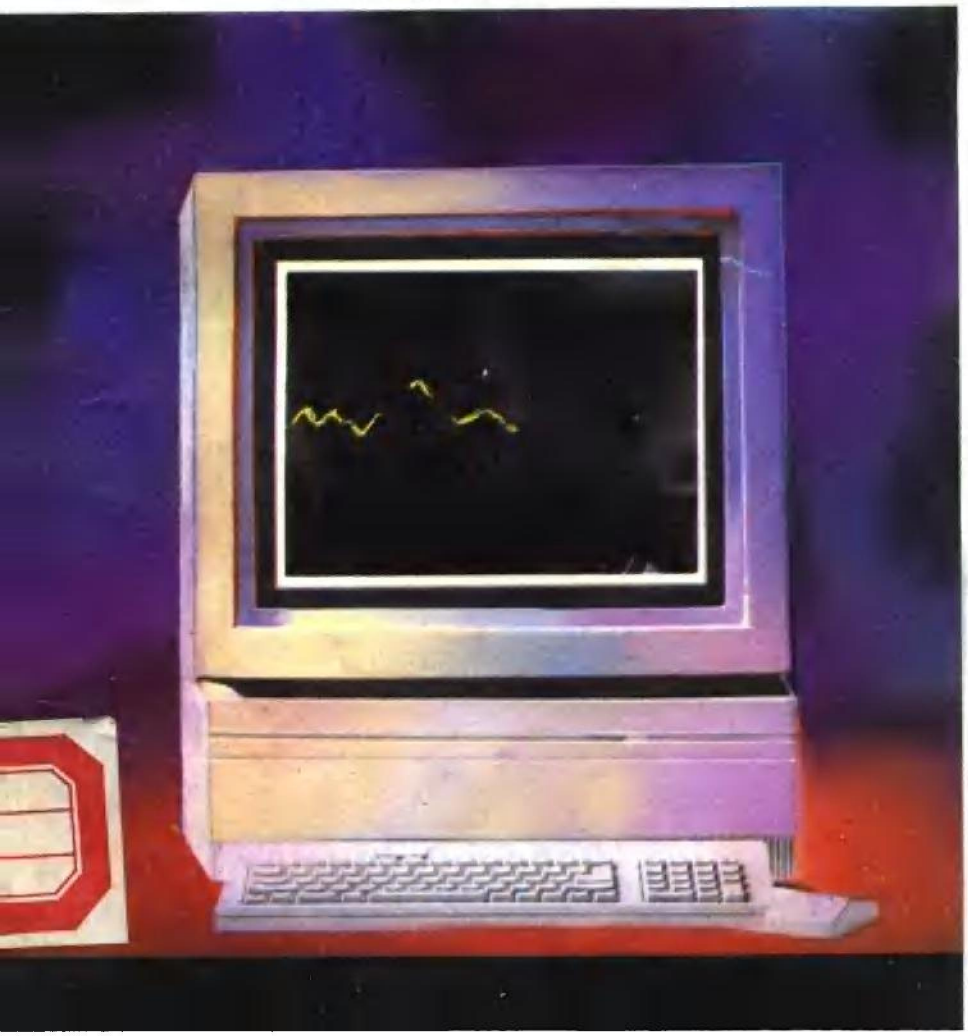
JI SUAN JI AN QUAN BI DU

计算机安全必读

公安部计算机管理监察司



计算机安全必读

公安部计算机管理监察司

群众出版社出版发行　新华书店经销

巨山印刷厂印刷

787×1092毫米　32开本　7.5　印张　154千字

1990年8月第1版　1990年8月第1次印刷

ISBN7-5014-0318-7/TP·1　　定价：3.70元

印数：00001——7000册

前　言

计算机技术的发展和普及，给人类创造了巨大的财富，同时又给社会带来了许多严重的问题。损失惊人的计算机犯罪与事故已导致了计算机安全学这个新学科的诞生。

我国的计算机应用水平还不高，但形形色色的计算机犯罪与事故已经出现，普及计算机安全知识已成为当务之急。鉴于国内计算机安全类书籍十分缺乏的现状，我们编写了这本普及教材，初步介绍了有关计算机安全各方面的基本知识，供计算机管理、应用与教育部门的同志参考。

