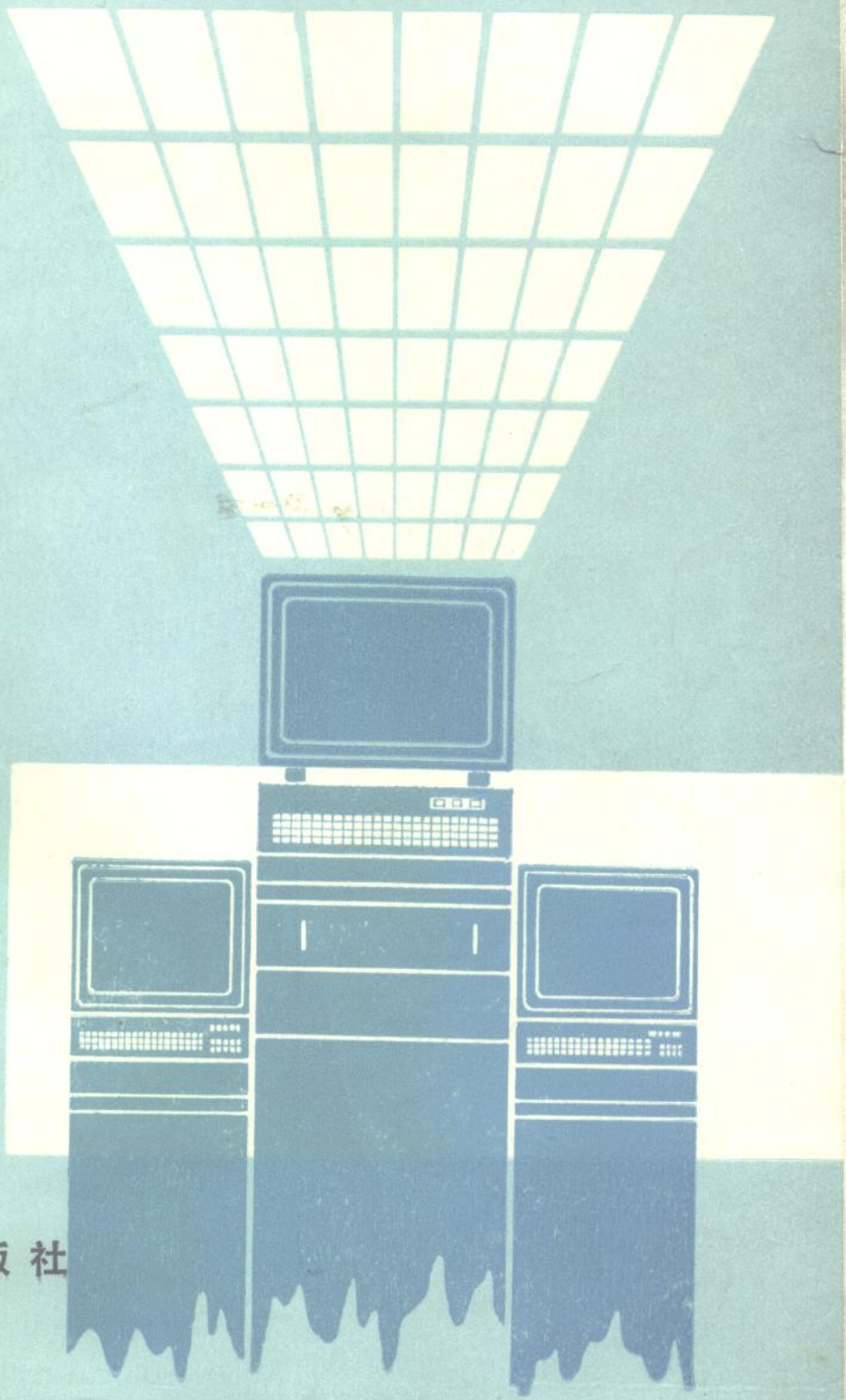
国家自然科学基金资助项目专著

# 计算机信息保护

魏仲山 编著



天津大学出版社

国家自然科学基金资助项目专著

# 计 算 机 信 息 保 护

魏仲山 编著

天 津 大 学 出 版 社

## 内 容 提 要

本书讲述计算机信息保护的原理和方法。全书以信息保护七层模式为起点，阐述了信息特征及其保护环境，提出信息保护法原则、管理操作保护和实体保护措施，并对硬件保护、通讯网络保护、软件保护、数据库保护的理论和方法做了详细的论述。

