**内江市东兴区人民医院**

**网络安全等级保护安全整改建议报告**

成都卓越华安信息技术服务有限公司

2019年11月

目录

[1. 方案背景 3](#_Toc23966092)

[2. 整改依据 3](#_Toc23966093)

[3. 整改原则 3](#_Toc23966094)

[4. 防护能力 4](#_Toc23966095)

[5. 安全现状 4](#_Toc23966096)

[6. 整改建议 5](#_Toc23966097)

[6.1 整改方式 5](#_Toc23966098)

[6.2 产品整改 6](#_Toc23966099)

# 方案背景

本整改方案是通过分析内江市东兴区人民医院（以下简称“医院”）提供的网络拓扑图，并根据其与等级保护第三级要求之间的差距，提出合理的整改建议，巩固医院信息系统的安全性。为满足医院的信息系统符合国家网络安全等级保护三级要求的需求，我们依据国标等级保护三级安全防护要求对医院的信息系统现状进行分析，并给出相应的安全整改建议，供医院在安全建设过程中参考。

# 整改依据

* 《中华人民共和国网络安全法》
* 《计算机信息系统安全保护等级划分准则》（GB/T 17859-1999）
* 《网络基础安全技术要求》（GB/T 20270-2006）
* 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）
* 《信息安全技术 信息系统等级保护安全设计技术要求》（GB/T 24856-2009）
* 《信息安全技术 信息系统安全等级保护实施指南》（GB/T 25058-2010）
* 《信息系统安全等级保护体系框架》（GA/T 708-2007）
* 《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429号）

# 整改原则

确定安全技术策略，设计总体技术方案。

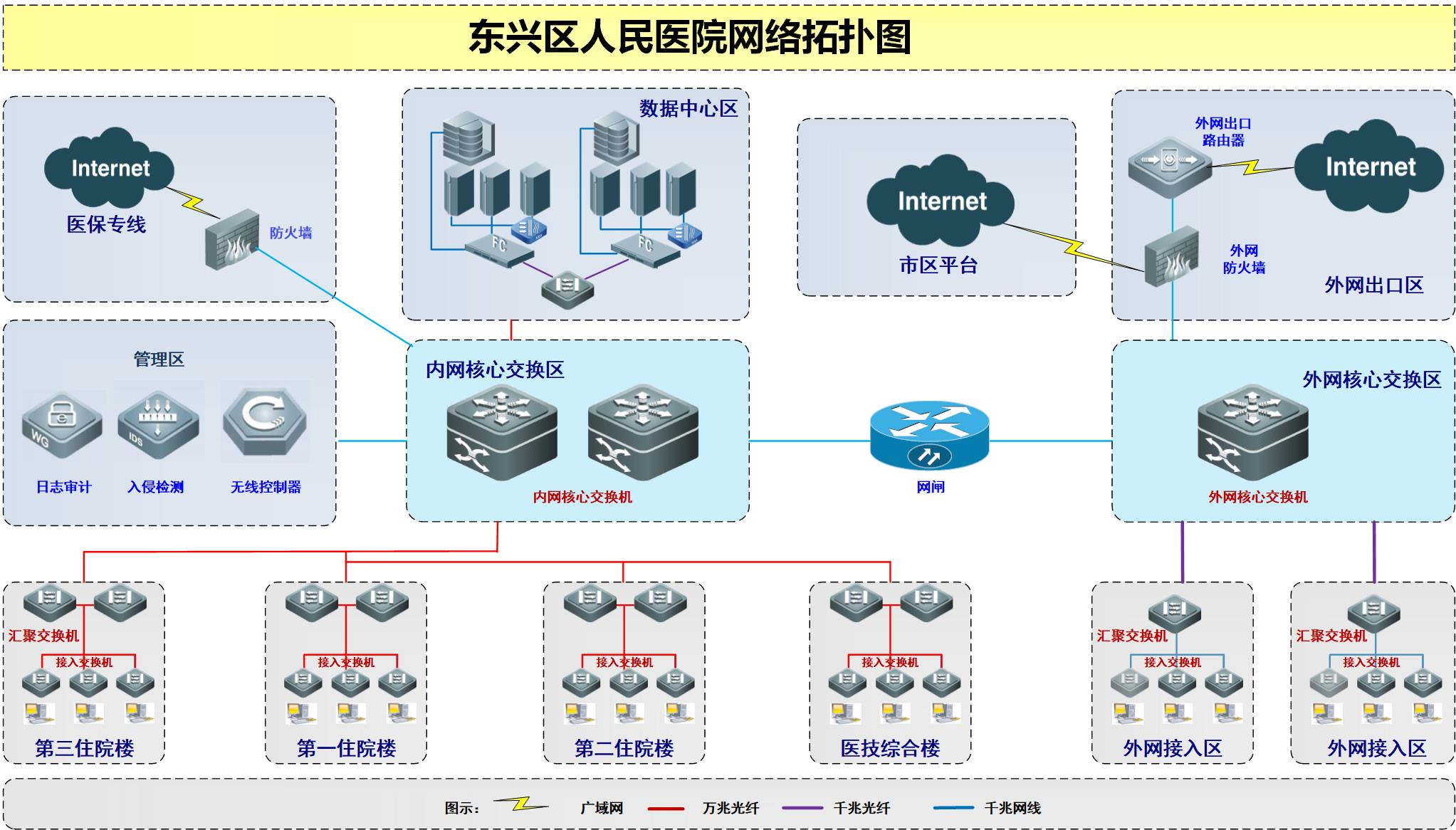
首先，根据安全需求分析，确定安全技术策略，包括业务系统分级策略、数据信息分级策略、区域互连策略和信息流控制策略等，用以指导系统安全技术体系结构设计。

