高等学校法学系列教材

信息犯罪与计算机取证

王永全　齐 曼 ⊙主编

LAW

北京大学出版社
PEKING UNIVERSITY PRESS

信息犯罪与计算机取证

四川师范学院图书馆
藏书

主　编　王永全　齐　曼
副主编　孟庆华　徐玉麟
　　廖根为　王　弈
参　编　刘　琴　唐　玲　程　燕
　　邹　瑛　李　玮

北京大学出版社
PEKING UNIVERSITY PRESS

图书在版编目(CIP)数据

信息犯罪与计算机取证/王永全,齐曼主编. —北京:北京大学出版社,2010.8
(高等学校法学系列教材)
ISBN 978-7-301-17443-2

Ⅰ. ①信… Ⅱ. ①王…②齐… Ⅲ. ①计算机犯罪-研究-高等学校-教材②计算机犯罪-证据-调查-高等学校-教材 Ⅳ. ①D914.04②D914

中国版本图书馆 CIP 数据核字(2010)第 125123 号

书　　名:信息犯罪与计算机取证
著作责任者:王永全　齐　曼　主编
责任编辑:杨丽明　王业龙
标准书号:ISBN 978-7-301-17443-2/D·2635
出版发行:北京大学出版社
地　　址:北京市海淀区成府路 205 号　100871
网　　址:http://www.pup.cn　电子邮箱:law@pup.pku.edu.cn
电　　话:邮购部 62752015　发行部 62750672　编辑部 62752027
　　出版部 62754962
印　刷　者:北京鑫海金澳胶印有限公司
经　销　者:新华书店
　　730 毫米×980 毫米　16 开本　23 印张　436 千字
　　2010 年 8 月第 1 版　2010 年 8 月第 1 次印刷
定　　价:38.00 元

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有,侵权必究
举报电话:010-62752024　电子邮箱:fd@pup.pku.edu.cn

序

随着科学技术的发展和互联网的广泛应用与普及，借助于信息技术手段开发与利用信息资源已逐渐成为经济社会生活中的重要组成部分。人们在学习、工作和生活中得益于科技发展和信息网络的应用所带来的巨大便利的同时，也面临着前所未有的信息安全威胁。当前，利用信息技术等高科技手段实施的以信息内容、信息价值、信息载体、信息运行为对象和工具的严重危害社会的信息犯罪现象呈现逐年增长的多发态势。因此，与信息安全问题相关联的刑事、民事、行政案件或纠纷也大幅增长。为适应对这类案件或纠纷的诉讼需要，采取有效的科学技术手段和方法对存储在高科技产品及其相关设备中的数据进行收集、固定、分析与鉴定，并形成具有法律效率的电子证据，不仅具有重要的司法应用和实践意义，而且也是目前法庭科学技术随着信息技术的发展和应用迫切需要解决的重要问题之一。这些问题的解决涉及法学与计算机等学科领域交叉研究的进一步展开和知识的融合，以及相应复合应用型人才的培养。

信息犯罪以及计算机取证与司法鉴定是法学和计算机等学科紧密结合、交叉研究的前沿领域。在我国，这方面尚处于研究和发展的初期，方兴未艾。这一交叉、新兴学科领域的研究及其所取得的成果与目前司法实践的现实需求还有很大距离，相关知识还需要进一步系统地加以总结和凝练。鉴于此，《信息犯罪与计算机取证》一书的作者在这方面作出了自己的探索和努力。

王永全等作者主编的《信息犯罪与计算机取证》一书，从一个新的视角，对社会信息化以及信息社会法治化建设所涉及的信息犯罪与计算机取证相关技术与法律等问题进行了梳理。作者在教学和研究工作的基础上，通过参考国内外相关研究成果和资料，从信息安全所面临的威胁以及司法实践的应用需求出发，较为全面地介绍了信息安全、信息犯罪、计算机入侵、计算机取证、电子证据发现与收集、电子证据保全、电子数据恢复、电子证据分析与评估、计算机取证工具以及计算机司法鉴定等内容。

该书具有以下特点：

1. 系统全面

该书内容丰富，系统全面，涵盖了信息安全的基本概念、目标与需求、面临的安全威胁以及信息系统安全体系所涉及的重要方面，同时还较为详细地介绍了入侵攻击、黑客追踪以及木马、病毒、蠕虫等计算机入侵与控制方面的具体内容，并对信息犯罪及其防范进行了探讨。另外，还对计算机取证与司法鉴定涉及的一些技术方法、工具的使用以及具体的司法应用实践等方面内容进行了较为系

