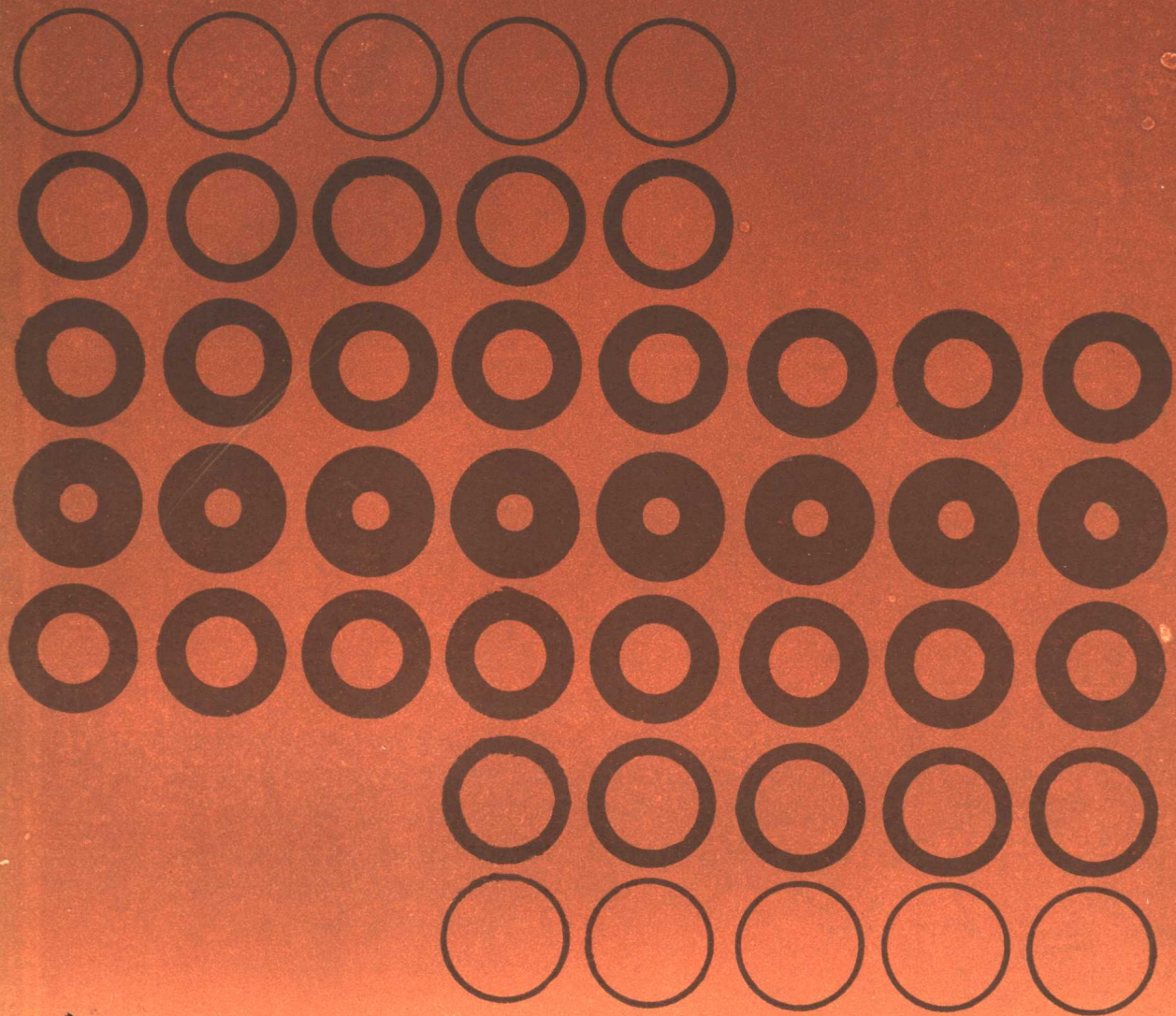

李学诗　主编

计算机系统安全技术

计算机系统安全技术

吉林工业大学

李学诗　主编

华中理工大学出版社

内 容 简 介

本书是关于计算机系统安全技术基础的书籍，主要讨论计算机系统安全技术领域中关于建筑、附属设备、消防、法律、防止犯罪、保险等方面的问题。此外，还扼要介绍了有关计算机系统高可靠性技术的基础知识。书中主要内容有：信息化和安全性，计算机犯罪，计算机房的灾害，微型计算机系统安全技术。

本书可供大专院校计算机应用、计算机软件、计算机系统结构、信息工程与管理信息等专业的学生作为学习计算机系统安全技术的教科书或参考书，也可供从事计算机研究、设计、制造、使用和维护的科技人员、管理人员和领导干部阅读参考。

