• 医学信息技术 •

区域医疗信息共享平台的数据审计研究*

赖 炜 辛小霞 吴汝明 郭清顺

（中山大学网络与信息技术中心 广州 510080）

〔摘要〕 数据审计作为信息系统审计的重要组成部分，对信息系统的安全与稳定具有十分重要的意义。研究区域医疗信息共享平台数据库审计机制，结合应用系统需求，比较各种数据库安全审计方案，探讨基于数据库的区域医疗信息共享平台安全审计方案。

〔关键词〕 区域医疗信息共享平台；数据审计；数据库；系统安全

Research on Data Audit of Regional Medical Care Information Sharing Platform *LAI Wei, XIN Xiao – xia, WU Ru – ming, GUO Qing – shun, Network and Information Technology Center, Sun Yat – sen University, Guangzhou 510080, China*

〔**Abstract**〕 Data audit is one of the most important parts in information system audit, it has important significance to maintain the security and stability of information system. The paper firstly studies the database audit mechanism of regional medical care information sharing platform, combined with application system requirements, through comparing different database safety audit plans, discusses safety audit plan for regional medical care information sharing platform based on databases.

〔**Keywords**〕 Regional medical care information sharing platform; Data audit; Database; System security

1 引言

区域医疗信息共享平台通过整合区域医疗资源，建立居民健康档案，从而全面跟踪居民健康状况。整个系统通过计算机技术、现代通信技术等高科技手段为市民一生的健康提供追踪管理，及时准确地为每一个市民服务。而随着区域医疗信息化应用的日益普及和深入，针对操作系统、应用系统和网络连接等安全性问题，一般采用防火墙、入侵检测、内网监控、防病毒等权限控制和安全审计措施，作为信息系统核心的数据库的访问监测和安全审计亦同等重要[1]。

信息系统审计（Information System Audit，ISA）是指根据公认的标准和指导规范，对信息系统及其业务应用的效能、效率、安全性进行监测、评估和控制的过程，以确保预定的业务目标得以实现[2]。具体而言，信息系统审计就是以企业或政府等组织的信息系统为审计对象，通过现代的审计理论和 IT 管理理论，从信息资产的安全性、数据的完整性以及系统的可靠性、有效性和效率性等方面出发，对信息系统从开发、运行到维护的整个生命周期过程进行全面审查与评价，以确定其是否能够有效可靠地达到组织的战略目标，并为改善和健全组织对信息系统的控制提出建议的过程。区域医疗信息共享

〔修回日期〕 2010 – 10 – 15

〔作者简介〕 赖炜，硕士，工程师，发表论文 15 篇。

〔基金项目〕 广州市医药卫生科技项目（项目编号：2006 – YB – 042）。

平台数据库存储着患者的疾病诊断、治疗方案、检查检验结果、处方等敏感信息，这些信息的非法访问和修改将会造成重大的医疗纠纷及经济损失。作为安全事件追踪分析和责任追究的数据库安全审计的运用是必要的，通过对数据库操作的痕迹进行详细记录和审计，使数据的所有者对数据库的访问有据可查，及时掌握数据库的使用情况，并针对安全隐患进行调整和优化[3]。

2 区域医疗信息共享平台数据库审计方案

2.1 概述

数据库安全审计系统主要用于监视并记录对数据库服务器的各类操作行为，通过对网络数据的分析，实时地、智能地解析对数据库服务器的各种操作，并记入审计数据库中以便日后进行查询、分析、过滤，实现对目标数据库系统的用户操作的监控和审计[4]。可以监控和审计用户对数据库中的数据库表、视图、序列、包、存储过程、函数、库、索引、同义词、快照、触发器等的创建、修改和删除等，分析的内容可以精确到 SQL 操作语句一级[5]。还可以根据设置的规则，智能地判断出违规操作数据库的行为，并对违规行为进行记录、报警。

由于数据库安全审计系统是以网络旁路的方式工作于数据库主机所在的网络，因此它不需改变数据库系统任何设置而对数据库的操作实现跟踪记录、定位，实现数据库的在线监控。是在不影响数据库系统自身性能的前提下，实现的数据库在线监控和保护，可及时发现网络上针对数据库的违规操作行为并进行记录、报警和实时阻断，有效地弥补现有应用业务系统在数据库安全使用上的不足，为数据库系统的安全运行提供有力保障。

2.2 利用各类数据库审计功能的方案

各类数据库系统提供对数据库操作的权限、对象、语句、网络进行监视和审计功能[6]。审计内容包括登录时间、终端标识号、SQL 语句的使用等。Oracle 针对 select、insert、update、delete 语句的细粒度审计（FGA），当满足设置检查条件时，可以把细粒度对指定时间段的操作、表中某列的数值进行审计。Oracle 能够对数据库里发生的一切进行审计。审计的结果可以记录到操作系统中，也可以保存到 SYS. AUD $ 表中。利用审计信息，可以审查可疑的数据库活动，发现非法操作。Oracle 中值得审计的操作行为主要有 3 大类[7]：登录尝试、对象存取以及数据库动作。在默认设置中，Oracle 审计功能激活后，记录成功和不成功的所有命令，但实际应用常常不需要对两种行为都进行跟踪。

