计算机审计中的电子数据轨迹分析

崔应留,李 娅

(南京审计学院 信息科学学院, 江苏 南京 210029)

摘 要:不同阶段电子数据的操作都会留下表现各异的轨迹。从操作系统、计算机应用系统、数据传输、数据采集和分析等不同层面深入分析审计电子数据轨迹在计算机系统中表现形式,可以为审计人员提供有效的审计方法。

关键词:数据轨迹;计算机审计;审计效率;日志文件

中图分类号:F239.1 **文献标识码**:A **文章编号**:1672-8750(2010)02-0032-04 **收稿日期**:2010-02-05

作者简介:崔应留(1974—),男,安徽六安人,南京审计学院信息科学学院讲师,南京理工大学博士生,主要研究方向为数字信号处理、计算机审计;李娅(1980—),女,江苏徐州人,南京审计学院信息科学学院讲师,主要研究方向为计算机审计。

一、研究背景

计算机技术在提高企业信息化水平的同时,也对审计工作提出了更高的要求。如何适应企业信息化的快速发展,提高审计人员的计算机审计能力,成为当前计算机审计领域的研究热点[1-3]。计算机审计包括两方面内容:对会计信息系统的安全、内部控制和设计、数据处理过程和处理结果进行审计;审计人员利用计算机辅助审计[4]。我国计算机审计技术在数据采集技术、数据分析方法、数据转换原理、审计软件开发和使用等方面都有很大发展[5]。目前理论界和实务界对计算机审计风险的定义、形成原因、表现特点做了大量研究和论述,同时也从提高审计主体的素质、完善审计机构的内部质量控制制度、改善审计人员组成结构等方面对计算机审计风险控制作了初步研究和探索[6-8]。

当前许多企业采用计算机信息系统来管理和处理财务和业务数据,电子数据在计算机系统中按照软件流程经过输入、转发、处理、存储、输出、修订等一系列规定程序,完成最终操作。针对不同来源、不同系统、不同数据库、不同开发者、不同功能的各种数据和信息系统软件,掌握其中电子数据轨迹的表现特征,可以为开展计算机审计、降低计算机审计风险提供有效方法[9-12]。

二、计算机审计电子数据轨迹概述

计算机系统是一个信息处理系统,主要完成信息的输入、传输、存储、加工处理和输出利用等操作。信息在计算机系统中以电子数据的形式表现,而电子数据的具体形式各种各样,通常以文件的形式存放在物理介质中。一个专业的计算机审计人员必须充分了解被审计单位的电子数据在计算机系统中的各种存在方式,其中掌握电子数据轨迹的表现特征尤为重要。

电子数据轨迹是指在数据核算和业务操作中通过映射、抽象提取、交叉索引和流程控制,连接电子操作与原始交易数据而提供的一系列信息。计算机系统应为每笔业务、每项经济活动提供一个完整的电子数据轨迹,该电子数据轨迹需要有迹可循并长期保存。审计人员在掌握业务流程的基础上,必须掌握电子数据轨迹的表现形式,才能分析和评价计算机系统内部控制的完善程度(主要反映在计算机软硬件系统的可靠性程度、数据从输入到输出整个过程的正确性和有效性、数据在传输过程中的安全性等等)。

三、各层面电子数据轨迹分析

（一）操作系统层面

操作系统是控制和管理计算机硬件和软件资源、合理地组织计算机的工作流程以及方便用户使用的程序的集合，故其安全性成为计算机审计安全的一项重要内容。目前，常见的操作系统有Windows、UNIX、Linux 和 Netware 等，在进行操作系统安全审计过程中，审计数据轨迹表现为日志文件。日志文件是操作系统中一类特殊的文件，它们是计算机审计线索和证据的重要来源，记录着计算机系统发生的一切活动情况，包括系统各项服务的细节。日志可以监控系统资源，寻找可疑行为，确认入侵范围。