统全面的介绍。全书内容具有一定的广度和深度。

2. 结构新颖

该书以保障网络与信息安全“预防、控制和打击”的“前、中、后”思想为主线加以展开，结构新颖。全书各章节内容紧凑，编排合理。

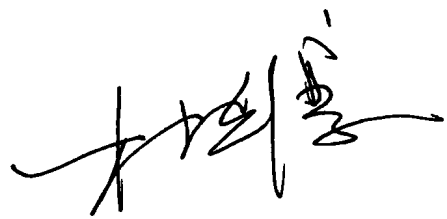
3. 实践性强

该书在介绍相关内容理论知识的基础上，强调理论与实践相结合，操作实践性强。比如，对计算机取证和数据恢复等知识，在进行理论介绍和分析的基础上，强调相关工具的使用方法与操作实践，同时还提供了相关学习内容的实验项目和操作指导，步骤具体而又详细。此外，关于计算机司法鉴定及其程序、文书制作以及质量控制等内容不仅是司法鉴定学科内容的进一步发展，而且对于具体的计算机司法鉴定实践也具有较好的理论指导作用。

4. 适用性强

该书不仅对法学与计算机等学科的交叉融合研究及其成果的司法应用和实践具有重要意义，而且也为“计算机”与“法律”复合应用型人才的培养提供了较为丰富的学习材料，因此适用性较强。该书可供高等院校和科研机构相关专业本科高年级学生及研究生学习使用，同时也可供法学、计算机、信息安全、通信等领域的科研、技术和管理人员以及公检法司系统的相关执法人员参考和借鉴。

在此，我期待该书的出版能够为法学与计算机等学科的交叉研究和发展起到应有的促进作用，并为相关课程的教学提供适当的教材。



2010 年 8 月 8 日

试读结束，需要全本PDF请购买 www.ertongbook.com

前　言

以微电子技术、计算机和网络技术、通信技术为主的信息技术革命是社会信息化的动力源泉。随着信息技术的不断更新、进步和发展，信息资源的增长和共享，特别是“物联网”、“云计算”和“三网融合”的推进与实施，人类社会已从农业经济、工业经济时代向知识经济和信息经济时代转变。在信息社会中，信息成为更重要的资源，以开发和利用信息资源为目的的信息经济活动将逐渐取代工业生产活动而成为国民经济活动的主要内容之一。

随着科学技术的日新月异，下一代互联网技术的迅速发展，互联网的普及和应用已涉及到生活与工作的方方面面，特别是电子商务与电子政务的发展壮大，使互联网发展日益深入。目前，无论政府机关、公司组织，还是团体个人都越来越依赖于计算机网络信息系统，因此，计算机网络与信息安全保障能力不仅是世界各国21世纪综合国力、经济竞争实力和生存能力的重要组成部分，而且也是各国奋力攀登的制高点。计算机网络与信息安全问题得不到妥善解决，必将全方位危急一个国家的政治、军事、经济、文化和社会生活各方面，从而使国家处于信息战和高度的经济金融风险之中。

在信息社会中，信息的产生、传递、接收形式均与传统形式存在较大差异。这种差异性决定了信息安全保护不能仅仅注重信息资源本身的安全保护，而是一个系统的全方位的保护体系。信息安全保护应以信息资源保护为内容，扩展到信息运行系统、基础设施的保护。即从信息内容、信息价值、信息载体、信息运行角度进行保护，实施的任何以信息内容、信息价值、信息载体、信息运行为对象和工具的严重危害社会的信息犯罪行为均应受到处罚。

鉴于信息与网络安全的脆弱性，近年来，危害信息与网络安全的事件（纠纷）或违法犯罪案件越来越多，为此，人们对信息与网络安全以及相关犯罪的打击成果越来越关注。信息安全事件（纠纷）或信息犯罪案件的增多，主要原因在于该类事件或犯罪“发现难、抓捕难、证明难、认定难”。要使信息安全事件或信息犯罪案件得到有效的遏制和打击，在事件或案件发生后，采取有效的信息技术手段对存储在网络（计算机）及其相关设备中的数据进行收集、固定、分析，从而寻找出与犯罪事实相符的证据（链）显得尤为重要。由于所收集的数据主要以数字化形式存储，要形成具有法律效力的呈堂证据，往往需要对原始电子数据采取科学的技术手段进行计算机取证和司法鉴定。为了预防、遏制和打击信息犯罪，保障网络与信息安全，国内外关于信息犯罪与计算机取证及司法鉴定的研究已成为新的热点，吸引了计算机和法学领域专家的极大重视和关注，并成为计算