本书可供计算机应用人员阅读，也可做为高等院校有关专业的教材。

计 算 机 信 息 保 护

魏仲山 编著

*

天津大学出版社出版

（天津大学内）

河北省永清县印刷厂印刷

新华书店天津发行所发行

*

开本：787×1092毫米 1/16 印张：17 字数：430千字

1989年9月第一版 1989年9月第一次印刷

印数：1—4500

ISBN 7-5618-0160-2

TP·21

定价：7.85元

# 前　言

随工业化社会向信息化社会过渡的世界潮流，计算机应用日益深入到各个领域，计算机网络迅速发展，智力产权也出现了。这说明，计算机信息已经并将成为高度文明社会的基础和支柱。然而，由于计算机信息系统和网络本身的脆弱性，计算机信息常常受到干扰、滥用、溢漏和丢失，甚至被泄露、窃取、窜改、冒充和破坏；计算机可能受到“病毒”感染而工作瘫痪。这些现象层出不穷，防不胜防。早期的计算机信息保护只限于防止计算机系统技术性事故和无意失误的特定范畴。随着计算机应用领域扩展，尤其是计算机通讯网络的出现和发展，对计算机重要、机密和敏感信息的窃取、窜改和破坏时有发生，因而造成了巨大损失。利用计算机犯罪成了突出问题。由于技术性事故、无意疏忽和蓄谋作案的界限混淆不清，若干技术、经济、管理上问题也交织在一起，所以当今世界计算机信息保护同计算机安全保密所面临的问题和采取的对策也就相互牵连、息息相关。基于此种认识，本书拟用计算机信息保护的概念把两者统一起来，对其面临的问题和采取的对策加以概括和综合。

计算机信息的共享和保护、破坏和安全、扩散和保密是互为条件、相互制约的。计算机信息保护学是研究计算机系统和通讯网络内信息保护方法的一门综合性学科。从方法论的角度看，它包括对隔离控制、加密控制、存取控制、信息流向控制和推断控制的研究。这使计算机信息保护理论更为完善和系统化。本书不是从理论角度，而是从实际应用角度提出计算机信息保护的七层模式。以此模式为基础，从第二章至第八章分别对每一层次面临问题作了探讨，并提出相应对策和措施。为了适应新技术的发展趋势，在阐明信息保护法原则、管理操作保护和实体保护三章之后，着重致力于阐明硬件、通讯网络、软件和数据库各层次保护及措施。

本书由国家科委信息技术政策顾问、国防科工委计算机顾问王运丰教授审阅，在此表示感谢。由于作者水平所限，望读者批评指正。

作者

一九八八年三月

# 目　录

# 第一章 引 论

电子和信息技术飞速发展，使当前世界处于信息化社会的前夜。在我国，电子和信息行业是新兴产业，代表了新一代技术和生产力。它的发展和振兴必将加快社会主义现代化的进程，对振兴国民经济起到难以估量的作用。计算机信息保护就是在这样形势下出现的新课题。

## 第一节 信息及其特征

信息是把数据加工成知识、智慧过程中的一个主要阶段。这就是说，数据是原始的，是信息的原材料，是一堆数字或符号的总括。信息是依据某种目的组织起来、经过加工处理和具有一定结构的数据总括。知识是经过整理、分析、评论和验证的一堆信息。智慧是一种不断显露出的、又经历与客观现实经常对照而得到充实的知识。

由此可见，信息及其提炼成的知识和智慧是重要资源。它已经和必将对人类生产活动和社会活动有重大影响。因此，必须找出信息的特征，从而更完善地掌握、运用和管理信息资源。信息的特征如下：

1．非物质性。信息存在于人脑，包括观察到的、记忆的一切事物和分析、归纳得到的结果。自然资源和信息资源不同。前者不依附于人的观念而独立存在，后者则是人的观念的反映。