计算机系统安全技术

李学诗　主编

责任编辑　唐元瑜

华中理工大学出版社出版发行

（武昌喻家山）

新华书店湖北发行所经销

华中理工大学出版社汚阳印刷厂印刷

开本：787×1092　1/16　印张：12　字数：260 000

1987年8月第1版　1989年4月第3次印刷

印数：5 001-8 000

ISBN 7-5609-0011-9/TP·2

定价：2.45元

前　言

随着科学技术的发展和社会的进步，信息的作用愈来愈重要，信息的数量也愈来愈多。在这“信息爆炸”的年代里，社会各个领域的信息处理都必须是高效率的，而且都必须借助于电子计算机来完成。也就是说，在信息占据的地位愈来愈重要的年代里，旨在保障计算机系统安全，不间断地运行，以及保护程序、数据等信息不被破坏和泄漏的计算机系统安全技术越来越为人们所重视。

计算机系统安全技术是一门新兴技术，它涉及建筑、附属设备、消防、法律、防止犯罪和保险等各个方面。对于如何确保计算机系统的安全，目前尚缺乏成熟的理论、科学的依据、标准的数据和严格的管理规章可遵循。因此，如何结合中国实际，总结自己的经验，将国内外的实践经验和理论研究成果，加工整理为系统的理论，本书便是初步尝试。

作者在编著本书的过程中，本着系统性、易读性和实用性的原则，重点介绍信息化社会和安全性、计算机犯罪、计算机房灾害以及微型计算机系统安全技术。假若读者只对与微型计算机系统安全技术有关的问题感兴趣，则可直接阅读第六章。

本书可作为大专院校计算机应用、计算机软件、计算机系统结构、信息工程和管理信息等有关专业的学生学习计算机安全技术的教科书或教学参考书，亦可供从事计算机研究、设计、制造、使用和维护的工程技术人员、管理人员和领导干部阅读与参考。

本书由李学诗主编，李宏柏同志参加编写了第五、六章，张家凤同志提供了第一、四章的初稿，最后由李学诗统一改编和定稿。在编写过程中得到哈尔滨工业大学陈光熙教授、李仲荣教授，吉林大学管纪文教授和吉林工业大学吴治衡教授的鼓励和指导。在讲授此课的过程中，曾得到吉林工业大学计算机应用教研室一些同志的具体帮助；历届本科生、研究生也提出了一些宝贵意见。华中工学院出版社为本书的编辑出版给予了大力的支持。在此谨致以谢忱。

本书内容较多，涉及面较广，不可能在每个方面都更深入地进行讨论。同时，由于作者的水平所限，书中缺点和错误在所难免，敬请读者批评指正。

编　者　1986.10.1

目 录

第一章　计算机·信息·安全

1.1 信息化社会与电子计算机

1.1.1 信息化社会

人类正处于信息“爆炸”的时代。一场以微电子技术为核心，以计算机技术的广泛应用及其与通信相结合为基础的新技术革命正在世界范围内兴起。随着计算机安装台数的增加，随着计算机与数据通信相结合的各种联机系统的普及，这场新的技术革命正在逐渐地改变着社会的结构。它将使人类社会由工业社会过渡到信息社会。有人说：计算机＋通信＋人≈明天世界。

二十一世纪被称为信息化时代，产业结构将由以工业为主导的产业体系向信息产业、知识密集型的产业发展。之所以能够如此，是因为有电子计算机系统的革新和发展作后盾。电子计算机系统本身开发出的超大规模集成电路(VLSI)，代替了第三代的集成电路；计算机的设计思想、系统软件、处理能力、生产成本都有了很大的变化，并有了进一步的发展。因此，所有产业、教育、公共机构的电子计算机都将迅速发展，这是不难预料的。

在信息化社会里，火车、飞机座席的预订，用计算机已是平常之事。当采用计算机之后，不但人工难以顾及的大量的座席预订能准确地发售，而且还可以借助于数据通信在全国各地设置座席预约终端。

日本、美国和欧洲的金融业设置电子计算机的投资额在所有行业中名列前茅，而且台数与投资额逐年在增加。尤其是在电子计算机运用的最先进形式——联机系统方面，终端机的台数及投资额都占全行业的一半以上，普及程度较高。

银行运用电子计算机的目的大致可以分为三种（见表1-1），并且这三种目的有着各自不同的发展方向。第一种目的是在于提高处理业务的效率和降低成本。谁都知道，如果不运用电子计算机实行联机化，就是再增加20～30%的人员，也难承担起随着日益大众化而不断增加的庞大的业务量。

提高经营管理内容之一的“决策支援系统”的水平是B领域里的最大成果。与此同时，还不能忘记的是需要把银行职工从计算利息及统计业务等单纯的作业中解放出来。在第三种目的中，也就是在C领域内，整个银行的存取款，准确迅速的业务处理，提供各种新型的服务，开展受托业务的计算等所有业务都可由电子计算机处理。

