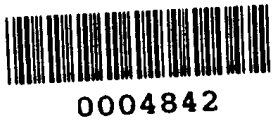
计算机安全指南

劳诚信 姜国雄 尹良瑸 姚伦淳

清华大学出版社

计算机安全指南

劳诚信　姜国雄
尹良瑸　姚伦淳　编著



清华大学出版社

内 容 提 要

本书是一本系统而实用的计算机安全指南书。内容丰富，选材新颖。本书介绍了计算机安全环境、机房的设备防护、供电系统、计算机系统的安全运行和管理等内容，并从计算机数据加密、网络安全、软件安全、数据库安全四方面讲述了实现计算机安全的逻辑控制的有关理论、技术和方法。本书既着重于计算机安全本身的技术和方法的阐述，又独具特色地介绍了计算机系统安全标准、评价方法以及产品和产业等内容。

本书适合于计算机、信息、通讯等专业的师生、广大的计算机用户和进行计算机安全管理与控制的有关部门人员阅读。

(京)新登字 158 号

计 算 机 安 全 指 南

劳诚信　姜国雄
尹良洽　姚伦淳　编著

☆

清华大学出版社出版
北京　清华园
通县人民文学印刷厂印刷
新华书店总店科技发行所发行

☆

开本：787×1092 1/16　印张：11　字数：272 千字
1993 年 9 月第 1 版　1993 年 9 月第 1 次印刷
印数：00001—10000
ISBN 7-302-01268-7/TP・478
定价：7.50 元

序

以计算机和通信技术迅猛发展为特征的新技术浪潮，正把人类社会推向信息化时代。计算机和通信技术的广泛应用不仅影响了工业结构、经济结构和社会结构，而且也影响了人们的工作方式、思维方式和生活方式。

但是，在计算机系统及其网络中却潜伏着严重的不安全性、脆弱性和危险性。为此在计算机科学不断发展的同时，也诞生了一门研究计算机系统安全性（即机密性、完整性和有效性）的子学科，这就是计算机安全学。尽管它的发展远远跟不上计算机科学和技术发展的步伐，但是近二十年来，由于其他基础学科（如加密学、审计学、应用数学和计算机的基础科学）更趋成熟，在许多计算机安全研究人员努力下，计算机安全学也逐渐成为一门具有较完善学科体系的新学科，并在理论、方法、技术、应用及产品等方面形成了内容丰富的各个分支。

IFIP（国际信息处理会议）第 11 学组就是计算安全专业组，国际上还有其他世界性的研究与讨论计算机安全的会议和组织。欧美各国也都有本国的计算机安全学术研究机构。这些组织和机构每年召开计算机安全学术交流会，出版很多有关计算机安全的书籍和杂志。70 年代中期，美国就已出版了计算机安全手册，到 80 年代一再修改再版，至今已有多种手册，几个版本。这一切使计算机安全的学科体系更趋完整，更加成熟。

我国自 80 年代初日益普及计算机应用，使用与熟悉计算机的人员不断增加，这也就越来越紧迫地把计算机安全问题摆在我们面前。

本书作者在计算机安全研究方面已做了多年工作，在国内的有关会议上也提交过很多重要论文。这次他们将国内外各方面研究计算机安全的理论、方法、技术整理成一本计算机安全指南，系统地、实用地指导广大计算机用户保护好信息资源、使用好计算机，这无疑是一件有价值的工作，也标志着我国计算机安全研究已有了一定的基础。

希望这本书能为广大读者所欢迎。能以此为姜国雄等同志的书作序，不胜欣慰。

王小谟

1991.12.16

王小谟同志是 IEEE 成员、全国有重大贡献科学家、研究员、中国电子部电子科学院常务副院长。

前　言

计算机科学和计算机产业在短短五十年内迅速发展，计算机应用已深入到社会政治、经济、军事、科技、文化、甚至人们的日常生活之中。1991 年初的海湾战争实质上是一场高科技电子战争，是一场计算机战争。在此次战争中，各种类型的计算机指挥、组织和协调了几十万人的多国部队的战斗行动。然而，计算机也不是尽善尽美的，它既有促进社会发展、造福于人类的一方面，同时也存在不完善、不安全的一方面。首先，计算机如同一座发射机，它随时都向周围空间发射各种重要信息，如果不加控制，这些信息就可能被无关人员接收并利用；其次，计算机网络的普及使非法访问和恶意进入很难控制，从而造成计算机信息资源被篡改、被盗窃和被破坏；第三，利用计算机程序的可复制性和非法读写功能，制造出的各种各样计算机病毒，使全世界成千上万的计算机用户胆战心惊。

