三级甲等医院信息系统等级保护安全设计

梁昂昂[①]　文黎明[①]　张浩[①]

①方正国际（北京）软件有限公司，100080，北京市海淀区北四环西路52号方正国际大厦5层

摘　要 以国内某三甲医院信息安全现状为切入点，结合国内严峻的信息安全局势，全面分析该医院在主机、网络、应用、数据完整性和保密性方面存在的信息安全隐患，并针对上述问题建立安全体系。方法：以构建“一个中心下的三重防护体系”在技术层面建立信息系统的信息安全架构。结果：依照该架构建立的安全体系确保了医院信息系统中重要信息的安全性。结论：从而按照卫生部所要求三级甲等医院的核心业务信息系统安全等级不低于三级的要求，符合《信息系统安全等级保护基本要求》中三级在主机、网络、应用、数据完整性和保密性方面的要求。

关键词 医院信息系统 信息安全 等级保护

医院信息化建设的程度已经成为现代化医院的重要标志之一，随着信息化进程的不断深入，医院部分工作已经摆脱了原来的手工模式正在逐步向网络化、自动化、数字化时代迈进，因此，医院信息系统的安全性将直接影响到医院的医疗活动能否正常运作。基于以上问题，为贯彻落实国家信息安全等级保护制度，规范和指导全国卫生行业信息安全等级保护工作，卫生部于2011年下发了 《关于全面开展卫生行业信息安全等级保护工作的指导意见》 的通知 （卫办综函【2011】1126号文），通知明确指出，我国要求三级甲等医院的核心业务信息系统信息安全保护等级不低于第三级。

基于以上原因，需要在三级甲等医院的核心业务信息系统中建立信息安全保护等级三级的安全体系。跟据《信息系统安全等级保护基本要求（GB/T 22239-2008）》（以下简称基本要求），需要在管理和技术两个层面上开展信息安全保护工作。技术层面又分为物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复5个方面，本文重点重点对网络安全、主机安全、应用安全、数据安全的安全体系结构进行设计。

1　该三甲医院信息系统现状分析

1.1 信息系统分析

1.1.1 外网应用类现状描述 目前，该医院门户类应用是该院的门户网站，主要业务为医院信息展现、院内办公OA应用、预约网上挂号服务。网站面向互联网用户开放，为不同的业务用户提供差异性服务。其中，院外用户可进行预约网上挂号服务和查看所展现的医院信息；院内人员通过VPN拨入后输入个人ID密码可进入办公OA应用。

1.1.2 内网应用类现状描述 内网承载着院内系统的核心应用，包含HIS、PACS、EMR等多个大型应用系统，系统面向院内职工开放，为院内不同岗位的用户提供差异性服务。

1.2 系统安全现状分析 经过长时间的建设与积累，该院已经建立起了一套安全防护体系，包含如下：院内安装了防病毒服务器，每个终端均安装防病毒客户端。院内网络与外网利用网闸物理分开，内网采用域管理模式，进入域的终端接受域控制器的管理，域控制器建立了一套安全策略，使终端C盘内容在安全策略内活动，普通用户无法对C盘内容更改。由于该院有分院和社区，不同位置的办公区域利用专线连接。医保服务器与医保中心通过路由器利用专线进行连接。门户网站与外网之间安装了防火墙和VPN设备。

2　该三甲医院信息系统与《基本要求》差异

由于三级信息系统安全防护能力完全覆盖二级系统的所有功能，因此，将以《基本要求》中的三级安全标准对该院信息系统目前可能存在的安全问题进行分析。

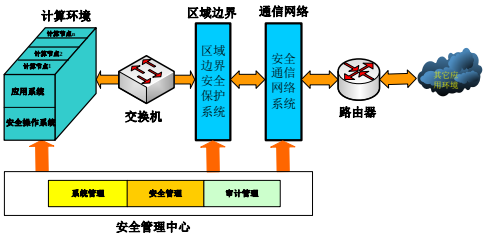
《基本要求》从技术和管理两个角度，对等保系统的建设、运营、维护等过程提出了很多很具体的指导和要求。下面，将主要针对基本技术要求中的“网络安全”、“主机安全”、“应用安全”、“数据安全”四部分分析该院目前信息系统中存在的不足和隐患。

具有以下差异：信息系统仅仅通过用户 ID、口令的方式进行身份识别，鉴别强度不够。并未建立系统管理、安全管理、审计管理三权分立的管理模式，导致某些角色拥有过大的操作权限。服务器、终端的操作系统和业务应用系统都没有基于标记的强制访问控制功能。服务器、终端的操作系统均不支持客体的安全重用，用户鉴别信息、文件资源等在使用后无法实现剩余信息的完全清除，攻击者通过使用相应工具有可能恢复这些信息并进行窃取。不支持对程序完整性的校验；对于已经被种植隐性病毒的应用程序没有足够的检测手段。应用系统缺少软件容错、抗抵赖等功能。缺少对数据完整性、保密性进行防护的功能。

