计算机科学2002Vol.29№.10

网络技术与企业信息风险控制

Network Techniques and Control Methods of Information Risk in Corporation

黄大勇　姜永德

（重庆工商大学　重庆400067）

Abstract Under the background of great development of network techniques, the information risk in corporation becomes serious. In order to resolve this question efficiently, this paper points out that we should stick to establish better some laws and regulations, invent and apply some safe techniques, manage and control the enterprise efficiently by all means.

Keywords Network technique, Information risk, Internal control, Exterior control

1　引言

随着信息技术与网络的飞速发展，整个社会的生产方式以至思想观念都在经历着一场史无前例的深刻变化，网络化、数据化、知识化已成为时代的主旋律。以微电子技术为基础的信息技术革命以及国际网络的形成和发展，使得信息处理、传递方式等发生了深刻的变化，在企业管理和会计信息系统等方面，网络将领导发展的新潮流，因此对网络条件下企业信息风险的控制也将越来越必要，技术难度和要求也将越来越高。

2　网络条件下信息系统的内部控制

2.1　一般控制

一般控制是对信息系统环境以及数据输入的控制。包括：

2.1.1　操作系统控制　由于操作系统面向所有用户，因此它时刻面临着来自各方面的潜在威胁，包括系统内人员的滥用职权、越权操作和系统外人员的非法访问甚至破坏。要提高操作系统的安全可靠性，除了要尽可能地选用安全等级较高的操作系统产品，并经常进行版本升级外，在管理上还应该采取以下控制措施：第一，是建立计算机资源授权表制度，明确每个用户的安全级别和身份标识，并分别定义具体的访问对象；第二，建立日志审计制度，对运行系统的事件类型、用户身份、操作时间、系统参数和状态以及系统敏感资源进行实时监视和记录；第三，对系统资源进行分类管理，根据用户级别限制系统资源的共享和流动；第四，特权牵制。即由若干个系统管理员和操作员共同管理系统，使其具有完成其任务的最少特权，并相互制约，以提高系统安全可靠性。

2.1.2　数据资源控制　对数据库系统安全的威胁主要来自两个方面：一是系统内外人员对数据库的非法访问；二是由于系统故障、误操作或人为破坏造成数据库的物理损坏。针对上述风险，经济数据资源控制主要可采取以下措施：①合理定义应用子模式。在网络环境下，为了限制合法用户或非法访问者轻易获取全部数据资源，应根据不同的应用项目（功能）分别定义面向用户操作的数据界面，做到需要什么数据，就开放什么数据；②建立数据资源授权表制度，明确每一用户对数据资源访问的范围和内容，并分别规定对数据库的查阅、修改、删除、插入等操作权限；③建立数据备份和恢复制度。即实时对数据进行备份，建立业务日志文件和检查点文件。

2.2　应用控制

2.2.1　计算机操作及其应用的控制　应用控制是指具体的应用系统中用来预防、检测和更正错误，以及处置不法行为的内部控制措施。大部分应用控制措施在系统开发时可直接嵌入软件功能中。这些控制措施可分为三大类：①输入控制。目标是确保网络环境下数据采集的合法性、准确性和完整性；②处理控制。目标是确保数据处理的正确可靠性，包括处理正确性控制、数据一致性控制、预留审计线索控制等；③输出控制。目标是确保信息系统信息输出或传输中没有被遗失、错发、截留，秘密没有被泄漏等，包括打印控制、分发控制、废报告控制、最终用户控制等。

2.2.2　计算机工作中心控制　计算机工作中心控制主要是对系统的物理环境及设备可靠性的控制，目标是确保系统设备能实时地、连续地运转。它主要包括三方面：①计算机工作中心安全控制。包括中心机房结构设置控制、出入机房控制以及电源、防火、防磁、温度、湿度控制等；②服务器系统控制。服务器系统实际上是一种针对网络环境下的多机工作制度，平时各计算机运行各自的应用项目，并保持系统和数据的相互联系，当一台计算机发生故障时，服务器系统中的另一台计算机会立即承担故障计算机的工作和数据的备份，保证了数据的连续性。

2.2.3　组织控制　基于网络条件下的信息系统是一种分布式处理结构，计算机服务功能（工作站）分布于企业内各业务应用部门。因此，计算工作中心对各工作站的控制由原来集中处理模式下的行政控制转变为间接业务控制。其主要内容包括：①工作站点设置控制。合理设置工作站点，并通过操作系统、数据库管理系统实现对各工作站的职责分工控制；②内审制度。设立内审组，监督和控制各工作站的日常运行；③风险管理制度。设立风险评估小组（可由系统分析员、内审人员、主要用户组成），定期对系统进行风险评估、弱点分析，以不断完善会计控制体系；④人事管理控制。实行业务考核制度，对特殊企业（如金融企业等）的重要岗位可实行轮岗制度等。

2.2.4　终端控制　终端可以是单机点，也可以是分服务器站点，它是整个网络系统在某应用项目（如库存管理、成本控制等）下的一个用户界面：终端既是系统日常应用处理（包括数据采集、处理和输出）的端点，也是潜在威胁系统安全的一个入口，因此对终端的控制显得特别的重要。终端控制包括：①终端内部控制。包括终端物理环境控制、操作权限控制、系统存取控制、操作规程控制和故障处理控制等等；②终端对整个系统访问的控制。根据最小特权原则，要严格控制工作站