其次，以《GB/T 22239-2019网络安全等级保护基本要求》为基本目标，可针对等保现场测评发现的问题进行加固改造。也可以进行信息系统的总体安全技术设计，将不同区域、不同层面的安全保护措施形成有机的安全保护体系，进一步落实网络安全等方面基本要求，最大程度发挥安全措施的保护能力。在进行安全技术设计时，可参考《信息系统等级保护安全设计技术要求》，从安全计算环境、安全区域边界、安全通信网络和安全管理中心等方面进一步落实安全保护技术要求。

# 防护能力

医院信息系统将按照第三级基本要求进行安全防护，三级系统需要达到以下安全保护能力目标：应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。

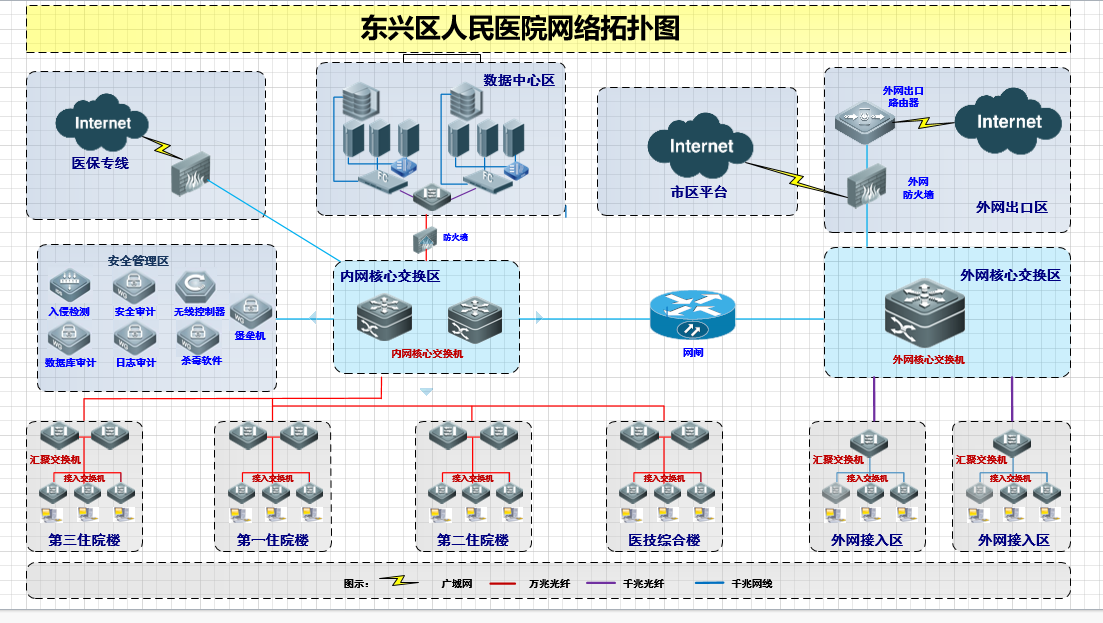
# 安全现状



但作为信息系统整体安全防护还存在一定的不足，主要风险点包括网络安全和主机安全两方面：

1. 网络共有3个出口，其中互联网和内网之间部署了网闸、医保出口部署了1台防火墙、市区平台部署了1台防火墙；
2. 未部署日志审计设备。网络设备与操作系统日志均保存在本地，无法达到等保要求日志保存时间6个月以上，若出现异常访问无法及时溯源。建议部署日志审计系统或专门的日志服务器，具备分析、查询、统计并生成报表等功能，能快速协助运维人员查询日志，溯源操作；
3. 未部署数据库审计设备。由于医院数据非常重要，所以建议部署数据库审计实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断；
4. 未部署安全审计。不能对对内部人员上网行为进行约束与审计；
5. 主机层面未安装防病毒软件。

# 整改建议



## 6.1 整改方式

1. 在网络边界处（互联网、医保）、内部核心交换机与数据中心区之间部署防火墙（集成入侵检测，防病毒模块，并启用其功能），配置访问控制、入侵检测与防病毒策略，保证网络边界处对流量的识别，监控与过滤；
2. 在安全管理区部署日志审计、数据库审计、安全审计，对主机和网络设备日志进行采集保存，提供统计、分析、查询并生成报表功能。实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断。对内部人员上网行为的约束与审计；
3. 在安全管理区防病毒服务器，防病毒服务器上部署防病毒软件的服务端，各业务服务器上部署防病毒软件的客户端，实现主机层面防病毒的统一管理；
4. 在安全管理区部署堡垒机，根据管理职责分配管理资源，对所有主机的访问、修改等进行记录，提高安全管理，避免安全事故责任。

## 6.2 产品整改

| **部署产品** | **数量** | **部署位置** | **部署作用** |
| --- | --- | --- | --- |
| **防火墙（带入侵防御、防病模块）** | 3 | 网络边界处（互联网、医保）、内部核心交换机与数据中心区之间 | 所有数据流量，阻止各类非法应用，执行既定安全策略。 |
| **漏洞扫描** | 1 | 安全管理区 | 扫描漏洞，发现漏洞。 |
| **安全审计** | 1 | 安全管理区 | 对内部人员上网行为的约束与审计。 |
| **数据库审计** | 1 | 安全管理区 | 对数据库操作进行记录、审计、授权、命令回放等。数据库审计起到关键作用。 |
| **日志审计** | 1 | 安全管理区 | 对服务器、网络设备、安全设备进行系统日志管理。 |
| **杀毒软件** | 1 | 安全管理区 | 实现业务服务器和主机终端病毒、木马查杀。 |
| **堡垒机** | 1 | 安全管理区 | 根据管理职责分配管理资源，对所有主机的访问、修改等进行记录，提高安全管理，避免安全事故责任。 |

——报告完结 以下空白——