谈拓展审计系统认证功能

林清林　杨　毅

（西南财经大学会计学院　成都　610074）

【摘要】本文回顾了近年来审计认证的发展和相关研究，并介绍了系统认证的原则和标准及信息系统认证的测试技术。

【关键词】审计认证　系统认证　系统测试

一、有关审计认证的研究文献

信息技术的发展使公司和信息系统的管理者都认识到信息系统是组织最有价值的资产，它和传统资产一样需要控制，需要独立第三方对信息资产控制的情况进行评价。信息系统认证是注册会计师采用计算机对被认证对象的信息系统的安全性、可靠性进行测试与评价，并对信息系统对财务报告的影响做出判断或单独提出信息系统认证报告的过程。

为了对信息系统的可信性提供合理保证，美国注册会计师协会（AICPA）和加拿大特许会计师协会（CICA）联合推出了信息系统认证服务（SysTrust），他们将其称为“系统认证”。根据 AICPA 和 CICA 对“SysTrust”的定义，系统认证是注册会计师按照可操作和可应用性、系统安全性、数据处理的完整性、系统的可维护性四个基本原则，对信息系统的可靠性进行测试和评价，并发表认证报告的一种服务，其目的是增强管理者、客户、商业伙伴对企业信息系统的信赖。

早在 1982 年，美国审计师协会前会长 Chenok 就认为，影响审计行业未来发展有十四个主要问题，其中“审计师服务的拓展”位居第一。Accounting Horizons 于 1995 年第九期刊载了临时性机构保证服务特别委员会（SCAS）主席 Elliott 在美国会计师协会年会上的讲话，详尽地介绍了审计认证，并指出开展新服务以了解客户需求和提供有用信息为最重要。

我国也有不少关于审计认证的研究，除了审计服务，早期研究主要集中在鉴证服务，王光远（1994 年）探讨了审计鉴证职能扩展的必然性——民间审计的总趋势：从财务鉴证到管理鉴证。白静、周建、华金秋（1999）通过分析国际审计师发展的最新情况，认为我国在调整延伸原有审计业务时，要积极开拓新的业务类型，培育新的经济增长点。

2000 年以来，越来越多的学者开始转向审计认证的研究。吕文基（2000 年）认为随着知识经济的兴起，新世纪审计领域将出现审计形态多元化趋势，财务审计、绩效审计、经营管理审计等将有更大拓展，许多派生审计形态将应运而生，诸如网络实时审计、知识资本运营审计、规划审计、人力资源审计、防范风险审计、质量管理审计、绿色审计（环保审计）、彩色审计、综合的多维责任审计等。王光远（2000 年）认为：鉴证受托管理责任是现代会计审计科学的重大问题之一。李若山、杜滨、曹利（2001）认为二十一世纪审计师业务范围的拓展主要表现在咨询与顾问、法务会计与审计和保证业务（即审计认证）。我国的会计师事务所要应对加入 WTO 的挑战与机遇，要应对国外会计师事务所的强大竞争，就必须在保持现有审计业务的基础之上，积极发展审计认证业务。

二、系统认证的原则和标准

目前国际上有很多安全标准和准则，其中影响最广泛的当属安全评估标准。1983 年美国国防部公布了可信计算机评估准则（TCSEC）。20 世纪 90 年代西欧四国（英、法、荷、德）在各自安全评估准则的基础上提出了信息技术安全评价准则（ITSEC），他们除了吸收 TCSEC 的成功经验，首次提出了信息安全的保密性、完整性、可用性，把可信计算机的概念提高到可信信息技术的高度来认识，他们推荐从以下八个方面来评估信息系统的安全性，即识别和认证、访问控制、责任、审计、客体复用、精确性、服务的可靠性和数据交换。该标准对国际信息安全的研究和实施带来了深刻的影响。

