全国财会人员后续教育教材



# 财会人员计算机安全知识读本

CAIKUAI RENYUAN JISUANJI ANQUAN ZHISHI DUEBEN

本书编写组编著

中国财政经济出版社

全国财会人员后续教育教材

# 财会人员计算机安全知识读本

CAIKUAI RENYUAN JISUANJI ANQUAN ZHISHI DUEBEN

本书编写组编著

中国财政经济出版社

**图书在版编目（CIP）数据**

财会人员计算机安全知识读本/《财会人员计算机安全知识读本》编写组编.
—北京：中国财政经济出版社，2003.11
ISBN 7-5005-6843-6

Ⅰ.财… Ⅱ.财… Ⅲ.会计—安全—技术 Ⅳ.F232

中国版本图书馆 CIP 数据核字（2003）第 099426 号

中国财政经济出版社 出版

URL：http://www.cfeph.com.cn
E-mail：cfeph@drc.gov.cn

社址：北京海淀区阜成路甲 28 号 邮政编码：100036
发行处电话：88190406 财经书店电话：64033436
北京财经印刷厂印刷 各地新华书店经销
787×1000 毫米 16 开 19.5 印张 320 000 字
2003 年 12 月第 1 版 2003 年 12 月北京第 1 次印刷
印数：1—3 000 定价：32.00 元
ISBN 7-5005-6843-6/F·5977

# 前　言

计算机信息安全，是一个涉及国家安全、社会公共安全和公民个人安全的重大课题。随着会计电算化的普及，特别是网络技术与会计电算化技术的融合，会计业务操作的电算化、网络化已成为行业发展的重要特征。但是，计算机病毒、网络入侵、“黑客”攻击也日益成为威胁会计行业计算机信息安全的主要问题。仅以计算机病毒为例，今年出现的计算机新病毒不仅数量远远超过往年，而且病毒越来越狡猾、破坏力越来越强。特别是席卷世界范围的“别惹我”、“冲击波”、“大无极 F”、“斯文”、“小邮差”、“高波”等病毒的大规模疫情，不仅导致许多单位信息网络和重要计算机系统的瘫痪，而且造成了全球商业界的数百亿美元的直接经济损失。据公安部公共信息安全监察局最新公布的数据显示，本年度我国计算机用户感染计算机病毒的比例就高达 85．57%。

与此同时，近年来针对财政、金融、证券部门的计算机犯罪正在逐年增加，危害的程度越来越严重，损失越来越大。向广大财会人员普及计算机信息安全常识，防患于未然，已经成为我国财会人员后续教育的重要内容。

目前市面上针对普通用户的计算机信息安全知识读本很少，面向财会人员的更是空白。为此，我们策划了本选题，并邀请了财政部信息中心的计算机专家和高校教师等成立了本书的编写组，编撰本书。他们根据广大财会人员计算机使用的实际，由浅入深介绍了计算机信息安全的基本常识和概念，并针对会计电算化涉及的计算机信息安全问题，提出了实用、简单的应对措施，用大量生动的实例提示财会人员加强计算机信息安全意识的必要性和重要性。本书可以作为各地财会人员电算化培

训的配套教材，也可以作为大中专财政、会计专业学生的选修课教材。

本书在策划、编写过程中，也曾向财政部会计司、国务院机关事务管理局等有关的主管部门征求意见，得到他们的支持和鼓励。财政部信息中心的饶望平、丁刚、王斌同志，北京石油管理干部学院彭宏韬同志，中国财政经济出版社王坚敏、王军同志，直接参加了本书的策划和编写工作。在此向他们表示最衷心的感谢。

由于计算机信息安全技术日新月异的发展，本书不可能完全概括该领域目前的最前沿问题和技术成果，这只能在以后的修订过程中予以弥补，敬请广大读者谅解并对书中的不当之处批评指正。

编　者

2003 年 11 月于北京

# 目　录

# 第一章
# 概　述

**内容提要：**计算机网络安全方面出现的大量案件，时时提醒人们网络信息安全的重要性。对会计人员而言，那些危言耸听的事件是否会在他们面前发生？本章着笔信息安全问题产生的背景，详细介绍信息安全的概念和信息安全问题产生的原因，分析了计算机黑客通过 Internet 攻击主机的手段，阐述了向会计人员普及以计算机网络安全为主要内容的信息安全知识的重要意义。