机与法学等学科交叉研究的前沿领域。

根据以上思考和认识，我们认为，构建具有自主知识产权的计算机网络与信息安全防御体系，不仅需要先进的技术和装备作为坚实的基础，而且还需要完善的法律法规和严格的管理规章制度作为保障，特别是需要培养和造就一大批既掌握先进的信息技术理论和实务知识，又具备法律专业知识和一定管理能力的高层次“计算机”与“法律”复合应用型人才作为后盾。为此，一些高校的计算机、信息安全、通信和法学等相关专业，根据这类复合型人才培养对学生应具备的知识和技能要求，开始为本科生高年级和研究生开设相关必修或选修课程，如“信息犯罪与计算机取证”等课程。为满足这类课程的教学需要，我们从相关课程具体教学目标的实现出发，组织具有丰富教学经验的教师，以“信息犯罪与计算机取证”课程教学讲义为基础共同编写了这本教材。

本书主要以计算机信息网络系统所受到的安全威胁为出发点，从信息犯罪的预防、控制和打击等方面所涉及的技术与法律问题展开，介绍了信息安全、信息犯罪、计算机入侵与计算机取证等方面的基本内容；为切合发生信息犯罪（或信息安全事件）后的侦查（或调查）取证与鉴定等司法运用实际需要，还较为全面、系统地介绍了电子证据发现与收集、电子数据恢复、电子证据保全、电子证据分析与评估、计算机取证工具和计算机司法鉴定等具体内容；结合相关内容的学习和实践需要，给出了若干实验项目，以进一步增强实践性。

作为计算机与法学等学科领域交叉研究和融合的前沿知识，本书可作为计算机、信息安全、通信以及法学等相关专业本科高年级学生和研究生的教科书，也可供高校教师，相关科研、技术与管理人员，以及公检法司等领域工作者参考和使用。

本书具有以下特色：

1. 系统性和新颖性

本书内容构思新颖，融“信息安全”、“信息犯罪”、“计算机入侵”、“计算机取证”与“计算机司法鉴定”等内容为一体，体现并贯穿了保障网络与信息安全“预防、控制和打击”的“前、中、后”思想，有利于读者以“技术”与“法律”为视角形成较为全面、系统的认识和把握网络与信息安全问题的体系架构。

2. 交叉性和融合性

本书作者在参考国内外学者相关研究成果和资料的基础上，结合自身所承担的交叉科研课题及其成果，进行了有机的融合。这对于计算机与法学等学科知识的交叉融合以及相关专业人才的培养更显其迫切性并具有重要意义。

3. 实践性和应用性

本书内容简洁，结构清晰，编排合理，衔接自然，重点突出，理论与实践相结合，具有很强的理论应用性和操作实践性，有利于提高学生学习效率和效果，满足司法运用的实际需要。

全书由王永全和齐曼任主编，孟庆华、徐玉麟、廖根为、王弈任副主编。第1章由王弈和李玮编写；第2章的2.1、2.2，第9章的9.1.2，第10章的10.2、10.5以及第11章的11.7由廖根为编写；第2章的2.3和第6章由程燕编写；第3章由孟庆华编写；第4章由刘琴编写；第5章由唐玲编写；第7章，第9章的9.1.1和9.2由徐玉麟编写；第8章，第10章的10.1、10.3和10.4以及第11章的11.1、11.2、11.3由王永全编写；第11章的11.4、11.5由王永全和齐曼编写；第11章的11.6由邹瑛编写。主编在审阅过程中对一些章节的内容作了合理的修改和整理。全书由王永全和齐曼拟定编写大纲，并由王永全统稿。

杜志淳教授对本书的编写工作给予了许多关心、鼓励、支持和帮助，并在百忙中审阅全部书稿，提出宝贵的修改意见，在此向他表示衷心感谢！本书在编写过程中还得到了华东政法大学各级领导，特别是刑事司法学院以及信息科学与技术系领导和许多教师的关怀与支持，在此向他们表示衷心感谢！此外，还要感谢龚艳和张晓为本书部分书稿的校对工作所付出的辛勤劳动。另外，特别感谢国家社会科学基金（项目编号：06BFX051）、上海市教委重点学科（第五期）司法鉴定建设项目（项目编号：J51102）和上海市教委科研创新项目（项目编号：08YS138）的支持。

