计算机安全
译 丛

（美）诺尔曼L．英格　　保尔W·霍威顿

计算机安全技术与方法

COMPUTER SECURITY

《计算机技术》编辑部

计算机安全技术与方法

《计算机技术》编辑部

计算机安全技术与方法

诺尔曼L·英格
〔美〕保尔W·霍威顿 著

陆小兵 黄 煦
陈敦文 刘金铎 译

方 普 校

《计算机技术》编辑部编辑出版
北京市期刊登记证号第410号

*

1986年7月第一版 1986年7月第一次印刷

译 者 序

在现代社会中，计算机的社会化程度正在迅速提高。大量与国计民生、国家安全有关的重要数据信息，迅速地向计算机系统集中，被广泛地用于各个领域。

但另一方面，计算机系统又处在高科技下非法的以至敌对的渗透、窃取、篡改或破坏的复杂环境中，面临着计算机犯罪、攻击和计算机故障的威胁。事实上，计算机的脆弱性所导致的诈骗犯罪，已经给计算机化发达国家和公众带来严重损失和危害，成为社会注目的问题。因此，许多国家在走过一段忽视安全的弯路后，都在纷纷采取技术、行政和法律措施，加强对计算机的安全保护，至今已有二十多个国家制定了计算机安全法律、法规，建立了计算机安全管理、监察和审查机构。

在我国，拥有计算机和计算机网络系统的单位愈来愈多，计算机在国民经济、科学文化、国家安全和社会生活的各个领域中，正在得到日益广泛的应用。计算机社会化道路是我们已开始步入并将继续发展的道路。世界计算机应用发展的历史表明，人们应当客观地看待计算机。既要看到它是推动社会发展的强大工具，又要看到它面临的脆弱性、危险性；既要重视发展它的应用技术和措施，又要重视发展它的安全技术和措施，保证“计算机安全与计算机应用同步发展”。

正是出于这样的认识，我们将这本外国专家的著述，介绍给我国关心或致力于计算机应用发展的工程技术人员、管理工作者、教育和安全工作者。

全书共十三章，向读者描绘了计算机安全工作的整体轮廓。包括人员和组织机构管理、系统开发安全设计和数据安全保护、机房设施的实体安全保护和计算机安全监察、管理、审查工作等四个方面。本书的主线是安全管理，围绕安全管理的需要，全面介绍了计算机安全技术设计的原则方法，防止计算机滥用和事故的技术要点和要求。读者会感到本书对安全措施的具体实现叙述得不够。据译者所知，这似乎是目前国外计算机安全文献资料的“通弊”，这或多或少地反映了对计算机安全的敏感性，是可以理解的。

应当指出，原书的某些取材、内容和观点，不尽符合我国的情况，有的与我国情况相差甚远。因此，切忌对原书不加分析地生搬硬套，而应吸取其中有益的东西。

由于计算机安全的术语尚未统一，本译文主要根据术语的前后文内容，参考通用译法译出，在书末给出了主要术语的英汉对照，读者可以在正文中找到这些术语的基本含义。

本书所涉及的学科和业务的门类相当广泛，译者虽然力求翻译准确，但由于知识水平和实践经验的限制，讹译之处在所难免，尚望读者给予批评指正。

在翻译出版过程中，始终得到国内计算机安全管理监察部门及有关业务部门专家的指导和帮助，译者对此深表谢意。

原书前言和第一至三章，第四章，第五至八章和书末名词索引，第九至十三章分别由陆小兵、黄煦、陈敷文和刘金铎译出。全书由方普审校并译出书后的附录。

译　者

一九八六年于北京

原 作 者 前 言

本书旨在填补有关计算机安全技术书籍中的空白。浏览计算机方面的出版物，虽然可以找到不少的著作来指导计算机工作者怎样使用计算机化的信息。然而对他们来说，在如何保护计算机各类信息资源的安全时；在决定对投资采取何种防护措施时；在估量信息资源受损失的后果时；在弄清计算机犯罪带来的现实冲击时，却找不到参考书。