如今，计算机固有的脆弱性和潜在的危险性、以及已发生过的大量的计算机泄密、计算机犯罪和计算机病毒等事件，都极大地影响了计算机的发展和应用，给整个计算机产业和广大计算机用户构成了严重的威胁。这就使计算机安全问题提到了非常重要、非解决不可的地位。进入 80 年代，许多国家颁布了计算机犯罪法，成立了计算机安全机构、防治计算机病毒协会，等等。国际信息处理联合会(IFIP)于 1984 年成立了计算机安全技术委员会，即 TC11，专门研究计算机安全问题。该委员会每年召开一次国际会议，讨论计算机安全政策、技术、管理和控制等问题。其他的国际性会议还有国际计算机和通信安全和保护大会、国际计算机安全会议以及世界计算机病毒专题会议、世界数据库安全会议等。欧洲共同体与欧美各国都有相应的会议和常设机构。我国自 1986 年 7 月第一次在青岛举行全国计算机安全技术交流会以后，至今已召开了第六次会议。这些都表明计算机安全作为计算机科学的一个子学科正在逐步形成其科学体系。同时计算机安全又是一门技术，越来越多的人研究这一技术，应用这一技术，并使这一技术形成产品，形成产业。

美国从 1973 年起就出版了计算机安全手册，它有多个版本，各版本也在不断修订、增加和更新其内容。国内也出现过一些译文、译著和有关计算机安全的小册子。为了将世界上计算机安全技术与理论的最新成果介绍给广大计算机用户，并为计算机用户提供一本可操作的手册，我们编写了《计算机安全指南》一书，目的是使读者更为全面地认识计算机安全领域所包括的内容和出现的新成果，以开阔思路，并在实现计算机安全管理和控制上有所借鉴。

本书由劳诚信、姜国雄、尹良瑛、姚伦淳撰写，由姜国雄、尹良瑛审阅。杨海音、童建刚分别参加了第七章和第十六章的撰写工作。

本书适合于广大计算机用户，对大学计算机、电子专业的高年级学生、研究生和计算机专业的教师也是一本很好的参考书。本书同时还适合一些管理工作者阅读。

本书大部分内容取材于国外书籍和杂志、会议录。在编排、叙述方式等方面作了些增补，以增加系统性和可读性。但由于著者水平有限，书中不足和错误之处难免，诚望得到读者批评指正。

作　者　1992 年 2 月于上海

目　录

第一章　计算机安全总论

1.1　计算机安全概述

当今社会是科学技术高度发展的信息社会，人类的一切活动均离不开信息，而计算机是对信息进行收集、分析、加工、处理、存储传输等的主体部分。计算机技术的不断发展和计算机的广泛应用，促进了社会的进步和繁荣，并为人类创造了巨大的财富。同时人类依赖于计算机信息系统的程度也越来越大，从政治、经济、军事、科技、教育、医疗以及交通运输等方面逐步深入到家庭个人，应用面越来越广。可是计算机并不安全，它潜伏着严重的不安全性、脆弱性和危险性。造成不安全的因素很多，有计算机系统本身的不可靠性、环境干扰以及自然灾害等因素引起的，也有无意的工作失误、操作不当造成的，而人为故意的未授权窃取、破坏、敌对性活动危害更大。加上近年来计算机病毒严重地侵入计算机系统，不安全性就显得更为突出。在计算机系统中以微型计算机安全的缺陷为最大，也最易受病毒的感染。从目前国内拥有计算机的数量来看，90%以上是应用微机，很多部门（如军事、外交、机要部门等）采用微机及局部网络来处理信息，因此存在着严重的不安全性。这些问题至今逐渐被人们所认识，并引起了关注和重视，亦采取了很多措施尽力来解决，但问题还是不断发生。例如 1987 年 12 月 IBM 专用邮电网中数千台计算机瘫痪，35 万台终端因被“圣诞树”蠕虫堵塞，而被迫关闭，以便清除该蠕虫。1988 年 12 月美国康奈尔大学研究生莫里斯将蠕虫植入 Internet 网，使 6000 台 DEC VAX 计算机失常。1989 年 10 月美国国家航空航天管理局使用的空间物理分析网络 SPAN 两次遭到蠕虫攻击。同时有人从法国将蠕虫引入 Internet 网，几小时后它感染了 DECNET 网中 60 多台计算机，虽然受攻击的计算机没有发生丢失数据现象，但其中某些文件的名字和系统的标识却被作了更改，使用户在较长一段时间内不能注册进网。1990 年据报导 bitnet 也受到蠕虫的攻击，并与 1987 年圣诞树蠕虫的情况完全一样。尤其最近在海湾战争中“沙漠盾牌”行动的秘密也曾被黑客们捕捉到，并声称他们掌握了有关“沙漠风暴”的大量情报。甚至有人预言，今后在现代化战争中可以利用传输病毒来破坏对方的军事指挥通讯系统，使其处于瘫痪状态。因而对计算机安全问题决不能掉以轻心。