由于时间紧迫以及作者水平有限，书中存在缺点和错误在所难免，恳请专家和广大读者不吝指正。

编者

2010年7月28日

目　录

第1章 信息安全

本章重点内容和学习要求

本章重点内容

信息安全的基本概念，信息系统安全的体系结构，以及从不同角度对信息安全概念的理解。

本章学习要求

通过本章学习，掌握信息安全的基本概念，理解信息系统安全体系结构的架构，理解结点安全与通信安全的联系与区别，及其在整个信息系统安全中的地位与作用。

在信息时代的今天，对信息的依赖程度越来越高，信息安全成为人们关注的焦点之一。信息系统如果缺乏安全保障，那么它所带来的各种优点将随着形形色色的攻击、入侵、病毒等安全事件的发生而丧失殆尽。

随着互联网应用广度和深度不断拓展，越来越多的计算机连接到互联网上，这对信息系统的安全提出了更高要求，由单个节点扩展到局域网、广域网，直至整个互联网。据 CERT 统计[①]，近十年来，信息安全事件的发生数量呈逐年上升趋势，并表现出攻击者所需的知识和技能下降而攻击的自动化程度以及破坏程度不断提高的特点。这意味着攻击的门槛降低，而防御的难度增高。

本章从信息安全的基本概念出发，按照信息系统中单个结点安全到结点之间联通成网络的顺序阐述信息系统安全体系结构的各个方面。

1.1 信息安全概述

1.1.1 信息安全含义

提到安全，人们总会联想到保护有价值的东西。一件物品只有具有价值才有保护的意义。信息安全也是如此，只是这里保护的东西不是传统意义上的物品，而是信息。若信息记录在纸张上，或者写在某件东西上，那么通过传统的物

① 资料来源：http://www.cert.org.

试读结束，需要全本PDF请购买 www.ertongbook.com

理保护就可以达到信息保密的目的。而今存储信息的介质发生了很大的变化，从磁带、磁盘、光盘到计算机网络上的结点和传输线路都是可以承载信息的载体。因此，传统的安全保护方法在信息载体发生变化后变得不完全适用。

信息安全不能单靠数学算法和协议实现，还需要通过程序技术和遵守法律法规才能达到期望的效果。[①] 比如，假设在现实生活中建立一个安全物流投递系统，除了从外包装上，即物理层面上保证投递物品的安全外，还要制定相应的规程和法律条款，限制投递人员在中途拆开包装，或者禁止非合法接收人打开不属于他的包裹等。这些都是构成一个信息安全系统需要考虑的因素。

因此，信息安全是一个整体概念，可以从信息系统需要达到的安全目标、面临的安全威胁、攻击手段等方面更全面和深刻地理解。

1.1.2 信息安全目标与需求

当谈到信息安全的目标时，一般要讨论三方面内容：机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）。

机密性是指确保信息内容仅被合法用户访问，而不能被非授权用户获取。这里的访问除包括读、写、修改等操作外，还包括打印、简单浏览和了解特定资源是否存在。机密性有时也被称为保密性（Secrecy）或私密性（Privacy），它们是同义词。

完整性是指信息资源只能由授权方或者以授权的方式进行修改。[②] 换句话说，数据完整性是为了防止数据遭受未授权的篡改。这里修改是指写、插入、替换、删除、创建、状态转换等操作。

可用性是指信息资源在合适的时候能够被授权用户访问。也就是说，当一名用户或系统对某个资源具有合法的访问权限，提出访问请求时，不应该被拒绝。可用性并不是在信息安全研究之初就被提出的，而是在系统的使用过程中，出现了由于安全问题而影响到系统的正常运行和使用，甚至使得系统完全瘫痪的情形下被提出的。

与上述三个安全目标相对应，信息系统的安全需求一般分为三个大类：机密性、完整性和可用性。然而，当谈及某个具体系统或应用时，提出的需求会更加细化，很少用上述如此粗线条的框架加以定义，而是结合实际情况阐述所需的具体要求。