除银行联机系统而外，由计算机处理的电视节目表自编系统、报纸排版系统、办公室自动化 (Office Automation)等对人类的日常生活、活动都有着极大的影响和改变。然而，受影响最大的要算是商业部门。大多数公司、企业的工资/价格都是用计算机来计算的。可以说，从掌握市场销售信息和库存情况、盈利亏损和借贷的计算到经营决策都要借助于电子计算机和数据通信。

表 1-1 银行运用电子计算机的目的

	使用电子计算机的目的	电子计算机化的发展方向
A	Advancement of productivity 提高生产效率，降低成本	Advanced On-line System 综合联机系统 Auto-Banking 发展无人服务业务 Advanced Inter-Bank Network 银行间数据通信系统
B	Better Management 提高经营管理水平	Better Decision Making System 决策支援系统 Better Utilization of Human Resources 有效地利用人的资源
C	Customer Services 改善对顾客的服务	Community Banking 整个社会、整个地区运用电子计算机 Cashless Society 非现金社会 Contribution to Society 金融机构的社会责任和电子计算机

不难看出，在信息社会里计算机和数据通信网占有很重要的地位。如果有人说没有计算机网络就没有信息化社会，则这是不算言过其辞的。因为，信息的价值在于流通性和共享性，若没有通信，则流通性和共享性就不能实现，信息也就失去它的价值。随着计算机技术的应用范围日益扩大，人们渐渐感到单台机器已不能满足要求，必须构成通信网络或公用网，要借助于这些来获得更多的资源。有了计算机网络之后，一个家庭就可享受到中、大型计算机的资源。

如果换个角度，即观察计算机和数据通信系统对人类社会的影响，那么会发现：

（1）计算机和数据通信的发展对社会的发展的的确确起到了推进作用，且反过来又向人类提出了新的挑战；

（2）人类社会模式化了，灵活性（是否可以说，人的容许能力）消失了，从而给人的身心和精神方面带来很大的影响；

（3）过多地甚至是夸张地宣传计算机技术对人类所起作用的好处，会导致对计算机失望的后果；

（4）计算机技术的发展导致信息知识“爆炸”，信息知识“爆炸”又把计算机技术推向一个新阶段，在此循环中伴随产生了信息公害和信息量公害。

最近，计算机技术的应用，特别是微型计算机在节能、生产过程控制、数据处理、事务管理等方面发挥了作用，获得了明显的经济效益。可以肯定，计算机技术在今后还会越来越高级化。它将更广泛地应用在各个领域，并将不断地提高经济活动与社会活动的效率。但是，利用电子计算机有其利，亦有其弊。所谓弊端是指，由于数据被破坏、被涂改、被抹除及计算机的损坏，导致人的生命和财产损失，造成经济活动和社会活动的迟滞，甚至混乱；数据被盗造成私人生活被侵犯等危害。由于弊端的存在，在计算机技术发展过程中，不得不考虑会发生犯罪和危险。

大家知道，二十世纪后半期在世界范围内产生了第三次产业革命，过去视为第三功能的信息流，如今上升到能主宰社会的最重要的地位。信息象商品那样具有流通权，信息与其它货物一样，也具有它的经济价值。但是，信息的经济价值只是在信息对生产效率和工作效率表露出有所贡献的时候，价值才体现出来并得到承认，而这又只能靠信息技术设备系统来实现。应当指出，并不是一切信息都有价值。如果信息不能满足一个公司、企业里信息工作人员的需要，不能在提高工作效率和完成任务方面起到明显的作用，它就一文不值。由于信息系统能给出有价值的信息，因此受到愈来愈广泛的重视。在信息化社会里，作为信息技术设备中枢的计算机系统，一旦发生事故而停止运转，就会引起社会的一部分或者全部瘫痪，会发生用计算机进行犯罪的活动，窃取计算机里存储着的情报。正因为如此，计算机安全技术问题就成为信息化社会中不可少的研究课题了。

最后要说明一下，如何给信息化社会下个精确的定义，即确切地回答信息化社会是什么样的社会。老实讲，这是个难回答的问题，到如今也还没有一个统一的、为大家所接受的说法。不过有一点是肯定的，即只是说我们每天的生活和活动，由于使用了计算机而变得方便。说这样的社会就是信息化社会是不全面的，因至少可以说，这样的社会不能算做信息化社会。

1.1.2 信息保护

我们知道，计算机系统是信息技术设备的中枢，其主要功能是“存储”信息与“处理”信息。早期的计算机系统侧重于信息处理功能，也就是说，把信息“输入”到计算机系统中，在其内部进行“处理”，从而得到“输出”。而信息存储功能是以“文件”概念出现的，信息作为文件被长期储存在计算机系统中。文件中的信息既可在必要时取出处理，又可根据需要进行更新。

