**网络的最大优点开放性与共享性恰恰是对安全性要求较高的会计网络的最致命的弱点**

**早该帮 编制**

网络的最大优点开放性与共享性恰恰是对安全性要求较高的会计网络的最致命的弱点。由于在网络会计中起主要关键作用的是计算机，因此审计人员应该根据自己处理传统舞弊案件的经验，较透彻地分析计算机舞弊手法，努力检查并处理计算机犯罪事件，针对不同的情况，运用相应的审计手段。

一、计算机舞弊分析

（一）篡改输入

这是计算机舞弊中最简单最常用的手法。数据在输入前或输入后被篡改了。它通常表现为：虚构业务数据，如将假存款单输入银行的系统中，增加作案者的存款数；修改业务数据；删除业务数据，如从存货系统中删除某个存货数据，消除购货业务凭证。通过对数据作非法改动，导致会计数据的不真实、不可靠、不准确或以此达到某种非法目的，如，转移单位资金到指定的个人账户等。

可能的舞弊者包括：参与业务处理的人员、数据准备人员、源数据提供人员、能够接触计算机但不参与业务处理的人员。

可能的证据包括：源文件、业务文件、计算机可读文件、磁盘、磁带、异常报告、错误的运行结果等。

（二）窃取或篡改商业秘密、非法转移电子资金和数据泄密等

窃取或篡改商业秘密是系统非法用户利用不正常手段获取企业重要机密的行为。借助高技术设备和系统的通讯设施非法转移资金对会计数据的安全保护构成很大威胁。

1、数据在传输过程中，由于使用的是开放式的TCP/IP协议，信息的传输路线是随机的。因而可能出现物理窃听、感应窃听、口令字试探、信息窃取、身份假冒。

2、数据在输出过程中，舞弊者能够把敏感数据隐藏在本来没有问题的输出报告中，采取的方法是增加数据块；控制并观察设备部件运转，如磁带的读和写，打印机打印和跳跃行次的结构所发出的响音，录在磁带上，可以得到二进制信息。

3、采取设备上的特殊配置，可以在CPU芯片中置入无线发射接受功能，在操作系统、数据库管理系统或应用程序中预先安置用于情报收集、受控激发破坏的程序。

可能的舞弊人员除了篡改输出报告为内部用户外，其他多为外来者，更多的是间谍人员。

（三）篡改程序

篡改程序是指对程序做非法改动，以便达到某种舞弊的目的。常见的手法有“陷门”和“特洛伊木马”。

1、陷门

从CPU、操作系统到应用程序，任何一个环节都有可能被开发者留下“后门”，即“陷门”。陷门是一个模块的秘密入口，这个秘密入口并没有记入文档，因此，用户并不知道陷门的存在。在程序开发期间陷门是为了测试这个模块或是为了更改和增强模块的功能而设定的。在软件交付使用时，有的程序员没有去掉它，这样居心不良的人就可以隐蔽地访问它了。

2、在系统中秘密编入指令，使之能够执行未经授权的功能，这种行为叫特洛伊木马。典型的特洛伊木马是窃取别人在网络上的账号和口令，它有时在合法用户登陆前伪造登陆现场，提示用户输入账号和口令，然后将账号和口令保存到一个文件中，显示登陆错误，退出特洛伊木马程序。用户以为自己输错了，再试一次时，已经是正常的登陆了，用户也就不会怀疑。而特洛伊木马已经获得了有价值的信息躲到一边去了。

可能的舞弊者绝大部分是计算机高手，包括系统管理员、网络管理员、系统操作员、网络黑客等。

可能的证据包括：源文件、数据库文件。

二、计算机舞弊的审查

对计算机舞弊的审查除了借鉴传统审计方法，如：分析性复核，审阅与核对法，盘点实物，查询及函证外，最有效的是根据网络会计系统的特点有针对性地进行审查。

（一）篡改输入的审查

1、应用传统方法审查手工记账凭证与原始凭证的合法性。首先，审计人员应抽查部分原始单据，重点使用审阅法确定业务发生的真实性，判断原始单据的来源是否合法，其数据有无被篡改，金额是否公允等。其次，采用核对法，将记账凭证的内容和数据与其原始单据的内容和数据进行核对，审查计算机处理的起点是否正确。最后再进行账账核对。

关键词：网络、的、最大、优点、开放、开放性、与、共享、共享性、恰恰、是、对、安全、安全性、要求、较、高、的、会计、网络、的、最、致命、的、弱点

参考文献：[1]早该帮https://bang.zaogai.com/item/BPS-ITEM-28466.html