内容进行详细记录以便事后查验。从而帮助员工养成远离低俗内容的上网习惯，协助推动“互联网低俗内容整治”，帮助企事业单位建立健康、规范、有序的上网环境。

黑名单控制：为防止网络资源的滥用和方便管理员管理用户，上网行为管理设备支持将用户加入黑名单的功能。对进入黑名单的用户可以采取惩罚机制，惩罚期限到了之后，该用户又可以正常使用网络。用户一旦进入黑名单，当再次上网时，网页回弹出已经进入黑名单、是什么原因进入黑名单的。灵活的黑名单功能可以帮助管理员快速、准确的定位出谁肆意占有网络资源。对黑名单的控制，有一个生效时间，在生效时间内才进行黑名单的控制。在生效时间外，不对用户的速率和会话进行限制，用户产生的流量也不计入黑名单的流量配额内。

白名单管理：对于公司领导或者重要的用户，他们的上网不希望受到各种控制策略的限制，也不希望上网的内容被记录。设备的白名单功能可以很好的满足这些需求。符合白名单规则的流量，将不受“防火墙规则、流控规则、认证策略规则、上网策略对象规则、黑名单规则”的控制；同时上网的流量和上网行为的内容（如发送的邮件、发送的帖子、访问的网页、即时通讯记录等）将全部不记录。

上网行为监控：支持制定精细化的信息收发监控策略，有效控制信息的传播范围，上网行为管理设备能够对以下信息发送进行监控与控制：WEB 访问记录、论坛发帖、电子邮件、即时通讯软件、FTP 记录、Telnet 记录。

上网行为审计：上网行为管理设备可记录全部的会话日志。通过检查完整的会话日志，管理者可以跟踪网络中的任何操作，尤其可帮助公安部门稽查案件。上网行为管理设备的会话记录包括：源 IP、目的 IP、协议类型、七层应用名称、源端口、目的端口、是否进行 NAT 转换（可显示转换后的 IP 和端口）、会话产生的时间和会话持续时间。

另外，还应关闭医院网络中所有路由器、交换机与安全设备等相关设备的闲置端口，进一步降低非法终端入网的风险。

# 安全计算环境

依据等级保护要求第三级中设备和计算安全、应用和数据安全等相关安全控制项，结合安全计算环境对于用户身份鉴别、自主与标记访问控制、系统安全审计、恶意代码防护、安全接入连接、安全配置检查等技术设计要求，安全计算环境防护建设主要通过身份鉴别与权

限管理、Web 应用攻击防护、网页篡改安全防护、主机安全加固、漏洞扫描、数据库审计管理，重要节点设备冗余备份，以及系统和应用自身安全控制等多种安全机制实现。具体如下：

（1）身份鉴别与访问

本项目在配置堡垒机实现身份鉴别与访问。在系统运维人员和信息系统（网络、主机、数据库、应用等）之间搭建一个唯一的入口和统一的交互的界面，针对信息系统中关键软硬件设备运维的行为进行管控及审计。通过将各设备、应用系统的管理接口，通过强制策略路由的方式，转发至堡垒主机，从而完成反向代理的部署模式，实现对管理用户的身份鉴别。通过“数字证书”认证方式作为“用户名+口令”验证身份的有效补充和增强，实现等级保护三级要求的双因素身份认证。

堡垒主机主要实现功能包括：

单点登录：提供基于 B/S 的单点登录系统，用户通过一次登录系统后，就可以无需认证的访问包括被授权的多种基于 B/S 的应用系统，使用户无需记忆多种登录用户 ID 和口令。单点登录可以实现与用户授权管理的无缝连接，可以通过对用户、角色、行为和资源的授权，增加对资源的保护和对用户行为的监控及审计。

集中账户管理：支持对所有服务器、网络设备登录账号的集中管理，是集中授权、认证和审计的基础，降低了管理大量用户账号的难度和工作量。同时，还能够制定统一的、标准的用户账号安全策略。集中账号管理可以实现将账号与具体的自然人相关联，从而实现针对自然人的行为审计。

统一身份认证：为用户提供统一的认证接口。采用统一的认证接口不但便于对用户认证的管理，而且能够采用更加安全的认证模式，提高认证的安全性和可靠性，同时又避免了直接在业务服务器上安装认证代理软件所带来的额外开销。集中身份认证提供静态密码、数字证书、一次性口令和生物特征等多种认证方式，而且提供接口，可以方便地与第三方认证服务对接。建议采用基于静态密码+数字证书的双因素认证方式。

统一资源授权：提供统一的界面，对用户、角色及行为和资源进行授权，以达到对权限的细粒度控制，最大限度保护用户资源的安全。通过集中访问授权和访问控制可以对用户通过 B/S、C/S 对服务器主机、网络设备的访问进行审计和阻断。授权的对象包括用户、用户角色、资源和用户行为。系统不但能够授权用户可以通过什么角色访问资源这样基于应用边界的粗粒度授权，对某些应用还可以限制用户的操作，以及在什么时间进行操作等的细粒度授权。

细粒度访问控制：提供细粒度的访问控制，最大限度保护用户资源的安全。细粒度的命

令策略是命令的集合，可以是一组可执行命令，也可以是一组非可执行的命令，该命令集合用来分配给具体的用户，来限制其系统行为，管理员会根据其自身的角色为其指定相应的控制策略来限定用户。访问控制策略是保护系统安全性的重要环节，制定良好的访问策略能够更好的提高系统的安全性。

操作审计：操作审计管理主要审计操作人员的账号使用（登录、资源访问）情况、资源使用情况等。在各服务器主机、网络设备的访问日志记录都采用统一的账号、资源进行标识后，操作审计能更好地对账号的完整使用过程进行追踪。为了对字符终端、图形终端操作行为进行审计和监控，堡垒主机对各种字符终端和图形终端使用的协议进行代理，实现多平台的操作支持和审计，例如 Telnet、SSH、FTP、Windows 平台的 RDP 远程桌面协议，Linux/Unix 平台的 X Window 图形终端访问协议等。

（2）Web 应用安全防护

网络安全系统的 Web 应用安全防护主要针对 Web 服务器进行 HTTP/HTTPS 流量分析，防护以 Web 应用程序漏洞为目标的攻击，能够防止包括 CGI 漏洞扫描攻击、SQL 注入攻击、XSS 攻击、CSRF 攻击防护，以及 Cookie 篡改防护、网站盗链防护、网页挂马防护、WebShell 防护等各种针对 Web 系统的入侵攻击行为。

本项目在外网核心区配置下一代防火墙，实现 Web 应用安全防护。对 WEB 应用服务和网页内容进行防护，屏蔽对网站的攻击和篡改行为，实现防跨站攻击、防 SQL 注入、防止黑客入侵、网页防篡改等功能，从而更有效地对网站服务器系统及网页内容进行安全保护，从应用和业务逻辑层面真正解决 WEB 网站安全问题。

下一代防火墙可实现以下 WEB 应用防火墙功能：

WEB 应用威胁防御：支持对 HTTP 数据流进行深度分析，内置针对 WEB 攻击防护的专用特征规则库，规则涵盖诸如 SQL 注入、XSS（跨站脚本攻击）等 OWASP TOP10 中的 WEB 应用安全风险，及远程文件包含漏洞利用、目录遍历、OS 命令注入等当今黑客常用的针对 WEB 基础架构的攻击手段。对于 HTTP 数据包内容具有完全的访问控制权限，检查所有经过网络的 HTTP 流量，回应请求并建立安全规则。一旦某个会话被控制，WAF 能对内外双向流量进行多重检查，以阻止内嵌的攻击，保证数据不被窃取。网站管理者也可以指定各种策略对 URL、参数和格式等进行安全检查。

网页防篡改：WAF 应能够监控网页请求的合法性，实时拦截篡改攻击。同时，通过比对请求页面的哈希指纹，校验被请求的网页是否被篡改。一旦检测到发生网页篡改紧急事件时，WAF 会将用户请求重定向到默认页面或指定的正常页面，使篡改攻击者的意图不能得逞。视

篡改的程度或网站特殊需求，启动专业的应急机制。一方面支持对网络流量进行有效控制，及时阻止篡改攻击行为，保证网站形象。另一方面可提供多种形式的告警机制，通知网站管理者进行事件分析和历史追溯，从而完成 WEB 服务器的配置及数据恢复，杜绝网页内容连续被篡改。

抗拒绝服务攻击：WAF 系统中集成抗拒绝服务攻击功能，能够防御迄今已知的所有种类 DDoS 攻击，如 SYN Flood、UDP Flood、ICMP Flood、ping of Death、Smurf、HTTP-get Flood 等。同时对未知攻击也能进行有效防护。主要技术包括：

攻击指纹识别：利用多种技术手段对网络数据包进行特征统计和发现，能够准确定位当前的攻击类型，并触发不同的防御机制，在提高效率的同时确保防护准确度。

异常流量识别：支持基于数据挖掘的 DDoS 攻击盲检测技术。利用关联算法和聚类算法自适应的产生检测模型，任何偏离这些正常状态的流量特征都可以被捕获，从而可以实时、自动、有效地识别出异常流量。

攻击特征挖掘：具备高效的攻击特征挖掘能力。系统通过对网络流量的显微分析，挖掘出攻击特征，并将攻击特征移交给规则执行机进行高效执行。

攻击流量过滤：针对检测出的攻击流量，采用规则执行机技术，准确彻底地过滤攻击流量，放行正常流量，保证网站服务的正常进行。

（3）日志审计管理

日志审计系统能够通过主被动结合的手段，实时不间断地采集用户网络中各种不同厂商的安全设备、网络设备、主机、操作系统，以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心，进行集中化存储、备份、查询、审计、告警、响应，并出具丰富的报表报告，实现全生命周期的日志管理。

通过使用 syslog、snmp 或其他协议采集各资源层安全资源、网络资源、主机资源的日志及告警信息，对各项资源的运行状态进行被动监控。

本项目配置数据库审计，实现平台日志审计管理。

1）数据库审计

数据库审计在后台数据库服务器与接入交换机之间串接，作为数据库系统的第一道安全防线，实现细粒度的访问控制，所有对数据库服务器的访问必须经过该系统进行检测和控制。提供事前预防（如 SQL 注入攻击防护）、事中控制（如高危操作阻断）、事后分析（如详细数据变更审计）等全面的数据库安全管控能力。

数据库审计主要功能包括：

数据库用户权限的细粒度管理：在不影响数据库用户配置的前提下，对于当前数据库用户所具有的权限提供更详细的虚拟权限控制，数据库用户如果需要访问数据库，那么就需要受到数据库安全网关的访问权限限制。数据库用户权限的细粒度管理功能，避免 DBA 花费大量精力对数据库用户的权限重新调整，同时，避免了数据库用户权限滥用造成的数据泄露等危险。

全面、精细、实时的审计分析和追踪：采用智能 SQL 语法分析技术，对发往数据库的 SQL 语句进行分析，并将 SQL 语句还原为对数据库的操作行为，进行细粒度的记录、审计和报表展现，对高风险的 SQL 操作进行告警甚至阻断。对于业务系统的特殊部署（比如应用系统与数据库系统同台部署）或运维操作（比如直接在服务器操作数据库、远程桌面访问数据库等），常规数据库审计方法是无法监控到的。数据库审计系统可以提供本地探针的部署方式，全面审计到对数据库的本地访问行为，确保审计信息无死角。数据库审计可以对违规操作数据库的行为进行记录、追踪和取证，这对内部网络犯罪是一种强大的威慑。

数据库审计日志数据脱敏：用其他内容代替检索结果以及报表中的敏感信息，在结果中会显示遮蔽后的内容。可以进行正则式的配置，如符合身份证正则式的信息全部替换为 XXX，则显示结果中凡是身份证号全部替换为 XXX。

数据库状态监控：通过监控数据库系统的内存使用状况、缓冲区管理统计、用户连接统计、Cache 信息、锁信息、SQL 统计信息、数据库信息、计划任务、线程信息、关键效率、缓冲区命中率等信息来判断数据库系统运行是否正常，保证数据库系统的可用性和响应能力。

（4）数据备份恢复

通过备份一体机备份机制，进行本地备份，每周定期全量备份一次，备份内容包含服务器的系统盘和数据盘。在服务器出现故障时，可选择快照进行恢复。

运维人员定期对业务系统、数据库系统、关键配置文件等进行全量备份和增量备份，并在业务系统出现故障时能确保正常恢复。

（5）个人信息保护

等级保护对象中业务系统在需要采集个人信息时，应当仅采集和保存必须的用户个人信息，与业务无关的个人信息应当禁止被业务系统或其组件采集。通过访问控制限制对用户信息的访问和使用进行限制，实现禁止未授权访问和非法使用用户个人信息。同时，组织应当按照等级保护相关要求，制定保障个人信息安全的管理制度和流程，严格按照个人信息保护管理制度和流程进行操作，对违反个人信息保护管理制度和流程的人员进行处罚，保障用户

个人隐私数据信息和利益不受到侵害。

采集的个人信息包括但不限于：姓名、性别、年龄、电话、地址等个人隐私数据，应当按照法律法规要求妥善保管，必要时采取加密措施对数据的传输和存储进行加密处理，以保障用户的个人数据不会被泄露或篡改。按照工作职能和人员的岗位职责分配业务系统账号和访问权限，保证业务系统数据库内存储的数据信息不被用户越权访问。

# 安全管理中心

依据等级保护要求第三级中网络和通信安全相关安全控制项，配置安全管理中心，结合安全管理中心对系统管理、审计管理、安全管理和集中管控的设计要求，安全管理中心建设主要通过运维管理平台、堡垒机等机制实现。实现平台的安全管理、审计管理、集中管控。

（1）安全管理

可通过堡垒机系统，将重要信息系统资产的地址均纳入运维管理系统的管理范围，通过运维审计系统使用系统管理员账号对系统的资源和运行进行配置、控制和管理。

（2）审计管理

审计管理通过数据库审计系统对审计数据进行查询、统计、分析，实现对数据库操作等行为的监测和报警功能，能够对发现的安全事件或违反安全策略的行为及时告警并采取必要的应对措施。

（3）集中管控

根据建立统一的纵深防御体系的要求，应建立安全管理中心，实现对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络的安全机制实施统一管控，确保系统安全可靠运行。安全管理中心是一个集合的概念，由安全管理区域或平台实现，核心是实现所有安全机制的统一集中管理。

在等级保护对象网络中按照安全域分域防护原则，单独划分特定的运维管理域，该区域部署所有涉及网络安全的设备或组件，包括主机安全管理系统、数据库审计系统、运维管理系统等，对分布在网络中的安全设备或安全组件进行集中管控。

本项目在医卫专网部署态势感知设备，实现慢病管理服务信息平台网络安全的统一风险感知。

# 应用数据安全

本项目配置数据库审计系统等实现平台应用数据安全防护。

（1）共享服务访问控制模型设计

共享服务访问采用 OAuth2.0 标准授权认证，采用的是简化方式。接入的其他局委非公开服务采用二次封装方式，发布于共享服务平台，供相关系统使用统一的方式授权调用。

共享服务访问流程：首先平台为每个接入的系统分配应用 ID 和密钥；然后系统在访问平台服务时，需要先根据分配的应用 ID 和密钥请求获取令牌；最后携带令牌去访问平台服务。

为确保访问安全，令牌有一定时效性，需要定期刷新或重新获取令牌。

（2）数据库访问控制模型设计

用户权限设计是实现数据安全访问的一种重要方式，数据库系统的用户层次、角色众多，并且潜在的用户也较多。仅从数据库自带的用户权限体系来考虑对数据的访问，既不利于安全（暴露了数据库信息），也不适应潜在的用户增多的情况（例如提供数据的信息发布，访问的用户不可预料），同时也增加了数据库的资源消耗（新建一个用户比增加一条表记录的消耗要大）。

本系统采用二级真用户的模型进行数据库访问，可以更方便灵活地控制数据库访问，也更便于权限的控制。

（3）数据库权限控制模型设计

数据库用户面向数据库，决定能否访问数据库。面向系统功能访问的用户更多的是面向系统，决定能否执行某项功能。

模拟通用关系型数据库的角色和用户控制体系，从大到小各方面对权限进行控制。

“数据库角色”是主要用来批量权限指定。可以自定义角色，让某个角色具备特定的功能。

对于用户而言，通过指定其隶属于某一角色，即可以批量赋予其指定权限。让用户和角色对应，可以通过角色来控制用户，以后修改角色可以批量修改指定的所有用户。存在一种特定的角色，“未知角色”，可以对此类用户指定自定义的权限。

**安全管理体系**

# 安全管理制度

根据等级保护基本要求对管理制度建设的要求，对安全策略体系进行规划。体系包括确定市域一体化慢病管理服务信息平台信息安全愿景和使命的信息安全总体目标，约束和指导人员信息安全工作的规章制度、管理办法和工作流程，规范市域一体化慢病管理服务信息平台、网络和安全管理员进行安全操作的技术标准和规范。

信息安全方针是纲领性的安全策略主文档，阐述了安全策略的目的、适用范围、信息安

全目标、信息安全的管理意图等，是信息安全各个方面所应遵守的原则方法和指导性策略。是安全方面工作的最高指导文件。

在项目的安全建设中为保证单位业务系统长期稳定运行以及业务数据的安全性，提高系统运维及人员管理的安全保障机制，实现信息安全管理的不断完善，制定信息安全工作的总体安全方针和策略，明确安全管理工作的总体目标、范围、原则和安全框架等。根据安全管理活动中的各类管理内容建立安全管理制度；并由管理人员或操作人员执行的日常管理操作建立操作规程，形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系，从而指导并有效地规范各级部门的信息安全管理工作。通过制定严格的制度规定与发布流程、方式、范围等，定期对安全管理制度进行评审和修订。

# 安全管理机构

安全管理机构的规划，应以安全组织架构设计为基础，定义架构中涉及的部门和岗位的职责以及管理方法，其内容包含但不少于等级保护基本要求中的第 3 级信息系统的管理要求中对管理机构的要求。

根据其在信息安全工作中扮演的不同角色进行优化组合的结果，反映了各部门在信息安全工作中的不同定位和相互协作关系。信息安全组织架构主要包括参与信息安全决策、管理、执行和监督工作的部门。

信息安全组织架构包含以下三个关键要素：

决定了信息安全工作中正式的报告关系，包括层级数和管理者的管理跨度；

决定了如何由个体组合成部门，再由部门到组织；

组织架构中包含了一套系统，以保证跨部门的有效沟通、合作与整合。

信息安全组织架构是开展信息安全工作的基础。在日常管理过程中，存在着多项信息安全管理事宜，需要对其中的重要事件进行决策，从而为信息安全管理提供导向与支持；对于所制定的信息安全管理方针需要进行有效的贯彻和落实；另外，对信息安全管理方针贯彻落实的情况还需要进行监督，以上各种情况都需要一个完善有效的信息安全组织架构来支撑。另外在未来信息安全保障体系建立的过程中，各种信息安全项目的开展将成为信息安全工作的一项重要内容，这也需要有相应的组织予以支持。

本方案提出的信息安全组织架构是以等级保护基本要求为指导，在借鉴国际最佳实践的基础上根据信息安全工作开展的需求进行完善的结果。

在完整的信息安全组织中一般包含以下几个重要组成部分：

信息安全决策机构

信息安全管理机构

信息安全执行机构

信息安全监管机构

以上组织机构的具体存在形式可以是多样的，如兼职的、虚拟的或者远程的。目前国际上普遍采用的信息安全组织架构如下图所示：

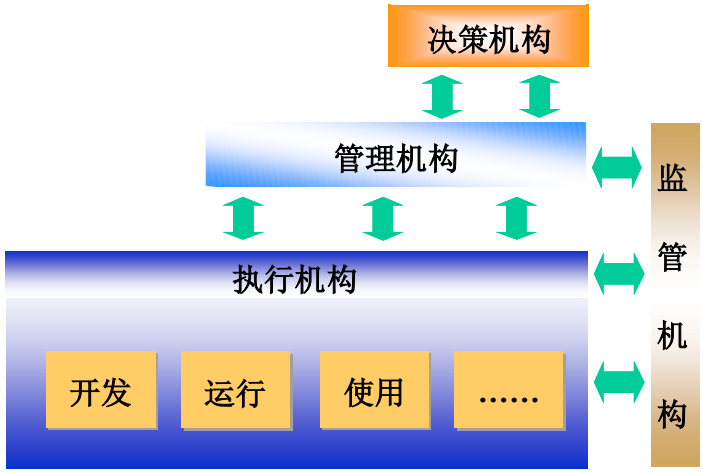


**图 2-5 信息安全组织架构图**

1. 信息安全决策机构

信息安全决策机构处于整个信息安全组织架构的顶端，主要从高层领导的角度对于信息安全方面的工作进行指导和控制，信息安全决策机构应当是安全工作的最高决定者，主要职能包括：