2.3 对数据库日志文件审计的方案

数据库系统的每个操作首先记录在日志文件中，记录数据库更改的时间、类型、SCN 号和用户信息等。通过分析各个时间段的日志文件内容，可以查看数据库的各种操作信息。日志中记录的信息还包括数据库的更改历史、更改类型（insert、update、delete、ddl 等）、更改对应的 SCN 号、以及执行这些操作的用户信息等，LogMiner 在分析日志时，将重构等价的 SQL 语句和 UNDO 语句[8]。使用日志文件格式化工具对数据库的 DML 和 DDL 操作信息进行审计，但不能对 select 操作审计[4]，缺少实时获得异常审计数据的功能。

2.4 基于触发器的方案

数据库都会为 logoff，logon，shut - down，servererror 等事件提供触发器，此类事件的发生会触发一条或一系列 SQL 语句[9]。使用数据库触发器可以完成的功能包括：允许或限制对表的修改；自动生成派生列；强制数据一致性；提供审计和日志记录；防止无效的事务处理；启用复杂的业务逻辑。通过 SQL 语句把审计需要的帐户信息、操作时间、操作语句、新旧值等审计信息存入特定数据表，审计系统根据需要设计程序对该数据表进行分析和审计。基于触发器的数据库安全审计，需要消耗数据库服务器的系统资源，且不能对 select 操作进行审计。

2.5 基于网络端口镜像监听的方案

基于网络端口镜像的数据库安全审计分为数据

采集、数据解析、数据分析 3 部分。数据采集引擎通过网络端口镜像的方式接入核心交换机，设置端口镜像模式监视进出网络的所有数据包，供安装了监控软件的管理服务器抓取数据[10]。医疗平台出于信息安全、保护机密的考虑，需要网络中有一个端口能提供这种实时监控功能。在企业中用端口镜像功能，可以对平台内部的网络数据进行监控管理，系统出现故障时，可以做到故障定位。一般通过配置交换设备端口镜像，并在监控机安装网络行为管理软件就可以实现对整个网络的监控。

在网络端口镜像监听模式下采集引擎能够监听到与数据库进行通讯的所有操作，并根据数据库操作协议进行还原和整理，发送到数据解析系统。数据解析系统根据数据解析和事件关联规则，对采集的数据库操作记录进行关联解析，将结果发送给数据分析系统。数据分析系统根据数据库审计要求对需要监控的内容设置审计规则，当接收到的解析结果符合管理员设置的审计规则时，数据分析将实时报警。基于网络端口镜像监听的数据库安全审计方法存在两个缺陷：当数据采集机器故障或网络断开时，就无法采集审计记录；另外，如果对数据库进行的操作是在数据库服务器上执行，其操作指令不经过网路传输，采集设备无法获取审计信息。

3 区域医疗信息共享平台的审计研究

3.1 审计过程

区域医疗信息数据在各医院端 HIS、LIS、PACS 等服务器中，经过医院端前置服务器对数据进行处理后，定时传送到区域临床药学服务数据中心服务器（存储阵列）中，数据中心应用服务器在收到数据的同时在数据库中建立对应医疗数据的索引，在索引服务器中建立病人服务的索引。医院客户端查询本院数据时，在通过院内用户认证后，默认查询本院服务器，直接以 On - demand 方式取回。医院客户端查询非本院数据时，先通过区域医疗服务数据中心用户认证服务器认证后，索引服务器配合数据库服务器将检索到的信息反馈回医院客户端，医院客户端发送调阅请求后，系统通过自动路由功能查询数据中心端应用服务器，并以 Web 浏览或 Viewer 浏览的方式取回。

3.2 用户划分及用户应用

3.2.1 *用户分类及管理机制* 二级用户分类：由用户的不同性质分为管理员和用户两大类，并根据应用需求进一步细分为多类用户。分级管理机制：构建分级管理的树型用户管理关系，减少集中式管理中管理员的工作负担，并与实际业务结合，实现责任制的管理机制。

3.2.2 *用户对信息的私有性* 患者电子健康档案的私有性：患者的健康档案仅授权患者本人及当前主治医生，在进行隐私处理后可向科研和教学人员进行授权访问。医院管理信息的私有性：各医院只能查看自有医院的管理信息，以及医疗信息共享平台处理后生成的公开信息。

3.2.3 *用户在应用中的约束性* 电子健康档案应用约束：如会诊中各医生对患者电子健康档案访问的时间性约束、科教人员对患者电子健康档案访问的颗粒度约束等。应用约束规则制定和管理：平台系统中的各类应用中，针对不同用户类型制定相应的约束规则，并配合专员落实，由平台管理员等进行约束规则的管理及优化。