美国要求注册会计师开展系统认证业务应遵循 AICPA 制定的《鉴证业务准则第 1 号——鉴证业务》。加拿大要求注册会计师遵循 CICA 制定的“鉴证业务准则”。在此基础上，AICPA 和 CICA 还专门为系统可靠性认证制定了专门的认证原则和标准。2003 年 4 月，AICPA 和 CICA 推出了“Trust Service Principles and Criteria”，将网站可靠性认证原则和标准与系统可靠性认证原则和标准合二为一，取消了网站可靠性认证原则和标准 3.0 版以及系统可靠性认证原则和标准 2.0 版，将网站可靠性认证原则由 7 个缩减为 5 个，系统可靠性认证原则则由原来的 4 个变为 5 个，取消了系统可维护性，增加了在线隐私保护原则和保密性原则。

由上可以看出，AICPA 和 CICA 推出“Trust Service Principles and Criteria”比起以前的 TCSEC 更加全面，它不仅继承了以前那些对系统安全性关注的思想，而且将数据处理完整性、系统可维护性、系统可操作和可应用性一起融入系统准则之中，从而形成了一个全面而完善的准则框架，也为其他国家制定系统认证的准则提供了借鉴模板。

2006 年，中国注册会计师协会在修订原有鉴证准则基础上，颁布了新的鉴证准则，包括《中国注册会计师其他鉴证业

务准则第 3101 号——历史财务信息审计或审阅以外的鉴证业务》、《中国注册会计师其他鉴证业务准则第 3111 号——预测性财务信息的审核》、《中国注册会计师相关业务准则第 4101 号——对财务信息执行商定程序》、《中国注册会计师相关服务准则 4111 号——代编财务信息》、《会计师事务所质量控制准则第 5101 号——业务质量控制》。这些业务准则的施行有利于审计功能的拓展，并为系统认证业务的开展提供了法规依据。尤其是在 2007 年 1 月 1 日起施行的《中国注册会计师鉴证业务基本准则》(以下简称"鉴证业务准则")中，增加了第五章"鉴证对象"的相关内容。鉴证业务准则规定鉴证对象主要可以分为财务业绩或状况、非财务业绩或状况、物理特征、某种系统和过程、一种行为等五大类，而这五类鉴证对象对应的信息形式分别为财务报表、反映效率或效果的关键指标、有关鉴证对象物理特征的说明文件、关于其有效性的认定、对法律法规遵守情况或执行效果的声明等。

三、信息系统认证的测试

对系统的测试主要包括系统安全性测试、数据处理完整性测试、系统可维护性测试、系统可操作和可应用性测试四个方面。在这四个方面中，笔者认为以系统安全性测试最为重要，一旦系统缺乏安全性，那么其他三个方面也就失去了意义，当然系统认证的其他三个方面也不能忽视。

1. 测试系统的安全性。系统的安全性是指系统已经采取了保护措施，能够防止未经授权的物理和逻辑进入。只有经过授权的用户才能进入系统，这种进入的限制不仅适用于系统的物理构成，也适用于系统执行的逻辑功能。对系统进入的授权限制有助于防止潜在的系统盗用系统资源、误用系统软件以及不当进入系统后修改、破坏和泄漏系统信息的行为。

2. 测试数据处理的完整性。系统数据处理具有完整性，说明系统处理数据过程是完全的、准确的、及时的，并经过适当授权。系统处理过程的完整性涉及系统的所有组成部分和所有的处理阶段，这也就是系统可靠性认证业务的范围。在处理系统外的数据输入时，系统必须建立确保处理过程的完全性、准确性和及时性的控制机制。因此，当信息资源和数据被明确地存在于系统可靠性认证业务所审查的系统之外时，对这种情况需要在系统说明中予以明确描述，这对界定注册会计师的责任非常重要。不过，倘若信息资源和数据都在系统控制的数据库范围内，系统公告中则应明确描述对所处理信息的完全性、准确性、及时性和授权的控制情况。

3. 测试系统的可维护性。系统的可维护性，即更新后的系统仍然能够保持其可靠性、安全性和数据处理的完整性。一般来说，系统通常都需要进行不断更新，以适应系统面临业务状况变化的需要和提升系统的效率，避免出现错误和故障。系统只有在及时的更新中才能保持其安全性、可靠性。系统在更新维护前要配备适当的维护资源，在更新维护过程中，按照事先定下的要求、方法、程序、准则进行，同时做好对系统更新维护的步骤安排、衔接计划、跟踪记录和意外故障排除准备。

