计算机安全与病毒防治

殷 伟 编著

安徽科学技术出版社

计算机安全与病毒防治

殷　伟　编著

安徽科学技术出版社

（皖）新登字02号

责任编辑：田　斌

封面设计：冯　劲

计算机安全与病毒防治

殷　伟　编著

*

安徽科学技术出版社出版

（合肥市九州大厦八楼）

邮政编码：230063

安徽省新华书店经销　　宿县地区印刷厂印刷

*

开本：787×1092　1／16　印张：42.25　字数：108 0000

1994年5月第一版　　1994年5月第一次印刷

印数：8 000

ISBN7—5337—0954～3／TP·9　定价：26.00元

序

信息时代离不开通信和计算机，而通信的革命性变化是基于计算机的强大威力，所以毫不夸张地说，没有计算机就没有信息时代，就没有现代化。发达国家计算机不仅广泛应用于社会的各领域和部门，而且已深入人们的家庭生活，预计到本世纪末，约百分之五十左右的家庭将拥有个人电脑。

计算机的应用如此广泛和深入，它的安全问题引起了人们的日益关注，尤其是计算机病毒的预防和消除显得越来越重要。自从发现世界上第一例计算机病毒以来，短短几年时间，计算机病毒的种类越来越多，造成的危害越来越大，甚至引起人们的恐慌，发生了所谓"黑色的星期五"那样严重的事件。计算机病毒是人为造成的，制造者有着不同的动机和目的，但其所造成的严重后果都是对计算机安全正常运行的破坏。

由于计算机安全关系到国家的根本利益，所以国务院将计算机安全作为国家安全的一个重要组成部分交由各级公安机关专门严格管理。本书作者长期专门从事计算机安全管理和监察工作，通过大量的实践，对计算机安全管理和病毒防治进行了广泛深入的研究，并具有较为系统、丰富的理论和实践经验。

全书内容广泛全面、系统丰富，既有理论的研究和介绍，又更侧重于实际应用、操作技巧、具体方法的指导和示范。纵观全书，作者不仅着重介绍了计算机病毒的检测、防治的具体方法，而且对计算机安全理论和计算机病毒的综合利用均进行了详细系统的阐述，这也是本书的一个显著特点。本书对预防和消除计算机病毒，保障计算机安全运行具有较强的实际指导功能以及较高的参考价值。只要全社会的高度重视和共同努力，并与有关管理部门密切配合，计算机安全是完全可以保障的。

尹曙生

一九九三年十一月

前　言

20世纪后叶，随着计算机科学技术的飞速发展，特别是微型计算机的日益普及和计算机网络的广泛应用，使人类社会的工作和生活方式发生了一系列巨大的变化，促进当今社会进入了崭新的信息时代。一方面由于计算机系统的开放性和信息共享，带来了计算机应用的飞速发展，另一方面也是由于这种开放性以及计算机本身安全的脆弱性，导致了计算机安全方面的诸多漏洞。1988年美国发生了震惊全球的"INTERNET网络事件"：大学生Morris将计算机病毒置入计算机网络系统，使该网络中约7000台计算机因感染计算机病毒而停机，造成经济损失约一亿美元。据不完全统计，目前计算机病毒种类约有2000多种，在世界各国迅速扩散，危害甚为严重。我国也不例外，据公安部门调查表明：我国约有70%的计算机感染过计算机病毒，使60多万台计算机不能正常工作。1987年我国计算机领域十大新闻之一就是大连、深圳相继破获计算机犯罪大案，这些罪案所造成的经济损失和社会影响都极其严重。尤为引人注目的是，计算机病毒已被应用于政治和军事目的，如我国发现的"6·4"计算机病毒就具有极强的政治性和破坏性；再如，海湾战争中，美军利用计算机病毒，使伊拉克的防空雷达和指挥控制中心的计算机系统瘫痪失灵，导致伊军陷入只有被动挨打，而无还手之力的困境。