2．可展性和可缩性。人类占有信息量越多，使用越广泛，对人类社会影响也就越深远。随着生产力的发展和社会的进步，虽然一部分信息将被淘汰，但在应用过程中，信息总是不断扩展和完善。利用信息可展性，兴起了若干智力行业，如科学研究、技术转让、计算机软件及有关出版、广告业等。另一方面，信息可压缩。可以把许多复杂事例总结为一条定理，把大量资料压缩成一个方程式，把许多实际经验归纳成规定和准则。

3．替代性。信息有广泛而强大替代功能。它可以替代资金、劳力和其他有形物质。例如，银行信息管理系统的运用，就使国家准确、全面、及时地管理和控制财政成为可能，这就加速了资金周转，方便了客户。在工矿企业中，计算机和机器人的使用，替代了劳力，提高了产品的质量和数量，从而提高了经济效益。

4．共享性。信息不同其他物质。其他物质具有独占性，即当一方把它转给另一方后，该物质为另方所有而不再为原方所有。信息则不同。它不采用转手交易。如果一方把一个信息告诉对方，该信息即为双方共有。

5．扩散性。信息很容易传播。人类习惯于独占物质，企图把信息禁锢起来。但是，信息是不受约束的。它总是伺机挣脱这种束缚。近百年来，人类活动速度和量都发生了重大的变革，而信息资源发生的变革尤为显著。计算机信息网络的发展已使信息高速扩散进入实用阶段。

应当指出，信息毕竟只是一种资源。信息技术不是万能的。计算机也只限于存储、处理和传递部分信息和数据；只限于对某些可以测定、可以用数字和逻辑描述的事物及其相互关

系，通过预先规定和设置的过程进行周密处理，并取得结果。对另一部分信息，诸如感觉和情绪等等，计算机不能有所作为。这些信息只能靠人脑处理。长期以来，信息一直是和人体的感觉器官联系在一起。通过人脑，人们在理解每个局部含义之前，就能理解整体的含义，学会区别确切和不确切的事物。计算机信息处理系统做不到这一点。计算机只按照人类大脑左半球的工作方式，即用逻辑、顺序和分析方法处理数据。计算机还不能按照大脑右半球工作方式，即类比地、直觉地、同时和全面地处理数据。一句话，计算机还不能进行创造性的活动。

不难看到，通向信息化社会的道路是漫长的。在整个变革过程中，对信息资源的管理、运用和保护，显得十分必要和迫切。

## 第二节　信息保护环境

正在工作的计算机系统是进程和资源的有机结合。计算机操作系统的主要任务之一，就是使并发性工作的各个进程最大限度地利用计算机资源。而计算机信息保护的一个主要目的是使各进程互不干扰、有条不紊地工作。计算机信息遭到破坏有许多原因，首先是并发运行各用户进程间的相互干扰，再是用户进程对操作系统正常管理的干扰和破坏，还有用户进程本身的错误。解决上述问题，要靠计算机的信息保护机构。

对第一个问题，不同用户的若干进程并发执行时，任一进程故障不应影响其他进程的正常工作。为此，信息保护机构要保护主存储器（或虚拟存储器）内的信息。主要策略是把用户各进程占有的存储器空间划分成相互隔离的区域，以互不影响。对于第二个问题，一个正常工作的操作系统，任何情况下不应因用户进程干扰而破坏。为此，信息保护机构采用状态切换开关。许多操作系统中，把计算机工作分成两种状态。一是管态，即系统状态；一是目态 即用户状态。在管态下，可以执行全部机器指令（包括特权指令和非特权指令）；在目态下，只可执行非特权指令。特权指令包含输入输出、更改机器状态指令等。用户进程在目态下工作。一旦目态下试图执行特权指令，势必引起中断，进入管态，由操作系统进行干预。由此可见，计算机资源的使用权归操作系统控制，用户进程无权支配。对于第三方面问题，用户进程本身有错时，信息保护机构应能限制错误扩散，并帮助查找出错源。另外，调试软件时，如果出现硬件故障或操作错误，信息保护机构也应能将其危害减到最低限度。