审计人员通过分析日志文件可以了解计算机系统使用情况和安全状况，分析来自内部威胁和外部攻击的可能性等，并快速地对潜在的系统入侵做出记录和预测。例如，Windows 操作系统自带安全机制，其中包含审核策略，是用来指定要记录的事件类型的，这些类型涉及从系统范围的事件（例如用户登录）到指定事件（例如某用户试图读取某个特定文件），这些事件包括成功事件、不成功事件或兼而有之，审核记录写入计算机的安全日志，即形成电子数据轨迹，审计人员可以充分利用日志文件分析系统的安全状况，合理评价系统内部控制的有效性。

（二）计算机应用系统层面

计算机应用系统是个较为宽泛的概念，它包括电子数据处理系统（EDP）、管理信息系统（MIS）、用于科学计算和工程设计的专用信息系统，它涉及对数据的输入管理、处理、存储、保护、传输和输出等多个过程，每个过程对数据的操作都会有所记录，所有电子数据均有迹可寻。

1. 数据输入

数据输入过程中，电子数据轨迹表现为上机日志，即操作员在进行数据输入时都有上机记录，每个系统随时对不同模块或产品的每个操作员的上机时间、数据输入、下机时间等情况进行登记，形成数据输入日志。通过查阅数据输入日志，审计人员可以了解计算机应用系统的输入控制情况，包括输入数据正确性控制、完整性控制和输入错误纠正控制等。

对于扫描拍照输入、传感输入方式，审计人员可以根据信号转换类型、系统接口标准、数据格式转换过程中系统参数和转换条件的设置等了解数据轨迹的表现特征。如光信号转换为电信号时的电荷耦合器件（CCD）性能指标和参数设计、模拟电信号转换为数字电信号（通过 A/D 转换器）时信号采样频率和编码方式的选择、输入设备与主机接口的匹配和参数的调用等，它们都表现为数据输入时的电子数据轨迹。通过检查上述数据输入时的电子数据轨迹，审计人员能够清楚理解数据输入的过程，同时判断数据输入控制的有效性和完整性。

2. 数据处理

数据输入信息系统后，系统要对电子数据进行加工处理，例如：对财务数据进行处理，产生流水线、报表；系统往往设置特定的数据处理条件，只有满足条件的数据才能被处理；系统通过相应的计算公式生成处理后的数据；系统对丢失数据、重复或出错数据的处理。电子数据处理的每一个环节，系统一般都设置操作日志，自动记录所有执行过的操作，其中包括操作员信息、各个用户终端的辨认、操作时间、所调用的功能模块等。审计人员根据电子数据轨迹存在方式的操作日志，就能即时了解数据流向，检查计算机系统中数据处理系统各个环节的控制措施，进而实施有效的控制。

经过初步处理的电子数据在数据库中要进行集中管理和进一步处理。数据库是计算机信息系统中最重要的组成部分，信息系统中大多数和信息有关的操作都与数据库有关。在数据库中，电子数字轨迹表现形式是用于描述所管理的表和对象的数据，即数据字典，是关于数据的数据，也称为“元数据”。数据字典存储有关数据库结构信息的一些数据库对象，它描述了实际数据是如何组织的。一般情况下，数字字典包括表或视图的一般信息（如表名，别名和描述等）、数字定义（包括数据类型，数据长度和结构组成）、数据的使用特点（包括数据的取值范围、使用频率和使用方式）、数据的控制信息（包括数据来源、用户、使用它的程序和改变）等主要内容。审计人员可以通过分析各种数据库表以及视图之间的关系，并选择出与核心业务处理直接关联的数据库表和视图，对表的结构，包括字段类型、取值、空值应用、各种编码的含义、有效性和一致性进行详细分析研究，找出属于系统内控有关的关键字段。然后