我国在充分重视和研究了发达国家曾走过的弯路——只强调推广计算机应用，而忽视计算机安全的深刻教训之后，于1983年成立了公安部计算机管理和监察局，主管全国的计算机安全工作。1991年，作者作为公安部计算机安全代表团的成员，参加了在英国布莱顿举行的第七届国际计算机安全会议，到会的各国计算机安全专家、学者一致认为计算机安全是一个全球性的新课题，有必要从理论和实践，立法和安全宣传、教育等各个方面全盘研究、综合治理。基于这种考虑，本书涉及面极为广泛：从系统安全到软件安全；从数据安全到运行安全；从安全软件到安全新产品；从防电磁泄漏到实体安全；从银行部门到军事系统安全；从计算机病毒特征到具体的检测、解毒方法；从计算机病毒的防范到加以利用；从立法到宣传、教育等诸多方面进行全方位的论述和介绍。全书共分12章，第一章介绍了计算机安全概述；第二章至第九章分别介绍了计算机病毒的起源和危害；计算机病毒解析必备知识；计算机病毒的机制；计算机病毒的检测和防治；典型计算机病毒的分析和清除；计算机病毒的预防措施；计算机病毒的利用；计算机病毒的理论研究等；第十章介绍了计算机安全学科体系，第十一章介绍了计算机文化和教育，第十二章叙述了如何建立一个安全的计算机系统。

本书力求既有理论体系的研究和介绍，又特别注重对实际应用、操作技巧、具体方法

的指导和示范。附录列出了目前世界上流行的612种计算机病毒及其性质和特征，以及计算机病毒全年活动时间一览表，另外还介绍了清除计算机病毒常用的软件工具的使用方法，以及计算机病毒防御产品的测试标准，信息量丰富、完整，实用性和可查阅性强。

本书可供高等院校计算机专业师生；从事计算机应用的工程技术人员；计算机安全管理人员；机关、企事业单位、银行、公安、军事等国家要害部门的计算机用户以及各系统、行业的广大计算机用户阅读参考。

本书的第三章由张莉同志编著。在此，作者要衷心感谢计算机安全界的同行们，书中引用了他们的部分观点，在此，谨向所有给予本书热情支持和大力帮助的人们一并致谢！

作　者

1992年5月

目　录

第一章　计算机安全概述

第一节　计算机技术发展对社会的影响

众所周知，社会的发展需要信息和信息交流，当今社会中，人们几乎无时无刻不和信息打交道，人若离开信息就会变得一无所知，社会离开信息就会停滞不前。信息存在于人类社会中的每一个方面。在19世纪，知识和信息每50年翻一番，20世纪初约每30年翻一番，20世纪50年代后期约每10年翻一番，而80年代只需3年就翻一番了。这种信息量的急剧增加，使得用手工方式进行信息处理已不能适应需要，必须要有更新更先进的信息科学技术来收集、处理、存储和传输信息。而电子计算机正是这种技术的杰出代表，它的出现使得信息科学技术有了飞速发展，信息的表示方式在不断更新，信息交流的质量、数量、速度也在迅速提高，对社会发展产生了深远的影响。

1. 社会计算机化的出现

计算机技术的高度发展为人类提供了高度的自动化和现代化，计算机网络的不断扩大，迅速地向着国际化方向发展，为人类社会的更高速、更高效、更广泛的信息交流提供了条件，过去人们想象不到的许多事情都已经变成了现实。在一些发达国家中，计算机应用已经渗透到政治、经济、军事、科学文化和家庭生活等社会的各个领域，广泛使用计算机信息系统网络、个人计算机、智能终端、远程终端、卫星通信、数字处理器、办公室自动化、家庭计算机、人工智能机等，实现了社会的计算机化，改变着社会生产方式和社会的其它活动方式，朝着社会信息化进军。西方有人把它称为“第二次工业革命”（第一次是机器代替体力劳动的革命，第二次是机器代替脑力劳动的革命）或“信息科学革命”。由此可见，社会计算机化的出现，使计算机安全问题提到一个非常重要的地位。