计算机安全问题引起了国际上各方面专家的重视，由国际信息处理协会（IFIP）从 80 年代初每年组织召开关于信息处理系统的安全与保护方面的技术交流会，欧洲地区也有相应的组织机构进行交流研讨。我国对计算机安全问题从 1981 年就开始关注并着手工作，由公安部计算机管理监察司牵头，在中国电子学会、计算机学会以及中央各有关部委的支持和推动下，从 80 年代初至今做了大量的工作。多次召开了全国性计算机安全技术学术交流会，发布了一系列管理法规、制度等。目前国内学者们提出，关于计算机安全的问题，正在形成为一门新学科——计算机安全学。所谓计算机安全，如何来定义，国际标准化委员会对计算机安全的定义提出建议，即“为数据处理系统建立和采取的技术的和管理的安全保护，保护计算机硬件，软件、数据不因偶然的或恶意的原因而遭破坏、更改、显露”。从这定义中可看出计算机安全不仅涉及到技术问题、管理问题，甚至还涉及有关法学、犯罪学、心理学等问题。我

们可用四部分来描述计算机安全这一概念，即实体安全、软件安全、数据安全和运行安全。而从内容来看，包括计算机安全技术、计算机安全管理、计算机安全评价与安全产品、计算机犯罪与侦查、计算机安全法律、计算机安全监察，以及计算机安全理论与政策。本书主要着重对前三方面内容进行论述。

1.2 计算机安全控制

计算机安全问题涉及到自然科学和社会科学等领域，是一门综合性新学科，要解决计算机安全问题，与社会各方面的工作有关，也是一项大的系统工程，需要综合管理和综合治理。

就是否安全而言，不管在技术上、管理上、政策法律上采取什么安全措施，都没有绝对的安全。因为任何科学均不是停留的，而是不断发展的，计算机学科发展更为迅猛，技术上总免不了存在一些薄弱环节，因此也就使犯罪者有机可乘。我们要获得绝对安全实际上是不可能的，而只能将安全分级控制在预期的范围内。因为在不同部门对安全的要求是不相同的，如军事、机要部门与厂矿企业，公司等对安全的要求差别显然会很大。即使同一部门中各种信息的重要性也是有差异的，所以不可能一概而论地控制到同一安全等级。我们一方面要从需要出发，另一方面又要考虑财力和物力的可能性。

如何将计算机安全控制在不同要求的范围内，方法有几种，其中一种是应用系统动力学的方法，可按照各部门实际所要求的系统建立一个模型，用这个模型来模拟系统的功能，考虑各种影响的因素及其相互作用关系，利用信息的反馈，需要采取的措施等使不安全因素控制在预期范围内，使造成的各种损失降低到最低限度。下面用图 1.1 所示的模型框图来说明。

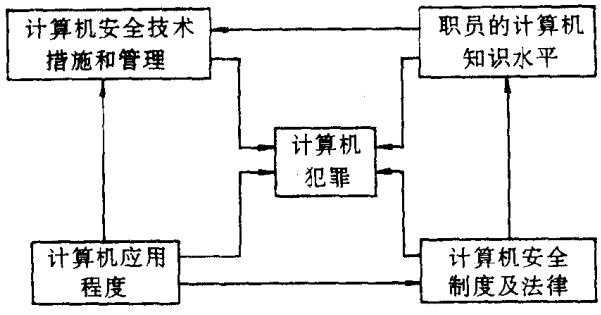


图 1.1 模型框图

计算机应用程度越高，面越广，计算机犯罪率相应增加，同时促使计算机安全制度及法律的健全。

使用计算机工作人员的知识水平越高，可能犯罪的程度亦增高(从国外计算机犯罪的统计中看出掌握计算机技术知识，从事数据处理活动的人占多数)，另一方面也促进计算机安全技术措施和管理水平相应的提高；而增加对安全技术措施的投资，反过来又抑制了犯罪率。