由于计算机安全已成为计算机应用人员必须具备的知识，因此，中国计算机应用软件人员水平考试也将其列入了考试大纲，并将本书定为考试的参考用书。

本书各章分别由景乾元、龙培英、王学海、王铁肩、李书旺、熊永祥、刘风昌、曲建生等同志编写。

杨智慧同志负责本书的统稿与主审工作。

一九八八年十月

目　录

第一章　计算机安全与立法概述

第一节　计算机安全问题的提出

一、计算机技术发展及其社会影响

社会发展需要信息和信息交流，而信息的发展又需要有更新更先进的信息科学技术来处理、存储、传输信息。信息并不是现在才有的，实际上人类社会一开始就有信息和信息交流存在。随着信息科学技术的进步，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。这一点，以下几个阶段的统计数字就能充分说明问题。十九世纪，知识和信息每五十年翻一番，二十世纪初约每三十年翻一番，二十世纪五十年代后期约每十年翻番，而八十年代只需三年就翻番了。在这期间，计算机科学技术的发展，尤其是计算机与信息科学技术的结合，构成计算机信息系统技术，从而使计算机由单纯的数学计算迅速转向信息处理，具备了数据采集、信息存储、信息检索、通信、信息表示、工业自动控制等多种功能。计算机技术也经历了四代，目前还在发展着。一些发达国家，计算机应用已经渗透到政治、经济、军事、科学文化和家庭等社会的各个领域，实现了社会计算机化，改变着社会生产方式和社会的其它活动方式。这

些国家又在大力普及个人计算机、发展更大范围的计算机信息系统网络、智能终端、远程终端、卫星通信、字处理器，办公室自动化、家庭计算机、人工智能机，进一步提高信息存储量和处理速度。社会上出现了信息产业，并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，当代没有任何其它新兴技术会象计算机信息技术，对社会具有如此强烈和深远的影响。

二、计算机资产的形成

随着计算机应用广泛深入，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。这种新的资产由两大部分构成：一是计算机信息系统资源，即硬件、软件、固件及其相关文件资料，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；一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。这种计算机化或电子化的信息资源代表钱、财、物，以及各种有价值的数据，包括统计报表、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。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。谁掌握或拥有它，谁就有力量。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，都会立刻认识到计算机安全的重大战略意义。

三、计算机安全问题的严重性

计算机技术的发展和计算机的普及应用，促进了社会进步和繁荣，为人类创造巨大财富，使人类征服自然和改造自然、造福人类自身的能力有了极大提高。但是与此同时也向各国政府提出了计算机资产管理与安全的无比重要性。商业界、金融银行界要依靠计算机处理事务，政府的行政管理要依靠计算机信息系统和数据库，厂家和公司的全部生产取决于数据处理系统的能力，陆海空、宇航等指挥控制系统、医疗卫生要依靠计算机技术，整个社会对计算机信息系统的依赖程度将越来越大，甚至离不开它。然而计算机并不安全，其不安全因素有计算机信息系统自身的、自然的，也有人为的。

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窃取。

通信部分：信息或数据要通过它在机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。

人为因素是指：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（下一章专门讨论计算机犯罪问题）。

四、计算机的脆弱性引起计算机化社会的脆弱性

前面所列举的计算机不安全因素说明计算机虽然有许多强大的功能，但它自身又有许多弱点，也就是说有不少薄弱环节或脆弱性。首先它是电子技术产品，它所处理的信息也是电子的；其次，系统运行是靠程序控制，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连结；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强大；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。如果民航、铁路、电力、银行或其它经济管理、政府办公、军事指挥控制等大型或涉及全国性的信息系统，某个关键部分出问题，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份依赖等，可能会引起包括文化侵略、国家主权、国家安全、贸易、技术转移方面的政治、经济和社会问题。

总而言之，计算机不能与电冰箱、电视机或小轿车相比，这些东西不会引起什么大的社会问题，而计算机则不同，它的应用直接涉及到政治、经济和社会问题。因此，计算机安全问题必然会引起社会等重大问题。计算机信息系统的脆弱性，也必然会导致计算机化社会或信息化社会的脆弱性。美国最近发生的“电脑病毒”事件使全国六千多台计算机受害，就充分证明了问题的严重性。

第二节　计算机犯罪概述

一、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，实际上计算机犯罪是当代社会出现的一种新的犯罪，很难形成较一致的看法，正处在讨论之中。这里只简单介绍几种定义法：