确定信息安全工作的战略和方向；

决定本项目信息安全组织；

总体调配信息安全工作的资源；

负责通过和决定信息安全策略和标准；

对信息安全方面的重大项目进行审批；

在协调安全工作中协调各部门关系；

一般信息安全决策机构在组织中的主要表现形式是由相关各部门主管负责人或代表组成的的信息安全领导委员会，参与人员主要取决于需要决策的内容。信息安全决策机构需要对信息安全工作开展中的重大事项进行决策，因此必须有信息安全专职管理机构的代表；信息安全工作的需求来自于业务的开展，因此很多情况下也考虑各部门的代表的参与；信息安全决策工作中的一项重要课题是资源保障，因此往往需要分别拥有资金调配、人员调配和设备调配权力的部门代表。至于对各部门选派代表的要求取决于决策机构的工作形式，一般来

说需要有相关决定权力的人员作为代表。

2.信息安全管理机构

信息安全管理机构是整个信息安全管理体系建立和维护的组织者和管理者，它同时具有两种角色：

信息安全管理机构是信息安全决策机构的决策支持者，由管理机构为决策机构提供必要的决策所需信息；

信息安全管理机构是信息安全工作的规则制定者和决策推行的管理者。可以说是信息安全决策机构的执行组织，也可以说是信息安全执行机构的管理组织。

信息安全管理机构的职能主要包括：

整个市域一体化慢病管理服务信息平台信息安全相关政策标准的制定、更新；

信息安全项目的规划、评审和质量控制；

对信息安全工作的开展进行日常管理和监督。

3.信息安全执行机构

信息安全执行机构主要负责具体信息安全工作的执行和开展。一般信息安全执行机构主要包括信息安全工程组织和信息安全运行组织两大类的组织。信息安全工程组织一般以独立项目小组的形式存在，由专门的信息安全开发和工程部门和相关工程人员组成。

信息安全工程组织主要负责的工作包括：

信息安全基础建设：包括各项信息安全技术的实施，如认证授权与访问控制系统的建设，信息安全运营中心的建设等。

信息安全管理项目实施：信息安全管理项目的实施也是信息安全工程组织的重要工作之一，例如信息安全规划，信息资产识别与风险评估，信息安全标准与规范的制定等。

对于信息安全运行组织在市域一体化慢病管理服务信息平台中主要负责日常信息系统监控维护方面的工作，并及时汇报日常运作中信息系统的安全情况。信息安全运行组织一般是一个虚拟的机构，包括运行维护、监控和技术支持在内的专职或兼职的信息安全人员，通常会分散安排在各个相关部门中，并统一向专门的信息安全运行管理人员汇报和负责。除此之外，专门的信息安全运营中心或是由外包商提供的监控服务也属于这一机构的范畴内。信息安全运行组织的主要职责可以概括如下：

依照各项管理政策、标准与规范、指南与细则开展工作

提供各种安全服务以直接支持业务，包括监控、事件响应、故障处理等

将工作中的各种需求和重要事项汇报给信息安全管理机构

接受管理机构和监督机构的监管、控制，并配合其开展工作

4.信息安全监管机构

信息安全监管机构的主要职能是对市域一体化慢病管理服务信息平台内信息安全工作的开展情况进行独立的审查和监督。它可以是市域一体化慢病管理服务信息平台的内部审计部门，也可以是独立的外部第三方审计机构，其主要职责如下：

监督各项信息安全策略、标准与规范、指南与细则的执行情况，检验信息安全管理机构和执行机构是否按照其开展工作。

检验信息安全管理机构和执行机构的工作效果，包括信息安全项目审查、信息安全服务效果审查，总体信息安全情况评估和信息系统安全性评价等工作。

信息安全监管机构是针对市域一体化慢病管理服务信息平台信息安全管理机构和执行机构的工作进行监管，其审查监督的结果直接向信息安全决策机构或者市域一体化慢病管理服务信息平台的决策层进行汇报，为信息安全组织改进工作提供支持。

5.信息安全角色和职责

从根本上来说，信息安全是市域一体化慢病管理服务信息平台中每一个和信息系统相关或是能影响信息系统的安全情况的人员的职责。每个人在信息系统的运行中，在不同岗位上都扮演着相应的角色。本部分将定义出市域一体化慢病管理服务信息平台中与信息安全工作相关的主要角色，并从总体上描述他们所承担的职责。

在信息安全工作方面一直在进行讨论的一个基本问题就是“到底是谁的职责？”，许多人对于信息安全相关职责仍停留在传统概念中，认为信息安全是信息技术部门或仅仅是信息安全部门的职责，这样给信息安全工作的开展带来了很大的困难。通过定义信息安全角色与职责，使市域一体化慢病管理服务信息平台中每个工作人员都能找到自己的位置，同时为以后具体岗位职责的定义打下了坚实的基础。

通常在信息安全相关的角色主要包括以下几种：

高层管理人员；

信息安全管理人员；

部门和项目管理者/应用所有者；

技术提供、维护和支持人员；

管理支持者；

用户。

由于各自的角色不同他们在信息安全方面也承担着不同的职责。

信息安全组织架构和相关职责：

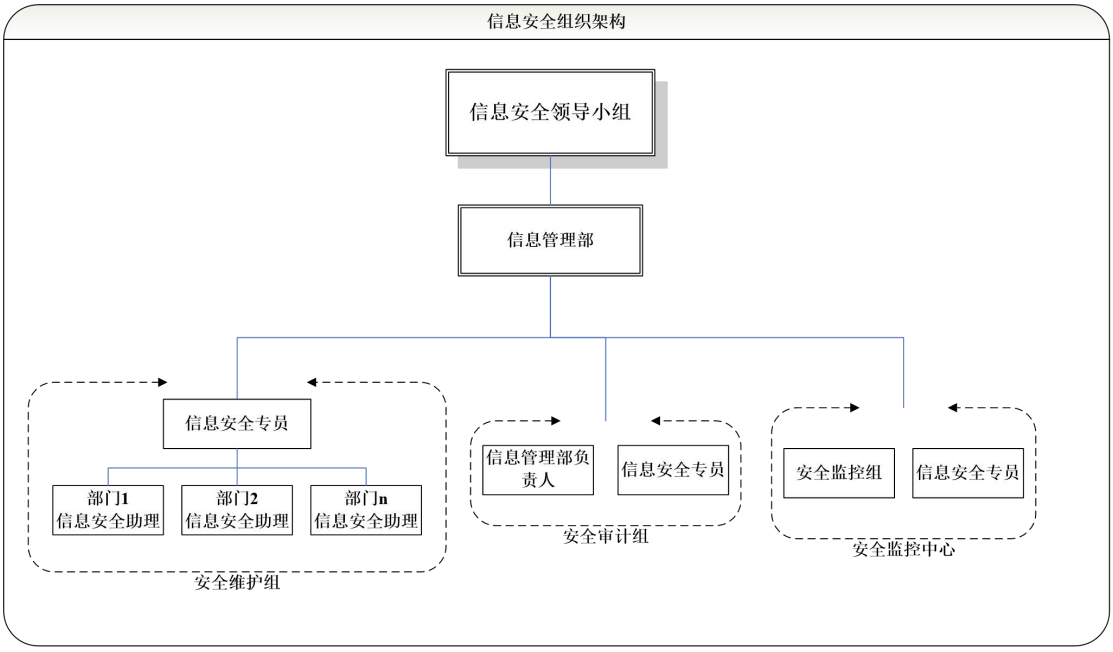


**图 2-6 信息安全组织架构图**

1. 信息安全领导小组

高层领导参加的信息安全领导小组，负责批准信息安全策略、分配安全责任并协调整个市域一体化慢病管理服务信息平台范围的安全策略实施，确保对安全管理和建设有一个明确的方向并得到管理层的实际支持。信息安全领导小组应通过合理的责任分配和有效的资源管理促进市域一体化慢病管理服务信息平台网络信息系统的安全。信息安全领导小组可以作为目前管理机构的一个组成部分。

信息安全领导小组有如下职责：

就整个信息管理部门的信息安全的作用和责任达成一致；

审查和批准信息安全策略以及总体责任；

就信息安全的重要和原则性的方法、处理过程达成一致，并提供支持。如风险评估、机密信息分类方法等；

确保将安全作为制定业务建设和维护计划、内部信息系统建设的一个部分；

授权对安全控制措施是否完善进行评估，并协调新系统或新服务的特定信息安全控制措施的实施情况；

审查重大的信息安全事故，并协调改进措施；

审核信息安全建设和管理的重要活动，如重要安全项目建设、重要的安全管理措施出台等；

在整个组织中增加对信息安全工作支持的力度。

2.信息管理部门

负责设计、建设安全管理体系，包括策略、组织和运作模式，并且进行宣贯和培训。职责如下：

贯彻执行政府相关主管部门有关网络及信息安全管理方面的方针、政策及各项工作要求，在各网上落实网络及信息安全的各项工作。通过等级保护工作保持与公安机关的联系，接受和执行公安机关的监督和指导。

负责建立信息安全策略体系，制定网络及信息安全工作制度及管理流程，起草、制定网络及信息安全的技术规范、标准及策略，聘请外部专家对网络及信息安全工作制度及管理流程进行评审，组织在全网范围内的实施。

组织、协调内部各部门实施网络及信息安全工作。

在市域一体化慢病管理服务信息平台内开展信息安全知识共享，建立有针对信息安全的知识共享的技术平台，促进内部交流与学习。

定期组织内部人员或聘请外部单位，公安机关等进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；汇总安全检查数据，形成安全检查报告，并对安全检查结果在安全组织内召开会议进行通报。

3.安全维护组

负责项目日常安全维护工作，包括信息安全专员和各部门信息安全助理。

安全维护组有如下职责：

（1）执行有关信息安全问题的处理：在日常维护中发现有安全问题，首先进行应急处理保证业务的连续性，然后通过提供安全事件报告的方式通知安全维护组相关人员，安全维护组人员在接到报告后，将和各专业组一起在保证业务正常运行的前提下解决安全问题，工作结束后，将由双方一起记录安全处理过程；对重点主机系统的安全职责；至少每月进行一次安全漏洞扫描；对主机系统和网络设备上的用户进行审核，发现可疑的用户账号时及时向系统管理员核实并作相应的处理。

（2）对网络设备的安全职责：监督信息安全管理机构制订的网络设备用户账号的管理制度的实行，在发现有可疑的用户账号时向网络管理员进行核实并采取相应的措施；根据业务保护要求，提出防火墙系统的部署方案，并制订相应的信息安全访问控制策略。

（3）对数据库的安全职责：协同数据库管理员对数据库系统进行安全配置，修补已发现的漏洞；协同数据库管理员对于数据库安全事件处理，并分析安全事件原因；协同数据库

管理员对于数据库安全事件进行处理，尽量减小安全事故和安全事件造成的损失，并从中吸取教训；验证数据备份策略的有效性，对数据恢复过程进行试验，确保在发生安全问题时能够从数据备份中进行恢复;监督数据库管理员对重要数据的备份工作,对于重要数据的备份，必须每个月做一次检查，确保备份的内容和周期以及备份介质的保存符合有关的规定。

4.安全审计组

对用户的各种行为进行审计，对安全监控中心的各项监控、处理和维护工作进行审计。

安全审计组有如下职责:依赖安全运行管理平台以及各种安全审计产品对管理网的用户行为进行审计。对安全监控中心的各项监控、处理和维护工作进行审计。

5.安全监控中心

可利用现有的本项目安全信息管理平台，对网络进行全面的安全监控。

安全监控中心有如下职责：

查看安全运行管理平台的各种告警，做出处理判断，并编制下发工单。

定期查看信息安全站点的安全公告，跟踪和研究各种信息安全漏洞和攻击手段，在发现可能影响信息安全的安全漏洞和攻击手段时，及时做出相应的对策，通知并指导系统管理员进行安全防范。

跟踪信息系统系统中使用的操作系统和通用应用系统最新版本和安全补丁程序的发布情况,在发现有新版本或者安全补丁出现发布时,通知并指导系统管理员进行升级或打补丁。

根据信息管理部门提出的安全标准，对主机系统上开放的网络服务和端口进行检查，发现不需要开放的网络服务和端口时及时通知系统管理员进行关闭；

定期对主机的网络服务进行全面安全检测,在发现安全设置不当或存在安全漏洞时及时通知系统管理员进行修补；

根据安全管理机构规定的周期和时间，对网络设备进行全面信息安全扫描，发现安全网络设备上存在的异常开放的网络服务或者开放的网络服务存在安全漏洞时及时通知网络管理员采取相应的措施。

# 安全管理人员

1.人员录用

对应聘者进行审查，确认其具有基本的专业技术水平，接受过安全意识教育和培训，能够掌握安全管理基本知识;对信息系统关键岗位的人员还应注重思想品质、历史方面的考察;

在签署劳动合同前，应由人力资源部进行人员背景、资质审查，技能考核等，合格者还要签署《工作保密协议》方可上岗；安全管理人员应具有基本的系统安全风险分析和评估能

力；

关键区域或部位的安全管理人员应选用实践证明精干、内行、忠实、可靠的人员。

2.人员离岗

人员离岗的立即中止被解雇的、退休的、辞职的或其他原因离开的人员的所有访问权限；收回所有相关证件、徽章、密钥、访问控制标记等；收回机构提供的设备等；

调离后的保密要求：管理层和信息系统关键岗位人员调离岗位，必须经人力资源部严格办理调离手续，承诺其调离后的保密要求；

离岗的审计要求：涉及组织机构管理层和信息系统关键岗位的人员调离单位，必须进行离岗安全审查，在审查合格后，方可调离；

对于在组织内进行岗位调动的工作人员，须根据新岗位的需要，增加、删除或修改该人员的计算机信息系统访问权限，包括电子邮件系统、业务应用系统、网络系统和其他计算机信息软硬件系统。与原岗位有关的所有资料文件，包括其软硬拷贝都需要移交，不允许私自带走。

3.安全意识教育和培训

定期的人员考核：应定期对各个岗位的人员进行不同侧重的安全认知和安全技能的考核，作为人员是否适合当前岗位的参考；

定期的人员审查：对关键岗位人员，应定期进行审查，如发现其违反安全规定，应控制使用；

管理有效性的审查：对关键岗位人员的工作，应通过例行考核进行审查，保证安全管理的有效性；并保留审查结果；

全面严格的审查：对所有安全岗位人员的工作，应通过全面考核进行审查，如发现其违反安全规定，应采取必要的应对措施。

应知应会要求：应让信息系统相关工作人员知晓信息的敏感性和信息安全的重要性，认识其自身的责任和安全违例会受到纪律惩罚，以及应掌握的信息安全基本知识和技能等；

有计划培训：制定并实施安全教育和培训计划，根据不同培训对象的需要，每季度或每半年进行安全培训，培养信息系统各类人员安全意识，并提供对安全政策和操作规程的认知教育和训练等；

针对不同岗位培训：针对不同岗位，制定不同的专业培训计划，包括安全知识、安全技术、安全标准、安全要求、法律责任和业务控制措施等；

按人员资质要求培训：对所有工作人员的安全资质进行定期检查和评估，使相应的安全

教育成为组织机构工作计划的一部分；

培养安全意识自觉性：对所有工作人员进行相应的安全资质管理，并使安全意识成为所有工作人员的自觉存在。

4.外部人员访问与管理

应对硬件和软件维护人员，咨询人员，临时性的短期职位人员，以及辅助人员和外部服务人员等第三方人员签署包括不同安全责任的合同书或保密协议；规定各类人员的活动范围，进入计算机房需要得到批准，并有专人负责；第三方人员必须进行逻辑访问时，应划定范围并经过负责人批准，必要时应有人监督或陪同；

在重要区域，第三方人员必须进入或进行逻辑访问（包括近程访问和远程访问等）均应有书面申请、批准和过程记录，并有专人全程监督或陪同；进行逻辑访问应使用专门设置的临时用户，并进行审计；

关键区域管理要求：在关键区域，一般不允许第三方人员进入或进行逻辑访问；如确有必要，除有书面申请外，可采取由机构内部人员代为操作的方式，对结果进行必要的过滤后再提供第三方人员，并进行审计；必要时对上述过程进行风险评估和记录备案，并对相应风险采取必要的安全补救措施。

# 安全建设管理

1.系统定级和备案

由信息化管理部门负责业务系统的定级备案工作，由外部安全咨询服务团队提供技术支持，协助信息化管理部门开展系统定级备案工作；

明确信息系统的边界和安全保护等级；

以书面的形式说明确定信息系统为某个安全保护等级的方法和理由；

组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定；

确保信息系统的定级结果经过相关部门的批准；

指定责任部门：由安全管理部负责管理系统定级的相关材料并控制这些材料的使用；

将系统等级及相关材料报系统主管部门备案；

将系统等级及其他要求的备案材料报相应公安机关备案。

2.安全方案设计

由信息化管理部门负责，由外部安全咨询服务团队提供技术支持，开展安全方案设计工作：

根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施；

组织有关单位对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；

根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；

组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，经过批准后，正式实施；

根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件；

3.安全产品采购

指定责任部门：由信息管理部门会同其他有关部门负责产品采购；

定义采购流程：选型测试、年度审定及更新；

确定采购和使用安全产品的国家有关规定；

确定确国家密码主管部门对采购和使用密码产品的规定；

定义选型测试所需文档的模板。

4.外包软件开发

由信息管理部门及有关软件开发管理、有关部门共同负责外包软件开发管理：

根据开发需求检测软件质量；

软件安装之前要检测软件包中可能存在的恶意代码；

在合同中要求开发单位提供软件设计的相关文档和使用指南；

在合同中要求开发单位提供软件源代码，并审查可能存在的后门；

在合同中要求：在服务期内如发现安全漏洞，则开发单位必须及时提供相关安全补丁或者进行及时升级。

5.工程实施

由信息管理部门协同有关部门负责工程实施管理；

督促施工单位或者部门制定详细的工程实施方案控制实施过程，并按照工程实施过程实施；

维护并推行工程实施管理制度，明确说明实施过程的控制方法和人员行为准则。

6.测试验收

指定信息管理部门和有关部门共同负责测试验收管理；

委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；

测评单位在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；

测评单位对系统测试验收的控制方法和人员行为准则进行书面规定；

由信息管理部门与相关部门对系统测试验收报告进行审定并签字确认。

7.系统交付

由安全管理部负责系统交付的管理工作，按照管理规定的要求完成系统交付工作；

制定详细的系统交付清单，根据交付清单对所交接的设备、软件和文档等进行清点。

对负责系统运行维护的技术人员进行相应的技能培训；

确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档；

定义系统交付控制方法和人员行为准则。

8.等级测评

指定责任单位：由信息管理部门负责，每年至少组织测评单位对系统进行一次等级测评，对发现的不符合项及时进行整改；

在系统发生变更时及时申请对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；

选择具有国家相关技术资质和安全资质的测评单位进行等级测评。

9.安全服务商选择

指定责任部门：由安全管理部负责选择安全服务商；

确保安全服务商的选择符合国家的有关规定；

与选定的安全服务商签订与安全相关的协议，明确约定相关责任、服务范围、服务期限、服务具体条款及服务质量要求等；

确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。

# 安全运维管理

1.环境管理

指定责任部门：由信息管理部门负责环境管理；

定期对机房供配电、空调、温湿度控制等设施进行维护管理；

负责机房安全，机房安全管理人员对机房的出入、服务器的开机或关机等工作进行管理；

建立《机房安全管理制度》，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面作出规定；

规范办公环境人员行为，包括：工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的文件等。

2.资产管理

指定责任部门：由信息管理部门及有关部门共同负责资产管理；

编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等；

规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；

对信息分类与标识方法作出规定，根据资产的重要程度对资产进行标识管理，并对信息的使用、传输和存储等进行规范化管理；

定义管理措施选择方案：根据资产的价值选择相应管理措施。

3.介质管理

指定责任部门。由信息管理部门负责介质管理；

规定介质的存放环境、使用、维护和销毁；

由信息管理部门负责对存储环境进行专人管理，确保介质存放在安全的环境中，对各类介质进行控制和保护；

对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点；

对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁；

根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；

对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。

4.设备维护管理

指定责任部门：由信息管理部门及网络管理部等有关部门负责设备管理；

对信息系统相关的各种设备（包括备份和冗余设备）、线路等每周进行维护管理；

定义基于申报、审批和专人负责的设备安全管理方法，对信息系统的各种软硬件设备的

选型、采购、发放、领用、维护、操作、维修等过程进行规范化管理；

定义配套设施、软硬件维护方面的管理方法，明确维护人员的责任，对涉外维修和服务的审批、维修过程等监督控制方法进行说明；

定义终端计算机、工作站、便携机、系统和网络等设备的操作和使用规范：针对主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；