安全制度及法律的健全对犯罪分子具有威胁作用，相应也可起到抑制犯罪率的作用；另一方面，加强对工作人员的道德教育和法制教育也相对地能降低犯罪的可能性。

根据上述模型框图，再加上各种条件，可得到因果与相互关系的回路图，以此来预测发展趋势，然后采取必要的措施将安全控制在预定的范围内。

从这简例中可看出要解决计算机安全，对计算机安全技术措施的投资是提高安全技术水平的主要途径，但除技术措施、管理措施外，建立一整套针对计算机犯罪的制度及法律是极重要的。目前西方工业发达国家从不同角度制定了计算机安全的法律和法规，亚太地区日本、香港、新加坡等也已实施了有关法律，但总的来看还不完备，不配套，未形成完整的独立体系。如美国虽然是一个对计算机犯罪立法较早的国家，但是自 1988 年 12 月至今美国对蠕虫设计者的起诉由于法律上没有明确定义而迟迟不能判决，直至 1990 年 5 月的审判结果，犯罪者还是逃过了监禁。我国虽然计算机应用水平与美国、欧洲等发达国家相比差距甚远，犯罪率亦极低。但要用发展的眼光来看，随着改革开放的深入发展，今后计算机应用数量将会更快增长，计算机网络必然会迅速发展，计算机犯罪问题应引起重视，应吸取他人的经验尽早作好准备。

1.3 计算机安全研究现状

近二十年来，由于其他基础学科（如加密学、审计学、应用数学）和计算机科学本身的更趋成熟，计算机安全学在理论、方法、技术、应用及产品等方面也逐步完善，我们看一下当前国内外在下列几方面的研究状况。

1.3.1 计算机风险分析与管理

计算机安全措施的第一步是对计算机系统的风险分析及管理，过去主要是针对主机系统环境的保护。如瑞典数据脆弱性局提出的 SBA 系统分析法。但现今网络化信息系统迅速发展，仅对主机系统的分析就不能满足，要考虑到外部的和对通讯系统的攻击所造成对网络的威胁，因此提出了网络风险分析与管理的概念。另外也提出了研究网络化信息系统的安全标准问题，包括开放的分布式处理系统互连规程等。关于局域网的安全标准也在制订。局域网安全是在各层协议上来实现的，并要求局域网安全朝结构化联结方向发展。

1.3.2 计算机病毒与反病毒

自 1988 年以来，几次影响很大的病毒传染事件威胁着人类社会，引起了人们极大的关注，并着手研究其发展及对策。但至今对计算机病毒在定义、分类、发展、预防、检测、恢复的方法上还未有一致见解。

制造病毒的人有各种动机，可能是业余的计算机“迷”恶作剧；可能是专业人员的报复；也可能是软件公司为让一些非法拷贝软件产品的用户受到惩罚；或作为企业之间的竞争手段，所以病毒在种类上与技术上不断翻新。至 1990 年底，病毒制造者的目标是延长病毒生命期，克服对病毒的控制，提高黑客技术，以便更有效地将病毒植入系统或网络中。目前设计得越来越复杂的病毒中出现两种情况，一种是新型病毒由两部分组成，它们各自无毒又不可测，一旦两者在系统内彼此发现，结合起来则毒性发作，实行破坏。另一种情况是过去一些已发现病毒的交叉感染而形成的新病毒。

对病毒的控制主要靠管理手段，在反病毒产品上有病毒检测、阻止传染、传染检测（也称

疫苗方法)等方法。由于这些方法需要用较多时间来计算校验和及运行比较程序。1990 年初 Cohen 博士研究了高级系统保护工具 ASP,它可以保护 PC 机引导块、中断表、系统文件、程序文件、数据文件,它利用加密的校验和来保证完整性,可迅速识别并处理任何企图对被保护系统进行的修改。这套工具可在 PC 机、小型机、大型机、局部网上运行。

近年来还有人以复杂度为基础作出病毒检测模型,检测对程序的修改,防止计算机病毒传染。目前安全控制软件的发展趋势是既可高速加密文件,同时也可对文件搜寻其病毒,并报告传染程度。

1.3.3 加密学的应用

加密学在计算机安全领域中的应用通常与计算机技术相结合,从加密体制和加密算法来讲,最为流行的是 DES 算法和 RSA 算法。DES 是对称加密体制,是一种非线性的加密算法。它已成为一种标准算法,而且可用硬件来实现,为此其运算速度可大大加快,深受商业和政府方面用户的欢迎,但正因为 DES 是在公开选择、公开评论的基础上形成的一种加密算法,所以其处境有两面性,一方面是得到多数人公认,因此具有权威性;另一方面在公众评论中暴露出很多弱点。如 56 位有效密钥太短,算法迭代次数太少等,所以美国安全部门力图取消 DES,理由是 DES 的应用已广为流传,并且算法也已公开,安全威胁大。但经人们分析后,认为 DES 仍有其优点,特别是美国政府、商界、国会支持 DES。近年在修改后准备推出 DES Ⅱ 算法,目前已出现了若干增强 DES 的设想,并已开发出了产品,如用适当增大密钥量、增加密钥产生器的复杂性等措施来增强 DES 的强度,还有用提高有效密钥位,使其高达 184 位,使密钥空间扩大 2^{128} 倍,并用公开密钥来分配保密密钥的办法来增强 DES 的强度。