3.2.4 *用户在平台中的可维护性* 用户行为审计：用户在平台系统中的关键行为/操作将被作为历史记录进行存档，以作为信息处理的凭证。用户信息管理：用户信息，尤其是患者有关信息的变更，需要引入人工审核，同时，每次变更均保存完整的患者个人信息，作为历史记录存档。

3.3 监测分析

3.3.1 *概述* 根据医疗行业及其应用系统的特点，以操作行为的正常规律和规则为依据，对相关计算机系统进行的操作行为产生的动态或静态痕迹进行监测分析，发现和防范内部人员借助信息技术实施的违规和犯罪。对信息系统运行有影响的各种角色的行为过程进行实时监测，及时发现异常和可疑事件，避免内部人员的威胁而发生严重的后果。

3.3.2 *对操作权限误用的行为监控* 区域医疗信

息共享平台的安全审计对几种操作权限误用的行为进行监控：医院工作站在班外时间段对数据库的操作和访问；应用模块在非法工作站上发生了相关操作引发的数据库访问；出现非业务系统的仿冒应用程序对业务数据库进行访问；数据库管理人员在业务窗口进行远程数据库访问等。

3.3.3 *数据存储管理* 数据库存储过程调用没有具体的 SQL 语句在网络上传输，审计系统难以根据 SQL 语句的特征进行监控，监控手段主要是设置白名单，对名单设置审计规则。在业务系统约定以外的存储过程调用、合法存储过程调用时出现参数异常或者非法机器调用等行为进行监控。

3.3.4 *数据库操作记录的重现* 区域医疗信息共享平台的安全审计重点监控医生工作站、医院前置机等异常情况，根据审计系统中的记录重现错误发生过程与场景，跟踪分析异常和事故原因。

3.3.5 *数据库高安全级别操作的审计* 对数据库的删除表、无条件批量删除或直接在数据库上修改数据等高危数据库操作行为进行审计。

3.3.6 *数据库高安全级别数据表的操作监控* 对数据库中高安全级别数据表中的患者姓名、电话、余额等操作；财务信息数据中的科目余额等操作；药品使用情况等敏感数据的操作进行监控。

3.3.7 *对数据库进行应用层监控* 根据业务需求进行重复预约挂号登记表、转诊转检记录、医疗咨询申请等应用系统频繁执行但缺乏有效监控的异常操作进行应用层监控。

4 结语

区域医疗信息共享平台的安全审计系统可通过数据库系统安全审计、网络端口镜像数据审计等方法实现。数据库系统安全审计对数据库存取时间以及应用系统的效率都会产生一定影响，随着工作量的增加，这种影响会更加明显。基于网络端口镜像监听的数据安全审计方案，只要在数据中心交换机配置端口镜像进行监控，不需要消耗其他网络和系统资源，但审计系统依赖网络端口可侦听的数据。因此审计系统必须在数据审计粒度与系统效率之间权衡，以获得一个安全和性能的平衡点，例如只针对某几种数据操作类型或某些数据表进行的审计，可适用网络端口监听方案，如需进行全面的数据库审计，则要结合数据库系统安全审计。数据审计是区域医疗信息共享平台信息系统审计的一个环节，除此之外还有应用系统审计、操作系统审计、网络安全审计等等，它们共同构成区域医疗信息共享平台的审计体系。

参考文献

1 谢健，赖炜，吴汝明，等. 构建区域临床药学服务数据中心〔J〕. 中国数字医学，2009，(1)：29－31.

2 赖炜，曾海标，吴汝明，等. 基于光交换宽带城域网的医学信息系统平台〔J〕. 中国数字医学，2007，(6)：21－23.

3 梁昌明. Oracle 数据库审计方法的探讨〔J〕. 中国医疗设备，2008，23 (4)：55－57.

4 陈晨，陈怀楚，高国柱，等. 基于 Oracle 数据库的数据审计系统的设计与实现〔J〕. 实验技术与管理，2005，22 (12)：76－79.

5 叶萍. 医院信息化建设风险与数据安全管理〔J〕. 医学信息学杂志，2010，31 (6)：21－23.

6 叶青. 建立计算机药物信息咨询系统. 提高临床药学服务水平. 现代医院管理杂志，2005，7 (3)：31－32.

7 陈强，马丽娅，赵伟，等. 数字化医院标准体系建设及问题〔J〕. 医学信息，2006，19 (1)：28.

8 庄炜. 浅谈区域医疗卫生信息化建设需要注意几个问题〔J〕. 现代医院杂志，2004，4 (7)：1－2.

9 朱海林，方乐，梁晟，等. IT 服务 (管理控制与流程) / 服务管理控制与规划系列丛书〔M〕. 北京：机械工业出版社，2006.

10 左天祖，刘伟著. ITIL 技术白皮书〔M〕. 北京：北京大学出版社，2004.