DOI: 10.16262/j.cnki.1000-8217.2011.05.013

·基金纵横·

科学基金管理系统的用户行为审计初探*

郝艳妮[1] 李 东[2] 施懿闻[3] 毛基业[3]

(1 爱瑞思软件(深圳)有限公司，深圳 518057；2 国家自然科学基金委员会，北京 100085；
3 中国人民大学商学院，北京 100872)

1 引言

随着信息系统在各类组织中的角色变得越来越重要，通过信息系统共享的信息资源也越来越多。很多研究发现，除了病毒或黑客此类外部入侵会对信息系统安全带来危害，内部用户的异常操作同样会对信息系统的安全运营带来极大的威胁[1]。信息系统用户行为审计就是对此类操作进行管理和监控。由于内部用户是信息安全最薄弱的一个环节[2]，用户行为审计成为了控制内部用户安全使用信息资源的重要手段。

用户行为审计是与授权和访问控制并列的3种防止信息泄露和非法修改技术之一，具有广泛应用[3]。例如，在美国的医疗系统中，信息系统审计有着严格的规定。美国健康保险流通与责任法案(HIPAA)要求卫生机构必须防止未经授权的使用或披露患者的健康信息[4]。对用户行为的审计可以达到两个目标：对非法的用户行为进行监控和管理以及改善用户的行为方式[2]。

作为国家科学基金管理单位，国家自然科学基金委员会(以下简称自然科学基金委)的工作具有高度保密性等特点，其项目信息管理系统的权限管理是至关重要的一个环节。因此，有必要从用户角度研究如何更有效地利用计算机技术，加强用户行为的记录与审计，规范科学基金管理工作，提高组织绩效。

信息安全的管理是复杂的，用户行为审计虽然是一种有效的手段，但很多安全问题需要通过管理和制度进行规范。这方面的探讨和对用户行为审计的模式进行创新，也会带动相关管理制度的完善，从而更好地加强基金委的信息安全管理。本文将在基金委用户权限管理体系的基础上，以目前基金委对项目管理信息系统用户行为审计的需求为依据，设计合理且灵活的用户审计模式，为科学基金管理提出一个较为系统性和有一般参考价值的解决方案，并为基金委新一代项目管理信息系统的建设提供参考建议。

本文主要包括两个主要部分：(1) 对相关文献进行综述，包括信息系统用户行为审计的目的、方法以及典型应用；(2) 分析科学基金管理系统常见的用户审计需求，并基于现有用户权限管理机制，提出相应的用户行为审计方案。

2 文献综述

本节主要分为3个部分：第一，总结用户行为审计的两个目的；第二，依据美国商务部下属的国家标准与技术研究所于1996年编写的《保障信息技术系统的普遍公认原则与实践》[5]，对信息系统审计的方法及相关原则进行总结；第三，通过信息系统审计在美国医疗系统的应用，总结目前信息系统审计为达到审计目的中采用的手段和工具。在对现有理论和应用总结的基础上，结合自然科学基金委实际的审计需求，对未来新系统建设的审计工作提出合理的建议。

2.1 审计目的

鉴于内部用户是信息安全最薄弱的一个环节，对用户行为的审计可以达到两个目标：对非法的用户行为进行监控和管理以及改善用户的行为方式[2]。

目前有3种技术在防止信息被不正当的披露和修改方面得到了广泛应用：授权，访问控制和审计[3]。访问控制就是根据某种控制规则来控制用户对系统的访问，从而达到保护信息系统资源安全的

* 本研究受国家自然科学基金资助(项目编号：M1021006)。
本文于2011年7月5日收到.

目的。然而，如果访问控制没有审计作为辅助，则不能成为保证信息系统安全的一个完整的解决方案。我们不仅需要对用户访问系统进行身份合法的验证，同时也需要对非法用户和用户的越权操作进行管理，即需要对信息系统进行审计。一旦用户没有通过合法身份访问系统时，审计就可以跟踪他们的行为和活动。

此外，如果用户意识到他们在系统中的任何行为都会被记录在审计日志中，就会有违反安全策略的顾虑[6]。所以，告知用户其信息系统使用活动会通过审计跟踪进行记录，须为自身行为负责，可以更好地改善用户的行为方式。但目前许多组织往往花较多费用从技术层面加强信息安全，而较少从用户层面考虑其对信息安全的影响。