由于存储器（磁盘等）的大容量化和存取信息的高速化，以及信息管理软件技术的不断发展，计算机存储信息的功能已从文件系统过渡到更加综合的数据库技术。数据库技术把信息存储功能和信息处理功能结合在一起，从而使得存储的信息更便于利用。于是，计算机系统逐渐能存储更有价值的信息了。例如，在企业的经营信息系统中储存着关于企业经营内容的信息；在银行联机系统中储存着关于个人或团体的存款数据。并且，从文件或者数据库可进一步形成“数据银行”（data bank），从而扩大了存储信息的范围，可将世界上各种信息（例如，关于个人的信息，其中包括户籍，信用保险，医疗信息等），全都集中存储、管理。数据银行的出现，虽使信息服务变得方便、效率得到提高，但由于把过去分散的信息全部集中了起来，于是使得取出（获取）这些信息也变得非常之方便。也就是说，从前分散的信息，要想取出（获取），需要到处去花功夫，如今却在一个地方花功夫就可获取了。显然，增大了信息泄密的可能性。

由此可见，计算机系统存储的信息的价值越大，保守信息秘密也就越重要。

随着从文件系统过渡到数据库技术，以及信息存储与利用方式的不断改进，信息的密集程度和共享程度也不断提高。例如，在分时系统（TSS）中很多用户共用文件系统或数据库，在计算机网络上系统用户的数量大幅度增加。并且，在公共信息系统中，势必有数量不等的许多用户同时利用着系统中的信息。在信息密集化，用户范围日益扩大的情况下，信息安全性就成为必须考虑的问题。也就是说，必须考虑信息泄漏与信息破坏的可能性。

所谓信息泄漏，就是故意地或偶然地获取了不属于自己的信息。在计算机系统中集中存

储着有价值的重要的信息，再加上用户范围的扩大，为许多用户接近这些信息提供了方便条件。从而使出于偶然事故造成信息泄漏的可能性增大，同时，坏人欲窃取他人信息也有可乘之机。

信息的破坏有两种：偶然因素造成的和故意造成的，一般来说，硬件或软件出故障造成的信息破坏属于前者；抱有恶意去破坏他人信息的属于后者。采用不正当手段故意泄漏或破坏他人信息的行为就是计算机犯罪（又称为信息犯罪）。

表1-2是H.E彼得森和R。特恩于 1967年对美国拥有联机终端用户的分时系统进行调查的情况。

表 1-2 造成信息失密的主要原因

类　型	手　段	影　响
事　故	系统故障 硬件的误动作 软件错误 用户错误	特权信息被错误地转送给他人终端、打印机等
故　意 （被动的）	窃听通信线路 电磁检拾(Pickup) 查看复写纸	通信内容泄漏
故　意 （主动的）	偷读文件 冒充其他用户 特别终端接入线路(线路在接续状态，用户不在；或者给用户送错误信息) 供系统中心的职员使用 通过系统的侧道使用 从存贮器转储获得残留信息 偷走可拆卸文件	特定信息被泄漏或被变更

存储在计算机系统中的信息是一种特殊形态的财产，为了防止泄漏或破坏，必须对它加以保护。再者，从保守私人秘密的角度来看，也应对储存在计算机系统中的个人信息在适当的范围内予以保密。我们把防止信息破坏和防止窃取而采取的措施称为“信息保护”。随着计算机系统的用户不断增加，系统机密保护功能（Security）已成为计算机系统必备的功能。

近些年来，计算机技术的不断发展，对计算机系统的信息保护功能要求愈来愈高，即要求具备完善的信息保护功能。但是，加强计算机系统的信息保护功能不是无限制的。也就是说，信息保护功能达到什么程度，取决于对保护费用与保护效果的要求。

提高计算机系统的可靠性是防止信息破坏的一个重要措施。系统可靠性分硬件可靠性与软件可靠性。通过提高元件的可靠性，虽然能增强故障排除能力，能够提高硬件的可靠性，但要想得到理想的可靠度是不可能的。软件可靠性包括排除程序错误和由软件实现故障排除。在最新的操作系统中，为了提高可靠性，其软件恢复功能大大加强，不仅具有排除硬件错误的功能，而且也有软件排除错误的功能。

从目前流行使用的计算机系统来看，在信息保护功能上都存在一些弱点，从而造成信息破坏和信息泄漏。欲求得信息保护就必须对一个计算机系统上所处理的应用业务、执行的程

序，或用户的范围给予必要的限制。应用业务和用户范围的不断扩大，迫切要求研制出在保护功能上没有弱点的计算机系统。那么针对造成信息失密的各种原因，打算投多少资金来保护信息呢？另外，即使有了理想的保护功能，若系统的成本很高，或性能差，也是不能采用的。因此，信息保护的限制原则，应该是在信息保护与投资两方面综合权衡。只要能够使企图泄漏或破坏信息的人付出高于信息本身价值的代价就可以认为是达到了信息保护之目的。做到绝对保护是不可能的。