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。

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。

瑞典也从司法角度在其数据法中作了很有限的定义：侵犯个人隐私的行为为计算机犯罪。如未经准许建立和保存计算机私人文卷；有关侵犯受保护数据的行为；侵害数据的行为，如非法存取电子数据处理记录或非法修改、删除、录入这种记录，或准备侵犯数据。这种定义并没有包括数据诈骗的全部内容，更不包括对计算机信息系统的破坏等犯罪行为。

也有人把计算机犯罪从概念上看成是"白领犯罪"，认为计算机或自动数据处理系统取代了手工作业，社会上一切事务处理都由计算机进行，计算机为"白领犯罪"提供了犯罪的环境、条件和机会，这是概念上的错误。最多只能说"白领犯罪"中有相当一部分与计算机犯罪有关或是计算机

犯罪，但不是全部。从发展趋势看，只能是计算机犯罪取代“白领犯罪”，而不是“白领犯罪”取代计算机犯罪。

澳大利亚有人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。他进一步解释说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）未经批准修改或使用应用程序；（4）对电子数据处理设备实施犯罪：盗窃设备、文件或数据；（5）破坏计算机设备；（6）未经批准进行数据截收。这种定义法本身是矛盾的，因为“滥用”一词含义中，无论如何包括不了计算机犯罪的全部内容，而从其进一步解释看，又似乎无所不包。

联邦德国有人把计算机犯罪定义为计算机犯罪行为。他解释说，计算机犯罪行为，是指针对计算机或把计算机作为工具的任何犯罪行为。

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。

以上是国外的一些定义。总之，计算机犯罪一词在国际上普遍使用，似乎已经成了一个惯用词，最终会有一个较统一的定义。国内目前有两个定义：一是政法大学信息技术立法课题组从学术角度所作的定义，即“与计算机相关的危害社会并应当处以刑罚的行为”；一是我们提出的定义，即“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）。也包括在犯罪进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。这种定义法在刑法中找不到相应概念的情况下是比较合理的。但究竟如何定义好，有待于各方专家们进一步研究。要定义好计算机犯罪一词，必须弄清楚计算机在犯罪方面所扮演的角色，国外有人认为计算机在犯罪方面扮演了四个角色：

（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人执行犯罪指令，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，或者进行恐吓等活动，迫使你屈服。

据说到目前为止，国外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。

二、计算机犯罪分类

计算机犯罪类型可以从不同角度进行分类。有五分法：向计算机信息系统装入欺骗性数据或记录；未经批准使用计算机信息系统资源；篡改或窃取信息或文件；盗窃或诈骗系统中的电子钱财；破坏计算机资产。其它分类方法还有从损失类型上分为：实体损害；暴力破坏；知识财产和钱财获益；

非法使用服务。从计算机所的作用方面分为：客体；主体（帮凶）；工具；象征。从对计算机、数据、程序和服务的行为上可分为：篡改；破坏；泄露；使用服务。从犯罪形式上可分为：诈骗；盗窃；掠夺；侵占；纵火；贪污；敲诈；破坏；间谍。从作案手段上可分为：实体袭击；假数据输入；超级冲杀；假冒；线上截收；寄生术；废品利用；特洛伊木马术；陷阱；异步攻击；香肠术；数据泄露；逻辑炸弹；电脑病毒等。

三、计算机犯罪分子的分类

随着社会计算机化的发展，社会上形形色色的犯罪将逐步转向计算机犯罪。除凶杀，强奸和其它人对人的犯罪活动外，计算机犯罪将几乎包括所有社会犯罪形式。美国有人曾对过去八年中发生的667起案件作了分析后指出：计算机犯罪已经涉及到绝大部分社会犯罪现象。如果对计算机犯罪分子分类，一般可以分为五类：（1）从事计算机业务工作的人员，其中工程技术人员占70%以上，内部人员占65%左右，同时也占“白领犯罪”分子的绝大部分。（2）青少年犯罪者，这部分人在计算机犯罪方面的比例正在迅速上升。（3）集团犯罪，也叫有组织的犯罪，公司或部门利用自己的计算机进行犯罪活动，如美国一保险公司为了掩盖亏损，欺骗顾客，在其系统上伪造保险合同，价值32亿美元的合同中假合同金额达21亿美元，占60%，此外，还有商业集团为了在竞争中击败对手，千方百计地从对方系统中窃取商业情报。（4）一国对他国的犯罪行为。（5）社会常规犯罪向计算机犯罪演变。由于计算机技术广泛应用及其对社会的影响，使得社会犯罪成份正在发生重新排列组合。