2.2 审计方法

美国商务部下属的国家标准与技术研究所于1996 年编写的《保障信息技术系统的普遍公认原则与实践》中，定位审计跟踪主要用于个人问责、事件重建、入侵检测和问题识别，以下主要通过 3 个方面对相关的原则和实践方法进行阐述。

首先，审计跟踪的内容应包括足够的信息来确定哪些事件发生，谁(或什么)导致了这些事件的发生。在定义审计跟踪的范围和内容时，需要着重在性能、用户隐私以及成本与安全需求之间进行权衡。Rostad 和 Edsberg(2006)通过调研发现，目前虽然有些组织存储了大量的日志，但并不能有效地调查可疑的误用情况。而想要得到一个有用的审计跟踪，需要为管理员提供一个良好的接口并需要充分的细节可以再造当时的场景[7]。同时，也有研究者强调在提取用户行为模式时，确定有利于行为模式挖掘的记录是一个关键问题[1]。

通常这些记录来自于主机日志和网络协议记录。一般情况下对于一个事件，需要记录如下内容：(1) 事件的类型及其结果；(2) 事件发生的时间；(3) 与事件相关的用户 ID；(4) 引起事件的程序或指令。

其次，需要保护审计跟踪自身的安全，以防范非授权的访问。主要的预防措施有以下部分：(1) 需要严格控制对在线审计跟踪的访问；(2) 权责分离，组织需要保证访问控制的管理人员与审计跟踪的管理人员的权责分离；(3) 机密保护，审计跟踪中部分信息的保密性需要重视，如对一些用户私人信息的记录。

最后，对审计跟踪的审查应该是周期性的行为，在审查时可以关注以下几点：(1) 识别常规活动。审查人员应该追求更有效的识别非常规活动，其前提是什么是用户的常规活动。(2) 搜索功能。如果包含搜索功能，审计跟踪的审查工作会更加轻松。比如，可以根据用户 ID，终端 ID，应用程序的名称、日期和时间，或其他一些参数用于筛选审计跟踪。(3) 后续审查。系统级和应用级的管理员需要审查已知的系统及用户的问题，用户违反现行规定的行为，以及原因不明的问题。(4) 制定审查指南。根据非授权行为的严重性，需要确定如何才能充分地审查审计跟踪，并制定相应的指导文件。(5) 自动化工具。对于常规性、批量性的审计工作，应使用自动化的工具。此类工具也可用于实时或近似实时的方式。

2.3 案例：信息系统审计在医疗系统的应用[4]

在医疗系统中，存在着各类重要的医疗数据，而且这类数据有高度的隐私性，对信息安全的要求很高。为了保证医疗保健的隐私性和安全性，美国健康保险流通与责任法案(HIPAA)要求卫生机构必须防止未经授权的使用或披露患者的健康信息。HIPAA 的安全标准要求通过管理、物理、技术的保障手段，来保护电子健康信息的保密性，完整性和可用性。其中一个重要的手段就是利用审计跟踪，它可以记录和检查信息系统的活动。

HIPAA 要求对健康数据访问的审计跟踪需要包括以下数据：(1) 访问数据人的身份确认；(2) 被访问数据的确认；(3) 访问数据的地点；(4) 访问数据的时间；(5) 访问的类型(创建、只读、写、修改、删除)；(6) 访问的状态(成功、失败)。

问题在于，现在的健康信息系统无法产生如上的审计跟踪。虽然系统中有大量的日志文件，但是这些相关的审计信息需要从大量的日志数据中进行提炼和整合，才可以生成所需要的疾病审计跟踪。

为了满足 HIPAA 的审计要求，研究者设计了 HIPAA 疾病审计系统，在医疗图像方面设计了一个 4 层系统。

第一层：记录层。该层存储了大量数据资源，包括各类应用日志，这些日志是系统各模块生成的初始的事件日志。如应用日志、用户登录日志、图像完整性日志、系统日志等。这些日志提供了生成 HIPAA 疾病审计跟踪所需的相关信息。