超越权限的操作行为，这主要可通过计算工作中心的职责分工、授权控制与日常监控来实现。③数据通信控制。终端与计算工作中心常位于不同建筑，甚至不同街区。因此在数据通信过程中，系统面临着因线路和设备故障导致数据丢失、毁坏的风险，以及人为拦截、泄密的风险。为此，需要采取数据加密、回响检查、奇偶检查、备份控制等技术手段和管理措施进行控制。

3 网络条件下的信息风险的外部控制

3.1 安全区域控制

安全区域控制是通过对安全区域的边界实施控制来达到保护区域内部系统的安全性目的，它是一切防外措施的基础。安全区域控制的主要内容包括：

3.1.1 *设置外部访问区域* 访问区域是系统内接待外界（关联方、社会公众）网上数据访问、与外界进行数据交换的逻辑区域。在建立局域网时，要对网络的服务功能和拓扑结构的布局进行详细分析，通过专用软件、硬件、管理措施，实现内部信息管理应用系统与外部访问区域之间的严密的数据隔离、访问限制。

3.1.2 *建立防火墙* 防火墙是指建立在被保护网络周边的分隔被保护网络与外部网络的一种技术系统。根据网络系统区域划分的不同，可设置多级防火墙系统。一般分为两类：一类是外层防火墙，用来限制外界对主机操作系统的访问；第二类是应用级防火墙，用来逻辑隔离内部信息系统与外部访问区域之间的联系，限制外界穿过访问区域对网络应用系统服务器，尤其是对会计数据库系统的非法访问。

3.1.3 *建立周边监控系统* 通过对系统日志和网络数据包的实时监控，实时检测来自外部的入侵行为和内部用户的未授权活动，同时为追究入侵者法律责任提供线索和证据。

3.2 大众访问控制

网上大众访问包括电子邮件传递、网上信息查询等内容。由于网络系统是一个开放的系统，对社会大众的网上行为实际上是不可控的；另外由于网络技术的飞速发展，网络问题也日益突出，如许多恶意的、非法的人通过他们掌握的网络技术进行网络破坏活动。因此，除了加强社会法律威慑作用外，企业也应在自身主要的系统外部访问区域内采取防护控制措施。包括：

3.2.1 *邮件系统控制* 一般将邮件系统限定在外部访问区域的服务器和终端上比较安全；

3.2.2 *网上信息查询控制* 社会大众可在网上查询企业的产品信息、财务报告等内容，这类业务一般也应限制在系统的外部访问区域内。系统要对提供信息的时间、内容作严格规定，并通过安全通道及时更新访问区域上的信息资料。

3.3 电子商务控制

由于电子商务的双方都是在网络的环境下进行交易的，因此会产生很多问题，为了避免发行量减少问题，可采用下列措施对电子商务活动进行管理与控制。

3.3.1 建立与关联方的电子商务联系模式，一般可分为两类：一类是数据浏览型模式，企业通过互联网向外部企业提供数据和条件检查功能，外部企业不能更改数据；另一类是事务处理型模式，交易双方可在网上直接进行电子凭证的交换，并更新双方的事务处理文件，为保证交易信息的安全可靠性，防止被窃取、被仿冒、被篡改，交易双方可对传输信息进行加密处理，对稳定、密切的合作伙伴还可进一步建立虚拟专用网，实现双方（或多方）之间具有相互操作性的数据联系；

3.3.2 建立网上交易活动的授权、确认制度，以及相应的电子文件的接收、签发检证制度；

3.3.3 交易日志记录、审计制度；交易日志用来自动记录电子商务每个步骤的交易时间和内容，对企业内外部来说都是重要的审计线索，企业需要同时也有义务保证它的完整性、可靠性。

3.4 远程处理控制

3.4.1 *分支系统安全模式设计* 分支系统是企业在异地具有独立局域网结构的信息系统，由于母系统的监控和访问直接伸入分支系统内部，而不是在通常的外部访问区域，因此，需要特别考虑由于远程处理给双方增加的风险问题。除了通信技术应采取互联网上的虚拟专用网外，在保证实时监控有效的前提下，分支系统可采取单独设置母系统访问区域的做法，以提高其信息系统的安全可靠性；

3.4.2 *远程处理规程控制* 由于远程实时处理双方一般不是通过系统的外部访问区域连接的，任何一方的安全问题很可能给另一方带来危害，因此，双方要制定严格的远程处理控制操作规程，包括操作权限控制、内容授权控制、处理程序控制、通道及两端服务器安全控制等等。对于需在线实时处理的内容，应在严格的操作规程下进行，确保处理结果的有效性和可验证性。

结束语 信息风险的控制对大到整个社会、一个国家，小到一个单位、企业或者一个部门，重视和建立良好、完善的网络信息风险控制系统是保证经济发展和信息安全的重要保证。当然，除此之外，对于网络信息风险的控制还应当不断提高网络信息产品、大力加强网络安全的立法等方面的工作。另外，基于互联网信息系统的建立为集团型企业实现远程查帐、远程报表、远程审计，以及对交易事项的远程财务监控创造了条件，所以网络信息技术的发展对企业管理理控制系统、会计信息系统、质量安全控制系统等的发展带来了更为广阔的空间。

参考文献

1 余峰. 论会计电话化发展的新趋势——网络财务. 财务与会计，2001(1)

2 郭益和. 会计电算化的特征和内部控制对策. 中国会计电算化，1999(2)

3 张秋宗，等. 基于C/S体系结构的养老保险管理信息系统. 计算工程，1998(1)