计算机信息保护发展有一个历史过程。早期计算机信息保护是以信息存取控制为轴心、以多道编程操作系统为基础的资源保护。近年来，计算机应用领域日益扩大，计算机联网技术迅速发展，共享全网资源更为经济和方便。因此，操作系统也由批量处理多道编程方式向多用户存取方式发展。计算机应用领域的扩大，同计算机网络和操作系统技术的发展相辅相成，使计算机信息保护含义和范围发生巨大变革。在这种环境下，计算机信息保护跳出了以存取控制为基础的资源保护范畴，由狭义信息保护向广义信息保护过渡。

前面提出的信息保护的三个功能属于存取控制为基础的保护范畴。它是存取方法上的保护，同所保护的信息内容并不相干。实质上这是狭义的信息保护。随着计算机网络和多用户存取操作系统的应用，涉及信息内容的安全问题十分突出。用户千差万别，人的作用与技术问题互相牵连。计算机信息遭到破坏，可能是技术问题，也可能是蓄谋篡改和窃取。很明显，存取方法上的保护和信息安全问题密不可分，这就是广义信息保护问题。

对现代计算机系统而言，信息保护有两个主要目标：一是保护信息的机密性，即防止未经认可的泄露；二是保护信息的真确性和完整性，即防止未经认可的修改。信息保护有两个重点环节：一是保护通讯线路上传输的信息，二是保护存储于计算机系统内的信息。

经通讯线路传输的信息，易受到两种威胁。一是无源被动窃取，即信息机密性遭到破坏；二是有源主动窃取，即信息真确性或完整性遭到破坏。无源窃取通常是指截取报文而不被察觉出来，使报文内容泄露。计算机网络中也可采用这种方法监控网络通讯流量。保护报文内容不被识破，是依靠对传输信息进行加密变换。有源窃取是指蓄意修改报文流。有各种手段达到任意窜改报文的目的。一是重置原先用过的某报文数据，以取代现行报文数据。例如，重置原报文内容“存款合计五千元”取代现报文内容“存款合计一百元”以达到窃取目的。二是插入假报文或删除报文。例如，删除“扣款一千元”的报文。对报文内容加密，使蓄意修改报文和插入假报文的企图不能得逞。但是，加密保护并不能阻止作案，只能发现报文遭到窜改。对于重置报文而言，加密不能起到保护作用，因为对手能够轻而易举地重置原先用过的加密报文。对于删除报文，虽然加密保护不能制止，但能发现报文流内的某些字块或字符被删掉。对于删除整个报文，可用有报文应答方式的通讯协议来发现。

存储于计算机系统的信息，易于受到和通讯线路同样的威胁。威胁到信息机密性的手段有浏览、泄漏和推断。浏览是从主存储器或外存储器查找信息(机密数据或有专利权的软件)。它与通讯线路上出现的无源窃取类似。但有二点重要区别：一是信息存储于计算机系统内的时间长，所以浏览比无源窃取更易受到威胁；但另一方面，通讯线路上传输的信息易于窃取，即使系统拒绝作存取时仍可作案。而浏览则有不同，只有用户获得对系统存取权的情况下方可实现。存取控制保护可制止浏览。

就浏览而言，加密保护只使信息不可理解，是存取控制保护的补充°它对保护磁带和磁盘上信息特别有用，因为一旦数据载体被窃，就不再受到系统保护。但是，信息在处理过程中是以普通文出现的，加密保护对处理中的信息不起作用。为此，在使用期间，存取控制就需包含有清除存储器的过程，以保证机密数据不因疏忽而暴露。若无存取控制，加密数据也难免因密码被猜中而受损。

泄漏是用合法存取信息的进程为掩护，把信息传给未经认可的用户。例如，编译器能在作编译同时，把有专利权的软件泄漏出去；征税程序可以泄漏用户机密数据；文件编辑程序不用安全许可证就可把机密军事信息泄漏出去。信息流向控制，加上加密方式和存取控制，可以防止信息失散。

推断是根据公布的一批综合性统计数据，推断出有价值的机密数据。例如，一项重点工程的效益是机密的，但可以从公布的同类工程的平均效益和非重点工程的平均效益关系中推断出来。虽然，存取控制和加密方式能够防止浏览，但不能提供数学结构做到既发布统计数据，而又不暴露敏感信息，因为这属于推断控制的范畴。