政府和工业部门对信息处理系统的投资逐年增长。即使就物质价值而言，信息处理系统及其各类资源也应和生产或服务资产一样受到保护。根根我们的经验，一些高级管理人员只把计算机和计算机技术看作从事工作的必要手段，并不考虑失去这种手段后对整个工作产生的后果。我们认为第一应提醒计算机工作者，我们现在已如此强烈地需要在各类工作中依赖计算机这种新型的工具；第二正因为如此，应向他们指出怎样针对犯罪性渗透和其它滥用，来设法保护计算机信息资源，以及信息系统的安全。

不断增长的白领（知识型阶层）犯罪表明，安全和保密是所有计算机工作者面临的重大课题。这涉及到机构面临的来自计算机系统不安全因素的威胁，它包括：贪污舞弊、盗用信息资源、篡改信息资源以及其它各种破坏。

还要考虑一些间接的问题。公众对政府和私营企业大量使用存在计算机中的个人数据越来越敏感。1974年美国《私人机密法》规定了政府机构处理私人数据的责任。目前美国各州也分别开始就保密和计算机犯罪问题立法。某些国际组织正在研究信息跨国传递问题。因此私营部门将受到有关立法的严格约束。这些法律规定了个人信息的收集、使用的控制，对计算机犯罪（如计算机贪污诈骗）的起诉，以及信息处理机构在保护机密信息方面应承担的责任，这些信息如医疗、信贷信息等与广大公众的利益有较大影响的信息。

我们确信，安全保密计划须经机构的最高领导审定才能成功。必要的安全政策应该传达到机构的各部门并被采纳。即便安全措施还不十分完善，领导也必须给予支持和实行。无此决心，机构就不可能有效地保护计算机各类资源的安全。

多年来，我们尽力帮助政府和私人部门的领导认识机构面临的与计算机有关的威胁。同时，我们还帮助他们就可行的对策进行决策性风险分析。这些分析的依据除来自从事计算机及有关技术工作近五十年的经验外，还取自于我们为联邦政府机构和许许多多州及市镇各级政府机构做出的工作。例如：美国审计总署、美国联邦调查局研究院、中央情报局、卫生教育福利部。我们在Sperry—Univac、National Cash Register、Control Data Corporation从事的工作和在私营公司的IBM设备上进行的系统设计和监察，也使我们获益非浅。这些机构遇到的特别问题，正是本书各章介绍的安全保密方法的基础。

我们和肖伯纳一样相信"没有实践的理论等于空话"。我们不是唯理主义者，我们提出的"改革样板"方案曾经全面验证。书中的审核检查表的目的是帮助机构针对各种与计算机有关

的威胁找出其脆弱性。

本书在手稿打印和编辑方面曾得到ELBA · HERNANDEZ与MARYLOU · BATSON的大力帮助，在此一并致谢。

N.L. 英格
P.W.霍威顿

原书作者介绍

原书由诺尔曼L·英格和保尔W·霍威顿共同著作。

诺尔曼L·英格是美国马里兰州伯茨达市应用管理系统公司的董事长，在他组成自己的咨询公司之前，曾任数据控制公司董事。英格先生著有《计算机应用》、《公众管理》、《计算机系统文件标准》、《检验管理信息系统（MIS）的AMACOM专题》、以及《开发信息系统的管理标准》等著作。

保尔W·霍威顿是华盛顿美国大学计算机专业的著名助理教授，在计算机安全领域中，他是系统设计，罪犯审判信息系统以及金融通用系统方面的私人顾问专家。

目　录

第一章　绪论……（1）
　第一节　安全问题……（3）
　第二节　私人秘密……（7）
第二章　机构的安全职能……（11）
　第一节　机构的职能……（11）
　第二节　各项工作中的责任……（13）
第三章　人事……（15）
　第一节　人事工作……（15）
　第二节　安全怎么会出问题……（18）
　审核检查表……（20）
　第一类：人事……（20）
第四章　系统开发……（22）
　第一节　项目管理……（22）
　第二节　结构化程序设计……（24）
　第三节　主任程序员小组……（26）
　第四节　结构化预查工作……（26）
　第五节　开发支援数据资料库……（27）
　第六节　系统开发生成周期……（27）
　第七节　项目文件……（29）
　第八节　系统测试……（30）
　第九节　系统验收……（30）
　第十节　安装后的检查……（30）
　第十一节　系统变更……（30）
　审核检查表……（31）
　第二类：系统开发……（31）
　附录：信息系统的功能说明概要……（35）
　功能说明表……（40）
第五章　输入控制……（61）
　第一节　职责分离……（62）
　第二节　文件控制……（63）
　第三节　总数控制……（63）
　第四节　控制小组……（64）
　第五节　程序控制……（64）