值得注意的是，不论是惯例性和非惯例性，对系统和相关数据的所有修改都必须经过报告、授权、计划和测试，同时应做好书面记录。所有的系统修改计划和完成修改后的情况，都要与系统的管理层和授权的用户进行必要的沟通和披露。

4. 测试可操作性和可应用性。系统的可操作性和可应用性是指系统可以运行和有效地应用以及按照对外披露或有关协议中确定的服务水平运行和应用。对于系统外部的用户而言，系统应能够满足其输入新的信息和修改信息的要求，即要求系统做到满足用户对在其操作权限内的所有合法操作不能出现故障，否则就意味着系统在运行上存在问题。尽管系统的可操作性和可应用性并不研究系统执行的特定功能，也不研究用户将系统应用于特定工作或解决具体问题的能力，但它必须关注用户是否能够顺利进入系统，以便对系统存储的信息进行日常处理、监控、修改乃至删除。

四、信息系统安全性的测试技术

1. 漏洞扫描技术。安全扫描技术是指使用手工或特定的软件工具——安全扫描器对系统脆弱点进行评估，寻找可能对系统造成损害的安全漏洞。扫描的目的是通过一定的手段和方法发现系统或网络存在的隐患，以利于自身(使用单位)及时修补或发动对敌方系统的回击。同时，自动化的安全扫描器要对目标系统进行漏洞检测和分析，提供详细的漏洞描述，并针对安全漏洞提出修复建议和安全策略，为网络管理员完善系统提供重要依据。

注册会计师运用安全扫描器进行扫描的项目主要有：网络端口扫描、系统信息搜集和侦查漏洞、身份认证机制漏洞；拒绝服务攻击设施；防火墙、包过滤及应用程序代理漏洞；包过滤规则确认；WWW、HTTP 和 CGI 漏洞；SMTP、POP、IMAP 及邮件传输漏洞；FTP 安全漏洞；NFS 安全漏洞；RPC 远程过程调用服务；网络协议欺骗；WINGDOWS NT 网络安全漏洞；WINGDOWS NT 信息搜集和侦查；错误配置和系统后门、特洛伊木马检测；硬件外设安全漏洞；其他。通过安全器扫描，一是可以提前警告系统存在的漏洞，从而预防入侵和误用；二是可以检查系统中由于受到入侵或操作失误而造成的新漏洞。进行漏洞扫描，要注意几个问题：

(1)升级问题。发现安全漏洞并不是一个静态的过程，安全专家、黑客都在不停地寻找系统分析、设计、实现及配置中可能存在的问题，新的安全问题不停地出现，这就决定了安全扫描系统必须要有良好的可扩充性和迅速升级的能力。选择产品首先要注意产品能否直接从 INTERNET 升级、升级方法能否被非专业人员掌握，同时要注意产品制造者能否有足够的技术力量来保证对新出现漏洞做出迅速的反应。

(2)可扩充性。对具有比较深厚的网络知识并希望自己扩充产品功能的用户来说，可首选有功能模块或插件技术的产品。这样，用户可以针对自己的应用系统设计专用的扫描模块，使扫描器能更好地满足自己机构的实际安全需要。

(3)局限性。安全扫描系统不是万能的，不能完全依赖它。首先，它不能弥补由于认证机制薄弱带来的问题，也不能弥补协议本身存在的问题。此外，它不能处理所有的数据包攻击，当网络繁忙时无法分析所有的数据流，当系统受到攻击后要进行调查，这些离不开安全专家的参与。

内部审计中人际关系的处理

蒋芝花　张小艳

（长沙理工大学管理学院　长沙　410076）

【摘要】良好的人际关系是确保内部审计工作顺利开展的基本条件。本文就内部审计中人际关系的主要内容、如何建立良好的内部审计人际关系及化解内部审计中人际冲突的方法作些粗浅的探讨。