除此之外，与处理信息的其它组织机构一样，为了保护信息，还有必要从管理方面采取些相应的措施。特别是对于那些承担信息处理系统设计、制造的工程技术人员和参与操作的人员来说，应给予充分的关注，因为这些人掌握着丰富的知识和具备着各种手段，且接近计算机系统的机会多。因此，也应从人员管理上把关，即对于从事信息处理系统制造、操作的人员，也应该象认可会计师那样，实行经官方批准的制度（或资格考试制度）。

1.1.3 计算机系统安全技术兴起的背景和现状

首先回顾一下世界上开展计算机系统安全技术研究的历史背景。

1968年　在美国的情报文献中开始见到关于安全对策的讨论文章。

1972年　美国有大量文章或专著发表。日本的杂志，也开始出现这方面的文章。

1974年　美国信息处理协会系统改进委员会出版了《计算机机密保护手册》。日本出版了《计算机的机密保护和安全管理》。

1975年　日本成立了通产省电子计算机安全对策委员会。

1977年　日本通产省颁布了《电子计算机室安全对策标准》。此外，还发表了许多文献和专著。

从过去来看，不但世界的动荡局势和恶劣的治安状况给计算机系统的安全带来影响，而且灾害也给予人们以沉重的教训。例如，1970年袭击美国东南部各州的台风；1972年美国洛杉矶郊外的大地震；1977年日本三陆海域地震等等。

由于社会治安状况的恶化和天灾，由于计算机应用范围的扩大及其在各个领域中占有重要地位，因此计算机系统安全技术问题已引起各国的高度重视。

1985年8月中旬在爱尔兰共和国首都都柏林（Dublin）召开了第三届计算机安全国际会议。在此之前还召开了国际信息处理协会第十一技术委员会（TC-11）会议。TC-11的宗旨是交流计算机安全工作的实际经验，估计现有的和将来的数据保护技术。我国于1985年初参加了该委员会。

TC-11委员会下设五个技术组：

第一工作组（WG11.1）安全管理。其宗旨是：研究计算机系统安全的目标和政策的制定问题；信息系统保护措施的实施；估价保护措施的方法等。

第二工作组（WG11.2）办公室自动化的安全。其宗旨是：研究办公室自动化安全措施；交流经验，开发安全系统。

第三工作组（WG11.3）数据库安全。

第四工作组（WG11.4）密码管理。其宗旨是：研究密钥管理；数据传输过程的加密技术。

第五工作组（WG11.5）审计。

众所周知，在过去的十五年里，计算机技术发展得很快，但是，计算机系统的安全技术

工作却远远没有跟上去。当机密和重要的信息密集到计算机系统的同时，间谍和犯罪活动也就把计算机系统当做瞄准的目标。据不完全统计，仅在计算机诈骗方面的经济损失，美国每年损失约达三十亿美元，英国每年损失约二十亿美元。更为甚者的是，一些国家的国防部所拥有的数据库也遭到非法存取。

世界上越来越多的人已看到计算机犯罪活动业已构成对国家独立安全和社会安定的主要威胁了。许多国家把计算机安全问题纳入政府工作的议事日程。当前，从社会整体出发制定计算机安全对策、颁布法律、建立计算机安全管理机构是保障计算机应用正常发展的根本办法。象过去那样，只是盯住某台计算机，以达到保卫之目的是不行了。如今由于计算机的网络化和大量微型计算机的投入使用，个人计算机进入家庭，数据的传输已跨出城市，甚至跨出国界，因此，不制定规章制度和数据保护法律，显然是不行的。所以许多国家制定了本国的关于计算机数据保护法，并正在磋商国际性的数据保护法。在一些国家里还成立了政府机构来监察计算机安全。我国在公安部设立了计算机安全监察室。对于计算机应用单位来说，还应有专门负责监督本部门计算机安全的行政人员。

由于社会日益依赖计算机，计算机犯罪将逐渐地成为信息社会中的重要犯罪方式，犯罪集团也将逐渐转变为计算机犯罪团伙，有的还会成为国际性的犯罪组织。例如，欧洲原先有一个名为马菲亚的犯罪组织，成立于二十年代初，现在已经变成严重的计算机犯罪组织。该组织不惜耗费巨资来训练其成员的计算机犯罪技能，他们声称其成员的计算机技术水平要比美国联邦调查局高明得多。这个集团现在已经渗透到欧洲、美洲、亚洲的许多国家，成为警察部门严加防范的对象。