第六节　操作控制……（67）
第七节　设备控制……（68）
第八节　建立文件规程……（70）
审核检查表……（71）
第三类：输入控制……（71）
第六章　联机处理……（75）
第一节　管理安全措施……（76）
第二节　用户标识……（76）
第三节　防入侵的安全措施……（78）
第四节　通信网络的安全……（78）
第五节　传输线路的安全措施……（81）
第六节　信息完整性的安全措施……（83）
第七节　终端的安全措施……（84）
审核检查表……（86）
第四类：联机处理……（86）
第七章　软件安全……（89）
第一节　应用程序……（89）
第二节　操作系统……（90）
第三节　数据库管理软件……（91）
第四节　软件维护……（97）
审核检查表……（98）
第五类：软件安全……（98）
第八章　输出控制……（101）
第一节　质量控制组……（102）
第二节　输出的传播……（102）
第三节　输出检查……（102）
第四节　用户机构……（103）
审核检查表……（104）
第六类：输出控制……（104）
附录：用户手册提纲……（106）
第九章　操作环境……（115）
第一节　责任的划分……（115）
第二节　计算机操作……（115）
第三节　产品控制……（115）
第四节　生产调度……（116）
第五节　产品文件……（116）
第六节　质量控制……（117）
第七节　记帐系统……（118）
第八节　设备维护……（119）

审核检查表……（120）
第七类：操作环境……（120）
附录：产品文件样本……（123）
第十章　实体安全*……（127）
第一节　实体设备的位置……（127）
第二节　实体访问的控制……（127）
第三节　机房的防火……（128）
第四节　电源保护……（131）
第五节　水灾和水的防护……（131）
第六节　风暴的防护……（132）
第七节　地震的防护……（132）
第八节　空调……（132）
第九节　电磁幅射……（133）
第十节　磁性媒体的处理……（133）
第十一节　磁带和磁盘库……（133）
第十二节　文件库……（134）
第十三节　贮存和处置手续……（134）
第十四节　要求无关人员离开现场的处理……（134）
审核检查表……（136）
第八类：实体安全……（136）
第十一章　应急计划和备份……（140）
第一节　应急计划……（140）
第二节　要害记录程序……（141）
第三节　备份和恢复计划……（141）
第四节　对应急计划的评定……（143）
第五节　交易处理登记……（144）
第六节　数据库备份过程……（144）
第七节　恢复和重新启动过程……（145）
审核检查表……（147）
第九类：应急计划和备份……（147）
第十二章　审核……（149）
第一节　审核检查员的资格……（149）
第二节　审核检查项目……（151）
第三节　系统设计的可检查性……（152）
第四节　环境控制……（152）
第五节　应用的检查……（153）
第六节　管理和实体安全……（154）
第七节　远程通信安全……（154）

* 也称物理安全(Physical security)，为统一起见，正文部分均称实体安全。

第八节　计算机程序……（154）
第九节　数据的完整性……（154）
第十节　审核检查技术……（155）
第十三章　风险分析……（157）
第一节　安全分析机构……（157）
第二节　定量技术……（158）
第三节　安全对策概述……（162）
附　录……（164）
佛罗里达计算机犯罪法
——美国佛罗里达州议院第1305号议案……（164）
索　引……（167）
英中名词对照表……（167）
补充读物……（191）

第一章 绪 论

每年因计算机诈骗造成的损失，美国总商会估计为一亿美元，而《哈佛商业观察》最近刊载的一篇文章估计为30亿美元。这仅是极粗略的估计。据美国商务部说，一百例这类犯罪中仅有一例被发现。而被发现的罪行中只有20%被披露。至于受起诉的就更少了。

还有更令计算机工作者（包括各类系统设计者、机器的使用者、管理者）关切的有关计算机的问题，如资源信息保护、个人信息跨国传送问题、越权使用计算机设备、程序以及贪污等的防护。更有甚者，很多观察家指出，最严重的损失是由某些心怀不满的雇员或前雇员引起的。他们蓄意修改、破坏机构日常工作程序，企图中断机构的活动。经常有这类败坏信用的惊人新闻。