通过相关数据库表之间关联,找出规律性的数据记录,发现疑点和审计线索。

触发器是一种特殊的存储过程,由数字字典创建和指定的,它在插入、删除或修改特定表或视图中的数据时触发执行,它比数据库本身标准的功能有更精细和更复杂的数据控制能力。触发器可以跟踪用户对数据库的操作,如审计用户操作数据库时所调用的语句和把用户对数据库的更新写入审计表等;触发器还可以基于数据库的值使用户具有操作数据库的某种权利,可以实现复杂的数据完整性规则,可以实现复杂的非标准的数据库相关完整性规则。触发器可以对数据库中相关的表进行连环更新、同步实时地复制表中的数据、自动计算数据值等作用。审计人员可以利用触发器技术实现对电子数据的跟踪和保护。

另外在一般的大型数据库中都存在用于捕捉系统活动的工具,如 Microsoft Sql Server 中,SQL SERVER PROFILER 工具就是用来捕捉系统的活动,用于 SQL 跟踪的图形用户界面,用来监视 Microsoft 数据库引擎或 Analysis Services 的实例。这些工具可以捕获每个数据库事件的数据,并将其保存到文件或表供以后分析。例如,可以用于监视产品环境,以了解哪些存储过程执行速度太慢并妨碍性能。审计人员可以先创建一个跟踪定义,然后就可以启动和运行跟踪,监测相关服务器上的 SQL SERVER 事件,并且为所选的事件捕捉满足过滤条件的指定数据。ORACLE 数据库从其安全性考虑,设有多个安全层,并且可以对各层进行审计,审计记录可以写入 SYS. AUD $ 的审计踪迹。可以被审计的三种不同的操作类型包括注册企图、对象访问和数据库操作。利用其中对对象的数据交换操作审计功能,就可以获得相应的电子数据轨迹。

因此,充分利用数据处理阶段产生的电子数据轨迹,可以有效分析和判断数据处理控制情况,包括处理权限控制、业务时序控制、合理性检验控制、参照检查控制和审计踪迹控制以及恢复和备份控制等。

3. 数据输出

输出是计算机数据处理的最后结果。计算机信息系统的输出如果出错或者输出数据未经允许被窃取或使用,都将可能给企业带来损失,故必须进行输出控制。实现输出控制措施有:只有经过授权的人才能下载数据,并进行操作登记;进行输出条件的检查、输出完整性和正确性检查、输出数据的安全保护、输出格式的控制等。通过了解系统输出控制措施的设置,就能清楚输出过程中电子数据轨迹的表现形式。

(三) 数据传输层面

电子数据是通过计算机网络进行传输的,传输的数据是否准确和安全,涉及计算机网络技术的可靠性和网络系统的安全管理问题。在电子数据传输过程中,通常会采用相应的通信控制措施,以保证数据传输的安全,电子数据轨迹也体现在安全控制方面,包括数据加密、数字签名、信息摘要和数据收发双方实现确认和重发机制等。

1. 数据加密

为了防止数据被窃取或非法修改,并实现在普通信道上安全传输,可以采取数据加密技术,通过对称加密技术或非对称加密技术,实现数据安全传输。

2. 数字签名

数字签名的目的是让对方相信数据的真实性,保证数据传输的正确性。电子数据轨迹体现在收发双方必须满足两个条件:一是接收方通过数字签名验证所接收的数据的确来自发送方,从而明确数据的来源;二是发送方在发送数据之后也不能否认他曾经发送过数据的事实,从而防止发送方对数据的抵赖。

3. 信息摘要

进行信息摘要的目的是保护信息数据的完整性。当前企业集团总部与分支机构进行财务、业务数据传递时,或者与外部供销商交流业务时,经常附带信息摘要,以确保通信的完整性不被破坏。