计算机网络尤其是国际互联网（以下简称“Internet”）的应用正在引发人类历史上一场根本性变革，伴随而来的网络信息安全问题也日益成为全世界所共同关心的重要问题。目前由网络安全问题引发的事件枚不胜举，国家、企业和个人随时都有遭受网络攻击或计算机病毒侵扰的危险，下面仅举两例予以说明。

**〔案例 1.1〕**

2001 年 5 月，国际间曾经出现一次网络黑客大战。其间，中国的一些政府网站、商业网站，例如江西宜春政府网、西安信息港、贵州方志与地情网、中国青少年发展基金会网、福建外贸信息网、湖北武昌区政府信息网以及桂林图书馆、中国科学院理化技术研究所、中国科学院心理研究所等近 1000 家网站遭到攻击，一些大型门户网站也相继被攻击。据可靠消息透露，这是近年来中国网络安全受到的最严重的挑战。而美国被攻击的网站总数多达 1600 个，其中政府网站占 72%，包括美国白宫、美国劳工部、卫生部等重要政府网站。

〔案例 1.2〕

近几年，中国人民银行系统发生了多起利用计算机处理系统的安全漏洞作案的犯罪案件，造成国库资金损失，严重损害了人民银行及国库部门的形象。这些案件已引起各级部门的高度重视。而且，中国人民银行总行、武汉分行等相继下发了《人民银行关于国库会计核算管理与操作的规定》、《关于加强国库案件防范工作的实施意见》，进一步强调国库业务的规范化操作，明确了国库安全防范工作的重要性、必要性和紧迫性。

在会计人员中普及计算机网络应用及会计信息系统安全常识，提高会计人员在使用计算机时的安全防范意识，是适应在高速发展的计算机及 Internet 下实现会计信息化的一个极其重要的保证，也是本书所要论述的主要内容。

## 1.1 信息安全问题的产生背景和原因

随着计算机技术，尤其是网络技术的发展，全球网络化的热潮正日益广泛而深刻地改变着整个社会的行为和面貌。Internet 的普及使众多商家看到了大量的机会，他们纷纷开展电子商务、在线交易等各种经营和网络服务。然而同时，面对计算机网络上进行政治、经济、商务、娱乐等活动而带来的巨大的社会和经济利益，越来越多的不法分子跃跃欲试，企图从网络信息中取得政治、经济情报，或从网络交易中窃取钱财，计算机犯罪活动的势头在上升。据统计，我国计算机网络上的各类违法行为正以每年 30% 的速度递增。在许多国家，信息安全已经等同于军事安全、经济安全而成为国家安全中重要的一环。那么，究竟什么是信息安全呢?

从广义上讲，本书所讲的信息安全是指电子信息的真实性、保密性、完整性、可用性、可控性和不可否认性。综合起来说，就是要保障信息的有效性。所谓保密性，就是保证信息不泄漏给他人；真实性和完

整性，就是保证信息是真实的，并防止信息被他人篡改；可用性，就是保证信息及信息系统确实可为自己所用；可控性，就是对信息及信息系统实施安全监控；不可否认性，就是保证信息的使用者或拥有者无法否认其使用过信息或拥有信息。

保证信息安全，就必须保证信息的存储安全、使用安全和通信安全。对于电子信息而言，保证计算机、网络系统及存储设备的使用安全及运行安全，是信息安全的核心内容。因此，为了研究信息安全，首先应研究计算机网络系统的安全。

计算机网络系统安全，是指计算机网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，使系统能连续、可靠、正常地运行，并保证计算机网络系统中信息的可靠性、可控性和可用性。

开放性和资源共享是计算机网络系统得以广泛应用的主要原因，但同时也是产生计算机网络安全问题的主要根源。

### 1.1.1 影响计算机网络系统的不安全因素

影响计算机网络安全的因素很多，有人为因素，也有自然因素，而以人为因素的危害最大。归结起来，对计算机网络安全的威胁主要来自三个方面：

- 人为的无意失误。如操作员安全配置不当造成的安全漏洞；系统管理员不合理地设定资源访问控制，一些资源就有可能被偶然或故意地破坏；用户安全意识不强，口令选择不慎，或者用户将自己的账号随意转借他人或与别人共享等。这些失误都会给网络安全带来威胁。