为了私利或报复而滥用计算机已极为严重，因而自1979年1月1日以来，美国各部门已提出了130项法案。第一个通过计算机犯罪法的州是佛罗里达州。该法成了其它州的样板。佛罗里达法案的提案人说他不能坐视--种新的犯罪出现在佛罗里达。他认为，认识计算机犯罪的可能性并立法治罪可起防止犯罪的作用。他显然是对的。因为自1978年8月1日《佛罗里达计算机犯罪法》（全文见本书附录）生效以来，还未曾引用该法提出过一次起诉或做过一次判决。另一位提案者——现为美国众议员的比尔·奈尔松（BILL NELSON）——建议以佛罗里达法案为蓝本在国会提出一项法案。目前一些法案正在经过国会的复杂立法程序，例如康乃狄格州参议员亚伯拉罕·里比考夫（ABRAHAM RIBICOFF）提出的法案。

这些法案奉劝主要依赖计算机进行管理的公司密切注视有关立法工作的进展，防止快速发展的公司业务和法案内容冲突。安全无疑带来限制，所以安全措施应以能恰当地保护公司利益为限。管理者应该谨记：安全在于深思熟虑，而不仅仅是规章制度。

为保护资源，怎样进行风险决策？我们发现，在这方面缺少供各计算机公司领导者使用的指导书。对此，我们奉献这本以长期工作经验为基础的指导书。我们的经验来源于各类计算机系统的设计、研制和使用。这些系统有的仅要求最基本的安全，有的则要求关系到国家安危的最高级安全。本书要讨论蓄意修改或窃取数据问题、机器失效问题、传输错误问题、火灾和水灾问题、程序错误和计算机操作员错误及玩忽职守问题，故意破坏、罢工和窃取计算机服务等问题。书中给出的《审核检查表》，可以监察这些威胁，并对机构弱点做出估计。例如，计算机工作者可用这些表做出风险分析，找到弱点，选取对策。

借助本书可以明确所有有关人员的职责，保证贯彻和遵守防护措施。本书还可帮助机构熟悉安全计划的范围、内容和步骤。计算机工作者运用本书的原则，做到：

①按照条件恰当地勾画安全计划并定义安全保护的级别。

②建立一支计算机安全队伍。

③指导风险分析和成本效益分析，平衡安全的要求和费用的增长。

④制定措施，尽量减少信息的越权使用。

⑤制定标准和方法，使安全措施的制订和实施能符合机构的总目标。

⑥采取措施加强数据处理设施的实体保护。

⑦制订处理各种灾害的应急计划。

高级决策者必须制订一项全面的安全行动计划和实施计划的方法。计划中应包括：软件安全、现场出入控制、恢复措施、关键数据登录程序、通信线路安全和人员安全等内容。本书提到的防护和控制，适用于所有工作人员、系统用户和支持服务的厂商。

总之，决策者必须把制订安全计划看作是和决定经营方向同等重要的领导工作。两项工作都是使各项工作持续发展所必要的。另外，他还必须清楚，在他所管理的某个大的部门或公司中，对计算机(除系统本身外，还包括各种软、硬件资源、数据等等)的投资远远超过办公设备的费用和操作人员的工资。因此高级决策者组成的指导委员会必须对各种可能情况进行决策，以适当的方式保护计算机资源，就像采取措施保护工厂不受破坏一样。管理工作者畏惧数据处理的时代已成过去。不应再指望数据处理负责人负责做出有关公司发达的决定。请记住芝加哥有家公司丢失了存在计算机中的全部收帐文件，不得不请顾客自报应付贷款。该公司由此领悟到公司计算机中的文件有多重要。

甚至于部门负责人只决定计算机文件的内容，而不负责制定应执行的安全措施的时代也已成过去。今天，部门负责人交给数据处理人员既要处理的数据、又要负责安全的任务会被直截了当地拒绝。