一些依靠进口计算机来实现信息现代化的国家，深感计算机系统安全的紧迫性，特别担心别国在出口计算机中暗藏了故障程序，只要任务量一大，它就使计算机出错。过份依赖进口计算机，对一个独立国家来说，不能不是个潜在的威胁因素。

在计算机系统所面临的威胁当中，安全技术至今仍是一个薄弱环节，1984年11月中旬在伊利诺斯州罗斯蒙特举行了美国第十一届计算机安全年会。在会上展出了与安全技术有关的展品，展出的展品都只能在一个窄小的领域起单一的作用，缺少的是一种全面解决的方案，即由一种产品或者一家供应商解决计算机用户所面临的全部安全问题。真正的安全问题并不在于计算机用户单位内的硬布线系统，而在于外部的数据通信环节。令人忧虑的是那些特许的用户远程存取总公司的信息，一旦数据调离了主机就无法控制，对此，目前也尚无解决办法。另外，现在研制的保障安全的产品价格过高，难以推广。例如，在每一个终端都配上一个存取控制盒，还不如用一个控制盒来控制全部终端好。

我国开展计算机安全技术的研究较晚，目前尚处于起步阶段，相继成立了官方机构和学术团体，并开展活动。相信我国的计算机系统安全技术会在不久的将来跨入世界先进行列。

1.2 威胁计算机系统安全的“危险”

1.2.1 围绕着计算机系统的“危险”

可以说，计算机系统给人类社会带来的好处如同水和电一样，已成为人类社会活动的神经中枢了，有着不可缺少的作用。在信息社会中计算机系统是个占地广阔的庞大的信息技术设备，是个数据处理工厂，它不但对物理环境条件有要求，而且还要求使用它的人员在多方

面配合。随着信息处理系统大规模化和数据的密集，人们对计算机的依赖性与日俱增。如果忽视这种依赖性，就制定不出相应的保护措施，会有许多“危险”包围着计算机系统。例如：

（1）灾害（火灾、风灾、水灾、地震）；

（2）破坏；

（3）犯罪和不正当行为；

（4）运用上的过失；

（5）机器设备的故障，软件的故障。

对于（1）项、（2）项的灾害和（5）项的故障，可以通过设备的高级化和技术进步，使其影响限制在较小的程度。并且千万不能掉以轻心，任何微小的疏忽，缺陷的集中和日积月累，同样是会酿成事故的。至于（4）项的运用过失是由人本身的弱点造成的，可以想办法减少，但也是做不到完全根除的。

（3）项是最棘手的，对于犯罪和不正当行为，难以做到完善的防备。可以说，它是信息社会的重要社会问题之一，是保卫和进攻的角逐场。对保卫者来说，只要在物理对策和技术对策上，能做到让进犯者付出大的代价和采取必要的经济制裁与法律制裁，就达到了防护之目的。

威胁计算机系统安全的主要因素示于图1-1。

关于计算机系统的灾害，日本JECC于1979年3月有个调查。调查结果表明，火灾件数占42.8%，其中起因于计算机系统本身的很少，大多数是由于遭受火灾延烧和灭火水（剂）的污染而造成损坏。从计算机系统本身起火来看，又多出于使用环境恶劣，保养不当。而这些又主要是管理方面的过失所造成的。由于设备不良发生灾害的占28.6%，其中多半是受漏水、污水之害。究其原因，也是由于设备保养不良，管理不善，设备陈旧及不合理的使用条件所致。随着计算机安装台数的增加，安装地点和环境就不那么好。那些安装在公用大楼内或在饮食店附近的计算机系统，还要遭受鼠害。JECC于1979年10月对用户的调查表明，在事故教训中有10%是鼠害，即老鼠啃坏配线、筑窝和鼠粪尿等引起计算机系统故障。

表1-3列出了日本JECC于1979年3月末对主要事故（地震灾害除外）的统计。

表 1-3 灾害的统计（日本 JECC调查）

件数	比[%]	内容	金额	比[%]
火灾	42.8 (22.4)	延烧，工程失误等直接失火；灭火水，灭火剂，烟等污染	26.3	(9.4)
	(12.2)	计算机配电盘起火		(3.9)
	(8.2)	空调设备起火		(13.0)
设施不良	28.6 (10.2)	由上层楼、天棚漏水	51.5	(1.7)
	(10.2)	加湿机故障，房盖防火不良，污水污染		(49.4)
	(8.2)	由于上水道、下水道等的破损而受污水污染		(0.4)
风水害	14.3 (8.2)	台风，大暴雨等污水污染	1.9	(0.9)
	(6.1)	台风，大暴雨等污水浸水		(1.0)
人灾	14.3 (8.2)	过激分子，精神异常者之类的人为破坏	20.3	(20.2)
	(6.1)	由于手动操作时不注意，移动设备时碰撞而使设备损坏		(0.1)