【关键词】内部审计　人际关系　沟通技巧

一、内部审计中的人际关系

内部审计作为一种独立、客观的监督和评价活动，其目的就是为企业（组织）增加价值并提高自身的运作效率。防弊、兴利、增值是内部审计的基本目标，监督和评价是内部审计的基本职能。为发挥其职能、实现其目标，内部审计必须服务于组织的各个层面，审计的范围包括风险管理、内部控制系统、经济责任制和企业治理结构。这就决定了内部审计人员不可避免地要和企业内外各个层面的人员打交道、碰到如何处理同企业内外各个层面人员的关系问题。为了搞好工作，内部审计人员必须建立和保持良好的人际关系。

首先，内部审计人员必须与组织内相关机构建立和保持良好的人际关系。内部审计工作是在组织内部进行的。它通过监督、评价企业的经营活动，为提高企业的经济效益服务。审计对象的选择、审计证据的收集、对企业报表的审计以及后续审计工作的进行都需要相关机构的配合。只有建立良好的人际关系，才能建立起相互信任的关系，促进彼此的交流与沟通，取得相关机构和人员的理解与配合，及时获得充分、相关、可靠的信息，从而提高内部审计的效率，并确保内部审计意见得到有效的贯彻，实现内部审计的目标。

其次，内部审计人员必须与国家审计机关、本系统上级审计机构和会计师事务所建立和保持良好的人际关系。内部审计是对组织经营活动及内部控制的独立、客观的监督和评价，

---

2. 入侵控制技术。入侵检测是对入侵行为的发觉。它从计算机网络或计算机系统的关键点收集信息进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测技术是根据入侵行为与正常访问行为的差别来识别入侵行为的，根据识别采用的原理不同可以分为异常检测、误用检测和特征检测三种。

进行异常检测的前提是确认入侵是异常活动的子集。异常检测系统通过运行系统或应用层的监控程序将当前主体的活动情况和用户轮廓进行比较来监控用户的行为。用户的轮廓通常定义为各种行为参数及其阈值的集合，用于描述正常行为的范围。当用户活动与正常行为有重大的偏离时即被认为是入侵。如果系统错误地将异常活动定义为入侵，称为错报；如果系统未能检测出真正的入侵行为则称为漏报。

进行误用检测的前提是所有的入侵行为都有可被检测到的特征。误用检测系统提供攻击特征库，当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵。如果入侵特征与正常的用户行为匹配，则系统会发生错报；如果没有特征能与某种新的攻击行为匹配，则系统会发生漏报。

特征检测关注的是系统本身的行为。定义系统行为为轮廓，并将系统行为与轮廓进行比较，对未指明为正常行为的事件定义为入侵。特征检测最大的优点是可以通过提供行为特征定义的准确度和覆盖范围，大幅度降低漏报和错报率。其不足是要求严格定义安全策略，这需要经验和技巧。另外，为了维护动态系统的特征库通常是很耗时的事情。

3. 防火墙技术。防火墙技术是一种安全隔离技术，它通过在两个安全策略不同的域之间设置防火墙来控制两个域之间的互访行为。隔离可以在网络层的多个层次上实现，目前运用较多的是网络层的包过滤技术和应用层的安全代理技术。包过滤技术通过检查信息流的信源和信宿地址等方式确认是否允许数据包通过；而安全代理则通过分析访问协议、代理访问请求来实现访问控制。

防火墙是不同安全域之间信息流通过的惟一出入口，所有双向数据流都必须经过它。注册会计师通过对防火墙的检查和认证，可以检测是否只有被授权的合法数据，只有防火墙中安全策略允许的数据才可以通过，如果该系统具有很高的抗攻击能力，则系统的每个安全域不会受相隔相邻的安全域的攻击，从而限制威胁从一个子网扩散到另一个子网。

通过防火墙测试技术，注册会计师可以分析通过防火墙的数据合法性情况，分析防火墙对非法或未授权数据的隔离情况，从而为进一步评价系统的抗攻击能力和评价系统安全性进一步提供依据。

主要参考文献

段云所，魏仕民，唐礼勇等.信息安全概论.北京：高等教育出版社，2003