---

① 参见〔加〕Alfred J. Menezes、Paul C. van Oorschot、Scott A. Vanstone：《应用密码学手册》（Handbook of Applied Cryptography），胡磊、王鹏等译，电子工业出版社 2005 年版，第 2 页。

② 参见〔美〕Charles P. Pfleeger、Shari Lawrence Pfleeger：《信息安全原理与应用》（第三版）（Security in Computing Third Edition），李毅超等译，电子工业出版社 2006 年版，第 8 页。

1. 机密性

机密性的概念比较容易定义，即只有授权用户或系统才能对被保护的数据进行访问。在许多系统的安全目标或安全需求中都会提到机密性。但是想要真正实现系统的机密性却没有看上去那么容易。首先要确定由谁（可以是系统，也可以是人）授权可以访问系统资源的用户/系统？访问的数据粒度如何定义？例如，是以文件为单位进行授权访问，还是以比特为单位进行访问？合法用户是否有权将其获得的数据告诉其他人？

信息系统中的机密性需求和其他场合或系统中提到的机密性需求在实质上是一致的，并且在具体的实施上也有很多相似之处。例如，信息系统的敏感数据在物理上要防止攻击者通过传统的偷窃数据载体（硬盘、光盘、磁带，甚至机器等）等方法获取数据。

机密性除了用于保证受保护的数据内容不被泄露外，数据的存在性也是机密性所属范畴。有的数据存在与否，比知道其具体内容更重要。例如，在商业竞争中，多个企业竞争相同的客户源，知道某个企业已经和某个客户签订了合同有时比知道合同具体内容更重要。在这种情况下，数据本身是否存在也是一项机密数据。

2. 完整性

完整性的定义比较复杂，对其进行全面的描述较为困难。在不同的应用环境下，对完整性的含义有着不同的解释。但是当具体考察每一种应用时，会发现它们所指的含义都属于完整性的范畴。例如，在数据库应用中，完整性需求可以分为不同的层次：数据库完整性和元素完整性。其中，数据库完整性又可以细分为数据库的物理完整性和数据库的逻辑完整性。

总体而言，完整性可以从两个方面进行考虑：一是数据内容本身的完整性，有时称为数据内容完整性；二是数据来源的完整性，有时称为数据源完整性。数据内容完整性是指数据本身不被未授权地修改、增加和删除等。而数据源完整性是指数据的发送者即其所声称的来源是真实的，经常通过各种认证机制实现。

对数据来源的完整性破坏通常有重放攻击（Replay Attack）、假冒和伪装等。其中，重放攻击可以将一个旧消息多次发送达到破坏的目的。例如，一个用户 A 通过网络和银行之间进行账务管理。用户 A 将 1000 元钱从自己账户划到用户 B 的账户上，用户 B 一直在网上侦听用户 A 和银行之间的通信，并将划账消息复制了一份到本地。当本次交易结束后，用户 B 和银行发起一轮新的会话，将上次侦听到的用户 A 与银行之间的消息再次发送给银行。如果没有使用安全认证机制，则银行会认为用户 A 又一次将 1000 元钱划给账户 B。

保证数据完整性的机制通常分为两类：预防机制与检测机制。预防机制用于防止未授权的用户修改数据，或者授权用户以未授权的方式修改数据。注意

区分这两种未授权的访问是很重要的。对于前者比较容易理解，即一个用户对于某项数据或资源没有修改和增删的权力却要去篡改数据；而对于后者而言，一个用户可以修改某项数据或资源，但是他/她采用的修改方式却是未授权的。例如，一个银行雇佣的内部员工，他/她有权对用户申请的转账操作进行操作，即他/她有权修改账务数据，但是如果他在转账之后，隐藏（擦去）了这次账务操作，即隐藏了这次转账的去向，则他/她是以未授权的方式修改数据，破坏了数据的完整性。

检测机制不能防止未授权的用户修改数据，但是它可以告诉数据所有者数据是否保持了完整性，是否还值得信任。

3. 可用性

可用性是指数据或资源的合法使用者在合法的时间段以授权方式可以访问到所需要的数据或资源。换句话说，可用性是指使用所需资源或信息的能力。[①] 在系统设计中，可用性是系统可靠性的一个重要方面。如果一个系统无法使用，就如同系统不存在一样糟糕。目前，威胁信息系统可用性的典型攻击手段是拒绝服务攻击（Denial of Service Attack）。这类攻击是最难检测到的。