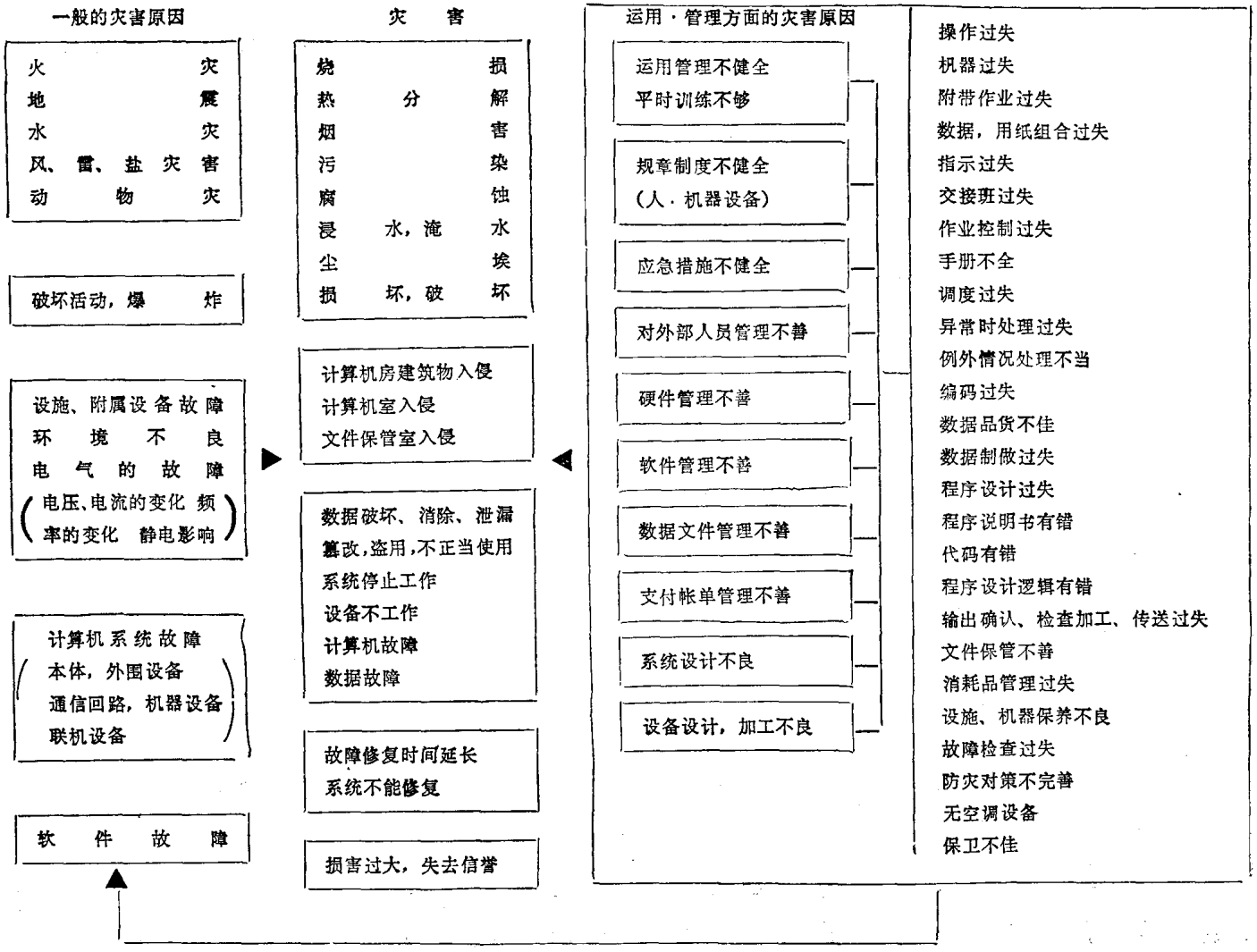

图1-1 威胁安全的主要因素

由表1-3可以看出，计算机系统的电气设备、空调设备和建筑物的防水性能，计算机房的防犯设备（出入口的管理）的事故居多。

归纳起来看，有以下几点共同情况：

（1）夜间或休假日，在无人情况下易发生事故，且损失程度与发现的早晚，善后处理恰当与否有关。安全工作的基本原则是及早地预防或发现灾害。

（2）设备的妥善管理和正确使用、保养，直接与人的因素有关，这些运用管理方面的问题，若处理不当会酿成千里之堤溃于蚁穴之恶果。所以，应用管理机构的各个部门必须具有确保安全的责任心和必要的知识，以便当计算机系统的安全受到威胁之际，通过组织机构能准确地查出原因所在。

（3）为了适应紧急情况的需要，要加强对工作人员的应变能力的训练，使有关人员能保持沉着冷静，能有条不紊地采取应变措施。也就是说，必需进行定期地或当系统变更时的紧急应变训练，防止忙乱之中酿成二次灾害。