那么目前数据处理发展到了什么阶段呢？显然，我们正变得或在某种程度上已经变得明智了。即在系统设计阶段计算机系统工程的设计人员就有明确的原则，并严格要求（系统设计）做到使用户满意。同时，拨出专款用于数据保护，就像拨款造围墙不使外人闯入工厂一样。系统设计者必须解决的基本问题是：如果不加保护，以信息形式存在计算机中的各种资产（例如：部门、公司、企业、个人的大量数据）会出什么问题？这些年来，管理信息系统（MIS）引起了人们的注意。我们认为，MIS至少在现在，意味着管理应参与到各个系统中，并贯穿在系统的整个生存周期中。它包括：需求分析、逻辑设计、物理设计、建成、测试、转换、运行和评价。用一句众所周知的话来说，就是：数据处理操作的实施极为重要，以致不能只让数据处理器和数据处理者单独负责。

本书建议的管理主要有：

①人员—人员的安全问题不仅关系到数据处理部门内部的全部管理、分析、程序和操作人员，还关系到由用户、竞争对手、罪犯、某些心怀不满的前工作人员、客户和数据中心职员的“朋友”等引起的外部问题。改进后的录用等人事制度，结合机房、软件及各方面的安全措施可以减少来自外部的威胁。例如，心理管理努力加强职工的“安全认识”，在机构内形成一种安全气氛。这包括加强职工的职业道德和坚持一项正规的安全培训计划。

②系统开发—在对新的计算机应用领域进行开发和老的应用进行修正的过程中要使用一系列控制，包括：定性控制（如编辑校验、一致性和关系校验），定量控制（如控制总数、计数和分批总数、冗余总数、会计总数），审计控制，程序维护控制（程序设计和编写保证日后正常修改易容），测试控制（用特意挑选的仿真数据测试系统，检查各种条件下的数据处理）。另外，管理参与系统设计，将保证对自从计算机成为共同管理的一种重要辅助手段以来，有了发展的这种“秘密语言”（arcane language）的理解。

③输入控制—输入控制的目的是：在把源数据转换成机器可读形式的处理过程中，检验这种处理过程的完整性。这关系到原始文件、数据转换、设备和数据录入、校验及编辑等各

种应用程序。

④联机处理—终端安全要考虑所用终端标识键的类型、终端安放场所的实体安全、终端安全锁装置、终端关闭方式、终端输出的分发、终端用户的唯一识别和数据加密。设备故障、信号幅射和线路窃听都可导致非法窃取机密信息。

⑤软件安全—可用软件检查用户识别号或用户识别“键码”，设定每个用户的主文件或用户描述，指定每个用户所能存取的特定文件。每个用户经授权可存取特定的文件，保密性软件可以大大减少用户意外地存取机密文件的可能性。软件控制包括用户应用程序、计算机操作系统和数据库管理软件。

⑥输出控制—输出控制的目的是确保计算产生的输出可靠并不受越权更改。输出控制既要保证给用户可靠的输出，又不必缓慢费事地检查每个输出记录。计算结果的分发也与输出控制有关。

⑦运行环境—运行控制关系到计算机系统的日常管理。磁媒体保管、存取保护、机密数据识别、信息存贮和传送、信息生产控制、磁带库管理、计算机运行、脱机处理等工作都必须有条有理。

⑧实体安全—实体安全包括保护计算机设备、程序和文件不受破坏、篡改和越权使用，还要防止火灾、洪水、风暴、事故等外界的危害。实体安全手段有：锁、警卫、证章和出入控制。计算中心必须保证硬件和软件正常工作，保证应用程序和数据传输的正确性、防止电源故障，防止磁带、磁盘受损伤，磁存贮媒体受损后信息就无法读出。

自然灾害有火灾、洪水、战争等灾害。火灾、洪水、风暴、地震、机械设备故障（空调问题、断电）、暴力行动（社会动乱、心怀不满的雇员或前雇员的恶意行为）等都会造成数据的丢失。轻则干扰或打断日常工作，重则造成机构瘫痪

⑨应急计划和后备—领导制定的灾害恢复计划必须包括后备、检查和恢复措施。应急计划的目的是在严重破坏或灾害情况下保证主要工作继续进行。对火灾、洪水、断电、社会动乱和炸弹威胁之类的危险应分别制定措施。应急计划的目标是保护生命、减少财产损失、缩小灾害对工作的影响。安全计划中应有救灾措施和救灾设备。在计算中心外应建立程序和文件后备，以便在重大灾害后恢复工作。