定义信息处理设备带离机房或办公地点的审批流程。

5.漏洞和风险管理

定期对系统进行漏洞扫描，识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；

定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

6.网络和系统安全管理

指定责任部门：由信息管理部门负责网络安全管理，由信息管理部门专人负责对运行日志、网络监控记录的日常维护和报警信息分析和处理工作；

对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；

定义更新流程：根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；

定义漏洞管理方法：定期对网络系统进行漏洞扫描，发现网络系统安全漏洞进行及时修补；

定义设备配置方法：实现设备的最小服务配置，并对配置文件进行定期离线备份；

定义外部连接审批流程：所有与外部系统的连接均得到授权和批准；

定义设备接入策略：依据安全策略允许或者拒绝便携式和移动式设备的网络接入；

定义非法上网管理方法：每周检查违反规定拨号上网或其他违反网络安全策略的行为。

指定责任部门：由信息管理部门负责系统安全管理，负责对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则；

根据业务需求和系统安全分析确定系统的访问控制策略；

每周进行漏洞扫描，对发现的系统安全漏洞及时进行修补；

安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；

依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记

录、参数的设置和修改等内容，严禁进行未经授权的操作；

每周对运行日志和审计数据进行分析，以便及时发现异常行为。

对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定。

7.配置安全管理

对记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等信息进行安全管理；

将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

8.恶意代码防范

指定责任部门：由安全管理部负责进行恶意代码防范；

每年进行定期培训，通过培训提高所有用户的防病毒意识、及时告知防病毒软件版本、在读取移动存储设备上的数据以及网络上接收文件或邮件之前先进行病毒检查、对外来计算机或存储设备接入网络系统之前也应进行病毒检查；

由信息管理部门负责对网络和主机进行恶意代码检测并保存检测记录，每周检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报；

定义防恶意代码软件授权使用、恶意代码库升级、定期汇报等流程。

9.密码管理

指定责任部门：信息管理部门负责密码使用管理；

总结在密码设备的采购、使用、维护、保修及报废的整个生命周期内的各项国家有关规定；

严格执行上述规定。

10.变更管理

指定责任部门：由信息管理部门负责变更管理；

建立变更流程：确认系统中要发生的变更，制定变更方案，系统发生变更前向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，在实施后将变更情况向相关人员通告；

建立变更申报和审批程序：对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录；

建立中止变更程序，中止变更并从失败变更中恢复，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

11.备份及恢复管理

指定责任部门：由信息管理部门负责备份与恢复管理；

识别需要定期备份的重要业务信息、系统数据及软件系统等；

定义备份信息的备份方式、备份频度、存储介质和保存期等；

根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

建立数据备份和恢复过程，对备份过程进行记录，所有文件和记录应妥善保存；

建立演练流程：每季度对恢复程序进行演练，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

12.安全事件处置

指定责任部门：由信息管理部门负责安全事件处置；

每年进行培训。通过培训让所有人能够报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

制定安全事件报告和处置管理程序：明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；为造成系统中断和造成信息泄密的安全事件制定不同的处理程序和报告程序；

13.应急预案管理

指定责任部门：由信息管理部门负责应急预案管理；

建立统一的应急预案框架，框架应包括事件分级方法、各级事件启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；

在应急预案框架制定不同事件的应急预案，应急预案要指明适用的系统、设备等；

资源承诺：从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；

培训要求:对系统相关的人员进行应急预案培训,应急预案的培训应至少每年举办一次；

演练要求：定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；

更新要求：规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。

14.外包运维管理

确保外包运维服务商的选择符合国家的有关规定；

与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；

保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；

在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

**安全设备配置**

**表 2-3 安全系统配置表**

| 序号 | 设备及软件名称 | 主要技术（性能）指标 | 单位 | 数量 |
|---|---|---|---|---|
| 1 | 防火墙 | 标准机架式，国产芯片，国产处理器，≥10 个千兆电口、≥8 个千兆光插槽,双电源,≥2 个扩展槽位,防火墙吞吐≥1G，并发连接≥100 万。含 IPSEC VPN、SD-WAN、应用识别功能；提供≥3 年入侵攻击特征库、URL 分类过滤库、专业版快速扫描查杀防病毒库、应用识别特征库升级服务许可。 | 台 | 2 |
| 2 | 数据库审计 | 标准机架式，国产芯片，国产处理器，配置≥6 个千兆电口，≥4 个千兆光口，≥2 个万兆口,冗余电源,≥2 个扩展槽位,记录事件能力≥5 万条/秒，抓包速率≥5Gbps。含应用识别功能，含≥3 年攻击检测、僵尸主机规则库升级许可，含≥1 个云审计代理/Agent 授权，≥5 个数据库审计授权。 | 台 | 1 |
| 3 | 堡垒机 | 标准机架式，国产芯片，国产处理器，≥1 个 console 口，≥2 个 USB 口，≥1 个 HA 口，≥1 个管理口，≥4 个千兆电口，≥4 个千兆光口，≥2 个万兆光口；冗余电源,≥2 个扩展槽位,≥200 个主机/设备许可。 | 台 | 1 |
| 4 | 网闸 | 标准机架式，国产芯片，国产处理器，内外端机各≥16GB 内存，内外端机各≥256GB 固态硬盘,内外分别≥1 个 HA 口、≥1 个管理口、≥8 个千兆电口和≥8 个千兆光口，≥1 个扩展槽位,冗余电源,文件传输速率≥1500Mbps；文件传输延时≤0.5ms；网络层交换速率（2 对千兆口）≥1900Mbps；网络延时≤0.2ms。配置包含安全浏览模块、文件传输模块、邮件访问模块、VOIP 访问模块、数据库访问模块、其他访问模块、文件同步模块、数据库同步模块、防病毒模块、数据中心模块。 | 台 | 2 |
| 5 | 防火墙 | 标准机架式，国产芯片，国产处理器，配置≥10 个千兆电口，≥14 个千兆光插槽，≥2 个万兆光插槽，模块化冗余双电源,≥1 个扩展槽位,防火墙吞吐≥8G，并发连接≥320 万。提供 IDP 特征库、WEB 过滤库、专业版快速扫描查杀防病毒库、应用识别特征库≥3 年升级服务许可。 | 台 | 2 |
| 6 | 上网行为管理 | 标准机架式，国产芯片，国产处理器，包括≥1 个串口、≥2 个 USB 接口、≥6 个千兆电口、≥4 个千兆光插槽、≥2 对 bypass 电口、≥3 个可插拔的扩展槽,双电源,网络吞吐量≥10G；授权用户数≥8000 人；包含≥3 年系统版本升级、URL 库及应用特征库升级许可。 | 台 | 1 |

| | | | | |
|---|---|---|---|---|
| 7 | 入侵检测 | 标准机架设备，配备≥8 个千兆电口，≥8 个千兆光口，≥2 个万兆光口；SSD 硬盘≥480GB，冗余电源。吞吐量≥3.5Gbps；IDPS 吞吐量≥3G，AV 吞吐量≥1.5G，并发连接数≥120 万；新建连接数≥9 万。包含≥3 年特征库升级许可。 | 台 | 1 |

## 密码应用方案

随着《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》《中华人民共和国密码法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规的颁布实施，国家在保障网络安全，维护网络空间主权和国家安全、社会公共利益中，在保护公民、法人和其他组织的合法权益中，提供了强大的政策依据和法规要求，项目建设单位应同步规划、同步建设、同步运行密码保障系统并定期进行评估。

2022 年 11 月 26 日，《河南省网络安全条例》审议通过，条例中明确县级以上网信、公安等有关部门应当指导督促网络运营者落实关键信息基础设施安全保护、网络安全等级保护、数据安全保护、个人信息保护、密码应用安全性评估、云计算服务安全评估、网络信息安全投诉举报等制度，落实相关国家标准的强制性要求，制定网络安全事件应急预案。

近年来，全国各地医疗机构注重加强网络安全建设，部署了防火墙、反病毒网关、漏洞扫描系统、入侵检测系统、数据防泄漏等传统的安全设备，但数据泄露事件依然频发。外部黑客攻击、内部人员窃取数据非法销售的事情层出不穷，数据泄漏频发的背后，归根到底是对敏感数据本身保护不够。目前来看，信息系统普遍缺失内建数据安全能力，同时随着内部各类信息系统之间打通共享，成倍放大了数据安全管理复杂度，面临着更为严峻的安全挑战。数据在不同系统之间流转，导致数据的所有者、控制者和处理者难以有效控制，数据可能被非法访问和处理，造成数据保密性和完整性等方面的巨大安全威胁。所以，基于安全隐患的应对，亟需密码技术实现边界的接入认证、数据的机密保护和用户身份的鉴别。

根据国家标准 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》中的第三级密码应用基本要求，本方案从密码应用的真实性、机密性、完整性、不可否认性四个方面对系统的现状和密码应用需求进行分析，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个密码技术应用层面及管理制度、人员管理、建设运行、应急处置四个管理层面，针对该项目设计了能满足 GB/T 39786 中三级指标要求的密码应用方案，为通过密码应用安全性评估奠定基础。

**密码应用需求分析**

为了更好地保护信息安全，本次项目信息系统的内部数据、公开数据的授权使用、安全

传输、安全存储、数据防篡改和接口防护等障碍和瓶颈，针对性解决目前本次项目各信息系统的安全问题，需要采用更加安全可靠的信息安全保护手段。

根据《中华人民共和国密码法》等法律法规、标准规范的相关要求，商用密码是当前各类不涉及国家秘密信息资源进行安全保护的主要手段，其通过采用密码技术或密码产品对信息进行加密保护，能够在保证信息的完整性和正确性的同时，防止信息被篡改、伪造和泄露。为此，本项目计划采用商用密码技术对本项目建设的信息系统进行安全防护。依据国家密码管理相关法律法规，结合网络现状、系统现状、数据现状和业务现状，对信息系统的密码需求分析如下。

（1）重要数据的机密性需求

基于对郑州市慢病管理服务平台的业务信息流、重要数据的现状分析，结合密码应用中机密性保护对象类型，分析信息流中可能存在的重要数据泄漏风险，最终确定郑州市慢病管理服务信息平台中重要数据的机密性保护需求。详细分析见下表。

**表 2-4 重要数据的机密性需求表**

| 保护对象类型 | 风险分析 | 安全性需求 |
|---|---|---|
| 身份鉴别信息 | / | / |
| 密钥数据 | / | / |
| 传输的重要数据 | 不能保证郑州市慢病管理服务信息平台业务系统各子系统间数据传输过程中的机密性 | 采用郑州市慢病管理服务信息平台各子系统间数据传输过程中的机密性 |
| 信息系统应用中所有存储的重要数据 | 不能保证郑州市慢病管理服务信息平台各子系统业务应用产生数据在数据中心存储过程中的机密性 | 采用密码技术保证郑州市慢病管理服务信息平台各子系统业务应用产生数据在数据中心存储过程中的机密性 |

（2）重要数据的完整性需求

基于对业务系统的现状分析，结合密码应用中完整性保护对象类型，分析业务系统信息流中可能存在的重要数据非法篡改风险，提出重要数据完整性保护需求。

**表 2-5 重要数据的完整性需求表**

| 保护对象类型 | 风险分析 | 安全性需求 |
|---|---|---|
| 身份鉴别信息 | / | / |
| 密钥数据 | | / |
| 日志记录 | 不能保证日志审计系统后台记录服务器设备系统日志的完整性 | 采用密码技术保证日志审计系统后台记录服务器设备系统日志的完整性 |
| 访问控制信息 | 不能保证网络边界访问控制信息的完整性；<br>不能保证郑州市慢病管理服务信息平台访问控制信息的完整性 | 采用密码技术保证网络边界访问控制信息的完整性；<br>采用密码技术保证郑州市慢病管理服务信息平台访问控制信息的完整性； |
| 重要信息资源安全标记 | / | / |
| 重要可执行程序 | 不能重要可执行程序进行完整性保护 | 采用密码技术对重要可执行程序进行完整性保护 |

| | | |
|---|---|---|
| 视频监控音像记录 | 不能保证机房视频监控系统视频监控音像记录数据的存储完整性 | 采用密码技术保证机房视频监控系统后台存储的视频监控音像记录数据的存储完整性 |
| 电子门禁系统进出记录 | 不能保证电子门禁系统后台存储的进出记录数据的存储完整性 | 采用密码技术保证机房电子门禁系统后台存储的进出记录数据的存储完整 |
| 传输的重要数据 | 不能保证通信过程中数据的完整性；<br>不能保证检索请求数据、身份检索结果集和检索报告在传输过程中的完整性。 | 采用密码技术保证通信过程中数据的完整性；<br>采用密码技术保证检索请求数据、身份检索结果集和检索报告在传输过程中的完整性。 |
| 信息系统应用中所有存储的重要数据 | 不能保证郑州市慢病管理服务信息平台业务数据在数据中心存储过程中的完整性；<br>不能业务日志信息、运维日志信息在郑州市慢病管理服务信息平台存储过程中的完整性； | 采用密码技术保证郑州市慢病管理服务信息平台业务数据在数据中心存储过程中的完整性；<br>采用密码技术保证业务日志信息、运维日志信息在郑州市慢病管理服务信息平台存储过程中的完整性 |

（3）实体身份的真实性需求

基于对业务系统的现状分析，结合密码应用中真实性保护对象类型，分析业务系统信息流中可能存在的实体身份假冒的风险，提出重要实体身份真实性保护需求。

**表 2-6 实体身份的真实性需求表**

| 保护对象类型 | 风险分析 | 安全性需求 |
|---|---|---|
| 进入重要物理区域人员的身份鉴别 | 不能重要区域进入人员身份的真实性 | 采用密码技术对进出机房的人员进行身份鉴别，保证重要区域进入人员身份的真实性 |
| 通信双方的身份鉴别 | 不能保证通信实体身份的真实性 | 采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性 |
| 网络设备接入时的身份鉴别 | 不能保证运维人员身份的真实性 | 采用密码技术对登录堡垒机的运维人员进行身份鉴别，保证运维人员身份的真实性 |
| 重要可执行程序的来源真实性保证 | 不能重要可执行程序来源进行真实性 | 采用密码技术对重要可执行程序来源进行真实性验证 |
| 登录操作系统和数据库系统的用户身份鉴别 | 不能保证运维人员身份的真实性 | 采用密码技术对登录堡垒机的运维人员进行身份鉴别，保证运维人员身份的真实性 |
| 应用系统的用户身份鉴别 | 不能保证郑州市慢病管理服务信息平台身份的真实性 | 采用密码技术对郑州市慢病管理服务信息平台的业务系统进行身份鉴别，保证业务系统身份的真实性 |

（4）业务信息或操作的不可否认性需求

根据业务系统重要数据和业务特点，说明哪些操作行为或结果数据存在被抵赖的风险及可能造成的影响。针对风险点分析系统现状是如何进行应对的，是否已有防护或缓解。综合上述两方面最终确定不可否认性需求。

**表 2-7 业务信息或操作的不可否认性需求表**

| 保护对象类型 | 风险分析 | 安全性需求 |
|---|---|---|
| 使用基于公钥密码算法的数字签名机制等密码技术来保证数据原发行为的不可否认性和数据接收行为的不可否认性 | 郑州市慢病管理服务信息平台业务操作记录存在数据篡改风险 | 采用密码技术提供郑州市慢病管理服务信息平台业务操作记录的原发证据，实现原发行为的不可否认性 |

（5）密码应用需求汇总与映射情况分析

综合上述分析，并依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的规定，郑州市慢病管理服务信息平台在机密性、完整性、真实性和不可否认性四个层面的具体密码应用需求能够对应到物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面，如下表所示。

**表 2-8 密码应用安全性要求与各层面密码应用需求、责任主体映射关系**

| 需求类型 | 保护对象类型 | 密码应用需求 | 对应层面 | 责任主体 |
|---|---|---|---|---|
| 机密性 | 传输的重要数据 | 采用密码技术保证郑州市慢病管理服务信息平台业务数据在郑州市慢病管理服务信息平台各子系统间传输过程中的机密性 | 网络和通信安全 | 郑州市第七人民医院 |
| | 信息系统应用中所有存储的重要数据 | 采用密码技术保证郑州市慢病管理服务信息平台业务数据在数据中心存储过程中的机密性 | 应用和数据安全 | 郑州市第七人民医院 |
| 完整性 | 日志记录 | 采用密码技术保证日志审计系统后台记录服务器设备系统日志的完整性 | 设备和计算安全 | 郑州市第七人民医院 |
| | 访问控制信息 | 采用密码技术保证网络边界访问控制信息的完整性；<br>采用密码技术保证业务服务中心访问控制信息的完整性； | 设备和计算安全 | |
| | 重要可执行程序 | 采用密码技术对重要可执行程序进行完整性保护 | 设备和计算安全 | |
| | 视频监控音像记录 | 采用密码技术保证机房视频监控系统后台存储的视频监控音像记录数据的存储完整性 | 物理和环境安全 | 郑州市第七人民医院 |
| | 电子门禁系统进出记录 | 采用密码技术保证机房电子门禁系统后台存储的进出记录数据的存储完整 | 物理和环境安全 | |
| | 传输的重要数据 | 采用密码技术保证通信过程中数据的完整性；<br>采用密码技术保证郑州市慢病管理服务信息平台业务数据在传输过程中的完整性。 | 网络和通信安全 | 郑州市第七人民医院 |
| | 信息系统应用中所有存储的重要数据 | 采用密码技术保证郑州市慢病管理服务信息平台业务数据在数据中心存储过程中的完整性；<br>采用密码技术保证业务日志信息、运维日志信息在郑州市慢病管理服务信息平台业务数据存储过程中的完整性 | 应用和数据安全 | 郑州市第七人民医院 |
| 真实性 | 进入重要物理区域人员的身份鉴别 | 采用密码技术对进出机房的人员进行身份鉴别，保证重要区域进入人员身份的真实性 | 物理和环境安全 | 郑州市第七人民医院 |
| | 通信双方的身份鉴别 | 采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性 | 网络和通信安全 | 郑州市第七人民医院 |
| | 网络设备接入时的身份鉴别 | 采用密码技术对登录堡垒机的运维人员进行身份鉴别，保证运维人员身份的真实性 | 设备和计算安全 | 郑州市第七人民医院 |
| | 重要可执行程序 | 采用密码技术对重要可执行程序来源进行 | | |

| 需求类型 | 保护对象类型 | 密码应用需求 | 对应层面 | 责任主体 |
| --- | --- | --- | --- | --- |
| | 的来源真实性保证 | 真实性验证 | | |
| | 登录操作系统和数据库系统的用户身份鉴别 | 采用密码技术对登录堡垒机的运维人员进行身份鉴别，保证运维人员身份的真实性 | 应用和数据安全 | 郑州市第七人民医院 |
| | 应用系统的用户身份鉴别 | 采用密码技术对郑州市慢病管理服务信息平台进行身份鉴别，保证业务系统身份的真实性 | | |
| 不可否认性 | 使用基于公钥密码算法的数字签名机制等密码技术来保证数据原发行为的不可否认性和数据接收行为的不可否认性 | 采用密码技术提供郑州市慢病管理服务信息平台业务数据的原发证据，实现原发行为的不可否认性 | | |

**密码应用总体设计**

1.密码应用设计目标

根据国家标准 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》中的第三级密码应用基本要求，本方案从密码应用的真实性、机密性、完整性、不可否认性四个方面对郑州市第七人民郑州市慢病管理服务信息平台的现状和密码应用需求进行分析，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个密码技术应用层面，以及管理制度、人员管理、建设运行、应急处置四个管理层面，针对该平台设计了能满足 GB/T 39786 中三级指标要求的密码应用改造方案，为通过密码应用安全性评估奠定基础。

2.密码应用设计原则

郑州市慢病管理服务平台密码应用设计应遵循以下原则：

（1）总体性原则。从防护整体性角度考虑，对郑州市慢病管理服务平台的密码应用开展顶层设计，明确密码应用需求和预期目标，并与郑州市慢病管理服务平台网络安全保护等级相结合，通过自上而下的体系化设计形成涵盖技术、管理、实施保障的整体方案。

（2）成熟性原则。本方案采用的商用密码产品均为市场上长期销售和应用的成熟的商用密码产品，均具有密码管理部门核准的商用密码产品资质。所有产品均采用成熟、稳定、可靠的网络架构，能够提供不间断的服务，并均具有很强的健壮性、良好的容错处理能力和抗干扰能力。

（3）经济性原则。结合郑州市慢病管理服务平台的规模以及所涉及责任主体的实际情况，在合理、够用可落地的前提下，设计满足 GB/T 39786 的密码应用改造方案，确保郑州市慢病管理服务平台密码应用安全投资合理，规模适度，避免资金浪费和过度保护。