第二层：审计层。该层为系统的核心。其将数据存储在一个集中的审计数据库，通过安全监控工具包用来进行审计分析和自动监测。HIPAA 疾病

审计跟踪就可以基于该数据库的数据生成。该层主要分为7个模块：(1) 审计日志收集：由于审计数据都分散在大量的日志中，需要将相关的数据从日志中发送到集中的审计数据库。该收集模块需要支持各种日志格式。(2) 系统日志服务器：系统日志是一个C/S机制，其采用用户数据报协议(UDP)来传输事件信息。其将各类数据转化成系统日志数据格式，并通过客户端发送至系统日志服务器，这样就可以进行下一步——日志数据标准化。(3) 日志数据标准化：从系统各模块产生的数据，对同一目标都用不同的专业术语进行描述，这一模块将这些数据标准化，然后将其加入审计数据库。(4) 审计数据库：为了能够短时间内生成审计跟踪，需要一个包括了所有审计数据的数据库：访问人、时间、地点、访问对象、访问方式和访问状态。采用数据库的方式保存日志数据有如下好处：首先，保证历史数据不会丢失。其次，为每个病人集中管理数据访问信息。(5) 审计分析工具：在没有此工具之前，对数据流的监测只能依靠系统管理员的经验，而审计分析工具可以自动监测并发现不正常的模式。但开发此类工具，需要收集系统各模块数据流信息，以及采用一些数据分析技术，如入侵检测技术。(6) 监测工具：当审计分析工具发现了数据流中不正常的模式后，就需要监测工具依照基于角色的规则判断该行为是否属于非授权的数据访问。一旦发现违反了规则，应自动产生警告或提醒。(7) 基于角色的策略：此部分规定了系统的各种角色，以及每个角色的访问权利。

第三层：通知层。该层从审计层接收警告信息，并通知终端用户的非授权访问或其他非正常的行为，如系统管理员。

第四层：行动层。该层用于终端用户动作，比如访问控制，防止非授权的访问或其他非正常的行为。

研究者基于审计层的部分模块开发了一个安全监测工具包，用于自动检测系统中的数据流。该工具包已在2003年RSNA年度会议中的InfoRAD展览中进行了展示。

以上文献回顾通过对用户行为审计领域的前沿文献进行收集，对目前该领域的理论研究进展和行业实际应用进行了整理。对实际应用和相关制度的总结，明确了当前信息系统中用户行为审计的必要性和一般的审计方法及使用的工具。本节总结的经验作为方案设计的依据，才能保证为基金委新系统的设计方案的可行性且符合行业最佳实践。

3　应用实例

本节将以自然科学基金委的业务系统——项目信息管理系统为例，从分析科学基金管理系统的权限管理需求出发，通过总结和分析，设计一套满足其需求的用户行为审计方案。首先，通过归纳基金管理系统目前面临的问题，抽取出当前在用户行为审计方面的需求和挑战，进行需求分析。然后，结合前沿文献的总结，以及未来信息系统的权限管理模式，提出合理的用户行为审计方案。

3.1　需求分析

用户需求是方案设计的关键，也是验证方案设计有效性的依据。本节将从自然科学基金委用户行为审计现状出发，对基金委的需求的调研，总结需要通过方案设计解决的问题。

目前现有系统已有部分审计功能，但尚未在系统中向用户提供审计服务，只有在用户有具体需求时，向信息中心提出申请，并由信息中心工作人员通过后台的数据库查询予以反馈。该方法已经不能适应自然科学基金委的业务需求，为科学基金管理工作带来了诸多不便，其具体情景将在之后予以详细描述。根据多次调研，本文总结出以下4类审计需求：

(1) 上级对下级工作情况的审查。根据基金委项目管理的工作需要，上级用户角色通常需要对自己负责的项目和下级的工作概况有一定的把握。审查的内容包括工作的进度，也包括具体的工作轨迹。需要合理的日志结构对各类信息进行记录。

通常审计的项目为评审阶段的项目，主要关注的内容是对评审专家指派或取消指派的操作。目前由用户通过提供项目代码，交至信息中心查询所有人员对该项目信息进行的所有操作。审计流程是这样的：首先，对搜索到的日志进行罗列。在数据库中，操作功能是用代码书写的，需要对代码进行翻译。其次，查看日志是否存在问题。通常，审计人员会积累一定用户的行为习惯，如项目查看的顺序等。一旦发现异常，再通过操作人或登录IP进行进一步查询。主要的检查步骤如下：

第一，操作人是否有执行该操作的权限(如：项目主管人员、相关项目主任以及项目评审专家等可以查看项目信息)。

第二，检查登录IP是否为常用IP(如：工作时间为办公室IP，下班时间为通过VPN访问的家庭IP)。

第三，检查其他不符合用户行为习惯的异常情况(如：某一用户通常只查询设定范围内的项目)。

对于项目群的审计是此类审计的难点(如:某一学部需要了解在一段时间内,对其学部某一特定类项目的所有操作)。由于目前只可利用项目 ID 对特定项目进行查询,而对某一类型的项目不能进行批量查询,带来了较大的工作量。