2. 计算机资产的形成

随着计算机应用的广泛深入，计算机信息系统日益在整个社会活动中发挥着巨大作用，逐步实现自动指挥与控制、生产、管理、办公。原先由人承担的繁重工作，逐步由计算机代替，生产和工作效率大为提高。计算机信息系统也逐步成为整个国家和政府机构运转的命脉和整个社会活动的支柱。因此，社会的计算机化产生了一种新的社会资产，即计算机资产。它由两大部分构成：一是计算机信息系统资源，即硬件、软件、固体及其相关文件资料，系统相关配套设备和设施、系统服务，甚至计算机业务工作人员等，系统资源具有相当高的价值和使用价值；二是系统生产和拥有的，或者叫由系统处理、存储、传输的电子信息资源。包括钱、财、物，以及各种有价值的数据，如统计报表、科学技术资料、计划、决策、秘密文件、情报、公民个人的隐私数据等。如果说系统资源是国家的重要财富，而信息资源则是国家的重要战略资源。谁拥有它，谁就掌握了战略主动权。由此，我们不论从计算机资产的属性，还是从它的社会价值方面看，都会

深刻地认识到计算机安全的重大战略意义。

第二节　计算机安全问题的重要性

前面我们列举了计算机有许多强大的功能，但是，也存在着某些缺陷。首先，它是电子技术产品，它所处理的信息也是各种电子信号；其次，系统运行是靠程序控制的，一个大型计算机信息系统具有数百万个受各种程序控制的逻辑联结；第三，自身抗外界影响的能力还比较弱，安全存取控制功能还不够完善；第四，其运行环境要求比较高；第五，现代化管理不够完善。因此，计算机资源最易受自然和人为有害因素的影响。1992 年 3 月 6 日，全世界对“米开朗基罗”计算机病毒的恐慌，就充分反应了计算机安全的重要性。

1. 计算机信息系统的脆弱性

计算机信息系统资源的脆弱因素包括：

数据输入部分：数据通过输入设备输入系统进行处理，数据易被篡改或输入假数据。

编程部分：用语言写成机器能处理的程序，这种程序可能会被篡改或盗窃。

软件部分：计算机系统离开软件就是一堆废铁，一旦软件被修改或破坏，就会损害系统功能，以至整个系统瘫痪。

数据库部分：数据库存有大量的各种数据，有的数据资料价值连城，如果遭到破坏，损失是难以估价的。

操作系统：操作系统是操纵系统运行、保证数据安全、协调处理业务和联机运行的关键部分，如被破坏就等于破坏了系统功能。

输出部分：经处理后的数据要在这里译成人能阅读的文件，并通过各种输出设备输出，信息有可能被泄露或被截取。

通信部分：信息或数据要通过它在计算机之间或主机与终端及网络之间传送，通信线路一般是电话线，专线，微波，光缆，前三种线路上的信息易被截取。

硬件部分：即除软件以外的所有硬设备，这些电子设备最容易被破坏或盗窃。

电磁波辐射：计算机设备本身就有电磁辐射问题，也怕外界电磁波的辐射和干扰，特别是自身辐射带有信息，容易被别人接收，造成信息泄漏。

辅助保障系统：水、电、空调中断或不正常会影响系统运行。

存取控制部分：安全存取控制功能还比较弱。

自然因素主要是：火、电、水、静电、灰尘、有害气体、地震、雷电、强磁场和电磁脉冲等危害。这些危害有的会损害系统设备，有的则会破坏数据，甚至毁掉整个系统和数据。

人为因素是：安全管理水平低、人员技术素质差、操作失误或错误、违法犯罪行为等。

以上计算机的不安全因素说明，计算机自身的脆弱性十分严重。现在计算机已经应用到民航、铁路、电力、银行和其它经济管理、政府办公、军事指挥控制等国家重大要害部门或涉及全国性的大型信息系统之中，如果某个关键部分出了问题，不但系统内可能产生灾难性的“多米诺”连锁反应，而且会造成严重的政治、经济损失，甚至危及人民生命财产的安全。如果系统中的重要数据遭破坏或某些敏感信息被泄露，其后果也是不堪设想的。此外，还有跨境数据流引起的问题。如通过国际联网系统，搜集、处理、传输有关某个国家的政治、经济、军事、科技文化等信息、记录媒体进出口，或者对外国的数据和系统过分依赖等，可能会引起包括文化侵略、国

