

喀什市人民医院防统方软件参数

填报科室：（喀什市人民医院信息科）

序号	项目名称	内容	备注
1	系统基本要求	管理、审计用户权限分开，相应权限的用户只能查看、管理相应的系统功能，责任明确。	
		★产品为专业防统方系统，提供“防统方系统”的《软件著作权登记证书》，提供加盖公章的证书复印件。	
		系统应具备对应用程序、数据库访问者、访问者IP地址等的统计功能。并能提供按月统计每天的数据接口流量，统计出每月最大流量和最小流量的日期、终端、应用程序等，且形成趋势图。	
		支持多种部署方式（串接/并接）都能够阻止客户端进行疑似的统方行为。	
		系统支持采用旁路部署方式，不需要更改现有网络结构、服务器相关配置，系统运行不得影响现有网络和业务的正常运行。系统应能独立完成审计数据采集，不依赖于数据库自身审计日志系统，不得在现有服务器上安装可能带来风险的程序。	
		系统确保最小报警监控时间间隔为5秒，保证统方事件的及时告警。	
		系统的时间可以和关键服务器中的数据库的时间进行同步，确保记录时间的一致性。	
		支持加密方式的数据库连接信息分析。	
		支持对Oracle、MS-SQL、DB2、MYSQL、CACHE DB、POSTGRESQL和Sybase 等数据库提供自动化评估、审计和保护功能,可审计的数据库或集群数量不少于6个，并且支持单家医疗机构多种类型数据库并存的信息系统。	
		具备用户行为记录功能，记录用户所有的操作（业务访问、系统维护、策略配置等）。	
		系统从业务流程角度入手，结合核心数据特征，形成高度集成的“事前+事中+事后”数据防护手段。	
		系统配置文件支持导入、导出。系统支持在线升级功能，通过厂家发布的升级包可在线对系统进行软件升级和规则库升级。	
		系统为软硬一体机，支持千兆以上网络环境及大概至少500个客户端同时并发的监控，应达到每秒50000个以上的事务处理能力。	
		采用B/S架构（兼容不同种类浏览器），提供中文WEB管理界面以便于管理。并应可以根据不同的安全级别采用不同的实时告警响应方式，包括记录、消息、鸣音、邮件等，并能支持短信平台。	
		审计数据能永久保存，并支持外接存储设备进行备份。数据进行加密保管，只能通过专门工具进行恢复和查询浏览。支持数据自动备份、手动备份且可修改备份策略。	



2	防统方模块	▲能够出具针对纪委、监察、行风监督处相关人员使用的防统方审计报告（支持每天或多天生生成统方审计报告，报告需简单明了，且具有主动将所有的计算机语言翻译成通俗易懂的自然语言的系统机制，支持将整条SQL语句翻译成中文，帮助医院建立基于内部网络的党风廉政、廉洁警示、院内敏感职权使用的防控专网，助力清廉医院建设，具有清廉医院系统的《软件著作权登记证书》，提供盖章的产品截图及证书复印件。	
		系统内置防统方知识库，具有自我学习功能。	
		★支持医院各生产系统中财务数据、病人资料、药品信息、医院资产等核心数据的审计监控。该模块具有内部审计管理模块《软件著作权登记证书》，提供加盖公章的证书复印件。	
		系统支持虚拟化、虚拟云等网络环境的数据审计功能，准确定位统方行为，具有该功能的虚拟化防统方系统的《软件著作权登记证书》，提供加盖公章的证书复印件。	
		★系统可针对耗材、高值耗材、SPD、检验试剂、合理用药、互联网医院等医院新的信息化系统进行审计,提供"防统方系统"的《中国国家信息安全产品认证证书》。提供加盖公章的证书复印件。	
		能够获取客户端访问数据库的应用程序。根据客户端应用程序名单，实时阻止非法客户端程序或伪装正常客户端程序对关键服务器的访问。	
		可疑对象定位功能，可以精确定位可疑对象的物理位置（记录操作人员工号、操作类型、IP地址、客户端工具以及存放路径、操作系统用户名、主机名、MAC地址、SQL语句和操作的时间等关键信息）。	
		可以对某统方行为的所有操作以及操作结果关联起来，以报表的形式呈现给使用部门，便于使用部门分析和追溯统方事件。	
		支持对接医德医风系统，具有医德医风系统的《软件著作权登记证书》，提供加盖公章的证书复印件。	
		★发现统方操作后，支持统方风险管控，某企业药品或耗材涉及非法统计后，系统可关联医药代表相关信息，系统自动将该企业加入管控黑名单，对该厂商、药代表进行重点监控，并实时提醒监管人员，具有医药代表管理系统的《软件著作权登记证书》，提供加盖公章的证书复印件。	
		阻止可疑会话功能，甄别数据访问，阻止非正常数据会话。能根据预定规则阻止SQL语句的"数据库墙"功能，如根据系统设置的客户端IP/MAC黑名单，以及数据内容中的敏感信息，实时阻止黑名单中的客户端对关键服务器的访问。	
		▲用户可以根据需要自定义规则，并能根据设定的条件产生审计报告。能对审计结果进行多条件组合查询，比如按下列条件查询：IP地址、MAC地址、表名、字段名、操作方式（可单独或者多选某种数据库操作）、计算机名、数据库名、程序名（可单独或者多选某个应用程序）等。并就能支持按关键词进行模糊查询。查询结果应支持多种格式(excel、pdf、txt等)导出。具有大数据检索系统的《软件著作权登记证书》，提供加盖公章的证书复印件。	
		统方白名单权限的设置，可对授权统方行为的操作人员工号、操作类型、IP地址、客户端工具、操作系统用户名、主机名、MAC地址、SQL语句和操作的时间范围等条件进行设置，只有通过了授权和验证才可以获得统方权限。	



3	抗菌药物试剂及耗材分析模块	▲支持对指定时间内全院抗菌药物、试剂及耗材的品种、剂型、规格、使用量、使用金额，使用量和使用金额分别排名前N位的品种进行分析，自动生成报表），具有抗菌药物管理系统的《软件著作权登记证书》，提供产品截图及证书复印件。	
		支持针对医院使用的抗菌药物、试剂和耗材进行全方位跟踪，提供条件筛选模糊查询和精确查询，系统能实时对抗菌药物、试剂和耗材的统计进行告警。	
4	扫描数据库	对于医院不断新增业务系统，防统方系统提供自主扫描业务系统数据库，在组网环境中扫描数据库，从而判断业务系统是否被防统方系统全面监控。	
5	精准筛查	对于医院不断新增业务系统，防统方系统提供自主扫描业务系统数据库，在组网环境中扫描数据库，从而判断业务系统是否被防统方系统全面监控。	
6	线上报备	对于正常合法统方行为，可以在现有防统方系统中做正常统方申请报备处理，在系统呈现统方报表时，给出此操作已完成相应报备手续，属于正常统方范畴，需提供截图证明。	
7	移动端展示	▲可以通过移动端收发报警并展示（非短信模式），报表查询，设备状态查看，可以在移动端上进行报备审批等。具有防统方系统移动端管理的《软件著作权登记证书》，提供加盖公章的证书复印件。	
8	告警模块	可根据用户自定义规则实时发出手机短信通知和邮件提醒等多种方式的告警信息，并支持配备相应的告警信息发送设备。	
9	服务支持	▲提供1年7×24小时对系统的维护服务。需提供厂家授权证明文件。	
科委会签字：  			