4. 数据收发双方实现确认和重发机制

根据数据在传输过程中系统实施的安全控制策略,即电子数据轨迹的表现形式,可以判断和评价安全控制是否合理、健全,并有效地发挥作用。

(四) 数据采集与分析层面

审计数据采集与分析包括数据采集、数据转换和数据验证等过程,电子数据轨迹表现为不同的形式。

数据采集由数据接口使用、数据源识别、数据交换处理等过程组成,其中数据接口是以电子数据文件的形式存在,该数据文件即为电子数据通过数据接口的电子轨迹,实现不同计算机软件系

统之间传送数据。通过数据接口的数据文件必须由原计算机软件系统在生成其数据文件时同时生成,当原系统数据文件发生变更时,数据接口的数据文件也同步改变。而利用数据文件进行数据交换时,常用的交换文件格式有文本文件和 XML。根据实际要求采用适当的数据交换处理技术,从而获取高质量的数据。根据此电子数据轨迹,检查数据接口的正确使用以及接口的控制功能,避免因数据接口不匹配而导致数据采集不能完成或发生错误。

为了进一步提高审计电子数据质量,并形成集成的数据,在进行计算机审计之前必须对数据进行转换。审计人员可以从审计中间表和审计数据转换日志分析电子数据轨迹,因为它们贯穿于每一个审计数据转换活动。审计人员可以从该电子数据轨迹分析数据转换的整个过程,包括数据转换的正确性、转换的变化情况,分别记载数据转换时由于各种冲突产生的错误、由于系统编程不当而产生的错误信息,以及记载数据转换过程和有关数据的变化情况。通过查阅错误日志和转换变化日志可以实现审计信息的可追溯性。通过分析数据接口的电子轨迹、数据转换日志和错误日志,审计人员可以检查数据采集与分析过程控制的有效性。

本文分别从计算机操作系统、计算机应用系统、数据传输、数据采集和分析等各个不同层面分析了电子数据轨迹在计算机系统中的表现形式,为审计人员从本质上掌握计算机信息系统内部控制的有效程度提供了审计思路和方法,从而实现有重点的数据跟踪检测,提高审计质量并降低审计风险。

参考文献:

[1]颜萍. 计算机辅助审计的作用与意义[J]. 中国乡镇企业会计,2007(8):58-59.

[2]杨莉. 实施信息系统审计的主要方法[J]. 中国审计,2002(11):63-64.

[3]任森. 数据式审计与分析性复核的比较研究[J]. 现代会计,2007(4):30-32.

[4]李素平. 计算机审计实务问题释疑[M]. 北京:经济管理出版社,2009.

[5]国家 863 计划审计署课题组. 计算机审计数据采集与处理技术研究报告[M]. 北京:清华大学出版社,2007.

[6]王风华. 计算机会计信息系统下审计风险的控制[J]. 财会与审计,2008(11):65-67.

[7]张继伟. 计算机审计风险成因及其防范对策[J]. 财会通讯,2009(8):82-83.

[8]赵立洋. 网络环境下的审风险及其控制[J]. 现代会计,2007(6):48-51.

[9]董化礼,刘汝焯. 计算机审计数据采集与分析技术[M]. 北京:清华大学出版社,2002.

[10]Ye Nong, Chen Qiang, Vilbert S. Multivariate statistical analysis of audit trails for host-based intrusion detection[J]. IEEE TRANSACTIONS ON COMPUTERS, 2002(7):810-820.

[11]邸丽清,熊智华,阳宪惠. 基于数据相似度的间歇过程在线监控[J]. 清华大学学报:自然科学版,2008,48(7):1217-1220.

[12]陈耿,王万军. 信息系统审计[M]. 北京:清华大学出版社,2009.

(**责任编辑:**杨凤春)

Analysis of Electronic Data Track in Computer Auditing

CUI Ying-liu, LI Ya

(School of Information Science, Nanjing Audit University, Nanjing 210029, China)

Abstract: The operation of electronic data will leave traces at various stages. If we analyze those traces from the aspects of operation system, application systems, data transmission, and data collection and analysis, we can provide effective auditing methods for auditors.

Key words: data track; computer auditing; audit efficiency; log file