3.密码应用设计依据

本方案主要依据以下标准规范和行业指导文件开展设计。

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》

GB/T 38540-2020《信息安全技术 安全电子签章密码技术规范》

GB/T 32918.1-2016《信息安全技术 SM2 椭圆曲线公钥密码算法 第 1 部分：总则》

GB/T 32918.2-2016《信息安全技术 SM2 椭圆曲线公钥密码算法第 2 部分：数字签名算法》

GB/T 32918.3-2016《信息安全技术 SM2 椭圆曲线公钥密码算法第 3 部分：密钥交换协议》

GB/T 32918.4-2016《信息安全技术 SM2 椭圆曲线公钥密码算法第 4 部分：公钥加密算法》

GB/T 32918.5-2017《信息安全技术 SM2 椭圆曲线公钥密码算法第 5 部分：参数定义》

GB/T 35275-2017《信息安全技术 SM2 密码算法加密签名消息语法规范》

GB/T 35276-2017《信息安全技术 SM2 密码算法使用规范》

GB/T 32905-2016《信息安全技术 SM3 密码杂凑算法》

GB/T 32907-2016《信息安全技术 SM4 分组密码算法》

GB/T 20518-2018《信息安全技术 公钥基础设施数字证书格式》

GB/T 36322-2018《信息安全技术 密码设备应用接口规范》

GB/T 38556-2020《信息安全技术 动态口令密码应用技术规范》

GB/T 36968-2018《信息安全技术 IPSec VPN 技术规范》

GB/T 38636-2020《信息安全技术 传输层密码协议（TLCP）》

GB/T 37092-2018《信息安全技术 密码模块安全要求》

GB/T 38629-2020《信息安全技术 签名验签服务器技术规范》

GB/T 38540-2020《信息安全技术 安全电子签章密码技术规范》

GB/T 25056-2018《信息安全技术 证书认证系统密码及其相关安全技术规范》

GB/T 20518-2018《信息安全技术 公钥基础设施数字证书格式》

GB/T 35291-2017《信息安全技术 智能密码钥匙应用接口规范》

GB/T 37033-2018《信息安全技术 射频识别系统密码应用技术要求》

GM/T 0014-2023《数字证书认证系统密码协议规范》

GM/T 0017-2023《智能密码钥匙密码应用接口数据格式规范》

GM/T 0019-2023《通用密码服务接口规范》

GM/T 0020-2023《证书应用综合服务接口规范》

GM/T 0023-2023《IPSec VPN 网关产品规范》

GM/T 0025-2023《SSL VPN 网关产品规范》

GM/T 0026-2023《安全认证网关产品规范》

GM/T0027-2014《智能密码钥匙技术规范》

GM/T0030-2014《服务器密码机技术规范》

GM/T0032-2014《基于角色的授权管理与访问控制技术规范》

GM/T 0033-2023《时间戳接口规范》

GM/T0036-2014《采用非接触卡的门禁系统密码应用技术指南》

GM/T0050-2016《密码设备管理 设备管理技术规范》

GM/T0051-2016《密码设备管理对称密钥管理技术规范》

GM/T0052-2016《密码设备管理 VPN 设备监察管理规范》

GM/T0053-2016《密码设备管理远程监控与合规性检验接口数据规范》

GM/T0067-2019《基于数字证书的身份鉴别接口规范》

GM/T0087-2020《浏览器密码应用接口规范》

4.密码应用技术框架

依据国家政策和标准要求，以本地环境模式下安全防护和密码技术应用，同时构建密钥管理制度，实现信息的完整性、机密性及可靠性防护能力。总体框架如下：


**图 2-7 密码应用技术框架图**

如图所示，密码应用技术框架分别从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度以及密钥管理来开展。

物理和环境安全主要对物理访问人员的身份鉴别、电子门禁记录完整性、视频监控记录的存储完整性进行设计。

网络和通信安全主要从设备的身份鉴别、通信数据完整性、重要通信数据的机密性、边界访问控制信息的完整性和内外部设备接入认证。

设备计算安全主要从对登录设备人员的身份鉴别、访问控制信息完整性、日志记录完整性、远程管理安全通道、资源安全标记完整性保护、日志记录完整性、可执行程序完整性保护。

应用和数据安全主要从登录业务系统人员的身份鉴别、访问控制完整性、资源安全标记完整性保证、数据传输机密性、数据存储机密性、数据传输和存储完整性、数据抗抵赖（不可否认性）来进行设计。

**密码应用防护设计**

本项目应用数据中心机房保障物理和环境安全，在物理和环境安全方面满足商用密码建设要求。

通过部署安全认证网关、签名验签服务器、服务器密码机等设备，并配合使用智能密码钥匙和移动端密码模块（二级），调用身份认证系统颁发的数字证书，各设备间相互协调工作，满足对网络和通信、设备和计算、应用和数据各层面的密码建设要求，整体网络部署如图所示：

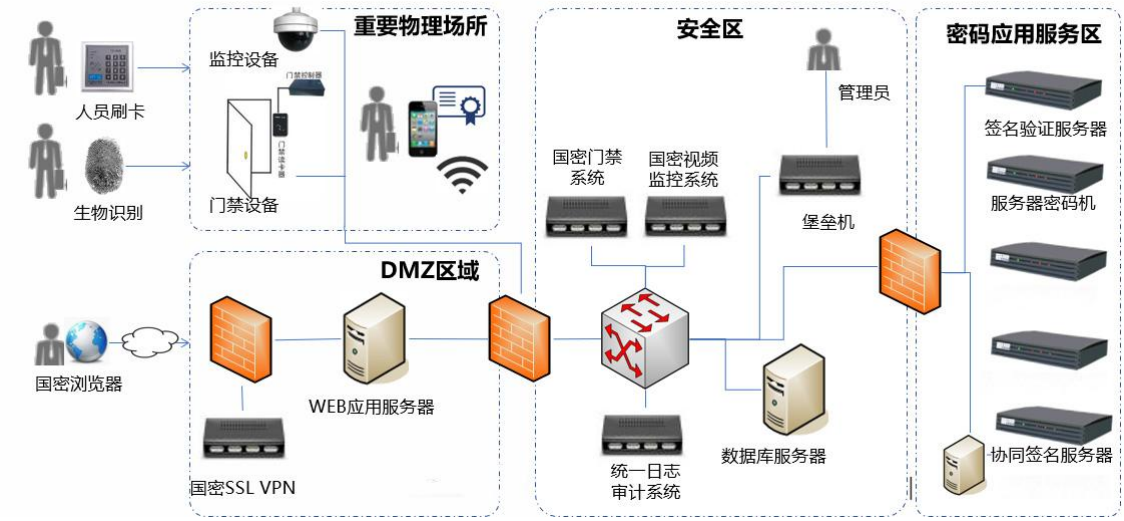


**图 2-8 密码应用整体网络部署图**

通过部署服务器密码机、SSL VPN、二级密码模块，部署在安全管理区的签名验签服务器和已部署的数字证书认证系统，实现市域一体化慢病管理服务信息平台的身份鉴别、访问控制信息完整性、重要数据传输机密性、重要数据存储机密性、重要数据传输完整性、重要

数据存储完整性、关键操作行为不可否认性。具体实现情况如下：

（1）在系统客户端部署符合密码相关国家、行业标准要求的密码模块（二级）、应用服务区部署符合密码相关国家、行业标准要求的SSL VPN集群，通过安全管理区的数字证书认证系统分别向终端密码模块（二级）、SSL VPN配置数字证书，实现终端客户端登录应用系统的用户身份鉴别，防止非授权人员登录。

（2）在应用服务区部署符合密码相关国家、行业标准要求的服务器密码机，在应用服务区部署符合密码相关国家、行业标准要求的服务器密码机，应用通过调用服务器密码机，对登录用户身份鉴别数据、系统中流转的重要业务数据进行传输、存储机密性、完整性保护，实现身份鉴别数据、重要业务数据防窃取和防篡改保护。

（3）应用服务区的应用服务器通过调用的服务器密码机，对应用日志记录进行完整性保护，防止应用日志记录被非授权篡改。

（4）应用服务区的应用服务器通过调用的安全管理区的签名验签服务器，对可能涉及法律责任认定的数据原发操作信息进行数字签名。

部署在应用服务区用于系统应用身份鉴别、应用层加密的SSL VPN应符合GM/T 0025-2023《SSL VPN网关产品规范》等标准要求；实现重要数据机密性保护、完整性保护和应用系统日志完整性保护的服务器密码机应符合GM/T 0030-2014《服务器密码机技术规范》，部署在安全管理区的签名验签服务器应符合GM/T 0029-2014《签名验签服务器技术规范》，配合上述密码产品使用的密码模块应达到GB/T 37092-2018《信息安全技术 密码模块安全要求》或GM/T 0028-2014《密码模块安全技术要求》二级及以上安全要求。

**密码应用详细设计**

（1）物理和环境安全

●密码应用基本要求

宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；

宜采用密码技术保证电子门禁系统进出记录数据的存储完整性；

宜采用密码技术保证视频监控音像记录数据的存储完整性；

以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

以上采用的密码产品，应达到GB/T 37092二级及以上安全要求。

●身份鉴别措施设计

通过使用医院机房符合国密要求的电子门禁系统鉴别机房进出人员的身份，进门需系统

可用感应卡、指纹、密码等，作为授权识别、出门需按出门按钮，对进出机房的人员进行记录和事件备查的，保证了机房区的安全性特点等。每套门禁安装有一把电插锁、一台感应式读卡机、一个出门按钮。控制器采用门禁控制系统，识别系统采用感应式读卡器：分别设在机房出入口，在监控室通过上位机可观看各控制点门禁系统出入状态。

本项目依托规划的医院机房进行建设，要求规划建设的医院机房采用国密门禁和国密监控。

●数据的完整性防护

本项目要求数据中心机房视频监控系统采用国密算法进行视频记录和门禁日志记录数据的完整性保护，密钥的备份与回复、归档、销毁均由密码设备管理员负责。

（2）网络和通信安全

●密码应用基本要求

应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；

宜采用密码技术保证通信过程中数据的完整性；

应采用密码技术保证通信过程中重要数据的机密性；

宜采用密码技术保证网络边界访问控制信息的完整性；

可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性；

以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。

●密码应用安全措施

在安全运维区域配置部署 1 台符合《SSL VPN 技术规范》《安全认证网关产品规范》的安全认证网关（SSL VPN），基于符合《基于 SM2 密码算法的身份认证系统密码及其相关安全技术规范》的身份认证系统向安全认证网关配置数字证书，基于密码技术构建安全通道，满足通信数据的机密性和完整性保护性要求。

（3）设备和计算安全

●密码应用基本要求

应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；

远程管理设备时，应采用密码技术建立安全的信息传输通道；

宜采用密码技术保证系统资源访问控制信息的完整性；

宜采用密码技术保证设备中的重要信息资源安全标记的完整性；

宜采用密码技术保证日志记录的完整性；

宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证；

以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。

●身份鉴别、远程管理通道和系统资源访问控制措施

首先在远程管理通道方面，通过符合国密要求的安全认证网关实现对远程传输通道的安全管理，确保运维人员远程登录的安全性，防止非法登录。通过安全认证网关认证后，运维人员使用 HTTPS 协议登录堡垒机，通过支持国密算法智能密码钥匙（以下简称 USBKey）的堡垒机作为跳板，使用 SSH 2.0 密码协议实现对各设备的运维管理，实现统一安全运维。

同时通过堡垒机对运维人员统一进行强身份认证进行登录授权，通过向运维人员派发国密算法的 USBKey 配合账号口令实现双因子认证，以此作为运维人员访问的登录的凭证，以实现系统强身份认证登录。

另外，通过堡垒机实现运维人员对被管理资产进行授权，同时解决系统资源访问控制。签名验签服务器配合堡垒机，对系统资源的访问控制进行管控，禁止无授权登录访问，实现统一的用户管理、身份认证、授权、定期修改口令等，其配置和策略管理相关信息应使用数字签名技术保证其完整性。

●日志记录完整性防护措施

通过部署签名验签服务器与审计系统对接，实现对设备日志记录的完整性保护。在本方案中审计系统每次写入日志时，签名验签服务器将同步对日志进行签名，保证数据真实性；在读取、查看日志时，签名验签服务器将对电子签名的真实性进行核查，如果签名验证失败，相关操作将被拒绝并执行相关安全处置规则。

（4）应用和数据安全

●密码应用基本要求

本级要求包括：

应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；

宜采用密码技术保证信息系统应用的访问控制信息的完整性；

宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；

应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；

应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；

宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；

宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；

在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性；

以上如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；

以上采用的密码产品，应达到 GB/T 37092 二级及以上安全要求。

●身份鉴别防护措施

在互联网和医卫专网网络接入区边界部署符合 GM/T 0026-2023《安全认证网关产品规范》的安全认证网关，在系统基础设施区部署符合 GM/T0034-2014《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》的身份认证系统，通过身份认证系统向安全认证网关配置数字证书，采用第三方电子认证服务机构的数字证书向移动端密码模块（二级）下发证书，实现移动端登录应用用户的安全身份鉴别，防止非授权人员登录。

●重要数据保护措施

业务系统数据。针对系统敏感请求数据通过数字信封技术对传输的数据加以保护，系统调用签名验签服务器进行数字信封的解密和验证，以保障重要数据传输过程中的机密性和完整性。

数据中心的数据库数据。针对数据中心的数据库传递到系统的业务服务器的重要数据，其中包含检索结果集，双方分别调用签名验签服务器，通过数字信封技术保障重要数据传输的机密性和完整性。数据中心的数据库传递到系统的业务服务器的数据将保存在数据中心的数据库，统一进行数据存储与管理。通过使用服务器密码机的加密功能，从而保证重要数据存储的机密性，并通过 MAC 技术保证数据存储的完整性。

●不可否认性措施

由于医院信息系统用户提交数据以明文形式传输，容易使业务数据被恶意拦截以及篡改，同时用户提交内容存在没有认证机制，存在抵赖的可能，因此存在严重的安全隐患，在方案中应基于数字证书、移动端密码模块（二级）、对系统中的关键操作行为（关键业务流转过程）做电子签名签章，保证认证返回结果在传输过程中消除被篡改的可能，同时确保认证结果的完整性、真实性和不可抵赖性。

（5）安全管理制度

系统安全管理是密码应用建设工作不可或缺的环节。依据国家标准 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》，系统的管理体系需涵盖管理制度、人员管理、建设运行及应急处置等四个方面的密码安全管理需求。这些需求与系统相关管理制度的对应关系如下表所示。

**表 2-9 系统管理制度与密码应用安全管理需求的映射关系表**

| 安全管理 | 标准合规性要求 | 与管理制度的对应关系和需求分析 |
|---|---|---|
| 管理制度 | 密码应用管理制度 | 对单位现有《系统平台安全管理办法》《机房管理制度》《运维管理制度》等系列制度进行修订构成。 |
| | 密钥管理规则 | 1.《机房管理制度》中包含物理层面的密钥管理内容，尤其注意密钥更新周期和策略的规定。<br>2.《机房管理制度》中包含网络和设备层面的密钥管理内容。<br>3.《系统平台安全管理办法》中包含业务层面的密钥管理内容 |
| | 建立操作规程 | 参照《密码产品操作手册》 |
| | 定期修订制度 | 《系统安全管理办法》中包含安全相关工作职责划分，其中说明制度定期修订情况，并包含必要的修订记录 |
| | 明确制度发布流程 | 《系统安全管理办法》中包含安全相关工作职责划分，其中说明制度发布流程和方式，以及版本控制方法 |
| | 执行过程记录留存 | 操作规程涉及的记录留存，各种《记录表单》中留存 |
| 人员管理 | 了解法律法规和制度 | 提供制度、培训、考核等安全管理资料 |
| | 密码应用岗位 | 在《系统安全管理办法》中规定系统负责人、安全主管、密钥管理员、密码安全审计员、密码操作员等 |
| | 上岗人员培训制度 | 1.《系统安全管理办法》中规定定义培训/定期考核的组织形式；<br>2.《密码安全岗位培训与考核计划》中定义密码培训内容（安全意识、制度、操作规程）以及考核内容（与培训内容相关）；<br>3.《岗位培训结果记录表》《考核结果记录表》等记录表单提供结果证据（人员、培训内容、培训/考核结果） |
| | 定期考核安全岗位 | |
| | 关键岗位保密制度 | 1.《系统安全管理办法》中定义基本要求；<br>2.《密码安全岗位人员保密协议》中包含细节（保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等） |
| 建设运行 | 制定密码应用方案 | / |
| | 制定密钥管理策略 | 在《系统安全管理办法》中规定； |
| | 制定实施方案 | 在密码应用方案中，有项目组织与实施方案章节内容 |
| | 运行前密码安全评估 | 在《系统安全管理办法》中规定； |
| | 定期评估和攻防 | |
| 应急处置 | 应急策略 | 可在《网络安全综合应急预案》中描述定义密码应用有关应急策略、定义事件分级，各级是否需要上报系统主管部门、事件处置流程以及是否需要上报系统主管部门 |
| | 事件处置 | |
| | 上报处置情况 | |

●机房管理制度

医院需要在滨河院区机房建设中制定符合国产密码应用要求的机房管理制度。

●运维管理制度

运维管理制度建设的目的是明确各单位日常运维工作的内容和责任，提升各单位履职范围内的网络安全工作重视程度，推动运维过程中网络安全工作的落实。主要内容包含运维管理操作规程、运维人员岗位职责和培训考核要求等内容。为满足密码应用安全需求，运维管理制度在原有条款的基础上增加“运维安全管理员”角色，履行为所有运维工程师管理、配发智能密码钥匙的职能，并负责对所有新安装或更新的重要业务系统软件包执行来源验证；增加“运维安全审计员”角色，履行设备运维日志记录的审计职能；原有的运维人员培训考核要求部分，增加对运维工程师、运维安全管理员、运维安全审计员等角色的密码应用安全意识、智能密码钥匙操作规程等内容的培训和考核；原有的“安全策略”部分增加密钥管理策略的条款，定义运维日志记录完整性密钥的管理要求，明确产生、更新这些密钥的操作规程和密钥更新周期；

●系统安全管理办法

建设目的是指导系统日常工作中的安全管理工作，明确各项安全要求，提升系统安全防护水平。内容涵盖系统安全管理相关的组织形式、工作流程、人员岗位、操作规程、安全策略等内容。为满足密码应用安全需求，系统安全管理办法在原有条款的基础上。明确系统的日常安全工作机制，说明制度定期修订情况，并包含必要的修订记录；明确本管理办法的发布流程和方式，以及版本控制方法；明确“系统负责人”“安全主管”“密钥管理员”“密码安全审计员”“密码操作员”等角色的职责，规定这些角色安全培训、考核的组织形式、奖惩制度以及人员离岗时的保密义务；明确平台安全策略，定义密钥相关操作所需遵循的操作规程制度文件，明确规定各类密钥的生命周期和相关管理要求。

●系统密码安全岗位培训与考核计划

建设的目的是规范各类角色的培训和考核的工作计划和主要内容，提升相关人员的安全意识和专业技能。内容涵盖培训及考核的组织形式，以及主要内容（安全意识、管理制度、操作规程等）。为满足密码应用安全需求，系统密码安全岗位培训与考核计划在原有条款的基础上增加培训及考核内容增加密码相关法律法规和政策、密码应用安全意识、密钥管理安全策略、密码设备操作规程等。

●系统网络安全综合应急预案

主要适用信息系统网络安全应急响应。明确信息系统网络安全应急管理机制，规范网络安全应急管理工作，提高网络安全事件的应急响应速度和相互协调水平，最大程度减少事件

造成的损失。内容安全事件分级、应急预案体系、应急组织机构和职责、预防和预警机制、应急响应流程等。为满足密码应用安全需求，《信息系统密码安全岗位培训与考核计划》在原有条款的基础上增加。事件分级中增加各类密钥泄露或密码安全事件的定级；应急响应流程中增加对密码主管机构的事件上报。

●其他相关手册和表单

其他相关手册和表单主要包含服务器密码机用户手册、签名验签服务器用户手册、电子签章系统用户手册、安全认证网关用户手册、时间戳服务器操作手册、堡垒机操作手册、智能密码钥匙操作手册、密码安全岗位培训结果记录表、密码安全岗位考核结果记录表、密码安全岗位人员保密协议等。

（6）密钥管理设计

密钥管理对于保证密钥全生命周期的安全性是至关重要的，可以保证密钥（除公钥外）不被非授权的访问、使用、泄露、修改和替换，可以保证公钥不被非授权的修改和替换。密钥管理包括密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节，以下给出可能会对密钥管理造成严重安全隐患的安全问题。

密钥产生。密钥产生环节可能会对密钥管理造成严重安全隐患的安全问题主要包括：1）未采用通过认证的随机数发生器生成密钥或密钥协商过程中的随机值，且无公开文献和证据证明随机数发生器的合理性和正确性；2）密钥在不可控的环境中生成；3）密钥协商之前或协商过程中没有验证对方身份真实性。