信息存储于计算机系统中，除受到上述机密性威胁外，真确性和完整性还会受到威胁。威胁的手段有：窜改和意外破坏。窜改类似于通讯线路上的有源窃取，两者区别犹如浏览和无源窃取间区别一样，不再重复。窜改可有各种手法。可更改数据，例如把一职工存款从一万元更改到二万元；把原先存储数据重置于同一记录内，如把原先盈余额重置于一收费记录内；或重置于其他记录内，如把高收入职工工资置于低收入者记录内；把信息冲掉而使其无用，如冲掉加密键而使加密数据的存取成为不可能；还可插入假记录，如把一个假收入记录加于盈利

文件内；或删除一文件和记录，如去掉坏的报告。同通讯线路传输信息类似，信息存储于计算机系统中，加密技术有助于对这些威胁的防护，它可以发现假密码文或重置密码文，但它不能制止这类威胁。存取控制仍然是主要保护方式。备用对系统遭破坏后的重新恢复起决定作用。

意外破坏是无意中冲掉或删除信息。无意冲掉信息系软件故障（如一阵列的下标超出范围）所致。加密不能对这种威胁加以保护。语言处理器和用硬件实现的存取控制，是靠制止把程序写至其他程序的存储区域或系统表内而起保护作用的。无意删除信息系软件或硬件故障（如盘上磁头破损）和用户出错（如编辑期间因粗心而删掉文件上一行）所致。系统和数据载体的备用对意外和蓄谋破坏后重新恢复均是必要的。许多文本编辑程序有自动复制备用文件的功能。

除上述各种威胁外，计算机系统还受到冒充的袭击。若袭击者能在别的用户帐号下获得对系统的存取权，他就能存取该用户的信息文件和所有其他准许用户使用的信息。同理，若一程序哄骗录入系统的各合法用户，使这些合法用户相信正在同系统对话，则该程序可以从这些用户获得机密信息（如用户的登录口令字）。防止冒充就要求系统和用户互相确认（即鉴定）。实现这种策略需采用加密口令字（即证明件）。数字签名是鉴定用户或进程的更为一般的手段。

综上所述，信息共享与保护、破坏与安全、扩散与保密是互相对立、互为制约的。计算机信息保护理论是研究计算机系统和通讯网络内信息保护方法的一门综合性学科。从方法学的角度，包括对隔离控制、存取控制、加密控制、信息流向控制和推断控制的研究。这些研究使计算机信息保护理论更为系统和完善。另一方面，计算机信息系统已经并将成为高度文明社会的基础和象征，但由于计算机信息系统本身的脆弱性，计算机信息安全正在受到日益严重的威胁，利用计算机犯罪将是不容忽视的问题。

因此，把计算机信息保护法纳入国家计划，制定出一整套综合的信息保护法律和政策，建立与之相适应的管理体制和制度，研究和采用技术先进、可靠有效、经济易行的保护对策和措施，已迫在眉睫。

## 第三节　信息保护实现方式

计算机信息保护环境的复杂多变性，使实现一个有成效的、经济可行和易为用户使用的信息保护系统十分困难。这是由于：

1．信息保护系统是否有成效，不仅取决于保护措施是否完善，也取决于袭击者的手段是否高超，取决于系统脆弱性是否易于识破，取决于系统一旦遭到破坏所造成的直接和间接损失。事实上，要估量袭击者采用的手段和系统潜在威胁是极其困难的。因为如果没有实际的破案知识经验，往往无从下手。

2．来自于内部和知情人员的破坏，这更加危险和难防。

3．技术事故和误操作造成的损失和破坏次数较之蓄谋作案大得多。

4．各类信息保护系统，例如，以流向控制为基础的军用软件保护，以加密、鉴定和数字签名为基础的银行业商业通讯网络保护，差异很大。研制通用的信息保护系统很困难。

5．计算机使用得越广泛深入，对信息共享和保护的需求就越突出。对存储、处理机密信息或享有专利权的各用户而言，计算机系统应把保护同易于使用结合起来。

6．计算机信息保护是计算机系统不可分割的组成部分，应将其结构、性能和应用作综合考虑。

7．降低信息保护软件、硬件的成本和管理费用，减少信息保护造成的多余开销，始终是一个主导因素。在商用系统中，这一点尤为重要。

计算机信息保护是一项复杂的系统工程。首先，必须制定信息保护法规，从道德和法律上定义和保护信息产权。这是一项政治决策。在此基础上，制定和落实组织管理体制、制度、过程和技术上的具体措施。实现计算机信息保护，采用七层模式，如图1-1所示。