- 人为的恶意攻击。这是计算机网络所面临的最大威胁，恶意的攻击和计算机犯罪就属于这一类。此类攻击又可以分为两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性，这是一种纯粹的信息破坏，这样的网络侵犯者被称为积极侵犯者。积极侵犯者截取网上的信息包，并对其进行更改使其失效，或者故意添加一些有利于自己的信息，起到信息误导的作用；或者登录进入系统使用并占用大量网

络资源，造成资源的消耗，损害合法用户的利益。积极侵犯者的破坏作用最大。另一类是被动攻击，它是在不影响网络正常工作的情况下，通过截获、窃取、破译等手段以获得网络用户的重要机密信息。这种仅窃听而不破坏网络中传输信息的侵犯者被称为消极侵犯者。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏。

• 网络软件的漏洞和“后门”。任何网络软件都不可能百分之百无缺陷、无漏洞，而软件中的漏洞和缺陷恰恰是黑客进行攻击的首选目标。从已经发生的黑客攻入网络内部事件统计看，大部分案件都是因为网络软件有漏洞，才导致安全措施不完善所招致。所谓“后门”，是指软件编程人员为了便于调试程序，在程序中设置的非常规运行方法。“后门”一般不为外人所知，但一旦“后门”洞开，造成的后果将不堪设想。

由于网络上存在的诸多不安全因素，使得网络使用者必须采取相应的网络安全技术来堵塞漏洞和提供安全的通信服务。如今，快速发展的网络安全技术已经可以从不同角度来保证网络信息不受侵犯。网络安全的基本技术主要包括网络加密技术、防火墙技术、网络地址转换技术、操作系统安全内核技术、身份验证技术、网络防病毒技术等。

### 1.1.2 国际互联网的不安全因素

• 操作系统本身的问题。无论是 Windows95、NT 还是各种 Unix 系统，都存在一些缺陷（Bug）。例如，1998 年 3 月初美国发生了一起严重的黑客袭击事件，数千台使用 Windows95 和 NT 的计算机遭到黑客攻击后造成临时瘫痪。其中，威斯康星大学计算机实验室 160 台 NT 工作站中的 145 台瘫痪。同时遭袭的还有麻省理工大学、西北大学、明尼苏达州立大学和加州大学伯克利、爱尔文、洛杉机与圣地亚哥分校。如此大规模的袭击让专家们感到非常震惊。调查结果表明，黑客使用了一种名为 TearDrop2 的工具，它的原理很简单，就是不间断地向工作站或者服务器发射有错误的 UDP（用户数据包协议）包，由于 Windows 不像 Unix 那样将这些坏包丢弃，而是被粘住——它总是企图对这些包进行诊断，结果导致死机。

• 各种应用服务存在安全问题。Telnet、Ftp、NFS、RPC、Rlogin、X11、DNS、Sendmail、Web 等都有安全问题。例如：Telnet（在 Internet 上普遍采用的登录网络的间隔仿真协议），FTP（文件传输协议）协议在用户认证时，Password（口令）以明文方式传送；X11 的纯文本可能泄漏，终端可能被接管，键盘输入被窃取；Web 服务器很难配置安全，CGI Scripts 也不安全等等。

• TCP/IP（传输控制协议/网际协议）协议在设计时主要考虑数据传输的可靠性和完整性，对于安全因素几乎没有考虑。

• 攻击可能来自 Internet 上的任何一个地方。它可以是匿名攻击，狡猾的黑客（Hacker）可以销毁证据，因此 Trace Back 非常困难。

• 对于一组相互信任的主机，其安全程度由最弱的一台主机决定。一个薄弱环节被攻破，则会殃及其他主机。

• 黑客的挑战。对黑客的攻击手段进行分析，发现有以下攻击步骤：

1）信息收集。可以通过以下方法：

☞ SNMP（简单网络管理协议）协议：可以获取路由表，了解网络拓扑结构。

☞ TraceRoute 程序：能够得出到达目标主机所经过的网络和路由器。

☞ DNS（域名系统）：获得 IP 地址和对应的域名。

☞ Finger 协议：得到目标主机上的用户详细信息。

☞ Ping（操作系统中检查网络连接的命令）：确定目标主机是否可达。

2）探测安全漏洞。在获得目标网段足够的信息后，黑客使用一些探测工具寻找目标网段的安全漏洞，水平较高的黑客可以自己编一些程序，更多的黑客则使用一些公开的安全扫描程序。下面介绍两个比较著名的安全探测工具：

