

# 会计电算化局域网共享资源的安全管理研究

张克友

(信阳师范学院,河南 信阳 464000)

**摘要:** 通过对会计电算化局域网主要功能和特点的分析,有针对性地提出了会计电算化局域网共享资源的安全管理技术和解决方案。

**关键词:** 会计电算化;共享资源;局域网;安全管理

中图分类号: TP393.08

文献标识码: A

## Safety management research on the shared resource of accounting computerization LAN

ZHANG Ke You

(Xinyang Normal University, Xinyang 464000, China)

**Abstract:** Based on the analysis of the main function and characteristics in the accounting computerization LAN, this paper put forward the safety management technique and solution of the shared resource.

**Key words:** accounting computerization; shared resource; LAN; security management

资源共享是建立单位局域网的基础,通过资源共享,可以减少财务运行成本,提高单位的总体效益。为了提高财务工作的效率,财务管理部门一般都建立起会计电算化局域网。会计电算化局域网的共享资源一般是单位的信息资源,主要包括数据库资源和文件资源。由于共享资源涉及到单位的核心机密,因此,各企业发布的共享资源应限制在一定的层次上,既能满足单位内部的资源需求,又能保证单位信息资源的安全。

资源共享作为会计电算化局域网中最常见的应用,在享受共享带来的便利时,很多人都在为资源的安全管理而发愁。例如,怎样才能让共享资源不被有意无意地删除?怎样让资源只有使用特定用户名才能访问到?鉴于此,笔者根据多年管理会计电算化局域网的经验,通过对会计电算化局域网的综合分析,利用会计电算化局域网中的现有资源进行设计,较好地实现了会计电算化局域网共享资源的安全管理。

### 1 会计电算化局域网的综合分析

#### 1.1 会计电算化局域网的主要功能

与利用单机进行会计核算工作相比,组建会计电算化局域网具有明显的优点,主要表现在以下几个方面:

#### (1) 共享软、硬件资源,节约资金投入

如果是单机操作,每台计算机可能要同时配备光驱、打印机等设备,这样重复投资,造成了资金的浪费。而组建网络后,在一个办公室或一个部门内部可以只配备1台打印机和扫描仪,其他计算机可以通过网络共享这些设备,不仅节约成本,而且提高了设备的利用率;另外,一些办公软件只需要购买1份,其他计算机可以通过网络进行共享,减少了经费支出;对于一些小型办公室,多台计算机可以共享1个帐号接入因特网,减少了上网费用。

#### (2) 可实现对重要数据的安全管理

网络的一个重要特点是资源共享,而资源共享就可以实现对数据的统一管理。一些重要的数据集中存放在专门的一台计算机(如网络服务器)上,只需要对这一台计算机采取一定的安全管理措施(如进行磁盘镜像、网络自动备份等),就可以保证重要数据的安全性,防止数据因系统产生故障而丢失。从安全使用的角度看,可以对一些重要数据设置安全访问权限,不同的用户可以根据不同的设置权限使用数据,避免了单机操作时的不安全性。

### (3) 可进行网络的远程访问

办公网络还应提供远程访问的功能,其他部门的计算机可通过电话线进行远程访问,形成一个更大范围的网络。例如,当出差在外时可通过远程访问功能登录到单位的网络,从网络上调用所需要的资料,或将一些重要文件传送到单位的计算机上。而且还可以通过网络进行远程对话,对一些重要内容进行“面对面”的交流。

### 1.2 会计电算化局域网的特点

由于会计电算化局域网在功能及使用者方面与在家庭、网吧、校园等地局域网的应用有所不同,因此具有一些自己的特点。

#### (1) 具有较高的网络安全性和稳定性

会计电算化局域网对安全性和稳定性方面的要求较为严格。在同一时刻可能有多个用户访问某一数据,而且有部分用户可能在进行数据的写入操作,如果此时发生网络连接故障,则可能使得一些重要数据丢失。为了避免这种现象发生,要求会计电算化局域网具有较高的安全性和稳定性。一个网络如果在安全性和稳定性方面得不到保障,由此造成的损失可能要比单机操作更为严重。

#### (2) 便于进行协同操作

一些部门的工作具有突击性,经常需要对某一事务进行突击处理。例如,上级主管部门可能要求单位对有关的人事档案进行分类汇总,并将结果在短时间内上报。这时就需要大家一起对这项任务进行协同处理,用最短的时间解决最多的问题。利用计算机网络,能够方便地对同一事务进行协同操作,以应付诸如此类突击性的工作。