RSA 是公开密钥体制,90 年代获得了较为普遍的应用,该算法以大素数的多精度处理为基础,为此它的破译极为困难,保密性强。其致命的弱点在于速度太慢,这使它的应用受到限制。

在 RSA 发展方向上,近年它与常规密钥体制的结合是一个弥补各自不足的好方法。国内也在这方面做了不少工作,如航空航天部就利用 DES 和 RSA 形成混合密码方法实现航天信息系统网络终端数据加密方案。

除上述两个密钥体制外,还有不对称算法即零知识证明技术也可用于识别、鉴别、产生和验证数字签名,且不引起信息泄露。它的计算复杂性小于 RSA。零知识证明方法自 1985 年提出后,经过多次修改,至 1988 年在 OSI 内被标准化为一种通用机制。另外 CCEP 算法是美国安全局秘密设计的算法,并对制造、销售及使用这种算法的芯片实行了严格控制,因此这种算法不可能公开,也不可能得到国际承认和商业、金融界的推广。

1.3.4 安全评价

在安全评价方面,美国国防部 1985 年公布可信计算机系统的评价标准后,不断进行修改。此外英国、西德、加拿大、新西兰、澳大利亚也公布了安全标准。

美国的标准是将计算机系统按其安全性分成七类,从 D 到 A,其中 D 是最小保护,C_1 是自主型安全保护,C_2 是可控访问保护,B_1 是标记安全保护,B_2 是结构化保护,B_3 是安全域,A_1 是验证设计。

英国 1989 年也就安全控制可实施和安全目标不可实施各分成六类和五类,但专家们认

为，按这种方法是很难对系统作出安全评价的。

西德信息安全部门1989年也公布了信息技术系统可信性评价标准。它定义了八个可信等级和十类功能，利用其中各类功能或各类功能的结合实施安全政策。十类功能为：F_1 自主型安全保护，F_2 可控访问保护，F_3 标记安全保护，F_4 结构化保护，F_5 安全域，F_6 数据和程序的高完整性，F_7 高有效性，F_8 数据通信中的高完整性，F_9 数据通信中的高机密性，F_{10} 具有高机密性和完整性的网络。八个可信等级为：Q_0 可信度不足，Q_1 被测试，Q_2 方法上被测试，Q_3 方法被测试并部分被分析，Q_4 非形式分析，Q_5 未形式化分析，Q_6 形式化分析，Q_7 形式化验证。国外专家认为按此标准目前还没有产品被评价出。

加拿大、新西兰等国家公布的标准与上述有极大的类似性。

1.3.5 EFT及审计安全技术进展

电子转帐EFT的安全技术在欧洲已有二十年实践经验，EFT实质上是一个系统和网络问题。EFT的安全措施是计算机各种安全技术的综合应用。欧洲对全球性网络的货币传送和债券支付服务的信息完整性提出了全面的管理与技术措施，并提出了EFT的安全结构。在这个结构中，有一个用户管理中心，它负责密钥管理和帐户的形成，用户负责指令的形成，支付点负责检查指令与帐户，并最后批准支付。为此对这个安全结构形成的系统极重要的是要求用户通过某种形式的"签字"来提供对用户的验证，所有真正的支付指令都能追踪到发出指令的人。为了进一步增强系统安全，信息也要经过加密，密钥的产生、分配、存储等管理都有专门的程序。

另外在网络中利用计算机审计，来有效地对计算机安全进行控制，使得收集与估计计算机系统资产是否安全、数据是否完整、系统是否有效等技术更系统和完善。各种审计软件的出现使这一技术已进入实用化、商品化阶段。近年来这些审计软件已延伸到PC机。但在国际性网络中，由于通过不同的国家，每个国家都要实行自己的网络存取控制，因此使得审计更为困难，需要提出新的概念。

第二章　计算机机房的安全环境

随着计算机技术迅速发展，计算机的质量和可靠性不断提高，对环境条件的要求不断降低，为计算机的普及推广应用提供了良好的条件，然而，计算机系统是由大量电子设备、机械设备和机电设备组成的，这些设备易受环境条件的影响。因此，计算机机房的环境条件是计算机可靠安全运行的重要因素之一。