密钥分发。密钥分发环节可能会对密钥管理造成严重安全隐患的安全问题主要包括：1）使用没有访问控制机制的存储介质（如普通信封、普通 U 盘）等传输明文密钥，且管理制度无法保证密钥在分发过程中的安全性；2）密钥在不可控的环境中分发时，未使用密码技术保护密钥的机密性和完整性。

密钥存储。密钥存储环节可能会对密钥管理造成严重安全隐患的安全问题主要包括：1）密钥（除公钥外）以明文形式存储在不可控的环境中，且可以被非授权的访问、使用、泄露、修改和替换；2）公钥存储在不可控的环境中，且可以被非授权的修改和替换；3）用于加密密钥的口令以明文形式存储或复杂度小于 10^12。

密钥使用。密钥使用环节可能会对密钥管理造成严重安全隐患的安全问题主要包括：1）在多个实体可以使用密钥的场景下，缺乏对密钥的使用控制机制；2）对称密钥使用过程中，由于使用不当导致密钥泄露；3）公钥与实体之间无任何关联关系；4）公钥与实体之间利用 PKI 技术进行关联，但使用前未验证公钥有效性或验证机制不完备；5）未按密钥用途正确

使用。

密钥更新。密钥更新环节可能会对密钥管理造成严重安全隐患的安全问题主要包括：未建立密钥已泄露或存在泄漏风险时的密钥更新机制。

密钥销毁和撤销。密钥销毁和撤销环节可能会对密钥管理造成严重安全隐患的安全问题主要包括：1）不具备密钥在应急或按需的密钥销毁/撤销的机制；2）未按照设定的机制进行密钥销毁/撤销。

密钥恢复。密钥恢复环节可能会对密钥管理造成严重安全隐患的安全问题主要包括：密钥在恢复使用时没有鉴别机制，可以被导入到其他系统中。

（1）物理和环境

| 密钥名称 | 生成 | 存储 | 分发 | 使用 | 更新 | 备份和恢复 | 归档 | 销毁 |
|---|---|---|---|---|---|---|---|---|
| 门禁系统身份鉴别对称密钥 | 由门禁系统密码卡生成 | 以密文形式存储在门禁系统密码卡 | 制卡时离线分发 | 门禁卡中进行 MAC 计算；<br>门禁系统采用国密算法进行 MAC 验证 | 根据机房门禁系统管理策略定期更新 | 不涉及 | 不涉及 | 不涉及 |
| 门禁记录完整性保护密钥 | 由门禁系统密码卡生成 | 以密文形式存储在门禁系统密码卡 | 不涉及 | 在采用国密算法进行 MAC 的计算和验证 | 根据机房门禁系统管理策略定期更新 | 不涉及 | 不涉及 | 不涉及 |
| 视频监控记录完整性保护密钥 | 由视频监控系统密码卡生成 | 以密文形式存储在视频监控系统密码卡 | 不涉及 | 在采用国密算法进行 MAC 的计算和验证 | 根据机房视频监控安全管理策略定期更新 | 不涉及 | 不涉及 | 不涉及 |

（2）网络和通信

| 密钥名称 | 生成 | 存储 | 分发 | 使用 | 更新 | 备份和恢复 | 归档 | 销毁 |
|---|---|---|---|---|---|---|---|---|
| 安全认证网关 SSL 签名证书对应的私钥 | 在安全认证网关的密码卡中产生 | 以密文形式存储在安全认证网关的密码卡中 | 不涉及 | 在安全认证网关的密码卡中进行签名运算 | 证书到期或撤销时更新 | 不涉及 | 不涉及 | 参照证书撤销流程 |

| 密钥名称 | 生成 | 存储 | 分发 | 使用 | 更新 | 备份和恢复 | 归档 | 销毁 |
|---|---|---|---|---|---|---|---|---|
| 安全认证网关 SSL 签名证书中的公钥 | 在安全认证网关的密码卡中产生 | 存储在 SSL 签名证书中 | 随证书分发 | 在 SSL 客户端中进行验签运算 | 证书到期或撤销时更新 | 不涉及 | 不涉及 | 参照证书撤销流程 |
| 安全认证网关 SSL 加密证书对应的私钥 | 签发 SSL 加密证书的 CA 内部产生 | 以密文形式存储在安全认证网关的密码卡中 | 签发加密证书时从 CA 离线分发至安全认证网关中 | 在安全认证网关的密码卡中进行解密运算 | 证书到期或撤销时更新 | 在 CA 的密钥管理系统中备份和恢复 | 在 CA 的密钥管理系统中归档 | 超出归档时限后销毁 |
| 安全认证网关 SSL 加密证书中的公钥 | 签发 SSL 加密证书的 CA 内部产生 | 存储在 SSL 加密证书中 | 随证书分发 | 在 SSL 客户端中进行加密运算 | 证书到期或撤销时更新 | 不涉及 | 不涉及 | 参照证书撤销流程 |
| 网络会话主密钥 | 国密 SSL 协议协商产生 | 不涉及 | 不涉及 | 分别在 SSL 客户端和安全认证网关的密码卡中进行密钥派生运算 | 会话恢复时更新 | 不涉及 | 不涉及 | 会话终止时销毁 |
| 网络传输机密性密钥 | 由网络会话主密钥派生产生 | 不涉及 | 不涉及 | 分别在 SSL 客户端和安全认证网关的密码卡中进行加解密运算 | 随会话主密钥更新而更新 | 不涉及 | 不涉及 | 会话终止时销毁 |
| 网络传输完整性密钥 | 由网络会话主密钥派生产生 | 不涉及 | 不涉及 | 分别在 SSL 客户端和安全认证网关的密码卡中进行 MAC 运算 | 随会话主密钥更新而更新 | 不涉及 | 不涉及 | 会话终止时销毁 |
| 防火墙访 | 由签名验 | 以密文 | 不涉及 | 在签名验 | 根据安 | 不涉 | 不涉 | 不 |

| 密钥名称 | 生成 | 存储 | 分发 | 使用 | 更新 | 备份和恢复 | 归档 | 销毁 |
|---|---|---|---|---|---|---|---|---|
| 问控制信息完整性保护私钥 | 签服务器生成 | 形式存储在签名验签服务器中 | | 签服务器中进行签名运算 | 全管理策略定期更新 | 及 | 及 | 涉及 |

（3）设备和计算

| 密钥名称 | 生成 | 存储 | 分发 | 使用 | 更新 | 备份和恢复 | 归档 | 销毁 |
|---|---|---|---|---|---|---|---|---|
| 运维人员身份鉴别私钥 | 运维人员配备的USBKey产生 | 以密文形式存储在USBKey中 | 不涉及 | 在USBKey中进行签名运算 | 证书到期或撤销时更新 | 不涉及 | 不涉及 | 证书到期或撤销时销毁 |
| 运维人员身份鉴别公钥 | 运维人员配备的USBKey产生 | 存储在数字证书中 | 不涉及 | 在签名验签服务器中进行验证签名运算 | 证书到期或撤销时更新 | 不涉及 | 不涉及 | 证书到期或撤销时销毁 |
| 系统资源访问控制信息完整性保护私钥 | 由签名验签服务器生成 | 以密文形式存储在签名验签服务器 | 不涉及 | 在签名验签服务器中进行签名运算 | 根据安全管理策略定期更新 | 不涉及 | 不涉及 | 不涉及 |
| 系统资源访问控制信息完整性保护公钥 | 由签名验签服务器生成 | 以明文形式存储在签名验签服务器端防止被非授权篡改 | 不涉及 | 在签名验签服务器中进行验签运算 | 根据安全管理策略定期更新 | 不涉及 | 不涉及 | 不涉及 |
| 日志记录完整性保护私钥 | 由签名验签服务器生成 | 以密文形式存储在签名验签服务器 | 不涉及 | 在签名验签服务器中进行签名运算 | 根据安全管理策略定期更新 | 不涉及 | 不涉及 | 不涉及 |
| 日志记录完整性保护公钥 | 由签名验签服务器生成 | 以明文形式存储在签名验签服务器端防止被非授权篡改 | 不涉及 | 在签名验签服务器中进行验签运算 | 根据安全管理策略定期更新 | 不涉及 | 不涉及 | 不涉及 |
| 代码签名密钥 | 由应用开发方负责，不在本系统范围 | | | | | | | |
| 代码签名验证公钥 | 由应用开发方负责，不在本系统范 | 以明文形式存储在签名验签服务器端防止被非 | 由应用开发方负责，不在 | 在签名验签服务器中进行验签运算 | 由应用开发方负责，不在本系统范围 | | | |

| 密钥名称 | 生成 | 存储 | 分发 | 使用 | 更新 | 备份和恢复 | 归档 | 销毁 |
|---|---|---|---|---|---|---|---|---|
| | 围 | 授权篡改 | 本系统范围 | | | | | |

（4）应用和数据

| 密钥名称 | 生成 | 存储 | 分发 | 使用 | 更新 | 备份和恢复 | 归档 | 销毁 |
|---|---|---|---|---|---|---|---|---|
| 业务系统签名私钥 | 由业务系统负责，不在本系统范围 | 由业务系统负责，不在本系统范围 | 不涉及 | 由业务系统负责，不在本系统范围 | 证书到期或撤销时更新 | 不涉及 | 不涉及 | 参照证书撤销流程 |
| 业务系统验签公钥 | 由业务系统负责，不在本系统范围 | 以数字证书形式存储 | 随数字证书分发 | 在服务器密码机中进行数字信封的验签操作 | 证书到期或撤销时更新 | 不涉及 | 不涉及 | 参照证书撤销流程 |
| 大数据平台解密私钥 | 由签名验签服务器产生 | 以密文形式存储在签名验签服务器中 | 不涉及 | 在服务器密码机中进行数字信封的解密操作 | 证书到期或撤销时更新 | 在CA的密钥管理系统中备份和恢复 | 在CA的密钥管理系统中归档 | 超出归档时限后销毁 |
| 大数据平台加密公钥 | 由签名验签服务器产生 | 以数字证书形式存储 | 随数字证书分发 | 由业务系统负责，不在本系统范围 | 证书到期或撤销时更新 | 不涉及 | 不涉及 | 不涉及 |
| 数据中心存储机密性密钥 | 由服务器密码机产生 | 以密文形式存储在服务器密码机中 | 不涉及 | 在服务器密码机中进行重要数据加解密运算 | 根据安全管理策略定期更新 | 由服务器密码机进行备份和恢复 | 根据安全策略在密钥更新过渡期内由服务器密码机进行归档 | 根据安全策略在超出归档时限后销毁 |
| 数据中心存储完整性密钥 | 由服务器密码机产生 | 以密文形式存储在服务器密码机中 | 不涉及 | 在服务器密码机中进行重要数据加解密运算 | 根据安全管理策略定期更新 | 由服务器密码机进行备份和恢复 | 根据安全策略在密钥更新过渡期内由服务器密码机进行归档 | 根据安全策略在超出归档时限后销毁 |
| 业务日志记录完整性 | 由签名验签服务器生成 | 以密文形式存储在签 | 不涉及 | 在签名验签服务器中进行签 | 根据安全管理策略定 | 不涉及 | 不涉及 | 不涉及 |

| 密钥名称 | 生成 | 存储 | 分发 | 使用 | 更新 | 备份和恢复 | 归档 | 销毁 |
|---|---|---|---|---|---|---|---|---|
| 保护私钥 | | 名验签服务器 | | 名运算 | 期更新 | | | |
| 业务日志记录完整性保护公钥 | 由签名验签服务器生成 | 以明文形式存储在签名验签服务器端防止被非授权篡改 | 不涉及 | 在签名验签服务器中进行验签运算 | 根据安全管理策略定期更新 | 不涉及 | 不涉及 | 不涉及 |
| 认证结果电子版报告不可否认性公钥 | 由电子签章服务器生成 | 以明文形式存储在电子签章服务器 | 不涉及 | 在电子签章服务器中进行验签运算 | 根据安全管理策略定期更新 | 不涉及 | 不涉及 | 不涉及 |
| 认证结果电子版报告不可否认性私钥 | 由签名验签服务器生成 | 以密文形式存储在电子签章服务器 | 不涉及 | 在电子签章服务器中进行签名运算 | 根据安全管理策略定期更新 | 不涉及 | 不涉及 | 不涉及 |
| 业务日志数据时间戳公钥 | 由时间戳服务器生成 | 以密文形式存储在时间戳服务器 | 不涉及 | 在时间戳服务器中进行签名运算 | 根据安全管理策略定期更新 | 不涉及 | 不涉及 | 不涉及 |
| 业务日志数据时间戳私钥 | 由时间戳服务器生成 | 以密文形式存储在时间戳服务器 | 不涉及 | 在时间戳服务器中进行签名运算 | 根据安全管理策略定期更新 | 不涉及 | 不涉及 | 不涉及 |

**密码算法配置设计**

**表 2-10 应用和数据安全密码算法配置表**

| 保护层面 | 应用环节 | 配用的密码算法 | 承载算法的密码产品 |
|---|---|---|---|
| 应用和数据 | 身份鉴别 | SM2 | SSL VPN 身份鉴别平台密码模块 |
| | 应用访问控制信息完整性 | SM3 | 服务器密码机 |
| | 重要数据传输机密性 | SM4 | SSL VPN 密码模块 |
| | 重要数据存储机密性 | SM4 | 服务器密码机 |
| | 重要数据传输完整性 | SM3 | SSL VPN 密码模块 |
| | 重要数据存储完整性 | SM3 | 服务器密码机 |
| | 不可否认性 | SM2、SM3 | 签名验签服务器 |

**密码应用工作流程**

1.身份鉴别密码应用工作流程

应用系统身份鉴别基于 USBKey 中数字证书与应用系统账号口令相结合的方式实现。

USBKey 中存储有用户的个人证书，基于 USBKey 的身份鉴别采用基于证书的方式进行认证，同时 USBKey 提供数据签名、验签等功能，与 SSL 网关结合，实现系统中的传输安全。SSL 网关只允许通过了身份鉴别的用户对指定的应用端口进行连接，SSL 网关与终端用户的鉴别，采用基于 PKI 的双向认证机制，使用终端 USBKey 中存储的签名私钥以及根证书公钥，与 SSL 网关进行认证，在使用 USBKey 中私钥进行运算前，必须通过 USBKey 的 PIN 码认证。

应用系统身份鉴别流程如下：

用户插入 USBKey，客户端程序向 SSL 服务端发起随机数请求；

SSL 服务端生成随机数，返回给用户客户端，并记录本次登录请求的会话句柄；

客户端输入 PIN 码，密码模块依据 PIN 码对用户身份进行鉴别；

密码模块通过对用户的身份鉴别后，在密码模块中用签名私钥对得到的随机数进行签名并将签名结果和用户证书发送给 SSL 服务端；

SSL 服务端验证客户端提交的数字证书和签名值的有效性；

若证书和签名值有效性验证返回值为正确，获取证书中的用户账号，按照 SSL 网关访问控制策略对应用系统进行代理访问，在 SSL 网关中将用户证书和应用系统账号进行了绑定。

2.重要数据传输过程的机密性和完整性保护应用流程

业务系统作为 B/S 架构系统，系统需在用户端配备二级密码模块和安全浏览器，应用服务器前端配置 SSL VPN 网关，在用户端与 SSL VPN 之间建立 SSL 通信隧道，实现系统应用数据传输过程中的机密性和完整性保护，如下图所示。

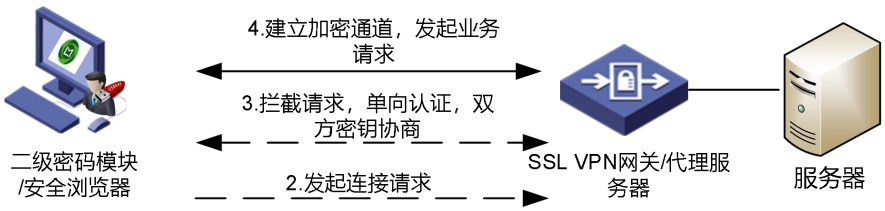


**图 2-9 重要数据传输过程的机密性和完整性保护应用流程图**

工作流程：

业务平台 PC 端用户，启动客户端认证软件；

客户端基于二级密码模块中存储的用户数字证书，与 SSL VPN 设备多次握手，服务端对客户端进行认证通过后，建立 SSL 安全通道。服务端利用 SSL 安全网关的 SSL 服务进行数据加密、数字签名，实现服务端数据传输的机密性、完整性、真实性。

PC 端用户打开浏览器，登录系统应用。

3.重要数据存储机密性应用流程

为保证系统中重要数据的存储安全，防止数据以明文形式暴露，系统中重要数据存储在数据库中，调用服务器密码机对重要数据进行加密实现保护。

（1）重要数据存储机密性保护流程

重要数据存储时，调用服务器密码机对重要数据使用 SM4 密码算法进行加密保护，对于重要数据写入操作，在写入前，调用服务器密码机加密算法，对数据进行加密处理，再执行写入操作，以密文形式进行存储。