四、计算机犯罪手段

计算机犯罪手段主要分暴力和非暴力两种。暴力手段是指对计算机资产实施物理破坏，如使用武器摧毁系统设备和设施，炸毁计算机中心等活动，而非暴力手段是指用计算机技术知识及其它技术进行犯罪活动。后者称高技术犯罪或智能犯罪，而且这部分犯罪最为常见。所谓高技术犯罪是因为犯罪者使用了下列技术手段：

1．数据欺骗：非法篡改数据或输入假数据；

2．特洛伊木马术：非法装入秘密指令或程序，由计算机执行犯罪活动；

3．香肠术：利用计算机从金融银行信息系统上一点一点窃取存款，如窃取各户头上的利息尾数，积少成多；

4．逻辑炸弹：输入犯罪指令，以便在指定的时间或条件下抹除数据文卷，或者破坏系统功能；

5．线路截收：从系统通信线路上截取信息；

6．陷阱术：利用程序中用于调试或修改、增加程序功能而特设的断点，插入犯罪指令，或在硬件中相应的地方增设某种供犯罪用的装置，总之是利用软件和硬件的某些断点或接口插入犯罪指令或装置；

7．寄生术：用某种方式紧跟受有特权的用户打入系统，或者在系统中装入“寄生虫”；

8．超级冲杀：用共享程序突破系统防护，进行非法存取或破坏数据及系统功能；

9．异步攻击：将犯罪指令掺杂在正常作业程序中，以获取数据文件；

10．废品利用：从废弃资料、磁带、磁盘中提取有用的

信息或可供进一步进行犯罪活动的密码等；

11．截获电磁波辐射信息：用必要的接收设备接收计算机设备和通信线路辐射出来的信息；

12．电脑病毒：将具有破坏系统功能和系统服务与破坏或抹除数据文卷的犯罪程序装入系统某个功能程序中，让系统在运行期间将犯罪程序自动拷贝给其它系统，这就好象传染性病毒一样四处漫延。这种犯罪手段一般用于联网系统；

13．伪造证件：如伪造他人的信用卡、磁卡、存折等。

以上是目前国际上计算机犯罪的一些主要和常见的犯罪手段。此外还有其它手段，而且新的犯罪手段也在不断出现，只不过尚未定型罢了。

五、计算机犯罪的特点及其与常规犯罪的区别

计算机犯罪是一种新的社会犯罪现象。这种犯罪总是与计算机和信息紧密联系在一起。其特点是：

1．掌握计算机技术知识，从事数据处理活动的人占多数；

2．作案者多采用高技术犯罪手段，有时多种手段并用；

3．作案工具一般是具有强大功能的计算机信息系统；

4．作案范围一般不受时间和地点限制，在全国和世界联网的情况下，可在任何时间和任一省到某省作案，甚至可以到某国作案；

5．作案的直接目标往往是无形的电子数据或信息；

6．作案时间短：按计算机时间算，计算机执行一项犯罪指令，有的只需零点零几毫秒或几微秒；

7．作案后可以不留痕迹，不易被人发现，不易侦破，

既便是他正在作案，你还以为他在工作呢；

8．危害大、损失严重、影响面广。

9．作案者所冒风险小而获益大，只要轻轻按几下键盘，就可以获得几千几万、几十万、几千万，甚至上亿款项。

六、计算机犯罪的社会危害性

在计算机化程度较高的国家，如美国等，计算机犯罪已经形成了一定的气候，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。我们只要看一下几个初步的统计数字，就能认识到计算机犯罪的社会危害性的严重程度。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，平均每起案件为四十五万美元。西德每年损失五十亿美元。英国为二十五亿美元（现在在英国每40秒钟就一起计算机诈骗案发生）。据说这些数字只是很初步的，实际数据可能要大的多，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、香港等。我国在报刊上公开报导的计算机犯罪案件已达九起，据了解尚未被发现和发现了而未报告的案件远不止这些（这一点和国外的情况完全相似），这些案件中金额最小的有数千元，最大的87万元（很可能这并不是最大的案子）。

计算机犯罪的社会危害性的大小，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普及广度。作用越大，程度越高，应用面越广，发生犯罪案件的机率就越高，社会危害性也就越大。这一点是国际