第一层为信息保护法。受保护信息必须是有据的。必须明确信息主体权利和信息用户职责。对于信息管理体制、制度和正常异常使用过程必须制定细则，保证信息完整、准确、及时和机密。任何侵犯行为必须追究法律责任。

第二层为管理操作保护。必须建立完善安全的管理体制和制度，应当采取预防措施和恢复手段，防止内部威胁和外部干扰。应当坚持职责分工原则，加强在职人员安全教育。有必要确定信息价值，准确估价可能的威胁和所付代价与效果。应当确定管理目标和责任，切实落实有关措施。

第三层为物理（实体）保护。制止实体受到破坏和损害，首先必须对自然灾害（尤其火灾）加强防护。其次应当采取周密的戒备措施，识别和鉴定出入人员。对于电子电磁行窃也应采取相应对策。应急计划和保险措施是在不得已的情况下的补救措施。

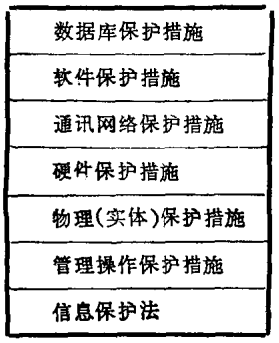


图1-1 信息保护实现层次模式

第四层到第七层分别为硬件、通讯网络、软件和数据库保护。硬件保护侧重于保护存储的信息，通讯网络保护侧重于保护传输的信息，软件保护侧重于保护处理的信息，而数据库保护侧重于保护共享使用的信息、即数据完整和安全。这四层相互关联和渗透，但又各不相同。本书是根据这个模式进行研究的。

# 第二章　信息保护法

在我国，有必要把制定计算机信息保护法提到议事日程上来。这是整个社会日益广泛深入应用计算机的重要标志，也是改革和开放政策之需，是引进国外高科技和智力投资急待解决的问题。

## 第一节　背　　景

由于计算机的广泛应用，美国最早提出制定信息保护法。1965和1966年，美国计算机和保密分会举行的意见听证会，建议建立国家数据库。这是取得美国当局确认的。1972年，美国科学院全面概括了计算机信息系统的工作状态。该院调研了55个大型计算机信息系统，并就其中14个作了详细研究。调研的方式是选择很不相同的机构，其中包括社会安全管理机构、联邦调查局、警察局、美国银行信贷数据公司、教堂和药品管理局。此项研究报告的目的在于说明当时的情况，并不打算解决存在的问题。1973年，美国卫生教育和福利部提出有据信息实施基本准则，为制定信息保护法奠定了基础。1974年，美国正式颁布信息保护条例。随后，美国各州相继颁布补充条例。除美国外，1973年瑞典、1976年西德和1978年法国也先后颁布了信息保护法。

近10年来，在新材料、超大规模集成电路、微电子技术、光电子技术、系统技术和软件技术的基础上，通讯技术和信息处理技术已经融合在一起，成为两个不可分割的领域。传统制度下的通讯和信息处理已不能满足社会需要，也无法利用最新技术。随着信息化社会主体从硬件转向软件，对于保护合法权利，只限历来的工业所有权就显得不够了。除保护权利外，有必要采取新的法律对策，以适应不断出现的新情况。技术大变革促使国际社会竞争的变革。为适应这种变革，也需要法律的变革。如果不能适应从工业化社会向信息化社会这一重大转变，就无法生存下去。把信息，也包括各种计算机软件为主体的智力产权作法律保护，是国际社会发展的总趋势。这种趋势产生巨大冲击力，将会使全世界多少年来对财产的固有观念为之大变。