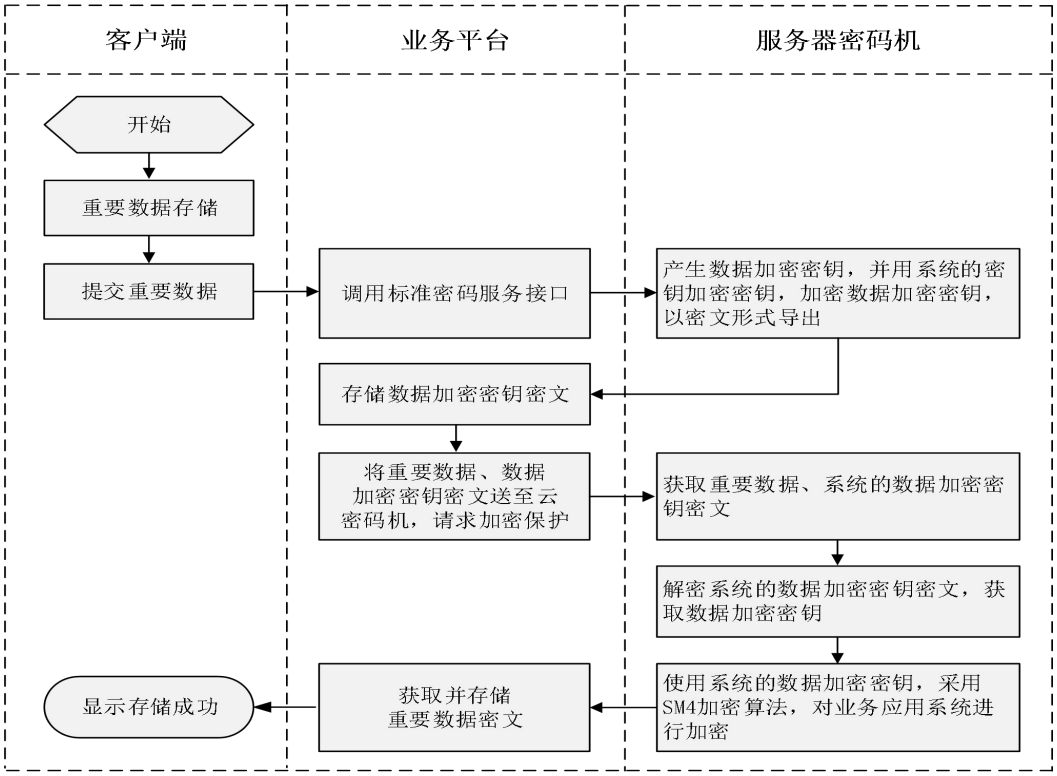


**图 2-10 重要数据存储机密性保护流程图**

加密存储流程：

业务系统重要数据存储；

业务系统获取存储的重要数据，调用标准密码服务接口申请数据加密密钥；

密码机产生业务系统的数据加密密钥，并用业务系统的密钥加密密钥，加密数据加密密钥，以密文形式导出；

业务系统存储数据加密密钥密文，将录入的重要数据、数据加密密钥密文送密码机，请求加密保护；

密码机获取录入的重要数据、业务系统的数据加密密钥密文；解密业务系统的数据加密密钥密文，获取业务系统的数据加密密钥；

密码机使用业务系统的数据加密密钥，采用 SM4 加密算法，对录入的重要数据进行加密；

业务系统获取并存储录入重要数据的密文；

用户终端显示存储成功。

（2）重要数据存储密文的读取流程

对于重要数据的读取操作，调用服务器密码机密码算法，对数据进行解密处理，将明文数据返回给上层接口。

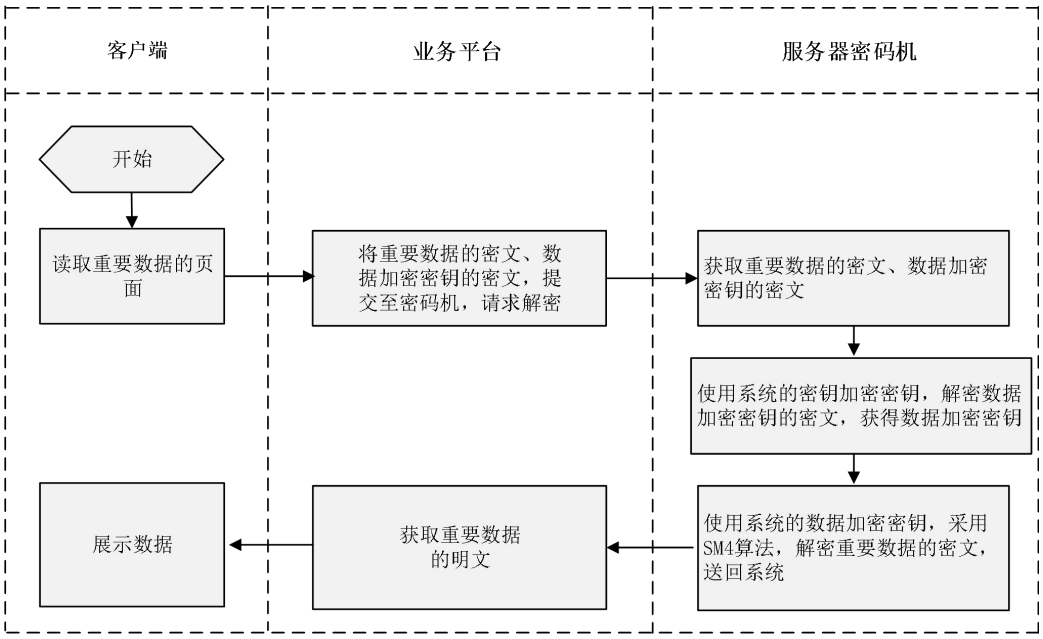


**图 2-11 重要数据存储密文的读取流程图**

访问加密存储的重要数据的解密浏览流程工作流程如下：

点击已加密存储的重要数据页面；

业务系统将重要数据的密文、数据加密密钥的密文，提交至密码机，请求解密；

密码机获取重要数据的密文、数据加密密钥的密文；

密码机使用业务系统的密钥加密密钥，解密数据加密密钥密文，获得数据加密密钥；

密码机调用业务系统的数据加密密钥，采用 SM4 加密算法，解密重要数据的密文，获得重要数据明文，送回业务系统；

业务系统获得重要数据的明文，向终端展现数据。

4.重要数据存储完整性应用流程

（1）重要数据存储完整性保护流程

录入重要数据时，业务系统底层调用服务器密码机，对其使用数据加密密钥通过 SM3 杂凑算法计算其 MAC 值，及时防范可能的篡改行为。应用流程如下：

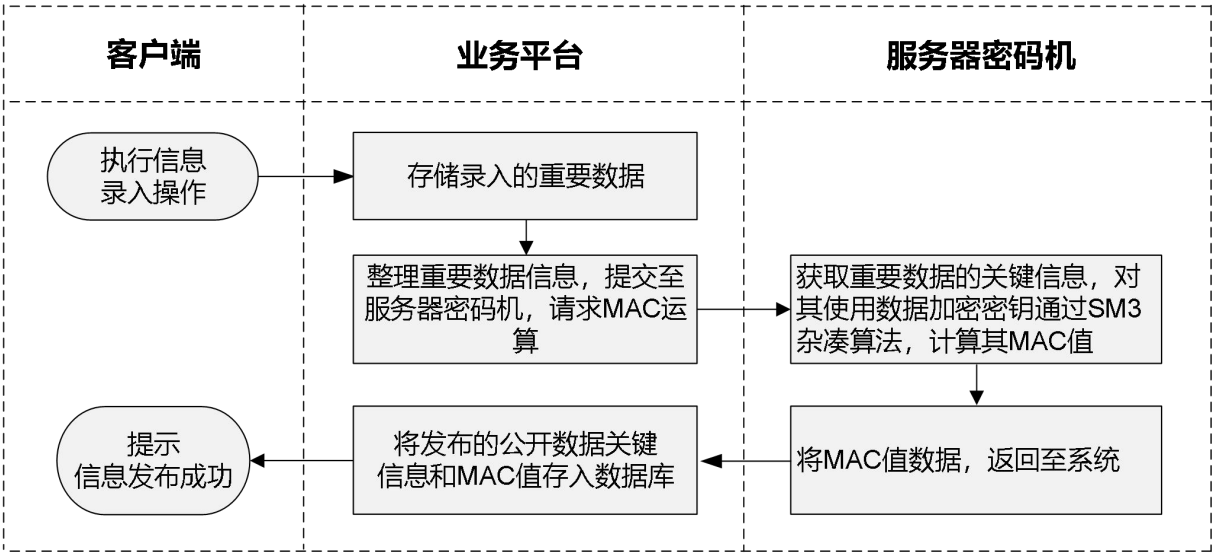


**图 2-12 重要数据存储完整性保护流程图**

对业务系统录入的重要数据信息 MAC 运算流程如下：

用户在业务系统执行信息录入操作；

业务系统将发布的重要数据信息，提交到服务器密码机，请求进行 MAC 运算；

服务器密码机获取重要数据信息，对其使用业务系统的数据加密密钥通过 SM3 杂凑算法计算其 MAC 值；

服务器密码机将 MAC 值返回给业务系统；

业务系统将重要数据信息及其 MAC 值一同存储到数据库系统中；

提示系统信息录入成功。

（2）重要数据访问完整性验证流程

访问重要数据时，系统自动调用服务器密码机，使用 SM3 杂凑算法，验证服务器密码机的相关关键信息的 MAC 值，确保服务器密码机的完整性。应用流程如下：

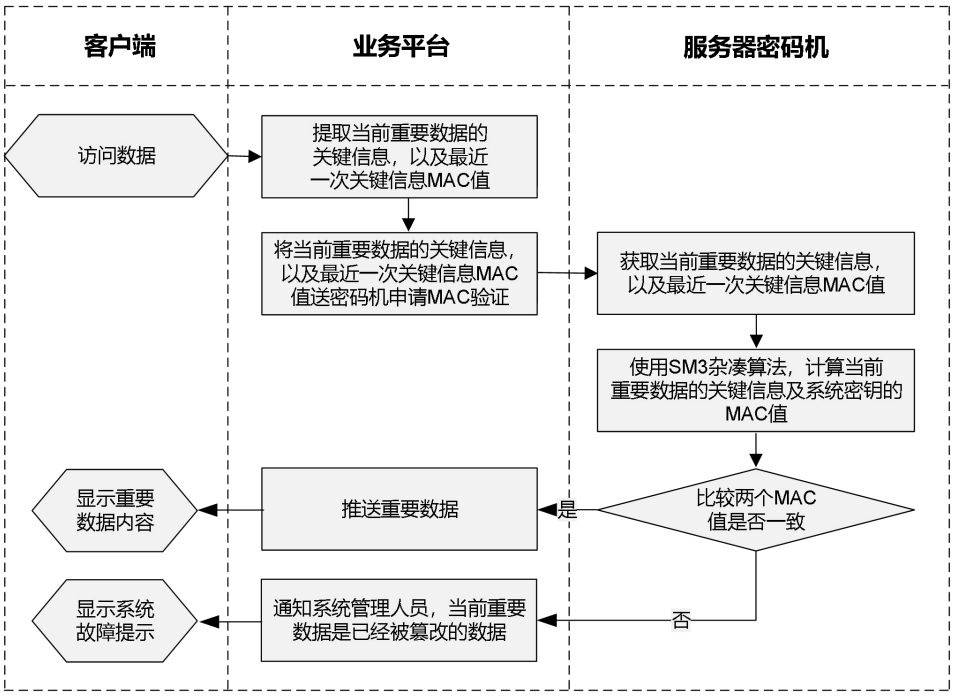


**图 2-13 重要数据访问完整性验证流程图**

验证重要数据完整性 MAC 值流程如下：

访问业务系统重要信息；

系统提取当前重要数据的相关关键信息，以及最近一次关键信息的 MAC 值；

系统将以上信息提交至服务器密码机，申请 MAC 验证；

服务器密码机获取当前重要数据的相关关键信息，以及最近一次关键信息的 MAC 值；

服务器密码机使用 SM3 杂凑算法，计算当前重要数据的相关关键信息及系统密钥的 MAC 值；

服务器密码机比较当前重要数据的相关关键信息和最近一次敏感数据的相关关键信息的 MAC 值，是否一致，并向系统平台返回结果；

如果两个 MAC 值一致，说明当前重要数据未被篡改，业务系统根据推送重要数据；如果两个 MAC 值不一致，说明当前重要数据已经被篡改。

5.不可否认性

在业务系统中，部分行为可能涉及法律责任认定，需要调用签名验签服务器对相应的业务操作信息进行数字签名，以实现上述操作行为的抗抵赖（不可否认性）。

**密码设备部署设计**

项目的部署方式和实现业务功能，在满足总体性、完备性、经济性原则的基础上，通过配置相关软硬件设备，同时正确部署配置，以满足本系统密码应用需求。

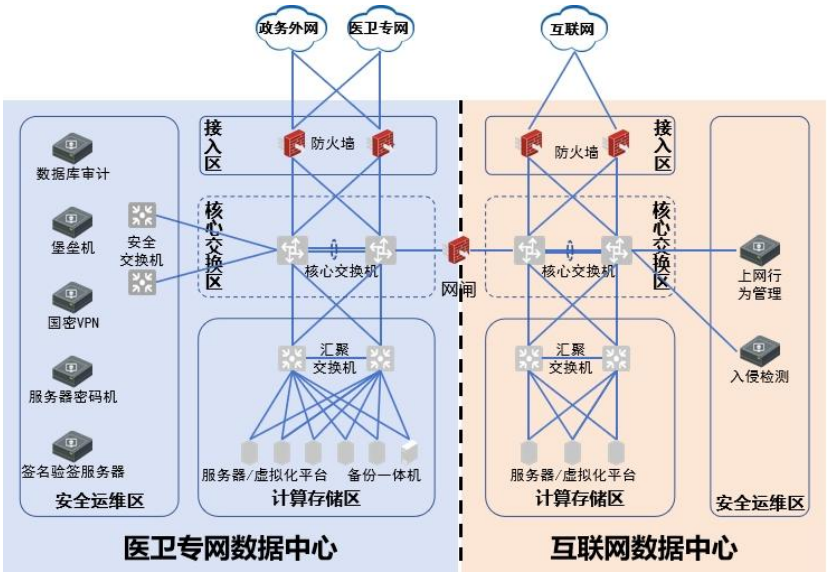


**图 2-14 密码设备部署架构图**

其中：

系统用户登录身份鉴别：通过部署在客户端的密码模块与应用服务区 SSL VPN 实现基于数字证书的身份鉴别，在应用系统中对用户账号和用户证书进行绑定，实现系统用户到 ERP 系统访问的身份鉴别。

访问控制信息完整性：调用服务器密码机，对两套业务应用系统访问控制策略、数据库表访问控制信息等使用 SM3 算法进行单向散列函数构造消息认证码（HMAC）实现数据的完整性。

重要数据存储机密性：调用服务器密码机，业务系统调用服务器密码机 SM4 算法，实现 CBC 模式的对称加密。

数据存储完整性：调用服务器密码机使用 SM3 算法进行单向散列函数构造消息认证码（HMAC）。

数据传输机密性和完整性：通过用户终端到应用服务区的 SSL 通信隧道实现应用层传输加密。

不可否认性：通过业务系统调用签名验签服务，对特定业务的操作进行数字签名。

**表 2-11 密码设备配置表**

| 序号 | 设备及软件名称 | 主要技术（性能）指标 | 单位 | 数量 |
|---|---|---|---|---|
| 1 | 国密 VPN 安全网关 | 机架式设备，≥6 个千兆 10/100/1000Base-T 自适应接口，≥4 个 SFP 接口，2 个 SFP+接口，冗余电源；支持国密 SM2/3/4 算法；整机吞吐率≥4Gbps，IPSec 加密速率，64 字节≥250Mbps，1428 字节≥2.5Gbps，IPSec 最大并发隧道数≥5000 条；SSL 最大并发连接数≥30000，SSL 每秒新建连接数≥400，SSL 最大并发用户≥30000，SSL 最大加密吞吐≥300Mbps，实际配置≥200 个 SSL VPN 用户授权；支持 SSL VPN、IPSec VPN 功能；支持 IP | 台 | 1 |

| | | | | |
|---|---|---|---|---|
| | | sec VPN 隧道自动建立，无需流量触发；可基于每个 SSL VPN 用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控；支持 IPsec VPN 智能选路，根据隧道质量调度流量。 | | |
| 2 | 服务器密码机 | 机架式硬件架构，≥4 个以太网千兆电口，≥2 个 10GE 光口，冗余电源；同时符合 GM/T 0030《服务器密码机技术规范》、GM/T 0028《密码模块安全技术要求》等相关技术要求；SM2 密钥产生速率≥4 万对/秒，SM2 签名速率≥4 万次/秒，SM2 验证速率≥3 万次/秒，SM2 加密速率≥2 万次/秒，SM2 解密速率≥4 万次/秒，SM3 计算速率≥1Gbps。整机密钥容量≥5 万；符合商用密码管理和规范要求。 | 台 | 1 |
| 3 | 签名验签服务器 | 机架式硬件架构，≥4 个以太网千兆电口，≥1 个接口扩展槽位，冗余电源；同时符合 GM/T 0029《签名验签服务器技术规范》、GM/T 0028《密码模块安全技术要求》等相关技术要求；SM2 签名速率≥40000 次/秒；SM2 验证速率≥10000 次/秒；SM2 制作数字信封≥800 次/秒；SM2 解析数字信封≥1000 次/秒；SM3 杂凑算法≥800Mbps；提供基于 SM2 算法的数字签名和认证功能，可用于证书生成和验证、身份认证等。 | 台 | 1 |
| 4 | 智能密码钥匙 | 具备国密局证书，支持国密 CSP、SKF，支持 SM2\SM4，RSA1024/2048； 支持标准 CA 功能，配合自建 CA 和运营 CA 进行终端身份认证、私钥存储、应用加解密、电子签章、SSLVPN 登录等。 | 套 | 20 |
| 1 | 个人证书 | 第三方机构（CA）颁发的数字证书，用于证明个人在网络通信中的身份。它使用公钥加密技术来保护通信数据的安全，确保只有授权方才能读取信息，具备 3 年有效期。 | 套 | 20 |
| 2 | SSL 证书 | 作为客户端和服务器之间建立一个安全的加密通道，确保数据在传输过程中的安全性和隐私性，具备 3 年有效期。 | 套 | 5 |

备注：智能密码钥匙和个人数字证书仅考虑系统管理和运维人员，医护人员和公共卫生人员个人数字证书利用现有证书。

## 备份系统设计

### 备份需求分析

为了保证郑州市慢病管理服务平台数据的安全性，按照信息系统容灾备份要求，本项目配置备份一体机，实现对郑州市慢病管理服务平台的备份。

采用数据备份一体机，对虚拟机、操作系统、文件、数据库等进行在线保护，核心数据库做到连续日志实时保护，达到数据库秒级保护，解决数据不丢失问题，备份系统可以对历史误删除或篡改的数据进行恢复找回，细颗粒度可达到表、字节、事务等，保证数据的可追溯性。即使中了勒索病毒，也可以恢复到勒索前的有效状态和数据。

### 备份系统设计

采用数据备份一体机，对虚拟机、操作系统、文件、数据库等进行在线保护，核心数据

库做到连续日志实时保护，达到数据库秒级保护，解决数据不丢失问题，备份系统可以对历史误删除或篡改的数据进行恢复找回，细颗粒度可达到表、字节、事务等，保证数据的可追溯性。即使中了勒索病毒，也可以恢复到勒索前的有效状态和数据。

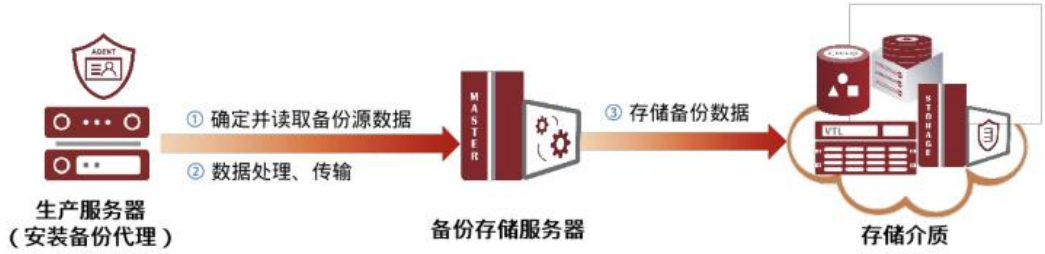


**图 2-15 备份系统业务流程图**

在配置备份一体机 1 台；各个业务服务器安装备份代理端连通备份一体机。配置备份策略，代理端根据作业配置发起备份，通过网络向备份一体机传输数据。备份一体机接收数据加密并保存到内置的磁盘存储上。未来通过远程复制，实现异地数据级容灾。

**数据备份策略**

从备份策略来讲，备份可分为三种：完全备份、增量备份、差异备份。下面来讨论以下这几种备份方式：

完全备份就是拷贝给定计算机或文件系统上的所有文件，而不管它是否被改变。

增量备份就是只备份在上一次备份后增加、改动的部分数据。增量备份可分为多级，每一次增量都源自上一次备份后的改动部分。

差异备份就是只备份在上一次完全备份后有变化的部分数据。如果只存在两次备份，则增量备份和差异备份内容一样。

累加备份采用数据库的管理方式，记录累积每个时间点的变化，并把变化后的值备份到相应的数组中，这种备份方式可恢复到指定的时间点。

一般在使用过程中，这三种策略常结合使用，常用的方法有：完全备份、完全备份加增量备份、完全备份加差异备份。

完全备份。完全备份会产生大量数据移动，每天完全备份直接把备份数据存放在高可靠性存储阵列上。完全备份可以保证数据的完整性，但同时需要大量磁盘空间存储备份数据。

完全备份加增量备份。完全备份加增量备份来自完全备份，减少了数据移动，同时减少完全备份的次数。

完全备份加差异备份。增量备份考虑自前一天以来哪些文件发生变化，而差异方法考虑自完全备份以来哪些文件发生了变化，对于完全备份后立即备份的备份过程（上例中周六），因为完全备份发生在前一天，所以两种备份方式的结果是一样的，但到了周一以后两种备份

方式产生的数据量就不一样：增量备份会备份 24 小时内改变了的文件，差异备份会备份 48 小时内改变了的文件；到了周二，差异备份方法备份 72 小时内改变了的文件。尽管差异备份比增量备份移动和存储更多的数据，但恢复操作简单多了。在完全备份加差异备份方法下，完整的恢复操作首先恢复上周六晚的完全备份。

备份时间窗和业务忙时错开。由于备份系统对虚拟机进行备份期间会占用网络带宽，故备份窗口设置为凌晨业务闲时。首次备份的数据量大，一般在用户将业务部署到数据中心后，选在周末统一对一批次数据进行备份。

根据现网的网络和业务情况，备份时间窗内能将当天需要执行的备份数据全部备份完毕。由于备份时，会对虚拟机所在存储进行大量读操作，备份时间窗最好和其他存储消耗型的应用执行时间错开。

**备份系统配置**

生产数据包含结构化数据、非结构化数据，备份数据均将以文件的形式进行备份。考虑业务数据 70%的重复数据删除率，数据至少保留一个月。

备份一体机按照备份策略对全量业务进行全备和增备，根据数据量估算，各系统业务产生结构化数据总量为 10TB，考虑备份策略下的多备份副本需求，确定副本系数为 3；存储利用率按照 80%计算，则备份需求容量=10×3÷80%≈37.5TB，本项目配置备份容量为 40TB 的备份一体机 1 台。

## 运维系统建设

**运维维护目标**

建立规范化、标准化、制度化的运行维护体系，完成对系统运行状态的全面监控和运行问题的及时处理，支持医院信息化平台的安全、稳定、高效、持续运行。同时，通过运行维护制度与运行维护技术支持队伍的建设，实现运行维护工作的高效率，提高整体的运行维护水平。

本项目运行维护服务包括信息系统相关的硬件设备、操作系统、数据库和存储设备的运行维护服务，保证用户现有的信息系统的正常运行，降低整体管理成本，提高信息系统的整体服务水平。同时根据日常维护的数据和记录，提供信息系统的整体建设规划和建议，更好地为用户的信息化发展提供有力的保障。