(2) 用户对所授权限/委托行为的审计。用户在使用分级授权后,应对所授权限进行的工作进行审计,与上级对下级工作的审查类似。针对委托行为的审计,应在收回委托后,对委托期间的工作进行审查。

(3) 用户的自行审查。此类审计主要为用户关注自己在某段时间的所有操作。可以考虑在项目评审阶段等敏感的时间段内,系统应定期向项目主管人员反馈此段时间内的账号操作情况。

(4) 对非常规操作的警告。为防止用户非法访问或使用信息资源,系统应对用户非常规的操作提出警告,这是对可能发生的非法操作进行的提醒。如检查登录 IP 是否为常用 IP(如:工作时间为办公室 IP,下班时间为通过 VPN 访问的家庭 IP)。虽然当前系统会在每次登录时显示上次登录 IP 与登录时间,但是没有达到理想的提醒效果,有些用户甚至不清楚自己的 IP 是什么。可以考虑将用户与常用 IP 进行绑定,如果登录 IP 与绑定 IP 不一致,对用户进行警告。

根据本节对基金管理系统现状和需求的分析,本文总结出其用户行为审计工作具有以下特点,即目前的日常审计工作基本上是通过用户提出需求,由信息中心工作人员通过在后台对日志查询的模式进行的。在此方面,主要的挑战在于通过信息系统来自动提供基金委的日常审计需求。

3.2 解决方案

根据需求分析的情况,结合基金项目管理的工作特点,并结合用户角色体系中角色层级可以支持用户行为审计的工作。根据用户行为审计的 4 种情景,给予分别的用户权限方案设计。

(1) 上级对下级工作情况的审查。这一需求可以依托权限管理中"组织机构"和"角色等级"的两个维度进行。某一等级较高的角色,可以审查其管理范围内各低级角色的关键行为。如拥有某科学部项目主管处处长角色的用户,有权审查赋有该处项目主任/流动项目主任,以及兼聘用户角色的关键行为。

(2) 委托行为的审计。此处的委托行为主要针对以职能备份的情况展开,即某人出差或长期休假,因而需要将其工作权利委托给其他人,以保证原工作职能的继续。任何人(委托人)可以将自身的权限委托全部委托给其他用户(受托人),但委托人和受托人应为其所属同一组织机构内。日志中应对受托人的代操作有相应的标识,且委托人应在收回权限时应有权审查受托人在接受委托期间的所有操作。

(3) 用户的自行审查。与上一点类似,此类审计仅限于用户对自己账户行为的审查。

(4) 对非常规操作的警告。非常规操作的定义是该方案设计的关键,需要对用户的行为进行长期的积累和学习,从而总结出一套符合用户工作习惯的常规操作模型。一旦出现了非常规操作,系统需要提供主动服务,提醒和警示用户。目前,根据基金委的实际需求,非常规操作主要通过系统登陆地点、时间以及对系统各项操作功能进行衡量。

最后,关于审计日志的记录,根据文献和需求的综合,日志内容应包括但不局限于以下内容:(i) 操作的用户 ID;(ii) 操作的对象及相关属性;(iii) 操作的时间;(iv) 操作的地点(登录系统的 IP 地址);(v) 操作造成的后果。

本节结合前沿文献,针对目前自然科学基金委的日常审计的 4 个情景,分别在上级对下级工作情况的审查、用户对所授权限/委托行为的审计、用户的自行审查和对非常规操作的警告给予解决方案,并对审计日志内容方面给予建议。

4 结论

管理信息系统的应用都会涉及信息安全问题,用户权限管理和行为审计可以在一定程度上有效解决访问控制方面的安全问题,从用户角度研究如何更有效地利用计算机技术,加强用户行为的记录与审计,规范科学基金管理工作,提高组织绩效。

通过对自然科学基金委现有信息系统的调研,发现仅通过用户工作职能划分角色已经不能适应不同种类业务的个性化需求,也难以根据角色的等级进行相应的管理工作。如果系统的权限管理没有合理的角色结构,也难以通过系统的方式落实基金委的用户行为审计需求。