图1是安全保卫与系统组成单元和安全问题的关系。本书阐述的安全计划力求减少不安全因素，并在一旦安全出问题时把损失降到最低，尽量缩短恢复损失的时间。但是读者必须记住，没有百分之百的安全。我们所能做的一切就是把数据处理系统的脆弱性和面临的威胁讲清楚，而保护程度或等级的确定完全取决于管理的需要。

第一节　安全问题

安全问题指防止篡改、越权获取和蓄意破坏信息以及自然灾害的破坏。在经济和其它领域中使用计算机技术产生了新型的犯罪行为。由于计算机环境下的犯罪极难察觉，更助长了犯罪气焰。这类白领犯罪包括更改计算机程序磁带后，用正常手段从帐户上转移资金。有的案例中使用计算机程序非法检索不应获得的数据。因为根据现有法规、法典对计算机犯罪活动的侦察、定案、起诉和预防都是大问题，所以要控制计算机犯罪活动很困难。可以预见，由于投入使用的计算机系统迅速增加，问题会变得更严重。因此，对从事打击计算机犯罪工

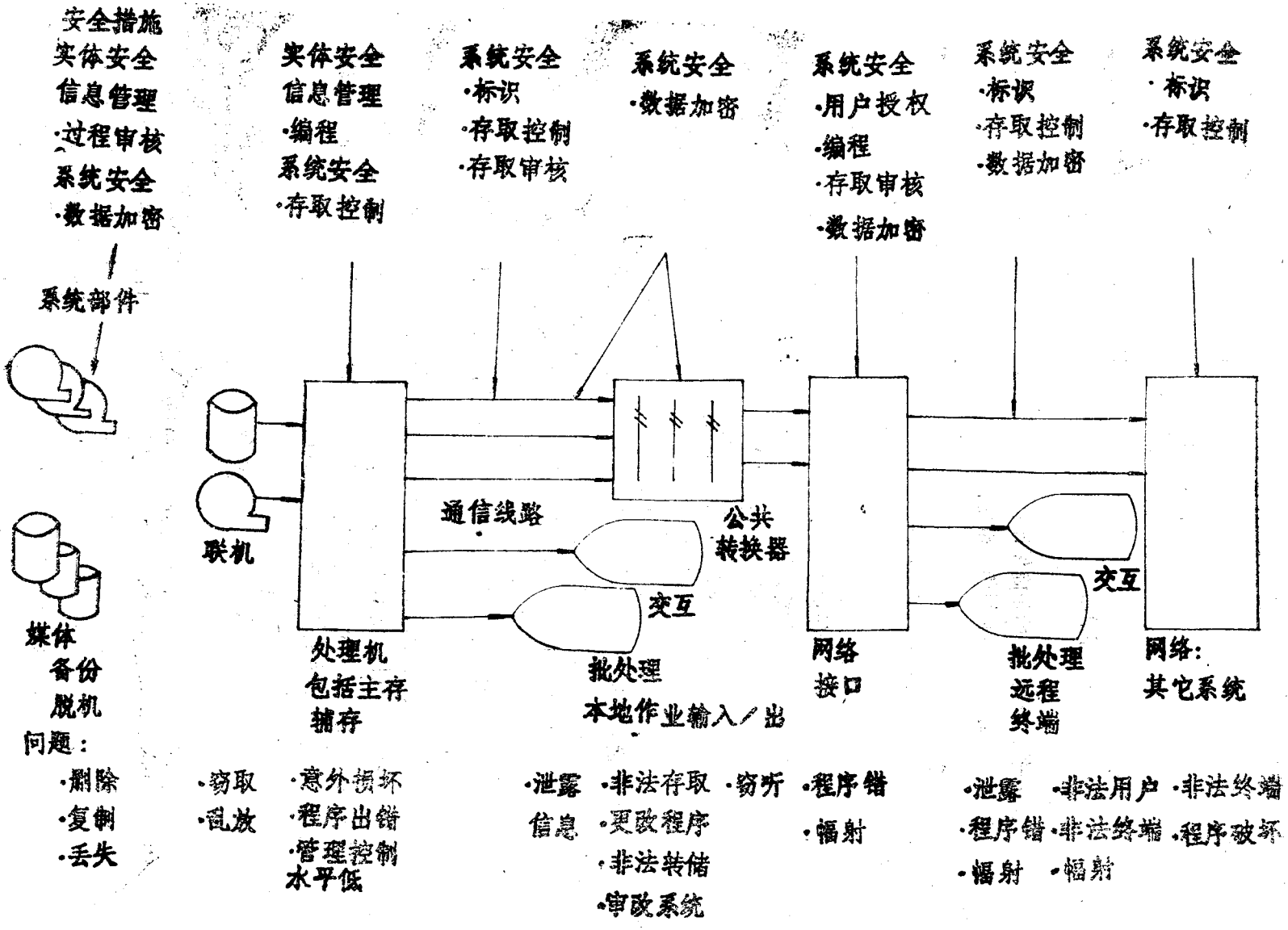

图 1　数据安全的技术保护和系统控制点

本图出自美国国家标准局计算机科学和技术研究所1975年4月公布的《执行1974年私人机密法的指导原则》。

作的人员进一步训练的必要性也大大增加。

报载的泄露机密事件的主要原因在人的因素。个人确实能错用或滥用设备以及信息文件，毁坏设备、程序和文件。有能力越权访问并进而修改和使用信息的人对系统安全的威胁最大。

（对计算机系统的）犯罪性渗透活动牵扯到贪污受贿、敲诈勒索。一起重大犯罪可能牵涉某个贪污者或领高额报酬的工业间谍。有些人试图从远程终端上，击破安全防范进入计算机系统，并从计算机文件中取得信息。计算机中心内部人员可能和外部人员同谋窃取、修改、滥用信息。蓄意侵入信息系统进行经济犯罪是影响重大的问题。政府和企业的某些文件有很高的商业价值，因此就成了隐藏入侵者的目标。最常见的有敲诈、盗窃、贿赂、造假帐、间谍。