信息系统的组成主要分为硬件设备和软件系统。

硬件设备包括网络设备、安全设备、主机设备、存储设备、终端设备；

软件设备分为操作系统软件、典型应用软件（如：数据库软件、中间件软件）、业务应用软件。

平台通过运行维护服务的有效管理提升用户信息系统的服务效率，协调各业务应用系统的内部运作，改善网络信息系统部门与业务部门的沟通，提高服务质量。结合用户现有的环境、组织结构、IT 资源和管理流程的特点，从流程、人员和技术三方面来规划用户的网络信息系统的结构。将用户的运行目标、业务需求与 IT 服务的相协调一致。

提供的信息系统服务的目标是，对用户现有的信息系统基础资源进行监控和管理，及时掌握网络信息系统资源现状和配置信息，反映信息系统资源的可用性情况和健康状况，创建一个可知可控的 IT 环境，从而保证用户信息系统的各类业务应用系统的可靠、高效、持续、安全运行。

服务项目范围覆盖的信息系统资源的关键状态及参数指标、运行状态、故障情况、配置信息、可用性情况及健康状况性能指标。

**运行维护机构**

可靠的运维工作是系统实现建设目标、发挥效用的重要保障，为了避免“重建设、轻应用”的弊端，需要建立平台建设运维体系，为此成立了由主管领导为组长，以医院信息科为核心的运维领导小组，下设网络安全组、计算存储组、应用管理组、终端维护组。

（1）网络安全组

网络安全组负责网络的维护工作,保障网络的畅通;负责平台建设安全体系的管理维护、保障网络的安全；同时负责网站的建设、更新、维护。

（2）计算存储组

计算存储组负责服务器、存储核心硬件设备的管理维护，保障设备正常运转，负责核心数据的存储、备份、管理。

（3）应用管理组

应用管理组负责应用系统、数据库、中间件的运行维护，保障系统的良好、稳定地运行。

（4）终端维护组

终端维护组负责对工作人员的 IT 技术支持，及时响应工作人员请求，保障每个终端用户正常使用网络、终端、应用系统。

**运行维护管理**

运行维护内容规划。为确保运行维护工作正常、有序、高效地进行，必须针对运行维护的管理流程、管理内容和建设方案，制定相应的运行维护管理制度和运行维护技术方案，实

现各项工作的规范化管理。运行维护管理制度分为网络管理制度、应用系统管理制度、安全管理制度、存储备份管理制度、故障处置制度、人员管理制度和质量考核制度等。运行维护体系的各技术支持方案包含软件平台、基础平台、网络平台、安全系统等运行维护。具体的建设内容如下：

1.设备运维

建立设备台账，记录设备的基本信息和运维记录，包括设备名称、型号、序列号、采购日期、维护保养记录。

制定设备巡检计划，定期对设备进行巡检，排查故障和隐患，并记录巡检结果，及时进行故障处理。

建立设备库存清单和备件管理制度，确保备件的充足性和及时更新。

制定设备报废和更新的程序，定期评估设备的性能和可靠性，及时淘汰老化设备并进行更新。

2.环境运维

定期进行机房环境巡检，包括温度、湿度、空气质量等，确保机房环境符合设备要求。

设立健全的机房温湿度控制系统，保持机房环境的稳定性。

对机房进行定期清洁和维护，包括机柜、地面、天花板等，保持机房的整洁和安全。

3.软件运维

保证系统正常而可靠地运行，并能使系统不断得到改善和提高，以充分发挥作用。因此，要有计划、有组织地对系统进行必要的改动，以保证系统中的各个要素随着功能需求、环境等的变化始终处于最新的、正确的工作状态。

根据需求进行系统业务逻辑调整。即对系统程序的修改和调整，扩充在使用过程中提出的新的功能及性能要求。

随着系统应用范围的扩大，应用环境的变化，系统中的各种代码都需要进行一定程度的增加、修改、删除，以及设置新的代码。

定期检查程序错误日志，清除系统运行中发生的故障和错误。

4.数据维护

业务处理对数据的需求是不断发生变化的，除了系统中主体业务数据的定期正常更新外，还有许多数据需要进行不定期的更新，或随环境和业务的变化而进行调整，以及数据内容的增加、数据结构的调整。此外，数据的备份与恢复等，都是数据维护的工作内容。

5.数据库维护

监视数据库的状态、SGA 的各种参数、日志事件（警告）、侦听器状态、进程状态、可用性如死锁、资源争用、不一致性以及会话和 SQL 活动、等待状况、数据库碎片情况等。

监视数据库归档日志和可用空间量，以及数据库归档日志目的地中可用空间的百分比；监视转储目的地目录的使用空间百分比。

监视并警告当前分配的扩展数据块数超出指定阈值的数据库对象。

对表空间的使用情况和增长情况进行定期分析和预警。

针对数据库中的 I/O 情况进行实时监控。

定期提供数据库运行性能的分析、帮助提出诊断和优化调整建议。

将监控到的数据库性能指标保存下来，生成性能趋势报告，为管理者提供决策依据。

定期检查系统日志和备份作业日志，根据日志解决存在和潜在问题。

**运行维护内容**

运行维护内容包括网络管理、系统（主机系统、数据库系统、中间件系统）和应用管理、安全管理、存储备份管理、故障管理、技术支持管理。

1.系统和应用管理内容

系统管理主要实现对各子系统的配置管理，性能管理、可靠性管理。配置管理包括对系统资源的发现、提供、配置和控制；性能及可靠性管理主要对各系统的关键参数或重要资源进行监控和检查，了解系统运行情况，及时察觉系统可能的故障，从而保证系统的正常运行，提高系统可靠性。

应用管理主要实现对各应用系统的可靠性管理、版本管理和数据管理。可靠性管理包括及时监控应用系统运行情况，及时发现潜在的问题，保证正常运行；版本管理包括对应用系统的版本/补丁的管理、发布及升级，配合相关部门进行应用系统的相关测试、试运行和推广；数据管理包括按照有关规定及工作流程对后台数据必要的修改。

2.故障管理内容

故障管理包括网络、系统和应用、安全、存储备份的故障发现、故障分类、故障转发、故障诊断、故障处理、故障处理记录和统计等过程。

3.技术支持管理内容

技术支持管理包括对运行维护技术支持平台中的技术支持手段和工具、技术支持人员等的管理。

4.安全管理内容

安全管理内容包括从系统、网络、数据、操作维护等多个层面提供了多种安全保障机制。

系统安全性：系统安全包括操作系统、数据库、中间件可以正常运行，以支撑应用各个应用软件的运行。

网络安全性：网络安全包括交换机、路由器、防火墙等网络设备的正常运行，以确保网络层的安全策略得到落实。

数据安全性：数据安全包括用户身份信息、系统正常运行的配置信息、系统运行的日志、数据库数据等数据的存储、传输、管理的安全性。

**运行维护流程**

平台运行维护流程涉及服务台、事件管理、问题管理、配置管理、变更管理、发布管理、服务级别管理、财务管理、能力管理、可用性管理、服务持续性管理、知识管理及供应商管理等，随着运维活动的不断深入和持续改进，其他流程会逐步独立并规范。

（1）服务台

服务台是支持平台运维服务的核心功能，与各个流程联系密切。所有管理流程都要通过服务台为平台用户提供单点联系，解答用户的相关问题和需求，或为用户寻求相应的支持人员。

在本项目中，服务台是接收各种来源服务请求和相关信息反馈的唯一入口和出口，同时服务台还负责一般请求、通过知识库（历史事件）能够解决的请求；也是复杂问题二线处理的桥梁。

（2）事件管理

事件管理流程的主要目标是尽快恢复平台服务提供并减少其对业务的不利影响，尽可能保证最好的 IT 服务质量和可用性等级。事件管理流程通常涉及事件的侦测和记录、事件的分类和支持、事件的调查和诊断、事件的解决和恢复以及事件的关闭。

本项目把所有服务请求和报警归结为事件。事件管理是提供服务台和事件管理者对于事件记录、处理、查询、审核、派发等功能。

（3）工单管理

工单是运维服务供应商现场运维、二线支持的任务载体，运维工程依据所接收工单进行 IT 运维工作。工单管理包括工单创建、变更、查询浏览、派发、监督等操作。本项目工单管理由运维服务供应商提供相关工单管理制度、流程、相应支撑工具，经用户审核通过后，在本项目中应用。

（4）问题管理

问题管理主要目标是预防问题和事故的再次发生，并将未能解决的事件的影响降低到最

小。问题管理流程包括诊断事件根本原因和确定问题解决方案所需要的活动，通过合适的控制过程，尤其是变更管理和发布管理，确保解决方案的实施。问题管理还将维护有关问题、应急方案和解决方案的信息。

（5）变更管理

变更管理实现所有 IT 基础设施、软件平台和应用系统的变更，变更管理应记录并对所有要求的变更进行分类，应评估变更请求的风险、影响和业务收益。其主要目标是以对服务最小的干扰实现有益的变更。

（6）配置管理

配置管理流程负责核实基础设施、软件平台和应用系统中实施的变更以及配置项之间的关系是否已经被正确记录下来；确保配置管理数据库能够准确地反映现存配置项的实际版本状态。

配置管理实际上是全部 IT 资源的统一管理的功能，包括 IT 资源整个生命周期的参数或配置的变化记录的管理。管理信息主要涉及分类、型号、版本、位置，状态、相关资料等基本信息还包括核心参数等。

（7）知识库管理

知识库是提供给运维人员重要的技术资料内容，汇集了工作中遇到的典型案例、归纳总结的知识要点和全面的实用资料手册。

**应急响应流程**

在运行维护过程中，意外情况难以完全避免，项目运行维护组需要制定详尽的应急处理预案，针对各类突发事件，设计相应的预防与解决措施，同时提供完整的应急处理流程，要求整个流程严谨而有序。

1.运行维护值班人员平时应做好应急事件的监控工作，对于突发事件应认真分析、准确判定故障发生的数据域，负责跟踪该事件直至其结束。

2.正常情况下，要求运行维护值班人员在 10 分钟内进行事件确认。如果属于一般事件则按照事件流程进行分派处理，否则应迅速启动《应急预案》，并严格按照《应急预案》所规定的步骤快速实施应急处置，及时汇报上级领导，掌握实时处理情况。

3.在处理过程中，如需其他部门去现场增援处理，应及时向上级领导部门汇报，协调沟通，尽快联系技术工程师或厂家技术支持赶赴现场援助处理。

**技术支持平台**

在运行维护体系建设中，技术支持平台的建设占有重要地位，它包含了实施运行维护管

理的手段和工具，是运行维护体系的技术保障。

为提高本项目日常运行维护的自动化水平和效率，本项目利用本次建设的运维管理系统及医院现有运行维护工作等，进行网络、主机、数据库、中间件及各应用系统的日常监控、维护和安全管理，定期产生运行维护报告。系统监控发现的问题或潜在的隐患转入问题跟踪系统进行处理过程的跟踪。日常运行维护平台包括综合监控系统及其所需的运行环境，包括管理服务器、管理终端、数据库、中间件等。

本项目运维管理系统建设以“管理体制标准化、工作流程规范化、运行情况可视化、质量评估数字化、故障分析智能化、工程管控一体化”为目标。

建设完备的运维管理系统，整合数据中心、计算、存储、网络、安全、应用及前端设备等各类运维管理内容，综合监控、统一运维和统一服务，实现全医院信息化系统的统一展现、统一告警、统一流程处理和自动化运维管理。

运维管理系统应实现对基础服务设施、平台服务设施、数据服务设施和应用服务设施的统一运维、自动监控、故障预警处置等信息化管理，同时对各层资源实现全生命周期的运维管理，事后能够追溯，提供资源管理、统计、监控调度、服务掌控等端到端的综合管理能力。

数据采集系统包括前端设备监控、服务器监控、存储监控、网络监控、日志监控、流量分析、应用监控、虚拟化和第三方接口等。需要对云平台内各类软硬件系统进行状态监控，包括网络、主机、存储等硬件设备，以及虚拟化平台、中间件、数据库等软件系统。

基础设施监控平台监控内容包括：前端设备、服务器、存储设备、交换机、路由器、防火墙、网关和动环设备等机房硬件设施，还包括虚拟化资源、中间件、数据库、操作系统、工作流引擎、第三方接口、电力、空调、温湿度以及机房等资源的监控。

业务数据监控平台监控内容包括：云资源池内部数据的交换，外部数据通过信息交换共享平台与共享数据库的数据交换，共享数据库和业务数据库中数据的生产、修改、删除，还包括日志监控和流量分析。

应用软件监控平台监控内容包括：应用软件的安装、校验、升级、修复和删除。

要求将采集的数据汇聚后，经过资源建模、业务建模等数据抽象环节，形成用户管理数据库、告警事件数据库、系统性能数据库（PMDB）、配置管理数据库（CMDB）。要求将服务台、业务管理、资源管理、可视化管理、告警管理、统计分析、系统配置、知识库等实现集成管理，并满足 ITIL 中的 IT 服务持续性管理、可用性管理、服务级别管理、IT 服务财务管理、能力管理、事故管理、问题管理、配置管理、变更管理、发布管理等要求。

各种资源可接入运行维护管理平台，向运行维护管理平台传送监控信息（包含从联网平

台推送的图像、报警信号、业务数据等）。用户可通过 Web 或者用户终端访问运行维护管理平台，实现对各种信息资源的共享、处理和分析。

**运行维护制度**

为确保运行维护工作正常、有序、高效地进行，必须针对运行维护的管理流程和内容，制定相应的运行维护管理制度，实现各项工作的规范化管理。运行维护管理制度分为网络管理制度、终端管理制度、系统和应用管理制度、安全管理制度、存储备份管理制度、故障管理制度、人员管理制度和质量考核制度等。

1.网络管理制度

包括网络的准入管理制度、网络的配置管理制度、网络的运行/监控管理制度等。

2.终端管理制度

包括摄像机等终端设备的建设、配置、加密、用电、安全管理制度。

3.应用管理制度

包括对主机、数据库、中间件、应用系统的配置管理制度、运行/监控管理制度、数据管理制度等。

4.安全管理制度

包括网络、主机、数据库、中间件、应用软件、数据的安全管理制度及安全事故应急处理制度。

5.存储备份管理制度

包括备份数据的管理制度和备份设备的管理制度。

6.故障管理制度

包括对故障处理过程的管理制度、故障处理流程的变更管理制度、故障信息利用的管理制度及重大故障的应急管理制度等。

**运维保障服务**

为确保平台的安全稳定运行，本项目将要求项目承建单位提供项目竣工验收后三年免费质保和运维保障服务，三年免费质保和运维保障服务结束后，将采用符合相关法律法规的方式公开选取专业的运行维护服务商，保障系统的安全稳定运行。项目运行维护服务商和在质保和运维保障服务期内的承建单位应提供包括不限于电话支持服务、邮件支持服务、在线远程支持服务等运维保障服务。

1.电话支持服务

电话支持服务是一项基于电话的技术支持服务，要求承建方提供 7×24 小时电话响应，

转给相应技术工程师进行处理，帮助迅速有效地解决问题。

2.邮件支持服务

通过邮件的方式，用户对问题的出现提供详细的描述，承建方将对问题解决回应，以邮件的形式提供解决方案。

3.在线远程支持服务

通过技术支持中心与客户端系统的网络连接，可以在远程对系统问题进行分析，检查和数据搜集。

建议保留一个专门用于支持的账户。该账户必须有口令保护。为每次事件设定一个口令并随后取消、重置。

维护安全，从用户、应用、审计等多个层面提供安全机制，构建操作维护的安全性。

## 机房及配套工程建设

结合郑州市第七人民医院滨河院区信息化发展规划郑州市第七人民医院数据中心机房建设面积为219平方米，由主机房设备区、配电间、疏散缓存区等功能区组成。其中主机房设备区面积约147㎡，配置标准服务器机柜4kW机柜34台，配置20柜位冷通道组件2套、配电间面积约34㎡、疏散缓存区面积约38㎡。建设标准为《数据中心设计规范》（GB50174－2017）B类标准。能够为本项目提供可靠的基础环境支持。

本项目配置服务器、存储、交换机、安全设备等38台，经核算设备共需机柜U数80U，考虑实际机柜承载情况，本项目需要3台42U标准化机柜，现有机房机柜能够满足项目建设需要。当前机柜供电功率按照4KW进行设计，能够满足项目建设需要。现有机房消防、制冷、通风、承重等均按照《数据中心设计规范》（GB 50174-2017）B级机房标准进行设计，能够满足项目建设需要。

## 主要软硬件选型原则、软硬件配置清单

### 2.4.1 主要软硬件选型原则

1.国产化原则

本项目落实国家深化安全可靠应用替代工作要求，本项目的网络交换设备、虚拟化集中式存储、分布式存储、网络安全设备、备份设备等均采用国产自主可控产品；

2.开放性和扩展性原则

一方面，要采用开放性、标准化的设备、软件资源；另一方面，系统对于未来可能增添

的新的系统、新的功能、新的用户都要留有接口，并符合相关技术标准，系统可以随形势的发展而不断成长扩大。

本项目按照国家有关政策要求，全面推动 IPv6 规模化部署和应用，打造基于 IPv6 的下一代医院互联网，在硬软件设备选型中，全部采用符合 IPv6 要求的产品。

3.先进性和成熟性原则

信息技术发展迅速，新理念、新体系、新技术竞相推出，这造成了新的、先进的和成熟的技术之间的矛盾。而大规模、全局性的系统，其功能和性能要求具有综合性。因此，在产品选用方面要求先进性和成熟性的统一，以满足系统在很长的生命周期内有持续的可维护性和可扩展性。

4.可靠性原则

在社会向信息时代迅速发展的同时也有潜在危机，即对信息技术的依赖程度越高，系统失效可能造成的危害和影响也就越大。因此，本系统的软硬件选择在尽可能在有限的投资条件下，从系统结构、网络结构、技术措施、设备选型以及厂商的技术服务和维修响应能力等方面综合考虑，确保系统整体运行的可靠性。