1980年美国修订了著作权法，正式认定计算机软件是独特的智力产品，是著作权保护的对象。1984美国国会通过保护半导体芯片电路布局法案。1985年美国总统在新贸易政策中提出要努力保护智力财产权。同年，在美国倡导下，召开了世界智力所有权组织第一次会议，开始制定国际协定。1986年，美、日、欧洲共同体、加拿大四方贸易会议一致提出要讨论智力产权问题，并制定国际法规。目前世界上已有美、日、英、法等10个国家和地区为保护软件修改和实施了著作权法。有13个国家和地区的法院在审理有关案件时，肯定了以著作权保护软件。为了在高科技产业中保持领先地位，美国竭力以法律保护软件。不言而喻，这种法律的效力必须在国际社会、特别是竞争对手国家中通用。所以，美国在促使日本和其他工业国家修改、充实著作权法。日、英、法等国出于战胜竞争对手的目的，步美国后尘，也先后修改了著作权法。

1985年，“中共中央制定国民经济和社会发展第七个五年计划的建议”第40条指出，对外开放是我国基本国策，我们要根据独立自主、平等互利原则，进一步加强同世界各国包括发达国家和发展中国家的经济贸易往来和技术交流。第46条指出，要通过多种方式和多种渠道，加强国外智力的引进。由此可见，对外开放政策是我国的长期方针。向工业发达国家引进智力和技术一个主要方面，就是引进计算机信息系统，包括其在各个领域的应用软件。在各主要工业国家实行智力产权政策的今天，如果我国没有一个信息保护法可依，就无法为引进国外智力投资创造必要的条件，也无法衡量和保证我国引进技术的质量，因而达不到平等互利的目的。再从国内建设需要看，信息保护法将维护软件开发者合法利益，促进软件业的发展和竞争，防止重复投资，避免低水平重复劳动。所以，制定出我国的信息保护法，是改革和健全我国社会主义法制所需，势在必行。

智力产权与社会所有制紧密相关。我国是公有制为主体的社会主义国家，不同于资本主义私有制国家。所以，我国的信息保护法与西方国家有本质区别。就我国经济成分而言，除公有制外，又允许集体、个体和国家资本主义所有制并存。我国的信息保护法，首先是对社会主义公有制的捍卫和加强，同时也是对集体、个体和国家资本主义所有制的正当权益的保障。再者，从社会基础、财产观念、技术水准和实现目标等因素来看，我国与西方也有差异。因此，在制定信息保护法时，需以我国的国情和现状为起点，认真作好调查研究和试点。同时，应慎重行事，力求法律的完整、周密、准确和稳定。

## 第二节　信息立法要素

信息立法的要素有：有据信息条例、信息用户职责、信息主体权限、信息质量标准、系统修改和信息流通条例等。

**一、有据信息条例**

被保护信息必须是有据可查的，即法律可以猎获的。其要点为：

1. 必须是不以秘密为宗旨的计算机信息系统。
2. 必须确认记录中信息内容和使用的方法。
3. 在未经许可条件下，必须确认一种方法，禁止把为一目的所取得信息供另一目的所用。
4. 对于信息记录的更改，必须能够辨认。
5. 必须保证信息可靠性，设置合理措施预防错用信息。

在此基础上，制定适用于计算机信息系统的法律条款。其要点为：

1. 规定有具体保护要求的有据信息实施细则。
2. 若违反有据信息实施细则，就以无据信息实施论处。
3. 对无据信息实施，课以民事和刑事惩处。
4. 确立诉讼权，对无据信息实施起诉。

**二、信息用户和信息主体**

信息用户是指使用保密信息（或私人信息）的用户而言。它负责采集、处理信息，也可能负责信息的传播。信息用户常是一个企业或实体。所有公共事业单位均以信息用户形式出现。信息主体是被保护信息记录牵涉单位或个人，其保密（或私人）信息受信息用户保存和