为计算机系统提供合适的安全环境有下述三个目的：

（1）充分发挥计算机系统的性能，确保其可靠安全地运行；

（2）延长计算机系统的使用寿命；

（3）确保工作人员的身心健康，提高工作效率。

2.1　计算机机房场地

2.1.1　计算机场地的组成

计算机场地的组成是依据计算机系统的性质、任务、业务量的大小、所选用的计算机设备类型以及计算机系统对供电、空间等方面的要求和管理体制的不同而确定的。我国《计算站场地技术要求》(GB2887-82)规定一般应由主机房、基本工作间、第一类辅助房间、第二类辅助房间、第三类辅助房间等组成，这些房间可以是独立的，也可以是共用的。

（1）计算机机房：是放置计算机系统主要设备的房间。

（2）基本工作房间：主要是指终端室、磁记录介质存放间、上机准备间等。

（3）第一类辅助房间：主要是指维修间、仪器室、备品备件间、资料室、硬软件工作人员办公室等。

（4）第二类辅助房间：主要是指配电室、空调系统用房、值班室等。

（5）第三类辅助房间：是指储藏室、灭火器材室、更衣换鞋室、上机人员休息室等。

除了计算机机房是必不可少外，其他房间均可视具体情况而定。

上述诸房间的组合，应坚持以下几个原则：

（1）业务上相关联的房间应尽可能的组合在同一区域内，使之便于管理和维护；

（2）对于装有振动大、噪音高（如发电机、隔离变压器等）设备的房间，应尽量远离机房或采取相应的技术防护措施；

（3）避免人员从毫无关系的房间内穿越，最大限度地防止内外界的干扰。

（4）办公室、接待室和对外开放的房间，应尽量离工作间远一些。

（5）房间的组合应使空调风管和电缆铺设距离最短，以减少投资和运行费用。

2.1.2　计算机机房面积的估算

计算机机房的面积估算的方法有下述两种：

第一种，在计算机系统配置已确定的情况下，可按计算机机房安装设备的面积进行估

算。即计算机机房的面积按下式估算：

$$S = (5 \sim 7)\Sigma S_{设备}(m^2)$$

式中：S——计算机主机房使用面积(m^2)；

$\Sigma S_{设备}$——在计算机机房平面布置中占有位置的计算机系统及其他设备的投影的面积(m^2)的总和。

式中的系数(5～7)是机房实际使用面积与设备所占面积之比。由于微型计算机设备体积较小，其系数可适当放大一些。

第二种，在计算机系统的设备尚未选型的情况下，可按计算机机房安装设备的数量进行估算。即计算机机房面积按下式估算：

$$S = (4.5 \sim 5.5)A(m^2)$$

式中：S——计算机机房的面积(m^2)；

A——计算机机房内所有设备台架数量的总和。

式中系数 4.5～5.5 也是使用面积与设备台数之和的比。对微型计算机设备来说，可适当考虑放大一些。

其他各类房间面积的计算也可参照上式两种公式进行估算。为了保证计算机用户有效地开展信息处理活动，基本工作房间和第一类辅助房间所占的面积之总和，不宜小于计算机机房的 1.5 倍。而且还应考虑到计算机系统设备的扩充，计算机机房的面积一般应留有一定余量空间，可考虑 15%～30%左右。

对于微型计算机来说，设备较小，数量较少，因此，面积可适当放宽一些。硬件与软件人员办公室等面积可按每人(3.5～4)m^2 计算。

2.1.3 机房场地的选择

1. 外部环境的选择

一般来说，计算机机房不应靠近气体污染严重的化工厂和设在强电磁场区域内，尽量避免建立在经常有落地雷、低洼潮湿、人口密集、排烟量大、有害气体或尘埃很多的区域，而应尽量建立在环境清洁、电力和水源充足，交通运输及通讯方便的地方。实际场地选择，应注意以下因素：