### 2.4.2 主要软硬件配置清单

# 软硬件设备购置清单

| 序号 | 设备及软件名称 | 主要技术（性能）指标 | 单位 | 数量 | 部署位置 |
|---|---|---|---|---|---|
| | 合计 | | | | |
| （一） | 计算和存储系统 | | | | |
| 1 | 服务器 | 标准机架式服务器；国产芯片、国产处理器；≥2 颗 24 核 X86 架构 CPU 或 2 颗 48 核 ARM 架构 CPU,主频≥2.2GHz；≥512GB 内存；≥2 块 960GB SSD 硬盘;≥4 个 10G 光口(含光模块），≥4 个千兆电口；≥1 块独立 RAID 卡（≥4GB 缓存）；冗余电源；≥4 块 4 TB SATA HDD 硬盘，≥2 块 1.92TB SSD 硬盘。 | 台 | 4 | 医卫专网 |
| 2 | 服务器 | 标准机架式服务器；国产芯片、国产处理器；≥2 颗 24 核 X86 架构 CPU 或 2 颗 48 核 ARM 架构 CPU,主频≥2.2GHz；≥256GB 内存；≥2 块 960GB SSD 硬盘;≥4 个 10G 光口(含光模块），≥4 个千兆电口；≥1 块独立 RAID 卡（≥4GB 缓存）；冗余电源；≥2 块 4 TB SATA HDD 硬盘，≥2 块 1.92TB SSD 硬盘。 | 台 | 3 | 互联网 |
| 3 | 虚拟化软件 | 支持 CPU 虚拟化,将物理服务器的 CPU 虚拟成虚拟 CPU（vCPU），供虚拟机运行时使用。当多个 vCPU 运行时，会在各 vCPU 间动态调度物理 CPU 的能力。支持主流的操作系统虚拟化。支持虚拟机管理，包含虚拟机资源管理、虚拟机生命周期管理、虚拟机模板管理、CPU QoS、虚拟资源动态复用、虚拟机资源动态调整、虚拟网卡、网络 I/O 控制、迁移网络、内置负载服务、分布式虚拟交换机、跨主机热迁移、跨存储热迁移、虚拟机高可用性（HA）、虚拟机回收站、动态资源调度（DRS&DPM）、虚拟机资源 QoS、网络安全组、VMware 虚拟机模板导入等功能。支持支持虚拟机和其他物理服务器统一管理。支持对系统环境检测,支持常见的虚拟资 | 套 | 2 | 23.8 |

| | | | | | |
|---|---|---|---|---|---|
| | | 源和物理资源报警，支持虚拟服务器自助申请、自助缴费功能，支持虚拟使用报表导出，支持其他虚拟化平台统一纳管，提供 B/S 和 C/S 两种虚拟机控制台使用方式，支持网络流量优化、宿主机自治、迁移工具、虚拟机迁移工具等功能。满足本项目配置服务器虚拟化需要，具有扩展至≥10 台服务器虚拟化能力。 | | | |
| （二） | **备份系统** | | | | |
| 1 | 备份一体机 | ≥2 颗处理器（国产芯片，国产处理器。单颗处理器≥12 核 CPU，≥2.0GHz 主频），≥128GB DDR5 内存，≥2 块 960 GB SSD，≥72TB SATA 硬盘，≥1 块独立 RAID 卡（≥4G 缓存）；≥2 个 10GE 光口（含多模光模块）；≥2 个 1GE 电口；支持在线文件备份。 | 台 | 1 | 医卫专网 |
| （三） | **网络系统** | | | | |
| 1 | 核心交换机 | 交换容量≥500Tbps；包转发率≥100000Mpps；双主控，双电源，≥48 个万兆光口，≥8 个万兆多模光模块，≥8 个千兆多模光模块；≥2 个交换插槽，≥6 个业务插槽；支持 IPv4/IPv6 双栈协议；支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；支持横向虚拟化功能；支持纵向虚拟化技术，含项目所需线缆等组件。 | 台 | 2 | 医卫专网 |
| 2 | 业务交换机 | 交换容量≥2.8Tbps，转发性能≥2000Mpps；10GE 光口数量≥48 个（含光模块），≥2 个 40GE QSFP+口（含光模块），≥4 个 100GE 光接口（含光模块）；≥1 根≥40G 堆叠线缆；≥4 个风扇，冗余电源；支持 IPv4/IPv6 双栈协议；支持集群或堆叠多虚一技术，支持纵向虚拟化技术。 | 台 | 2 | 医卫专网 |
| 3 | 安全交换机 | 交换容量≥2.8Tbps；包转发率≥1200Mpps；≥24 个千兆电口，≥4 个万兆 SFP+，≥1 个扩展插槽；双电源；≥2 个万兆多模光模块；≥1 根万兆堆叠线缆；支持静态路由、RIP V1/2、RIPng、OSPF、OSPFv3 等；支持 IPv4/IPv6 双栈 | 台 | 2 | 医卫专网 |

| | | | | | |
|---|---|---|---|---|---|
| | | 协议；支持 Telemetry 技术，支持 SNMP 协议。 | | | |
| 4 | 核心交换机 | 交换容量≥500Tbps；包转发率≥100000Mpps；双主控，双电源，≥48 个万兆光口，≥4 个万兆多模光模块，≥4 个千兆多模光模块；≥2 个交换插槽，≥4 个业务插槽；支持 IPv4/IPv6 双栈协议；支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；支持横向虚拟化功能；支持纵向虚拟化技术，含项目所需线缆等组件。 | 台 | 2 | 互联网 |
| 5 | 业务交换机 | 交换容量≥2.8Tbps，转发性能≥2000Mpps；≥48 个万兆光口，≥2 个 40GE QSFP+口，≥4 个 100GE 光接口；≥40 个万兆多模光模块，≥1 根≥40G 堆叠线缆；≥4 个风扇，冗余电源；支持 IPv4/IPv6 双栈协议;支持集群或堆叠多虚一技术,支持纵向虚拟化技术。 | 台 | 2 | 互联网 |
| 6 | 管理交换机 | 交换容量≥1.30Tbps,转发性能≥550Mpps，千兆电口端口数量≥48 个，万兆 SFP+端口≥6 个；≥4 个 SFP+万兆多模光模块，≥1 根≥万兆堆叠线缆；支持 IPv4/IPv6 双栈协议；支持 RIPv1/RIPv2/RIPng，OSPF v1/v2/v3。 | 台 | 2 | 互联网 |
| **（四）** | **安全系统** | | | | |
| 1 | 防火墙 | 标准机架式，国产芯片，国产处理器，≥10 个千兆电口、≥8 个千兆光插槽,双电源,≥2 个扩展槽位,防火墙吞吐≥1G，并发连接≥100 万。含 IPSEC VPN、SD-WAN、应用识别功能；提供≥3 年入侵攻击特征库、URL 分类过滤库、专业版快速扫描查杀防病毒库、应用识别特征库升级服务许可。 | 台 | 2 | 医卫专网 |
| 2 | 数据库审计 | 标准机架式，国产芯片，国产处理器，配置≥6 个千兆电口，≥4 个千兆光口，≥2 个万兆口,冗余电源,≥2 个扩展槽位,记录事件能力≥5 万条/秒，抓包速率≥5Gbps。含应用识别功能，含≥3 年攻击检测、僵尸主机规则库升级许可，含≥1 个云审计代理/Age | 台 | 1 | 医卫专网 |

| | | | | | |
|---|---|---|---|---|---|
| | | nt 授权，≥5 个数据库审计授权。 | | | |
| 3 | 堡垒机 | 标准机架式，国产芯片，国产处理器，≥1 个 console 口，≥2 个 USB 口，≥1 个 HA 口，≥1 个管理口，≥4 个千兆电口，≥4 个千兆光口，≥2 个万兆光口；冗余电源,≥2 个扩展槽位,≥200 个主机/设备许可。 | 台 | 1 | 医卫专网 |
| 4 | 网闸 | 标准机架式，国产芯片，国产处理器，内外端机各≥16GB 内存，内外端机各≥256GB 固态硬盘,内外分别≥1 个 HA 口、≥1 个管理口、≥8 个千兆电口和≥8 个千兆光口，≥1 个扩展槽位,冗余电源,文件传输速率≥1500Mbps;文件传输延时≤0.5ms；网络层交换速率（2 对千兆口）≥1900Mbps；网络延时≤0.2ms。配置包含安全浏览模块、文件传输模块、邮件访问模块、VOIP 访问模块、数据库访问模块、其他访问模块、文件同步模块、数据库同步模块、防病毒模块、数据中心模块。 | 台 | 2 | 医卫专网与互联网之间 |
| 5 | 防火墙 | 标准机架式，国产芯片，国产处理器，配置≥10 个千兆电口，≥14 个千兆光插槽，≥2 个万兆光插槽,模块化冗余双电源,≥1 个扩展槽位,防火墙吞吐≥8G，并发连接≥320 万。提供 IDP 特征库、WEB 过滤库、专业版快速扫描查杀防病毒库、应用识别特征库≥3 年升级服务许可。 | 台 | 2 | 互联网 |
| 6 | 上网行为管理 | 标准机架式，国产芯片，国产处理器，包括≥1 个串口、≥2 个 USB 接口、≥6 个千兆电口、≥4 个千兆光插槽、≥2 对 bypass 电口、≥3 个可插拔的扩展槽,双电源,网络吞吐量≥10G；授权用户数≥8000 人;包含≥3 年系统版本升级、URL 库及应用特征库升级许可。 | 台 | 1 | 互联网 |
| 7 | 入侵检测 | 标准机架设备，配备≥8 个千兆电口，≥8 个千兆光口，≥2 个万兆光口；SSD 硬盘≥480GB，冗余电源。吞吐量≥3.5Gbps；IDPS 吞吐量≥3G，AV 吞吐量≥1.5G,并发连接数≥120 万；新建连接数≥9 万。 | 台 | 1 | 互联网 |

| | | | | | |
|---|---|---|---|---|---|
| | | 包含≥3 年特征库升级许可。 | | | |
| （五） | **密码系统** | | | | |
| 1 | 国密 VPN 安全网关 | 机架式设备，≥6 个千兆 10/100/1000Base-T 自适应接口，≥4 个 SFP 接口，2 个 SFP+接口，冗余电源；支持国密 SM2/3/4 算法；整机吞吐率≥4Gbps，IPSec 加密速率，64 字节≥250Mbps，1428 字节≥2.5Gbps，IPSec 最大并发隧道数≥5000 条;SSL 最大并发连接数≥30000，SSL 每秒新建连接数≥400，SSL 最大并发用户≥30000，SSL 最大加密吞吐≥300Mbps，实际配置≥200 个 SSL VPN 用户授权；支持 SSL VPN、IPSec VPN 功能；支持 IPsec VPN 隧道自动建立，无需流量触发；可基于每个 SSL VPN 用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控;支持 IPsec VPN 智能选路，根据隧道质量调度流量。 | 台 | 1 | 医卫专网 |
| 2 | 服务器密码机 | 机架式硬件架构，≥4 个以太网千兆电口，≥2 个 10GE 光口，冗余电源；同时符合 GM/T 0030《服务器密码机技术规范》、GM/T 0028《密码模块安全技术要求》等相关技术要求；SM2 密钥产生速率≥4 万对/秒,SM2 签名速率≥4 万次/秒，SM2 验证速率≥3 万次/秒，SM2 加密速率≥2 万次/秒，SM2 解密速率≥4 万次/秒，SM3 计算速率≥1Gbps。整机密钥容量≥5 万；符合商用密码管理和规范要求。 | 台 | 1 | 医卫专网 |
| 3 | 签名验签服务器 | 机架式硬件架构，≥4 个以太网千兆电口，≥1 个接口扩展槽位，冗余电源；同时符合 GM/T 0029《签名验签服务器技术规范》、GM/T 0028《密码模块安全技术要求》等相关技术要求；SM2 签名速率≥40000 次/秒；SM2 验证速率≥10000 次/秒；SM2 制作数字信封≥800 次/秒；SM2 解析数字信封≥1000 次/秒；SM3 杂凑算法≥800Mbps；提供基于 SM2 算法的数字签名和认证功能，可用于证书生成和验证、身份认证等。 | 台 | 1 | 医卫专网 |

| | | | | | |
|---|---|---|---|---|---|
| 4 | 智能密码钥匙 | 具备国密局证书，支持国密 CSP、SKF，支持 SM2\SM4，RSA 1024/2048； 支持标准 CA 功能，配合自建 CA 和运营 CA 进行终端身份认证、私钥存储、应用加解密、电子签章、SSLVPN 登录等。 | 套 | 20 | 医卫专网 |
| **（六）** | **系统软件购置费** | | | | |
| 1 | 个人证书 | 第三方机构（CA）颁发的数字证书,用于证明个人在网络通信中的身份。它使用公钥加密技术来保护通信数据的安全，确保只有授权方才能读取信息，具备 3 年有效期。 | 套 | 20 | 医卫专网 |
| 2 | SSL 证书 | 作为客户端和服务器之间建立一个安全的加密通道,确保数据在传输过程中的安全性和隐私性，具备 3 年有效期。 | 套 | 5 | 医卫专网 |

# 第 3 章 项目组织管理

## 3.1 项目组织管理，实施进度安排

### 3.1.1 项目组织管理

为切实搞好项目建设，建议由郑州市第七人民医院成立项目领导小组，统筹协调本项目建设工作。

项目领导组织结构如下图所示：

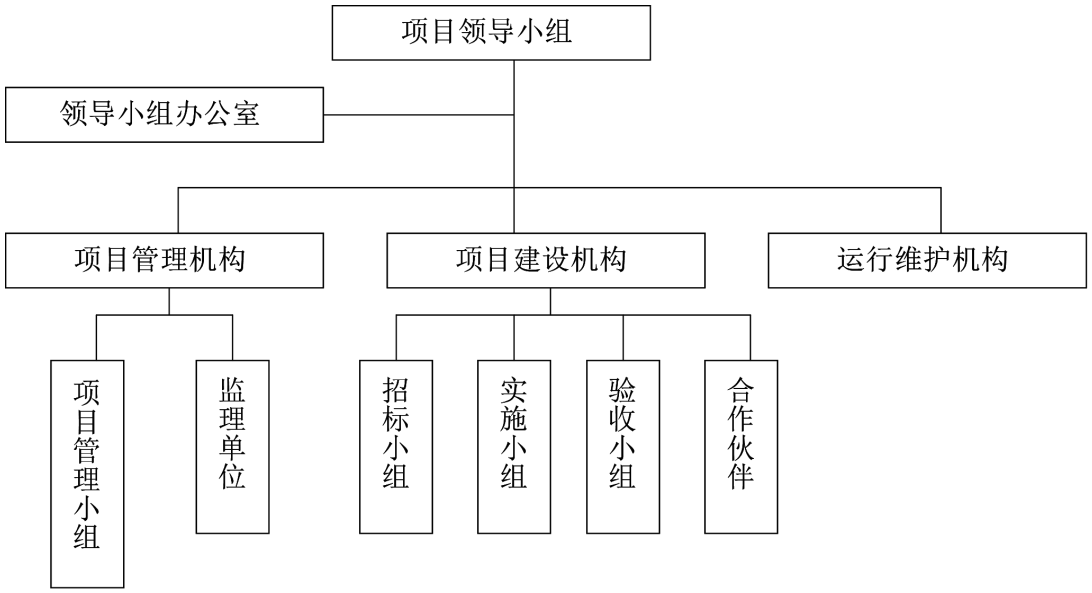


**表 3-1 项目领导组织结构图**

项目领导小组全面负责项目建设和运行的领导、组织工作，对重大的技术、管理、业务规范和部门关系协调等进行决策，确定建设目标，审查建设方案，按照批准的建设方案组织实施。组织编报设计方案，配合有关部门进行论证、评估或审批等项目的前期工作，负责项目经费的申办和计划管理，以及与有关部门进行项目的协调工作。

项目领导小组下设项目领导小组办公室，项目领导小组办公室设在郑州市第七人民医院，项目领导小组办公室具体负责项目建设和运行的领导、组织工作，对重大的技术、管理、业务规范和部门关系协调等进行决策，确定建设目标，审查建设方案，按照批准的建设方案组织实施。组织编报设计方案，配合有关部门进行论证、评估或审批等项目的前期工作，负责项目经费的申办和计划管理，以及与有关部门进行项目的协调工作。

### 3.1.2 实施进度安排

本项目建设周期为 6 个月。

项目进度计划涵盖前期方案编制及批复、项目招投标、项目实施、项目试运行、项目验

收等阶段，具体安排如下：

方案编制及批复：此阶段的核心任务是完成建设方案的编制、送审、专家评审以及项目备案工作，预计耗时约 1 个月。

项目招投标阶段：在该阶段，主要工作是完成项目的招标采购，并顺利签署合同，预计耗时约 2 个月。

项目实施阶段：该阶段需完成现场勘察、方案深化、软硬件设备的采购与部署实施等工作，同时同步开展人员培训。本阶段预计用时约 2 个月。

项目试运行阶段：在此阶段，重点工作是开展项目试运行，针对项目各部分联调以及试运行期间出现的问题进行修正，试运行期为 1 个月。

项目验收阶段：本阶段在试运行期结束后开展，主要进行项目最终验收。按照项目最终验收的相关要求，依次开展项目内部验收、专项验收以及最终验收工作。

为保证计划进度的有效实施，需做好以下几方面：

（1）建设资金及时到位，以满足项目进度要求。

（2）做好软件系统及硬件设备的前期准备工作，包括询价、考察，以及谈判和签订供货合同等。

（3）产品提供商及设备供货商应及时提供设计方案所需的基础资料，并保证这些资料的准确性及完整性。

（4）设备供货及产品提供商必须按时交货并保证产品质量可靠。

**表 3-2 实施进度计划安排表**

| 自然月<br>内容 | | T+1 | T+2 | T+3 | T+4 | T+5 | T+6 |
|---|---|---|---|---|---|---|---|
| 方案编制及批复 | | | | | | | |
| 项目招投标阶段 | | | | | | | |
| 项目实施阶段 | 现场勘察、方案深化 | | | | | | |
| | 设备采购、到货 | | | | | | |
| | 软硬件设施部署实施 | | | | | | |
| | 软硬件联调测试 | | | | | | |
| | 人员培训 | | | | | | |
| | 项目交付 | | | | | | |
| 系统试运行 | | | | | | | |
| 项目验收 | | | | | | | |

备注：以上进度安排只是工程实施的初步规划，具体执行需根据进展情况，进度可能会适当提前或顺延。

## 3.2 人员配置、人员培训需求和运行维护计划

### 3.2.1 人员配置需求

在项目建设过程中，人的因素是最主要的。良好的人员组成，合理的管理，充分调动项目参与人员的工作积极性，是关系到整个项目成败的关键。我们要求项目的实施方采用层次式的人员配置。

1.项目经理

负责项目实施计划的制定，技术人员的安排，总体经费的调配使用，项目的总体进度控制，对外联络等工作。

2.技术主管

负责项目的技术方案评估与确定，项目系统分析与设计，技术工作分工协调，技术文档的审定，总体质量监测。

3.实施主管

负责整个系统实施工作的计划落实、组织和任务分配协调。

4.质管员

负责系统测试和质量检查工作的组织分配协调。

5.项目工程组

由实施公司工程技术人员组成，负责工程项目的工程实施方案制定、技术督导、工程实施和调试工作；用户方系统工程技术人员配合完成。

6.系统技术组

由实施公司的软硬件工程师组成，负责系统的安装和调试工作。

7.测试与质量管理组

负责分系统及全系统的测试工作，以及测试计划与测试报告的编写工作。

8.培训及支援小组

由用户方工程技术人员和部分行政工作人员组成，负责项目前期、中期和后期的人员培训、行政支援工作。

9.后勤组

由用户方部分行政工作人员组成，负责项目过程中行政后勤支援工作。

在上述的人员安排中，可根据具体情况，充分利用人力资源，人员的职责可按实际工作交叉安排或身兼数职。

### 3.2.2 人员培训需求

项目的建设对运行的安全性、稳定性、可靠性要求都很高，为保证系统日常的运行、维护和管理工作，信息化管理人员和运维人员要接受必要的技术基础和业务培训。

## 3.2.2.1 培训对象

为了成功实施并应用本项目，充分发挥优势，将根据不同人员的工作内容和权限，提供不同层次的培训。培训对象主要有以下几类：

建设人员：对项目建设的主要内容、实现的目标和要完成的任务有一个全面地了解。

应用人员（技术人员、系统维护支持人员）：对各系统操作和维护手册，系统的初始化和主要参数的设定方法，系统的体系结构、性能；服务器、存储设备、网络设备、安全设备等软硬件系统的安装、管理、配置；网络安全维护及信息传输等各类信息的集成；应用、数据库、管理服务器系统的维护、更新与扩充的应用；一般性故障进行诊断、定位和排除，系统故障后的恢复方法等方面进行系统培训。

管理人员：通过培训使其了解信息化项目上的相关设备管理功能操作，使其能够熟练使用操作各项管理和业务功能。

通过以上培训，使操作人员能够掌握系统的初始化和主要参数的设定方法；对一般性故障进行诊断、定位和排除；掌握系统故障后的恢复方法；熟练查阅各种系统操作和维护手册。

## 3.2.2.2 培训形式

为了使培训达到最佳效果，将采用多种途径对用户进行培训：

授课：由专业资深的厂家的技术人员，在现场对所有人员进行培训，由课堂讲授和现场操作讲授组成，通常由使用手册或编写培训教材支持，适当的操作为辅助。

现场指导：在项目执行过程中，详细讲解操作步骤，指导技术人员操作，并解答问题；参加原厂商的系统培训，主要包括对硬件设备、软件系统的安装、调试、应用。

## 3.2.2.3 培训内容

根据不同的培训对象，培训内容分为普及性、应用性、专业性三类。设备供应厂商的专业技术人员负责医院信息科技术骨干的培训，信息科其他人员、医院相关科室等相关人员的培训在信息科培训的基础上组织对广大业务人员的培训。

（1）普及性培训内容

本项培训内容针对医院各级领导及相关人员，普及信息系统知识，提高信息素养，为医院信息化打好基础。

（2）专业性培训内容

本项培训内容针对专业技术人员，要求参与培训人员完成培训后能基本承担信息化设施的日常的、基础的运行维护工作，培训具体内容包括网络基础、数据库、虚拟化技术、存储技术、网络信息安全等。

（3）应用性培训内容

本项培训主要针对各应用系统的使用人员中的骨干，要求其在完成培训后能熟练掌握各类应用系统的操作、使用方法，进而在工作过程中对其他相关业务管理人员进行再培训。

### 3.2.3 运行维护计划

本项目建成后，由郑州市第七人民医院信息科负责系统的正常运行和维护。项目招投标过程中，会要求供应商提供人员培训等方式，解决目前运维服务问题，同时郑州市第七人民医院应加强自身技术人才和配套机制建设，保障系统的稳定运行。项目运行维护具体要求如下：

（1）维保服务要求

从最终验收合格之日算起，供应商负责本项目为期 3 年维保年限，3 年维保期内提供系统的全部软硬件的免费维修维护和升级工作，保证整个系统和设备正常稳定运行。

供应商须为本项目开通专门服务热线，在 3 年免费维保期内，对各软硬件系统进行管理维护，故障响应时限须不高于 30 分钟。对于硬件系统故障应在 2 小时内响应，在 4 小时内确定故障原因和解决方案，在 24 小时内排除故障，24 小时内不能修复的，应替换同类型设备，保证系统正常运行。

（2）系统的升级

随着技术的进步，供应商应对系统提供免费的打补丁、升级等维护服务，有效迭代周期不大于 3 个月。