3　安全体系设计

3.1 总体框架架构 按照信息系统业务处理过程将系统划分成计算环境、区域边界和通信网络三部分：计算环境：计算环境由定级系统中完成信息存储与处理的计算机系统硬件和系统软件以及外部设备及其联接部件组成，也可以是单一的计算机系统。区域边界：计算环境的边界，以及计算环境与通信网络之间实现连接功能的部件。通信网络：计算环境之间进行信息传输的部件。

依据《信息系统等级保护安全设计技术要求》（报批稿）（以下简称《设计技术要求》），三级系统的安全建设要在安全管理中心支撑下，按照计算环境安全、区域边界安全、通信网络安全构筑三重防护体系。信息系统等级保护安全建设的体系结构和逻辑组成如下图所示。



等级保护系统安全建设体系结构

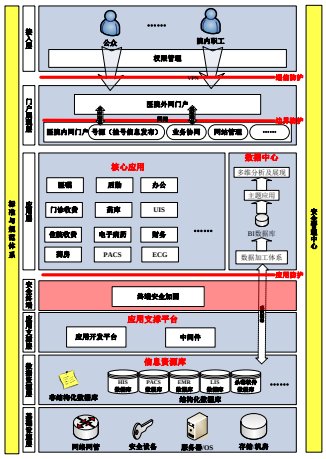
3.2 设计 三级甲等医院信息系统等级保护安全设计如下图所示。按照信息系统总体框架建立以安全管理中心支持下的计算环境安全、区域边界安全、通信网络安全所组成的三重防护体系结构。

3.2.1 安全管理中心设计 对计算环境、区域边界和通信网络进行统一的安全策略管理，确保系统配置完整可信，确定用户操作权限，实施全程审计追踪。从系统管理、安全管理、审计管理三个方面进行配置和建设，建成后将作用于计算环境、区域边界、通信网络等环节的安全保护措施，进行统一的协调和调度，从而实现了集中身份管理、集中认证授权、集中操作审计、主客体标记、访问控制等全过程的安全管理措施，并实现集中事件和风险管理，发挥出整体安全防护系统的作用，有效保信息系统的安全性。

3.2.2 计算环境安全设计 通过对终端进行安全加固，保障应用业务处理全过程的安全。系统终端和服务器通过在操作系统核心层和系统层设置以强制访问控制为主体的系统安全机制，形成严密的安全保护环境。通过对用户行为的控制，可以有效防止非授权用户访问和授权用户越权访问，确保信息和信息系统的保密性和完整性，从而为业务应用系统的正常运行和免遭恶意破坏提供支撑和保障，从而形成安全计算环境。

3.2.3 区域边界安全设计 通过在内外网交互处安装防火墙、网闸等设备，建立相应的访问控制策略，并对数据包进行过滤后在内网服务器和外网门户之间进行摆渡，使内外网之间实现真正意义上的物理隔离，从而防止非法入侵并保障了日常应用，形成安全区域边界。

3.2.4 通信网络安全设计 通过加装 VPN 设备，对通信数据包的保密性和完整性的保护，确保其在传输过程中不会被非授权窃听和篡改，保障了院内用户通过门户网站进行办公时所交互信息的完整性、保密性和安全性，同时也保证了系统自身的安全性从而形成安全通信网络



信息系统安全建设

4 设计效果分析

通过对终端安全进行加固，使其在原有基础上建立了两种组合机制对用户身份进行鉴别、数据保密性完整性校验、客体安全重用、程序可信执行保护，解决了本文“2 该三甲医院信息系统与《基本要求》差异”中“1、4、5、6、7”的问题。

通过建立安全管理中心，对信息系统的所有资源进行主客体标记、从而实现了真正意义上的强制访问控制；并建立系统管理、安全管理、审计管理三权分立的管理模式，解决了文本“2 该三甲医院信息系统与《基本要求》差异”中“2、3”的问题，实现了认证、控制、审计的全闭环控制。

原有的网闸和 VPN 在安全管理中心统一管理策略下运行，增强了信息系统区域边界、通信网络边界的安全。

5 总结

信息安全没有绝对性，从技术复杂度来说，单一防护模式很容易被突破，只有实施多层防护，才能消除单点隐患。通过建立“一个中心下的三重防护体系”才能增加突破难度，降低安全风险；做到全可达、全可控、全可查。层层防护旨在实现非法破坏“进不来”，即使进来也“拿不走”，即使拿走也“读不懂”，即使有恶意行为也“跑不了”。

信息系统的安全管理是一个动态的管理过程，随着观念、技术、信息化程度的发展，安全管理的指导思想也应该要与时俱进的动态前进，要根据阶段性的信息安全目标不断的对安全管理体系加以校验和调整，保证管理体系始终适应和满足实际情况的需求，只要做到这样，才能够建设健康的、合理的、有效的医院信息安全管理体系。

参考文献

[1] 《关于全面开展卫生行业信息安全等级保护工作的指导意见》 的通知 （卫办综函【2011】1126 号文）
[2]《信息系统等级保护安全设计技术要求》报批稿
[3]《信息系统安全等级保护基本要求》（GBT22239-2008）
[4]《计算机信息系统安全保护等级划分准则》（GB 17859-1999）
[5]《ISO17799》