例如，某个商务网站有多台服务器并行工作向终端用户提供服务，并且有一个负载平衡服务器可以根据客户流量自动平衡各个服务器上的负载。若攻击者A攻破了这台负载平衡服务器，则在其他用户提出服务请求时，该服务器会以所有服务器都达到满负荷运行为由不再为用户的请求分配服务器，那么用户会觉得这个商务网站不可用。

为了防止这类攻击的发生，往往要求系统的设计者在建立系统模型时就能考虑到异常的访问方式或运行模式，即使有些情形在特定运行环境下看上去属于正常运行，也有可能在其他环境下是非正常的。这对系统的设计者提出了很高的要求，因此实现的难度较大。

上述三个安全目标不是相互分立的，它们之间会有部分重叠之处。例如，实现信息系统保密性的时候，对系统的完整性也会有所帮助。实现保密性的安全机制在有的情形下也可用于实现系统完整性。因此，安全目标之间是相互联系的。在考虑如何使系统安全性能达到需求，同时成本可以接受时，应对各个安全目标之间的关系予以均衡。

1.1.3 信息安全威胁

针对安全目标的三个方面，现有的安全威胁可以分为四大类：截取、中断、伪

① 参见〔美〕Matt Bishop：《计算机安全、艺术与科学》（Computer Security: Art and Science），清华大学出版社2004年版，第6页。

造和篡改。它们可以破坏安全目标中的一个或几个，有的可以同时造成一个以上的安全目标被破坏。威胁是对安全的潜在破坏可能性，但是破坏本身不必真正发生。使得破坏真正发生的行为，称为攻击。执行攻击行为或造成攻击发生的人，称为攻击者。

1. 截取

截取是指资源被未授权地访问。例如，机密信息的泄露；网络上传输的信息被非法搭线侦听等。这些都是截取信息的例子。而执行未授权访问的实体可能是一个人、一段程序、一台计算机。在通常情况下，对资源进行截取不会对资源本身进行修改等操作，属于一种被动攻击行为。但是在有的文献中，提到一种主动攻击型的截取，这种攻击除了非法获取资源外，还对资源本身进行篡改，破坏了资源的完整性。

由于截取通常被动收集信息而不主动发起攻击，因此对于老道的截取者而言非常难于追查。有时信息已经被泄露了相当长的时间才会被发觉。只被动截取信息而不主动篡改信息，则仅破坏了系统的保密性；而主动型的截取会破坏系统的保密性和完整性。

2. 中断

中断是指将系统中存在的信息或资源抹去或变得不可用。例如，计算机系统的硬件出现故障，存储重要信息的硬盘坏了；或者用户无法访问指定的文件，可能是该文件被非法删除，或者通过其他手段使得用户访问不到，被隔离。这些都是中断造成的后果，可以被较快地发觉。

中断往往破坏信息系统的完整性和可用性。若系统的硬盘损坏，则系统用户将无法使用该硬盘上的信息，甚至会导致整个系统无法正常运行，合法用户不能使用系统。

3. 伪造

伪造是指未授权方假冒其他对象。通常它所假冒的对象是合法对象。伪造可能假冒一个人，如合法用户；或者一个操作，如在数据库中插入一个记录；或者伪造消息，如在网络通信中，在合法消息队列中插入一个消息。

伪造破坏了系统的完整性，有时通过伪造也可以获取系统的机密信息，这时它也破坏了系统的机密性。伪造有时难以发现，尤其当攻击者成功假冒成一名合法用户时。因此，信息系统通常采用身份鉴别机制预防伪造合法用户。

4. 篡改

篡改是指未授权方访问并修改了资源。例如，非法入侵者访问了系统中某些敏感文件，并在访问后将这些文件删除。更多时候，攻击者访问文件后，只是将其中部分内容篡改，而其他部分保持原样。部分篡改有时增加了安全防御的困难性。现有安全机制有的可以检测篡改的发生。例如，对系统中的重要文件

进行数字签名，并将这些数字签名进行备份。当有攻击者篡改了这些文件时，其修改后的文件的数字签名和原有数字签名将不相同，以此可以判定文件被篡改过。但是，有时篡改很隐蔽，无法及时发现。