#### (3) 有利于提高工作效率

网络的应用减少了日常工作中的许多环节,例如,当完成一份文件的起草后可以直接发送到主管领导的计算机上;当对某一问题需要讨论时,可直接在网络上进行,并可自动将讨论结果记录下来,减少人与人之间的直接接触,便于问题的公正解决;当需要使用别人计算机上的某些文件时,可以通过网络直接调用,不需要使用磁盘进行拷贝,在提高效率的同时,也避免了一些错误的发生。

## 2 会计电算化局域网共享资源的安全技术

### 2.1 关闭系统默认的共享资源

电脑系统要进行卓有成效的防范,最彻底的办法就是在计算机中关闭这些特殊共享资源。要禁止这些共享,打开“管理工具”→“计算机管理”→“共享文件夹”→“共享”,在相应的共享文件夹上按右键,点“停止共享”即可。但是,计算机重新启动后,这些共享又会重新开启。如果每次开机都要如此操作一番,很麻烦。按照下面的方法就可以避免每次开机都要进行的重新操作。

#### 2.1.1 批处理命令法

先用记事本编辑如下一个文件,共6行,分别为 net share cdefg\$ / del, net share c\$ / del, net share d\$ / del, net share e\$ / del, net share f\$ / del 和 net share g\$ / del,然后将它保存为 delshare.bat。注意:这个文件是假设您的计算机有 C、D、E、F、G 5 个分区,如果您的计算机只有 C、D、E 3 个分区,则上述文件中可删去 net share f\$ / del 和 net share g\$ / del 2 行。最后将该文件或其快捷方式放到 C:\Documents and Settings\All users\ Start Menu\ Programs\ 启动文件夹中即可。重启计算机时即可开机自动关闭这些特殊共享资源。

#### 2.1.2 注册表法

打开注册表中的“HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\Current Version \Run”分支,在其下新建“字符串值”,命名可随意,比如“delshareC\$”,鼠标右键单击“修改”,在接着出现的“编辑字符串”窗口的“数值数据”栏中输入“net shareC\$ /del”(不包括引号)按“确定”按钮。同样可添加“字符串值”如“delshareD\$”,“数值数据”为“net shareD\$ /del”等,机器有几个分区直到加完为止。之后保存注册表,重启计算机后也能实现开机自动关闭这些特殊资源。

### 2.2 在局域网中“隐身”——隐身术

在会计电算化局域网内,不同计算机之间要查看本机之外的财务信息数据和文件,必须将所在的文件夹设为“共享”。但是,一旦将文件夹共享之后,局域网内所有的计算机都可以在网上邻居中看到这个共享的文件夹了,如果只让部分需要访问这个文件的用户访问,而不让其他不相关的用户打开文件,其办法就是隐身。

#### 2.2.1 隐藏文件夹

要想其他用户无法通过网上邻居直接来访问某个文件夹,可以将其“隐藏”起来,具体方法如下:

右击文件夹图标,选择弹出快捷菜单中的“共享和安全”,在打开的窗口中选择“共享”标签,选择“共享该文件夹”,在“共享名”后面的文本框中输入共享文件夹名并在文件夹名后添加 1 个半角的“\$”字符,最后单击“确定”保存设置。如果没有在上面的窗口中给共享文件名添加“\$”符,也可以右击该共享文件夹,选择“重命名”,将这个共享的文件名称后添加 1 个半角的“\$”符(比如“CW\$”)。以后,其他用户打开网上邻居时,在网上邻居列表中将不会看到该共享文件夹了。

如果希望某个用户去访问你的这个共享文件夹,只要告诉他这个共享文件夹的绝对路径即可,此路径为“你的计算机 CW\$”,只要将其输入到资源管理器的地址栏中并回车即可访问了。需要注意的是,后面的“\$”是必不可少的,如果少了该字符访问将不成功。

#### 2.2.2 隐藏自己的计算机

上面的方法是在局域网内隐藏一个特定的文件夹,

## 网络与通信 Network and Communication

如果想将自己的计算机也隐藏起来,安全系数就更高:

单击“开始”→“运行”,在打开的“运行”对话框中输入“cmd”,打开命令行窗口,输入“net config server / hidden:yes”,再回车就可以了。这样,别人就无法从网上邻居中直接看到你的计算机,只有通过资源管理器地址栏中输入“计算机名”才能访问你的计算机。不过,上面的方法只能对当前有效,以后每次重新启动系统都要重新运行该命令。