ISS（Internet Security System）的 Internet Scanner SAFEsuite，它代表了网络安全测试工具的发展水平。ISS Internet Scanner SAFEsuite 是一

个综合的网络安全评估工具，能够检查、纠正、监视网络安全的许多方面。它由四部分构成：Web Security Scanner（Web 安全性扫描）、Firewall Scanner（防火墙扫描）、Intranet Scanner（企业网扫描）和 System Security Scanner（系统安全扫描），分别用来检查从 UNIX、Windows95、Windows NT servers、workstations 到 web sites、防火墙等方面的安全漏洞。它是一个商业软件，且购买的软件只能在预先登记的地址范围内使用。

SATAN（Security Analysis Tool for Auditing Networks），它是专门针对 Unix 操作系统的著名的网络安全测试工具，由 Wietse Venema（荷兰爱因霍温大学）和 Dan Farmer（美国加州大学）合作开发。它根据用户设定的初始目标和探测级别，通过主机间信赖关系的传递性自动推理出一定范围内的信赖关系网，然后沿着该信赖关系网检查诸如 finger、NFS、NIS、ftp、tftp、rexd 以及其他一些网络服务来搜集目标主机和网络的信息。这些信息既包括目的站点或网络所提供的服务，也包括潜在的各种安全漏洞。这些漏洞通常是由于服务配置不当或系统中的 bug 所造成的。探测结果以 HTML 文件的形式给出，用户可以通过浏览器如 Netscape 查询、分析探测结果。SATAN 的功能没有 ISS 的 SAFEsuite 强大，但它完全免费，且提供源码。该软件在制作时留有扩充的余地，Wietse 还专门写了一些文章告诉人们如何扩充。

虽然这些安全分析工具常常被黑客用来攻击目标系统，但是管理员也可以利用安全分析工具找出网络里的安全漏洞，防患于未然。这也是开发安全分析工具的真正目的。特别是在瞬息万变的网络环境下，只依靠网络管理员或系统管理员的手工检查很可能由于工作量过大或缺乏全面性而难以实施。只有依靠网络安全的测试工具随时检查网络中的潜在的漏洞并及时补漏，才能保证网络的安全。

3）实施攻击。入侵者根据探测的结果对目标系统实施攻击。在获得目标主机上的访问权限后，可能接着做以下工作：

- ☞ 销毁原始攻击的痕迹，在受损系统中建立一个新的更隐蔽的后门（受损系统上的安全漏洞，在原始攻击被发现之后，攻击者可以利用它来继续访问该系统）。

☞ 在受损系统中安装安全探测器、特洛伊木马来收集账号名和口令。然后利用这些信息攻击目标网络上的其他主机。

☞ 寻找与受损系统有信任关系的主机加以攻击。

☞ 窃取数据文件，或进行其他破坏活动。

### 1.1.3 计算机安全与会计信息安全

计算机安全的主要内容是保证计算机及操作平台、应用软件正常运行，保证所存储、使用的信息的安全。所以，计算机安全常识必然包括如何保护计算机的外部环境安全；如何安全地运行应用系统并能正确地应对自然灾难及计算机故障；如何保证用户既能发挥计算机及网络系统的开放性和资源共享的优势，又能了解其弱点和危险性以规避应用风险等内容。从这个意义上讲，向会计人员介绍计算机及网络使用过程中的安全常识，正确分析所使用的会计软件的安全防范措施，对提高会计人员的计算机应用水平，普及计算机及网络系统的安全知识非常必要。

此外，会计人员最关心的是会计信息安全。所谓会计信息安全，就是指会计信息的真实性、保密性、完整性、可用性、可控性和不可否认性。而如何使电子会计信息在这些方面得到保证就是本书所要讲述的主要内容。

本书的写作主要基于这样的现实情况：一方面，无论是管理层还是具体单位对会计信息安全都非常重视，但对实现会计电算化后的会计信息安全问题又缺乏必要的和系统的了解。另一方面，计算机及网络技术的发展速度实在太快，无法制定一个长期适用的管理制度。所以，希望通过本书向广大读者普及计算机信息安全的常识，介绍保证计算机信息安全的技术手段即发展趋势，让大家面对高速发展的计算机网络技术，能够制订出相应的信息安全制度，让财会人员可以放心使用会计软件、用计算机及网络代替手工记账的管理制度，这对实际工作将很有益处。