处理。

**三、信息主体权限**

信息主体权限有：

1. 确认计算机信息系统通知信息主体的途径，采用直接或公开通知方式。

2. 确定信息主体使用文件可能的变更。

3. 确认信息主体允许采用的存取技术、识别信息主体和数据项的手段。

4. 确定信息主体不得存取的数据项。例如，有关医疗保健的信息记录，其内容涉及到信息主体，但只能由医师提供，并为医师所用，信息主体不得触及。

5. 信息系统需说明系统用途、采集每个数据项的理由，以及许可谁作存取。

6. 一旦出现信息主体和所存取数据项不相符时，规定出异常处理的细则。

7. 保证信息是最新的。过时信息不予存取。

8. 信息记录涉及一个以上信息主体时，必须确定保护其他信息主体的措施。

9. 确定信息主体存取数据的收费条例。

10. 如果信息主体要求是正当的，或信息记录只涉及一个信息主体，则其对信息改正的申请应予接受。否则，需作核实。

11. 对有争议的信息，应予封锁。

12. 保证更改信息主体名称和地址的真实性。

**四、信息质量标准**

信息质量是指信息完整、准确、及时和安全而言。信息及时性尤应引起注意，其要点为：

1. 确定信息修改次数和方法。在线信息系统中，在线修改过程是即时的。批量处理系统中，信息修改时需显示出上一次修改日期。

2. 在存取信息前，需完成全部修改工作。

3. 计算机系统若有多个信息复制件时，应保证信息主体对最新件的存取。

4. 确定信息记录保存的标准，定期清除无用信息。

5. 如果信息在规定销毁期外仍须保留，则应保证不能任意存取该超期信息。

6. 销毁信息文件时应发出通知。对敏感信息的销毁是保密的。

7. 确定磁数据载体的收回日期。

8. 对外来用户只提供经批准的、有关的最新信息。

**五、系统修改**

计算机信息系统常常需要修改。修改可分成三类：一是预防性的，即防止出错的修改；二是纠错性的，即出错后作的更正；三是适应性的，即对系统的改进。信息保护对系统修改要求为：

1. 信息系统用途无明显变动。

2. 信息主体权限不受损害。

3. 不把信息泄露给未经认可的人员。

4. 信息准确性不受影响。

**六、信息流通条例**

流通的信息有三种形式：即人可直接阅读的纸文件、计算机可读的磁载体和经通讯线路

传输的信息。信息流通可以在一个组织内部、不同组织或不同地区间进行，甚至可以在不同国家间进行。国内信息的流通受同一法律管辖，而国际信息的流通受不同国家法律的管辖。国际信息流通的安全受到的威胁更多。

交换信息的各方是一种伙伴关系。伙伴可能是一对一、一对多个或多个对一个。伙伴的身分可以是信息主体、政府和其他管理机构、有合法存取权的用户、法院或其他仲裁机构。信息流通条例是信息立法的一个部分，其要点为：

1. 确定各种信息保存方式、伙伴身分及其对信息的合法权益（即不同伙伴对信息可以有不同权益）。

2. 确认信息流通的法律效力。特别在国际间信息流通时，协调不同的法律。

3. 建立信息流通的审批权限和手续。

4. 确定保密信息的分类和对其辨认的方法。

5. 估价非法复制受保护信息而出现泄密威胁，并采取反措施。

6. 保证全部输出均是合法和有收益的。

7. 保证信息流通时有兼容的信息交换装置。

8. 保证经过运输的磁载体能够适应标准温度和湿度，并供使用。

9. 保证能够准确辨认磁载体的所有者。

10. 确定离线存放备用载体的手续。

11. 认定全部通讯线路受事故性破坏和蓄谋窃取的威胁，并采取相应反措施。

12. 保证未经认可人员在各终端上不会检索到受保护信息。

13. 确定对流通信息组装和加封的方法。

14. 保证发送和接收的全部保密信息，有确切记录可查。

15. 保证作国际流通的软件包，宜于海关辨认和检查。

16. 对销毁过时的保密信息应作出安排。

## 第三节　信息保护法原则

把信息立法中所述的主要论点归并成以下信息保护法原则。

**一、总则**

1. 有据性：计算机信息系统保存信息必须有据，并能够辨认信息内容、用途和使用方法，制定有据信息条例付诸实施。

2. 信息用户职责：确认信息用户承担保存或处理信息的保护职责。需指定专人负责信息用户机构的信息保护事宜。

3. 采集和处理：经合法手续和合理渠道，采集和处理信息。

4. 明确信息用途：占有的信息应只用于有明确规定的目的，未经批准不应他用。

5. 信息范围：占有信息的范围，与规定用途相符，不得超越。

6. 完整和准确性：应采取相宜的预防措施，保持信息的完整和准确。信息完整和准确程度，取决于信息用途。

7. 及时性：信息应及时修改，满足准确性需要。超过信息用途规定期限的信息，不得存取。