家主权、国家安全、贸易、技术转移等方面受到损害和一系列的政治、经济和社会问题。

2. 计算机安全受到威胁

探讨计算机安全的实质是分析对计算机资源存在着的各种各样的威胁，以及找出如何对付这些威胁的有效措施。造成这些威胁的人员对计算机的接近程度不一样，大致可以分四类：

(1)外部人员：不能进入计算机中心或机房的人员。

(2)物理存取人员：这类人员能进入计算机中心但没有多少上机的权利。

(3)系统存取人员：这类人员通常是计算机中心的普通用户，他们在系统里拥有的权利不是太多。

(4)编程特权人员：这类人员能在计算机上编制自己的程序，通常是指那些系统编程人员和系统维护人员。

以上每一类的人员，对计算机具有的威胁是不一样的。

对于外部人员，由于不能进入计算机中心而只能在外面进行攻击，所以他们的主要攻击目标是网络中的通信线路等外部设施，可能产生的威胁有：

(1)窃听：通过各种窃听手段获得计算机中的机密信息。

(2)搭线窃听：在计算机的通信线路上，搭上一个侦听设备，从而获得线路上传输的机密信息。

(3)愚弄：愚弄或欺骗计算机中心的人员，从而达到自己的非法目的。

(4)重叠：在终端的合法用户登机键入口令时，重叠在该用户之上，从而达到非法目的。

(5)电磁辐射：通过接受计算机系统辐射出的信号而获得机密信息。

(6)测试：网络中的电话号码一般是不公开的，攻击者通过反复测试，从而得到想要的电话号码。

(7)电话转接：在北美的有些国家提供了这种服务，当你要下班离开办公室时，可以在电话里拨入你家里的电话号码，这样所有打到办公室的电话便会自动转到你的家里。由于这种公用服务里的电话号码是公开的，攻击者可将别人的计算机连接到自己的计算机上。

(8)口令猜测：通过猜测口令而进入到网络系统中。

(9)密文分析：通过分析线路上传输的加密信息而得到明文。

(10)流量分析：通过观察通信线路上的信息流量，得到信息的源点和终点、发送频率、报文长度等，从而推断出信息的某些重要特性。

防止以上的这些攻击的唯一有效办法是将通信线路上的信息加密，并且在网络中实行可靠的协议，防止信息在加密之前从机房中泄露出去。如果能做到这些，就能够保证系统比较安全。

对于具有物理存取能力的人员来说，他们的主要攻击目标是计算机中心内部，可以产生如下一些威胁：

(1)浏览：通过观察计算机中心内部的情况或机器中的某些公用文件(如 HELP 文件)而获得有用的信息。

(2)蒙面：在计算机中心的某些地方，得到粗心大意的人写下的口令，从而冒称该人，使用机器。

(3)插入：当用户离开终端后，攻击者利用仍开着的终端做他自己的事情。

(4)窥视：站在终端用户的身后，观察其操作过程。

(5)废物：从当作废物的打印纸中寻找有用的信息。

(6)窃听:将窃听器安装在中心里,录下中心人员之间的谈话。

(7)推导:从统计数据库中获得的统计信息出发,推导出某些不应该知道的信息。

(8)隐蔽通道:通过观察磁盘、磁带等的调用次数,或者其他资源的运转情况,推测机器干些什么。

(9)设备安装:攻击者将 EPROM 或类似的电路芯片替换并重新插入机器中,使机器按照攻击者的目的运行。

(10)目力监视:通过从机房的窗口上看,得到有用的信息。

对于以上这些攻击,有效的防范办法是加强机房的出入管理,包括人员的进出管理以及记录有机密信息的媒介出入机房的管理。

对于计算机中心的用户来说,他们能够实际操作机器,具有较大的危险性,构成的威胁有:

(1)聚合:将能合法得到的几项信息综合起来,从而知道一些不应该知道的保密信息。

(2)拷贝:将有关程序和数据拷贝下来带回家去。

(3)天窗:有些操作系统为了日后的维护而留下了入口,攻击者可利用这些入口作为进入操作系统的天窗。

(4)强制崩溃:在程序中制造某些故意的错误,强制使机器停止运转。

(5)骚扰:攻击者在终端上做出某些令操作员生气的事情,使其容易发生错误,从而达到自己的目的。

(6)管态调用:在 IBM/MVS 系统里,用户可以构造自己的管态调用,从而进入监控状态,获得管态特权。

(7)客体再使用:在共享系统中,攻击者可以读取前一个用户在存储器中留下来的信息。

(8)转向:攻击者利用自己对系统软件的了解,将自己由普通用户工作方式转为监控方式。

(9)缓冲区:攻击者直接从输入缓冲区中获得口令等机密信息。

(10)特权位:在有的机器里,特权位是存放在用户的地址空间里的,攻击者可能修改这些特权位,做系统管理人员才能做的事。

(11)连接:利用系统中提供的连接程序,将有关的几个文件连接成整体,从而暴露其整体意义。

(12)电子邮件:在传送给别人的电子邮件中插入一些控制信息,达到得到接收者的文件拷贝等目的。

对于具有系统存取的人员来说,主要是能够使用系统的用户,他们具有的特权比较少,很想扩大自己的特权。系统管理人员要严密监视他们的工作,特别注意一些奇异现象的发生,如机器发生的崩溃太多等,要立即采取有效措施。

具有编程特权的人员通常是能深入到系统里面去的人,他们构成的威胁极大,一般有:

(1)特洛伊木马:修改某些程序,使得这些程序仍能正常工作,看上去是好的,实际上其中隐藏着一些破坏性的指令。

(2)逻辑炸弹:一种只有当特定事件出现才进行破坏的程序。

(3)意大利香肠术:这是对财务系统进行的攻击。它从每个客户的帐目中偷出一点点钱,客户往往不注意这种微弱损失,而攻击者将众多客户的钱加在一起,其数目就可观了。

(4)滥用实用程序:有些机器上的实用程序可以被修改以满足不同的需要,攻击者可利用实用程序达到自己的目的。

(5)病毒:实际上是一种逻辑炸弹,不同之处在于它不断地繁殖其自身。

对于上面这些攻击，很难防止。有效的办法就是加强管理，选择可靠的系统工作人员，记录这些人的行为，以便及时准确地发现蓄意破坏者。

总而言之，计算机的应用直接涉及到政治、经济和社会问题。计算机信息系统的脆弱性，必然会导致计算机化社会或信息化社会的脆弱性。目前世界各国计算机犯罪案件的不断增加，就充分证明了问题的严重性。

第三节　什么是计算机犯罪

近20年来，在一些工业发达国家里，计算机应用已经渗透到社会的各个方面，许多政府机构、民间企业都由计算机系统来贮存文件、管理日常事务、参与决策，这些机构都已经完全计算机化了。这样无疑提高了整个社会运转的效率，但同时又带来了许多新问题。由于计算机信息系统自身的脆弱性，以及一些敌对分子和极端利己的不法之徒的存在，利用计算机进行犯罪活动就不可避免。

1. 计算机犯罪的出现

计算机犯罪开始于40年代末期，也就是开始推广计算机应用之时。首先是运用在军事领域，然后逐步发展到工程、科学、金融、银行和商业等民用领域。1958年，美国就有计算机滥用事件的记录，1966年首次对一起篡改银行数据的计算机犯罪案件提出起诉，到了70年代中期，发案率就迅速上升，1971年正式开始研究如何防止计算机犯罪和计算机滥用，1973年美国召开了首届计算机安全与制止犯罪的会议，有关方面提交了专题报告，许多报刊上刊登了种种与计算机有关的犯罪方面的报道，这方面的专著也陆续出现。1978年，美国佛罗里达州制定了第一个计算机犯罪法规，到目前为止，美国已有47个州制定有关法律，联邦政府也颁布了《计算机诈骗与滥用法》和《联邦计算机安全法》，其它国家也在法律制度、政策和技术方面采取了相应的措施，把计算机安全问题纳入政府的重要议事日程。1983年，国际信息处理联合会设立了第11计算机技术安全委员会，负责计算机安全与犯罪研究。有关的计算机公司也在积极研制防止计算机犯罪和保证计算机安全的新技术产品。可以预计，随着计算机应用的日益普及，计算机犯罪就会不断出现，如何预防计算机犯罪，有效地保护计算机安全必将形成一个独立的学科。