(1) 地质的可靠性

计算机机房所在地的地质一定要好，特别注意不要建立在以下地质区域内：

① 要避免建立在杂填土、淤泥、吹填土、流砂层以及地层断裂的地质区域上；

② 建设在山区的计算机机房，应注意避开滑坡、泥石流、雪崩、溶洞等地区；

③ 建设在矿区的计算机机房，则应避开采矿崩落区有害地段，也应避开有开采价值的矿体区。

(2) 环境的安全性

为防止计算机机房遭到周围不利环境的意外侵害，应尽量避免计算机机房建立在易燃、易爆的化工仓库附近，如汽车加油站、煤气站、军火库等附近。

另外，应避开污染区、如化工污染区、盐雾区、风沙区、煤场区及有害气体区域。

(3) 传达信息的方便性

计算机机房应有利于信息的快速处理和传递，也就是说，要充分考虑其交通运输上的畅

通性和通讯上的方便性。

(4) 场地的自然抗干扰性

为防止外界电磁场对计算机的干扰，计算机机房应与下列设施保持一定的距离。

① 计算机机房应尽量避开电气铁道、高压传输线、高频炉等设施 200m 以外；

② 应避开电波发射塔或微波线路的强电磁场干扰；

③ 应避开有强电流冲击的场所，以及强烈震动源和噪声源的地区；

④ 对有上述电磁场存在的场所，应查明电磁场强度，向供应设备厂商提供有关参数，是否允许计算机系统放置在这些地区。

在场地选择过程中，如果不能避开上述不利于计算机运行的因素，就应采取相应措施。

2. 内部场地条件的选择

为确保计算机系统的安全，对计算机机房的建筑结构提出下述要求。

(1) 计算机机房应辟为专用、独立的房间。

其目的是：① 易于限定使用人员及防止不必要人员进入机房，以简化进出管理；②有利于温湿度调整，防止灰尘进入；③ 有利于机密保护；④ 便于从自然灾害(如火灾、水灾、地震或爆炸)中保护人身安全；⑤ 简化运用计算机系统的管理；⑥ 有利于设备的安装施工。

(2) 为防止爆炸、火灾等危险，在与邻室相接处，最好设置一个缓冲地带或隔离构造。

(3) 经常使用的进出口，应限于一处，以便于进出的管理。但为了人员在事故中安全撤离及应急搬运工作简便可行，应在合适的位置上开设应急口，而进出口(包括应急口)的门，应具有足够的强度并装上锁。

要求门具有足够的强度，其目的在于：① 保护电子计算机系统、数据等不受人为破坏；② 防止外部火灾对计算机机房的影响；③ 防止地震时建筑物变形及破坏而造成进出口的封闭。

(4) 计算机机房内，为确保灾害发生时人员和设施的撤离及设备的维护，应留有必要的空间。

(5) 计算机主机房及基本工作房间建筑物的耐火等级至少应达三级标准；已记录的媒体存放间、建筑物的耐火等级应达一级标准(见国家建委标准：TJ16—74)。

(6) 计算机机房应采取防水、防漏和防渗措施，以及针对出水及灭火采取排水措施。

另外，在一些大城市，往往利用原有建筑，内部加以装修作为计算机机房。对此，场地的选择除考虑了上述条件外，尚应注意以下几个问题：

(1) 原建筑结构是否符合计算机机房的特定要求，如面积、楼板载荷等；

(2) 机房内的空间高度，在加装天花吊顶和活动地板之后，净空是否满足要求。

(3) 能否加装空调冷却水塔等设施(采用风冷式空调机则会增大投资)；

(4) 应考虑到设备从接收地到安装地的运输路线是否畅通，其中必须注意的是，建筑物的通道、门、楼梯等的尺寸是否能让设备顺利通过；

(5) 建筑是否远离变配电房，而使电源质量难以保证；

(6) 供电容量是否满足要求，有没有条件增加容量；

(7) 系统安装后，内部各设施之间的相互干扰，是否会影响系统的正常运行；

(8) 对于原建筑为高层建筑的情况，计算机机房及附属房间。应尽可能地位于二至四

层，其优点如下：

① 有利于大型和重型设备(如空调机、UPS 电源等)的安装和调试；

② 有利于计算机专用地线的安装和引入；

③ 可以减少振动的影响。当建筑遇到外界振动或发生地震时，建筑物上层的振幅远大于底层；

④ 机房设置在高层建筑的下层，有利于防火，避免建筑底层起火而自下而上蔓延，危及设在高层的机房的安全；

⑤ 可减少外界电磁场的干扰，因为空间位置越高，电磁干扰越强。

至于机房设置在底层，则不利于机房防潮和防水。这在我国华南部分地区尤为突出。

2.1.4 计算机机房的建筑结构

计算机机房的建筑结构有相当一部分不同于普通建筑，这由于系统对安装场地的特殊要求。

1. 辅助房屋的建筑结构

其要求主要是楼板载荷，因为要安装重型设备(如 UPS 电源、空调机等)。其他结构上的要求，可按国家现行有关建筑规范来确定。

2. 计算机机房的建筑结构

(1) 机房的地板(建筑楼板)

机房的地板必须满足计算机设备的承重要求。这是保证计算机系统长期、稳定运行的先决条件。依据国家标准规定，机房的地板载荷分为两级：

$$A\text{ 级：}\geqslant 500\text{kg/m}^2$$

$$B\text{ 级：}\geqslant 300\text{kg/m}^2$$

就机房地板制作材料来说，最好采用质地硬、不易起尘埃的原料，如水磨地面。而不能采用沥青瓦地板。若采用水泥地板，其表面处理必须光滑，如条件许可，应涂地板漆或采用防静电地板。