如果希望将自己的计算机从网上邻居中永久隐藏,可以通过修改注册表来达到目的:打开注册表编辑器,在左侧窗口中展开“HKEY\_LOCAL\_MACHINESYSTEM-CurrentControlSet-ServerslanmanserverParameters”,在右侧窗口中找到 DWORD 类型值改为“1”,按 F5 刷新注册表即可。

### 2.3 让共享资源更安全

现在很多朋友都是通过局域网连接上网,常常遇到这样的情况:自己没有运行什么文件,而硬盘灯突然闪烁不停,这就是其他人在访问你机器上的共享文件,到底是谁访问了你的电脑,如何才能增强系统共享资源的安全性呢?下面就以 Windows XP 为例介绍几种增强 Windows XP 共享资源安全性的方法。

#### 2.3.1 使用“计算机管理”工具找出“窃密者”

在 Windows 2000/XP 中,网络监视器不再监测访问本机的连接情况,但可以使用“计算机管理”来进行监视。单击“开始”→“设置”→“控制面板”,双击“管理工具”,再双击“计算机管理”,依次展开“共享文件夹”,下面共有 3 个选项:“共享”、“会话”和“打开文件”。

(1)共享:显示当前系统的共享资源,在这里可以创建设置共享及其权限。

(2)会话:显示当前来访者的用户名、IP 地址、打开的文件数以及访问时间等基本信息。在用户名上单击右键,还可以断开恶意来访者的连接。

(3)打开文件:显示所有来访者及其打开的文件,如果不希望对方浏览你的文件,则单击右键,在弹出菜单中可以关闭其中 1 个或所有打开的文件。

通过以上方法就能快速查看到是谁在窃取秘密,并迅速采取行之有效的措施来应对。

#### 2.3.2 修改组策略指定特定用户访问

由于共享资源在默认状态下是所有用户都可以访问的,这增加了潜在的危险性。但可以通过修改组策略来指定特定的用户才有权限访问共享资源。具体操作如下:

(1)依次点击“开始”→“运行”,在“运行”框中输入“gpedit.mse”,打开组策略设置界面。

(2)依次点击“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权利指派”,在右侧窗口中找到“从网络访问此计算机”项。

(3)双击“从网络访问此计算机”在弹出的窗口中点击“添加用户或组”来添加可以访问你共享资源的用户,当然也可以点击“删除”按钮来删除你不信任的用户。这样,就可以设置只让特定的用户访问你的共享资源了。

#### 2.3.3 禁止非法用户访问共享资源

(1)采用上面的方法打开组策略设置窗口后,依次打开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”,在右侧窗口中找到“设备:只有本地登录的用户才能访问 CD-ROM”项。

(2)双击该项,从弹出的窗口中勾选“已启用”,然后点击“确定”即可,这样局域网内的其他用户就不能访问你的光驱了。

(3)使用同样的方法,你还可以启用“设备:只有本地用户才能访问软盘”等选项,具体操作方法是相同的,这里不再介绍。

经过以上的几种方法,不需要任何的第三方工具软件,共享文件已经比较安全了。

### 3 网络共享资源不能互访的解决措施

网络提供了丰富的共享资源,但访问这些资源时却会经常出现“拒绝访问”或“权限不足”的错误提示信息,特别是在 Windows 工作组环境中,很难有效地对客户机的用户账号和访问权限进行管理。此外,网络中不同版本的 Windows 操作系统共存,网络防火墙配置不当,也是出现以上问题的主要原因。

#### 3.1 问题的产生

##### 3.1.1 访问权限设置不当

Windows NT/2000/XP/2003 系统支持 NTFS 文件系统,采用 NTFS 可以有效增强系统的安全性,但在访问控制列表(ACL)中对用户访问控制权限设置不当时,也会导致用户无法访问本机共享资源,出现“权限不足”的提示信息。

##### 3.1.2 账号和策略设置不当

在 Windows 工作组环境中,一般情况下,用户要使用 Guest 账号访问共享资源。但为了系统的安全,禁用了本系统的 Guest 账号。此外,在 Windows 2000/XP/2003 系统中,组策略默认是不允许 Guest 账号从网络访问这台计算机的,这样就导致其他用户无法访问本机的共享资源,出现“拒绝访问”的提示信息。