2. 计算机犯罪的危害

在计算机化程度较高的国家，计算机犯罪已经形成了一定的规模和气候，成为一种严重的社会问题，威胁着经济发展、社会安定和国家安全。据国外资料统计，美国计算机犯罪造成的损失已达上千亿美元，年损失几十亿美元，平均每起案件为45万美元。原联邦德国每年损失50亿美元，英国为25亿美元，且每40秒种就发生一起计算机诈骗案，这些数字只是很粗略的，实际数据可能要大得多，因为有许多案件并不被人所知，也没有向警方报案，目的是为了保住有关公司的信誉。亚洲国家和地区的计算机犯罪问题也很严重，如日本、新加坡、香港地区等。我国在报刊上公开报导的计算机犯罪案件已达十几起，据了解，尚未被发现和发现了而未报告的案件远不止这些。现实生活告诫人们，虽然计算机为人类提供了极为有效的现代化信息处理手段，但是，计算机系统对于人类的潜在威胁，从某种意义上说类似核武器。这里，我们列举几个实例来说明这一点。

事实之一：1978年，美国洛杉矶市"安全太平洋银行"的一名计算机系统分析员，利用他职

务上的方便和对于银行的安全预防措施的了解，假冒银行办事员，通过计算机系统向他本人在纽约一家信托公司的帐户里汇入了一大笔钱，然后他又将这笔钱转汇到瑞士银行，购买了价值800万美元的钻石，这一犯罪行为直到8天以后才被发觉。

事实之二：美国洛杉矶市"威尔福格国家银行"的一名业务经理利用在计算机终端上开空头支票的办法，到1981年1月为止，两年内一共贪污了2100万美元，这是当时洛杉矶地方法院所受理的最大一次银行盗窃案。

事实之三：1986年5月，原联邦德国的4名罪犯利用计算机系统，通过适当手段改变信用卡的磁带密码，欺骗计算机系统，非法获得10万马克，后经严密侦察，此案被破。

事实之四：1988年，原联邦德国汉诺威大学计算机系一个24岁学生马蒂亚斯·斯佩尔，将自己的计算机系统同美国军方和军工承包商的30台计算机联网，在两年时间收集了大量有关美国国防的机密资料，其中包括美国"星球大战"计划、北美防空司令部、核武器和通信卫星等方面的情报。他通过打入"航天飞机"、"挑战者号"、和"机密"等关键字进入美国航空航天局的数据网，利用一些自己编制的程序，接触美国国家航空航天局数据网用户的电子邮件，窃取信息，甚至可通过适当的程序设计手段使整个数据网络陷于瘫痪，此案曾震惊了美国国防部和联邦调查局。

目前，美国除用于国防和政府部门的"ARPA"网外，共有四大电子转帐系统，并与全国电话网融为一体，连接国内外八百五十多个银行，国内日转帐达4000亿美元，跨国日转帐达6000亿美元。如果被计算机犯罪分子或集团从中窃取1%，就相当于联邦储蓄银行的总资产，如果被窃取10%，美国经济就会发生灾变，并将波及世界其他国家，而对从事计算机犯罪的不法分子来讲，窃取100万与窃取1亿在作案技术上没有什么差别，只不过加两个零而已。此外，还有发生计算机战争的可能性，计算机战争的威胁和危害远比核武器大。由于现代战争的真正目的不是为了毁灭一个国家，而是为了占领和掠夺，敌对国只要用高科技或雇一名或几名高级计算机技术人员，破坏或扰乱他国的主要的或大型计算机信息系统（如国家决策、指挥控制、经济系统），就足以使该国的经济崩溃、指挥失灵、决策错误，或者别人掌握了攻入你的重要系统方法，或者掌握你的重要信息，就可以迫使你屈服就范，从而就可以达到先发制人以至不战而胜的目的。

综上所述，我们可以看到计算机犯罪的社会危害的严重性，在于计算机信息系统的社会作用的大小，在于社会资产计算机化的程度和计算机应用的普及广度。作用越大，程度越高，应用面越广，发生犯罪案件的几率就越高，社会危害性也就越大。因此，一个国家的计算机应用同信息安全技术应当同时起步，即计算机安全与计算机的发展应当同时起步，否则会造成严重后果和极大危害，这如同发展现代化工业必须考虑环境保护和防止污染一样。