(2) 机房的围护结构

计算机机房的围护结构——墙、屋顶围护结构应满足如下要求：

① 具有足够的热阻值和适当的热稳定性，以减少外界环境对机房室内温、湿度的影响。

② 机房的主体结构在温差大和一般振动时，不易产生裂纹和尘土，墙体表面不易沾附尘埃，同时，要具有消音和抗静电的功能。

③ 机房的屋顶应具有吸湿性小、隔热性能好的特性，并具有良好的防漏水性能。

为使机房的围护结构达到如上要求，可采用两种方法；一是采用特殊建筑结构，即是利用特殊材料和特殊建造方法，在内墙贴墙纸或喷涂料处理。二是采用二次建设，在原建筑结构的基础上，在室内墙的四周附加保温墙。它不仅可以满足计算机系统对墙体的特殊要求，而且也可美化室内环境。保温墙目前多采用轻钢龙骨外装石膏板，中间填充阻燃保温泡沫塑料板结构。

(3) 机房的内隔墙

为便于分类安装各类设备，有效地控制尘埃和噪音，防止系统间的相互干扰，人们通常利用内隔墙来构成各类房间。目前，机房的内隔墙多采用轻钢龙骨为框架，辅以玻璃或石膏

板，构成玻璃隔断墙和石膏板隔断墙。这种隔断墙具有自重轻、不起灰、防火、占地面积小等优点，并有利于室内环境的美化。

(4) 机房的门

机房的门应满足如下要求：① 应防火；② 门框的尺寸应能使设备顺利通过，但也不宜太大；③ 为减少空调能量损失、避免外界尘埃、噪音的影响，机房的门要密封良好，并具有自闭功能。作为人员出入的门应能双向开闭。

(5) 机房的窗口

国外一些机房不设窗口，但由于无自然采光，照明耗电大，加之人们的居住习惯，目前国内建成的机房多设窗口，机房的窗口应满足如下要求：

① 窗口要密封良好。为减少阳光辐射和外界直射光，最好采用茶色玻璃并设置窗帘。为减少空调能量的损失，降低外界噪音，应采用双层玻璃窗；

② 窗口最好朝北，避免西晒。

(6) 主机房的净高

主机房净高，应按机框高度和通风要求而定，宜为 2.40～3.00m。

计算机机房的建筑平面和空间布局应具有适当的灵活性。主机房的主体结构宜采用大开间大跨度的柱网，内隔墙宜具有一定的可变性。

2.2 温　　度

2.2.1 温度对计算机安全的影响

环境温度对计算机可靠运行影响十分明显，据有关试验统计资料表明：

1. 对集成电路和电子元器件，室温在规定使用范围内每增加 10℃，其可靠性降低 25%。器件周围的环境温度超过 60℃时，计算机就容易发生故障。

2. 当电阻器在高温环境条件下使用时，由于散热困难将导致额定功率下降。例如 RTX 型碳膜电阻，当其环境温度为 40℃时，允许使用功率为标称值的 100%；当环境温度增至 100℃时，允许使用功率仅为标称值的 20%。又如 RT—0.125W 金属膜电阻，环境温度为 70℃时，允许使用功率为标称值的 100%；当环境温度升至 125℃时，其允许使用功率仅为标称值的 20%。实验表明，温度每升高或降低 10℃时，其电阻值大约变化 1%。

3. 温度对电容的影响主要是使其使用时间缩短，其次是引起电容量和功率因数等参数的变化。实验证明，在超过规定温度工作时，温度每增加 10℃，其使用时间将下降 50%。温度过低，电解质会冻结，使电阻增大，损耗增加，等效电容减小，甚至完全失去作用。

4. 温度过高，会使半导体和机械装置内的腐蚀过程加速。例如，印制板，插座金属簧片等容易腐蚀，使接点接触电阻增大，性能变坏，可靠性变差。

5. 温度对磁介质导磁率变化也有影响。当温度升高到某一值时，磁介质导磁率下降，甚至失去磁性，高温会使磁带、磁盘中的数据发生错误，甚至丢失。

6. 温度过低会使绝缘材料变硬、变脆、结构强度减弱。由于收缩系数不同而使插头座发生接触不良。转动部分会因润滑油受冷凝结。粘度增大出现粘滞现象。

7. 温度梯度变化太大，其所产生的内应力以及交替冷热变化会加速元器件、材料的机械损伤和电气性能的变化。