据报导的大量案例中，对政府机构、银行、保险公司、交易所进行诈骗的，主要是数据中心内部的人员。外部人员问题则涉及用户、竞争者、罪犯、合同对方及计算中心职员的"朋友"。外部威胁总会牵涉到某个人，或者是计算中心内部人员，或者是内部人员的同谋，他们为不可告人的目的或个人利益，企图冲破安全防范获得机密或有价值的信息。

机密信息的意外泄露也是个严重问题。最典型的就是负责人把机密文件随便放在办公桌上。另一常见原因是从终端输出数据的方法不对。领导对安全措施支持不力，职工也就不会把安全措施当作一回事。领导把外人带入机要区会鼓励下属同样如此。

人员无意造成的错误有：操作员错误、数据转换错、程序或文件使用错、磁带和磁盘使用不当、程序出错、终端操作错误（这是影响工作的主要原因）。据估计60%的损失由人员失误引起。贪污、罢工和心怀不满的计算机操作员、程序员、磁带保管员和用户，能造成严重的损失。

调试不完善的程序，匆忙转换的源文件数据，对职工人品道听途说的了解，管理不严的信息系统等，这一切都会导致错误的、有害的、不完整的信息。

和安全问题有关的软件有用户程序、计算机操作系统和数据库管理系统。图谋从机构诈骗或贪污钱财，或许就得篡改计算机程序。计算机操作系统和数据库管理系统则控制生成、更改和检索文件以及控制用户对信息的存取。

至今最大的计算机犯罪是1973年揭露的公平债券（EQUITY FUNDING）公司丑闻。这桩诈骗始于1960年初，十年中经过了几次演变。美国公平债券公司经营相互债券和保险。公平债券公司搞了个别出心裁的计划，把相互债券和人寿保险搭着出售。这种搭配就叫作"公平债券"。这么做的想法是顾客可以用买下的相互债券作为买人寿保险贷款的副保。这种公司的成功取决于公司赚取利润的能力和保持公司普通股票价格稳定或上升的能力。这样才能建立顾客的信任和促进投资。公司合伙人策划的诈骗头一阶段（也叫"债券诈骗"）是资产膨胀并抬高公司普通股票的市场价格。

诈骗开始是虚报公司收入，在公司帐册上假造佣金收入。假造的账目既没有原始单据和实际顾客，也没有任何联系。直到1968年公司由于连年经营不善而面临严重的流动资金不足以前，骗诈花样虽然不少，但基本限制在这个范围内。