##### 3.1.3 网络防火墙设置不当

用户为了增强本机的安全性,防止非法入侵,安装了网络防火墙。但对网络防火墙设置不当,同样会导致其他用户无法访问本机的共享资源,出现“拒绝访问”的提示信息,这是因为防火墙关闭了共享资源所需要的 NetBIOS 端口。

#### 3.2 问题的解决

了解共享资源不能成功互访的主要原因后,就可以着手解决访问中出现的问题。

## 网络与通信 Network and Communication

### 3.2.1 启用 Guest 账号

在很多情况下,为了本机系统的安全,Guest 账号是被禁用的,这样就无法访问该机器的共享资源,因此必须启用 Guest 账号。

以 Windows XP 系统为例,在共享资源提供端,进入“控制面板”→“管理工具”后,运行“计算机管理”工具,接着依次展开“计算机管理(本地)”→“系统工具”→“本地用户和组”→“用户”,找到 Guest 账号。如果 Guest 账号出现一个红色的叉号,表明该账号已被停用,右击该账号,在 Guest 属性对话框中,去除“账号已停用”的钩选标记,单击“确定”后,就启用了 Guest 账号。此方法适用于 Windows 2000/XP/2003 系统。

使用 Guest 账号访问共享资源存在很大的安全隐患。不过可以为每个访问用户创建一个指定的账号:首先,在共享资源提供端创建一个新的账号,然后指定该账号的访问权限;最后,在要访问该共享资源的客户机中新建一个相同用户名和密码的账号,使用此账号登录客户机后,就能正常访问该账号所允许的共享资源。此方法较为安全,但要为网络中每个用户创建一个账号,不适应规模较大的网络。

### 3.2.2 修改用户访问策略

有时,虽然启用了本机的 Guest 账号,但用户还是不能访问本机提供的共享资源,这是因为组策略默认不允许 Guest 账号从网络访问本机。可采用下面的方法:

单击“开始”→“运行”,在运行框中输入“gpedit.msc”,在组策略窗口中依次展开“本地计算机策略→计算机配置→Windows 设置→安全设置→本地策略→用户权利指派”,在右栏中找到“拒绝从网络访问这台机器”项,打开后删除其中的 Guest 账号,接着打开“从网络访问此计算机”项,在属性窗口中添加 Guest 账号,这样就能使用 Guest 账号从网络中访问该机的共享资源了。此方法适用于 Windows 2000/XP/2003 系统。

### 3.2.3 正确配置网络防火墙

很多机器都安装了网络防火墙,若设置不当同样会

导致用户无法访问本机的共享资源,这时就要开放本机的共享资源所需的 NetBIOS 端口。以天网防火墙为例,在“自定义 IP 规则”窗口中选“允许局域网的机器使用我的共享资源”规则,最后点击“保存”按钮,这样就开放了 NetBIOS 端口。

### 3.2.4 合理设置用户访问权限

网络中很多机器使用 NTFS 文件系统,它的 ACL 功能可以对用户的访问权限进行控制,用户要访问这些机器的共享资源,必须赋予相应的权限。如使用 Guest 账号访问该机器的 Temp 共享文件夹,则右击该共享目录,选择“属性”,切换到“安全”标签页,然后将 Guest 账号添加到用户列表中,接着指定 Guest 访问权限,至少要赋予“读取”和“列出文件夹目录”权限。如果想让多个用户账号访问该共享目录,只需要添加 Every 账号,然后赋予“读取”和“列出文件夹目录”权限即可,这样就避免逐一添加和指定每个用户访问账号。此方法适用于采用 NTFS 文件系统的 Windows NT/2000/XP/2003 系统。

由于针对会计电算化局域网资源共享的设计是一项巨大的系统工程,它不仅涉及顶尖的操作系统设计技术、软件技术、加密技术等,而且需要大量的人力、物力的投入。本文主要是提出了会计电算化局域网共享资源的安全管理问题,针对网络操作系统、会计电算化局域网及其内部共享资源的特点,提出了具体的解决方法。但是,上述方法并不能保证会计电算化局域网的共享资源万无一失,还要根据实际工作中的应用情况,比如少量的财务信息可以采取移动硬盘(或 U 盘)进行文件的备份和传递,从而达到资源共享又保证安全的目的。

#### 参考文献

- [1] 帅仕麟.保护好 XP 上的共享资源[J].网络与信息,2004(9):102.
- [2] 赵炜,张浩.局域网系统的安全性研究[J].计算机工程与应用,2002(4):28-30.

(收稿日期:2009-04-08)