3. 计算机犯罪定义

到目前为止，国际上对计算机犯罪问题尚未形成一个公认的定义。计算机犯罪也许只是人类社会发展过程中一个暂时性的犯罪名称，因为人类从来没有把作案工具称作犯罪的先例，包括作案中使用率最高的刀枪也是如此。也有人把计算机犯罪叫做智能犯罪或科技犯罪，但似乎都不确切，因为计算机犯罪所包含的内容既有最原始的、传统式的破坏行为；也有高智慧型的犯罪，并且它还具有以下几个特征：

（1）计算机既是犯罪的手段和工具，也是罪犯攻击的目标对象。

（2）计算机创造了适合犯罪的独特环境，并强烈地刺激着犯罪，是典型的、收益甚高的低风险的作案方式。

(3)知识阶层专业技术人员直接参与了犯罪活动。

以上的三个特征,也使犯罪与非犯罪的概念和传统的常规犯罪完全不同,因为在计算机犯罪中,完全可以采用合法手段来实现非法的目的,因此,计算机犯罪实际上是当代社会出现的一种新的犯罪形式,很难形成较一致的看法,它的定义正处在讨论之中,这里只简单介绍几种定义方法:

定义方法之一:欧洲经济合作与发展组织的定义是:"在自动数据处理过程中,任何非法的、违反职业道德的、未经批准的行为都是计算机犯罪行为"。这是一个较广的定义,其中包括了数据处理职业道德问题,并把它提高到法律范畴的高度。

定义方法之二:美国司法部把计算机犯罪定义为:"在导致成功起诉的非法行为中,计算机技术和知识起了基本作用的非法行为。"这是一种从司法角度的定义方法,比较笼统,它并没有包括计算机犯罪的全部含义。比如说,破坏计算机信息系统的非计算机技术或知识起作用的行为,就不在此例,盗窃计算机设备的行为也不在此例。

定义方法之三:澳大利亚把计算机犯罪称为计算机滥用,并把计算机犯罪行为解释为与计算机有关的盗窃、贪污、诈骗、破坏等行为。计算机滥用行为包括:

(1)未经批准修改输入或输出数据。

(2)未经批准通过终端访问计算机系统。

(3)未经批准进行数据截收。

(4)对电子数据处理设备实施犯罪:盗窃设备、文件或数据。

(5)未经批准修改或使用应用程序。

(6)破坏计算机设备。

定义方法之四:美国斯坦福安全研究所高级计算机犯罪和安全专家帕克认为:计算机犯罪应当有三个概念,即计算机滥用——含有对计算机的任何故意行为;计算机犯罪——指在实施犯罪的过程中直接涉及到计算机;与计算机有关的犯罪——在成功起诉的非法行为方面计算机知识起了基本作用。

定义方法之五:中国政法大学信息技术立法课题组定义为:与计算机相关的危害社会并应当处以刑罚的行为,这是一个从学术角度所作的定义。

定义方法之六:中国公安部计算机管理监察司定义为:以计算机为工具或以计算机资产为对象实施的犯罪行为。这里所说的工具是指计算机信息系统(包括大、中、小、微型系统),也包括在犯罪过程中计算机技术知识所起的作用和非技术知识的犯罪行为。犯罪一词中包含了危害社会和应处以刑罚的含义。

以上定义究竟如何准确,有待于各方面专家们进一步研究。

定义好计算机犯罪一词,还必须弄清楚计算机在犯罪方面所扮演的角色,一般认为计算机在犯罪方面扮演四个角色:

(1)犯罪客体——计算机资产是犯罪分子袭击的对象或目标。

(2)犯罪主体——计算机为犯罪者提供了犯罪场所和环境,同时计算机可以替犯罪分子执行犯罪指令,进行犯罪活动,起了帮凶的作用。

(3)犯罪工具——有些犯罪活动和方法很复杂,需要把计算机作为工具,而计算机既可以是主动工具,也可以是被动工具。

(4)犯罪象征——犯罪者往往利用计算机进行诈骗,或者进行恐吓活动,迫使受害者屈服。

到目前为止,一些已知和已报案的计算机犯罪案件,尚无一例摆脱了上述四个原则。