到下一阶段，诈骗扩大到了保险。即假造保单并重保。重保在保险业是很普遍的业务，保险公司把保单转售给其它保险公司。这样做是为了在支付大笔赔偿时分散损失。通过计算机程序，把伪造保单和合法保单混合起来，以掩盖罪行。伪造的账目表面上完全合法。对假账目提的赔偿要求，当然得由重保假保单的公司支付了。提多少赔偿要求，怎么提法，怎么

做账，都由计算机统计完成。为了维持骗局，每年假造的文件在二万至五万之内。假保单署上新人名和保单号后和真保单混杂在一起。

问题的严重还在于仅仅是由于偶然原因，这桩罪行才遭败露。公平债券公司解雇了一名职员，该人为此大为恼怒、揭发了骗局。本案起诉了22名当事法人，向公平债券公司的股票持有者支付了约六千万美元。这笔大数目也只是赔偿了大多数人15—20%的损失。公司破产经纪人报告说，计算出公平债券公司在市场上流通的人寿保单纸面价值为32亿美元，而其中21亿是伪造的。

1978年10月发生了一起计算机盗窃银行案。《时代》周刊用整整一版篇幅作了报道。这起历史上最大的银行盗窃涉及联邦储备银行电子汇兑系统和洛杉矶安全太平洋银行。该银行的一个合同计算机顾问被指控有罪。这个顾问仔细研究了银行的安全措施和资金汇兑识别码冒充银行高级职员向一家瑞士银行户头转去了1020万美元，接着买下了价值810万美元的宝石。他返回美国时被联邦调查局逮捕。就在这起盗窃案开庭前二个月，这个32岁的计算机专家再次被捕，被控企图用计算机从洛杉矶联合银行向美国银行旧金山分行骗汇5千万美元。

在纽约，联合小额储蓄银行的出纳主任从储蓄账目上贪污了1500万美元。多年来，他用计算机终端篡改账目，掩盖痕迹，一直很得手。出纳主任篡改了银行计算机系统的纠错程序。这样，虽然账目实际上不对，但银行得到的计算机打印报告却表明账目正确。一次，警方袭击了一家赌场，发现出纳主任每天为赛马和其它比赛下的赌注达3万美元之多。这才发现了诈骗。

在来往账目上作假，贪污的数目历来超过其它诈骗。几年前，对华盛顿特区里格全国银行的诈骗手段高超极了。一天，一个不知名的人走进银行，拿走顾客台存放的全部存款单，换上了他的经过电子编码的存款单。三天中，到银行来的顾客，只要没用私人专用存单而用了桌上的“空白单”的，都把钱存进了罪犯的户头。罪犯第四天取出10万美元后大摇大摆地走掉。直到最近（1979年），该银行才规定用事先印好的存单存款要有存款人账号。

计算机犯罪还包括盗窃通信录和经营计划。例如，大英百科全书公司的一些职员窃取了公司存在计算机里的“最宝贵的”顾客名单，卖给了竞争对手。名单估价为3百万美元。又如，英国航空公司的经营计划被盗卖给了竞争对手，估价亦为数百万美元。

纽约有家大银行，曾是尾数骗取程序的受害者。尾数是一分或一元以下不计入利息的另头。一些程序员巧妙地修改了结账程序，把尾数加到自己户头上。会计审查，只能看到支付的利息总数是正确的。西德发生的一起类似犯罪，罪犯就是把兑汇的尾数加到自己户头上。

这类盗窃特别难发现。尾数窃取者从自动系统捞到了巨大好处，而在15年前的人工系统上同样的盗窃几乎不可能。同样的犯罪，手段却不一样。一般地判断某次犯罪是否是计算机犯罪，只要看如果没有计算机，这起犯罪是否造成同样的后果。

在华盛顿特区，国家税务总署计算中心的几名工作人员用计算机骗取加班费、病假和休假。这些人认罪后立即被开除了。几天后，总署头头得知，没有这几个人操作计算机，算出来的工资表怎么也不对。为此，只得临时把这几人请回来。真是令人难堪。

据另一案件公布的材料，加利福尼亚有个19岁的小伙子在垃圾桶里拾到一个太平洋电话电报公司的计算机代码本，于是就开始经营起自己的事业来。他只需要一台按钮电话并把电话与一台无保护的远程终端的正确口令搭接上。他很快准备好，用窃听电话订购了价值百万美元的开关板和电话机。这些货有的运到外地，有的由他伪装成电话工程车的卡车提走。他把窃