对于现有系统的改进,由于现在此类工作完全集中于信息中心,可以考虑开发相应的日志查询模块,为用户提供以下审计服务。

第一,用户对自身行为的审查。

第二,依据权限管理的等级体系,实现上级用户对下级用户工作情况的审阅。

第三,如果现有的日志结构不能对分级授权/权限委托进行很好的记录和追踪,自然科学基金委

可以权衡需求和开发的成本，决定是否实现此类内容的审计。

第四，对于用户非常规行为的提示，不应仅显示上次用户登录的IP和时间，而应根据判断对系统认为非常规的行为（如：非常规登录IP，非工作时间登录）进行更加明确和友好的提示（如采用提示框显示“本次登录为非常规登录IP”）。

在未来新系统的设计中，用户行为审计工作应基于支持等级角色的权限体系，并注意以下方面：

首先，在审计日志的内容方面，需要保证日志的记录内容可以还原用户的操作情景，这些内容包括不限于：操作的用户ID、操作的对象及相关属性、操作的时间、操作的地点（登录系统的IP地址）、操作结果。

其次，在审计数据的分析方面，除了目前用户较为明确的审计需求应通过系统功能予以实现之外，需要在日志的分析和用户行为模式的识别方面进行进一步挖掘，从中总结出一般用户的行为习惯和非法操作的特征，从而可以通过系统对用户行为的合法性进行判断。这需要较长时间的数据积累和学习。

最后，在审计内容的展现方面，通过一种合理的途径向用户展现审计内容，从而有效影响用户的安全行为是本文尚未讨论的，可以在未来展开进一步的研究。目前在科学基金项目的全过程管理中，对系统各类用户安全行为进行辅助或提醒方面不够完善与到位。在以后的研究中探索更好地实现业务系统的工作提醒和提示（例如，上次登录系统时间和地点，持续登录时间，完成的主要操作类型），研究以不同策略和方法主动为用户服务，检验不同提示和主动服务策略的效果。例如，主动提供用户使用系统和操作的统计信息，与历史记录的比较，以验证系统的主动服务是否对用户的安全行为起到了促进作用。

参 考 文 献

[1] 江伟，陈龙，王国胤. 用户行为异常检测在安全审计系统中的应用. 计算机应用，2006，26(7)：1637—1642.

[2] Vroom C, Von Solms R. Towards information security behavioral compliance. Computer & Security, 2004, 23(3): 191—198.

[3] Fernandez-Medina E, Trujillob J, Villarroelc R et al. Access control and audit model for the multidimensional modeling of data warehouses. Decision Support Systems, 2006, 42(3): 1270—1289.

[4] Zhou Z, Liu B J. HIPAA compliant auditing system for medical images. Computerized Medical Imaging and Graphics, 2005, 29(2): 235—241.

[5] Swanson M, Guttman B. Generally accepted principles and practices for securing information technology systems: NIST. 1996.

[6] 杨志彬. 浅析访问控制的审计跟踪. 计算机系统应用，2008，12：171—174.

[7] Rostad L, Edsberg O. A study of access control requirements for healthcare systems based on audit trails from access logs. Proceedings of the 22nd Annual Computer Security Applications Conference. 2006, Miami Beach, Florida, USA. 175—186.

A STUDY ON THE AUDIT OF USER BEHAVIORS OF RESEARCH GRANT MANAGEMENT SYSTEMS

Hao Yanni[1]　Li Dong[2]　Shi Yiwen[3]　Mao Jiye[3]

(1 *IRIS Systems (Shenzhen) Co., Ltd, Shenzhen* 518057; 2 *National Natural Science Foundation of China, Beijing* 100085; 3 *School of Business, Renmin University of China, Beijing* 100872)

·资料·信息·

2011年国家基础科学人才培养基金第三届管理委员会第六次会议在京召开

2011年国家基础科学人才培养基金第三届管理委员会第六次会议于7月26日在京举行。会议审议通过了2011年度项目评审结果。2011年度共资助项目101项，资助经费28 800万元。其中，条件建设项目35项，资助经费6800万元；能力提高项目55项，资助经费21 780万元；师资培训项目11项，资助经费220万元。

会议审议通过了2012年度资助计划和项目指南。2012年拟资助条件建设项目43项，能力提高项目39项，特殊学科点项目8项，师资培训项目15项。

会议还就国家基础科学人才培养基金实施细则的修订、野外实习基地的整合与共享以及特殊学科点的部署等问题进行了深入讨论。

（计划局 供稿）