（4）把安全技术工作纳入公司、企业业务监督范围之内，客观地评价安全技术工作，改进功能上的不足之处，提高安全技术水平。

过去有过几起大规模的灾害。例如，1959年7月，英国国防部出现了一起烧毁3台电子计算机和5000多盘磁带的事放，使其数据的恢复成了很大的问题。据日本电子计算机公司于1975年3月调查，发事故有：

（1）火灾18起，损失金额28607万日元；

（2）设施不良9起，损失金额65691万日元；

（3）人为灾害6起，损失金额26443万日元；

（4）风、水灾害6起，损失金额2307万日元。

美国联邦调查局的电子计算机系统在1979年由于洒水器误放水，造成重大损失。此外还有电缆失火造成大火灾，大地震造成区域性毁灭性的灾害等。若采取设备加固和后备支援措施，可以防止一般运用管理上所出现的问题。

据我国《计算机世界》总第143期报道：1986年9月18日上海南京路二轻局大楼遭特大火灾，殃及了二轻局、华东机电一级站和华东产管处三家电子计算机房。其中，位于五楼的华东机电一级站计算机房连同新近装修的终端室全部烧毁，仅计算机硬件系统及辅助设施直接损失达133万元。但更大的损失却在于数据资料信息的破坏。放置在同一栋楼中的应用数据备用副本也全部烧毁。使正在应用的计算机系统即使另有新机也无法在短期内马上恢复继续工作。几十年的资料和近几年的心血全部付之一炬。

另外，在1977年到1980年期间，设在意大利的多国籍企业的计算中心中有二十六个遭到爆炸破坏。1973年发现的公开窃取保险费事件的主角伪造64000件空头保险契约，诈骗了二十亿美元，造成巨大的损失。欲防止这类损害并非是轻而易举的。

存有经济、机密数据资料的计算机系统的高度集中和功能的合并，很容易构成区域性的系统。这样的系统在制定防护方法时不但耗资巨大，而且在防护的运用管理上还要投入较大的精力，否则就实现不了信息化社会。

计算机技术的不断革新，会使计算机系统的安全性有更可靠的保证。高度集中的功能合并将要向分散化过渡，实现在区域上、功能上都能由可靠的计算机系统来代替的前景。以上无论是从技术上还是从经济上来说，都是办得到的。因此说，信息保护问题和数据机密化问题将是计算机系统安全技术方面的主要研究课题之一。此外，还要研究防护方法，例如，根

据法律制定些规约，开展计算机系统安全教育。

1.2.2 地震灾害

我国虽不是地震最多的国家，但是，有些地方的地震还是比较严重的，应当予以重视。

一、有关地震的基本知识

首先谈谈震度和震级的概念，这两者往往被混淆。震度是表示在某一地点感受到地震强度的量，而震级是表示地震规模的单位。举例来说，把震级看成光源的亮度（即光度），把震度看成离开光源各处的亮度（即照度）。灯泡的瓦数虽大，但离得远的地方就暗；灯泡瓦数虽小，若离得近就亮。与此相同，震级很大的地震，离开震源远的地方震度就小。震级虽然小，但在震源附近的地方，就会有大的震度。

震度是用感到地震处测得的震动最大加速度来衡量的。加速度单位用m/s^2来表示。地震时如果超过$80\times10^{-2}m/s^2$，认为是相当强烈的地震。表1-4是国际通用的修正麦氏震度级

表 1-4 修正麦氏震度级表

震 度	说 明
	无感觉
1	地震仪能测到，个别对地震敏感的人能觉查到。 1.0以下
2	只有在大楼上层静止的少数人感觉到，易摇动的物体有摇动。 1.0～2.1
3	在大楼上层有明显感觉，停着的汽车轻微摇动。 2.1～5.0
4	白天屋内许多人都有感觉，器皿、窗玻璃、门扇等有摇动，停放着的汽车摇动很大。 5.0～10.0
5	所有人数都感觉到，放置不牢的物品翻倒，摆钟停摆。 10.0～21
6	许多人受惊跑到户外。 21～44
7	差不多所有人都跑到户外。放置不稳，设计不牢的东西有很大程度的损坏。 44～94
8	坚固的建筑物有些损坏，烟囱、纪念碑、墙壁等倒塌，家具翻倒，有飞砂走石，井水有变化。 94～202
9	坚固的建筑物损坏，部分地面出现明显裂缝。 202～432
10	石头结构工程损坏，地面裂缝又多又大，铁轨扭曲。 432以上
11	建筑物所剩无几，桥梁破坏，出现大的裂缝，地面凸凹。
12	所有的东西都遭破坏，东西被抛向空中。

［注］ 说明栏内的数字为地动的加速度，单位为$10^{-2}m/s^2$