篡改不但破坏了系统机密性和完整性，当篡改的内容对系统运行有影响时，如篡改了系统的配置文件，造成系统无法正常运行，那么它也会破坏系统的可用性。

上述四类安全威胁针对系统安全的三个目标，可以说是从另一个角度阐述安全的含义。

1.2 信息系统安全体系结构

作为一个安全的信息系统，系统的安全强度取决于系统中最薄弱的环节。当信息系统的安全性能作为一项系统需求提出时，最好的解决方案是在系统设计之初就将其考虑到整体设计中。这样可以将安全功能无缝整合到系统中，并能达到最好的安全效果。

而在实际应用中，有相当一部分系统是在上线之后，才发现安全性对系统的运行有着重要的意义，因此考虑在后续的维护运行中，增加安全模块。这种做法虽然在短时间内可以解决眼前问题，但是从长远发展而言，系统的安全性是不能得到很好保证的，总会出现新的安全问题，以至于目前的安全机制无论怎么修改和维护都不能满足需要，最终只能通过设计新的系统解决问题。

本章遵循从面到点的思路，在总体介绍信息系统安全整体结构的基础上，再从系统的各个安全环节入手加以阐述，从而希望使读者能对信息系统安全体系结构先有一个整体认识，然后再根据需要深入到具体的安全机制中。

1.2.1 信息系统安全体系

在信息高度发达的今天，信息系统随处可见，小到一个便携式设备，大到整个国家或区域性的信息基础设施系统，甚至整个互联网系统也可以被看成一个跨区域和国家的大信息系统。对不同的系统而言，其安全需求是不相同的。如前所述，安全需求大致可以分为保密性、完整性和可用性三大类，但是对具体系统而言，每一类需求都可以细化成一系列的安全需求。

作为一个系统的体系结构，最直观的观察视角是从系统的功能模块入手，对系统的各个部分进行划分。当谈及“安全体系结构”时，将系统中与安全相关的部分从系统各部分中提取出来就构成了信息系统安全体系结构。因此，信息系统的安全体系结构是一个集合，其中包含与安全相关的各种硬件、软件、实现机制、相关文档和规章制度，以及有关法律法规等。而这些部分之所以能有机地整

合成一个“系统”，既有系统安全功能的需求，也有系统正常运转的需求。

无论信息系统的规模如何，系统的安全体系结构之所以能够正常地发挥其应有的作用，都可以从其内部的具体实现机制或实现细节，以及各部分之间的相互配合找到相应的答案。但是作为一个系统而言，在系统层面上也有相应的部分与系统的各个安全环节相呼应。

从信息系统安全体系结构这个层面而言，安全策略是不能被忽视的。虽然安全策略是以文字方式表述的，但是系统在整个设计、运行和维护过程中将都遵循这样的指导思想。安全策略一般比较抽象，用于描述系统安全需求的大方向，对如何实现某个具体的安全需求不作具体描述和限制。对有的系统而言，安全策略可以简约成一句话，例如，“没有明确说明禁止的活动就是默认允许的”。而有的安全系统则需要厚厚的一本文档说明系统的安全策略。

通常在谈到信息系统的安全体系结构时，人们关注较多的是技术层面，即一个系统的具体实现，需要哪些硬件系统和软件系统等；而另一层面，所谓的“软环境”，经常被忽略，如安全管理制度（包括对物的管理和对人的管理，尤其是对人的管理常常存在疏漏）、人员培训，以及系统运行的社会环境——现行法律法规的支持等。越来越多的系统实例表明，硬件和技术层面的问题是容易解决的，而管理、制度和法律法规等软环境层面的问题较难解决。例如，电子商务系统的出现到现在已经有几十年的时间，国内外出现许多著名的电子商务系统，而与之相配套的电子商务法律在我国的发展却没有如此迅速，当出现纠纷等问题时，只能寻求原有法律体系的支持，而有的问题超出了传统法律的范畴，因此在该领域遇到一些困难。

在本章的余下部分，我们将更多地集中在技术层面，对信息系统的安全环节进行讨论。

1.2.2 物理安全

物理安全是信息系统的安全基础，可将其定义为在遇到偷盗、间谍活动、阴谋破坏和伤害时，为确保某人或某物的安全和物质存在所采取的措施。[①] 物理安全既包含传统产业（非信息系统）中已有的安全内容，也包含信息系统特有的安全问题。通常，当提及信息系统的物理安全时，人们的注意力会更多地聚焦在后者，而前者经常被忽略，或者在提及时表现出不耐烦的情绪。然而在实践中，传统的物理安全与信息系统特有的物理安全同等重要。因为系统的最薄弱环节决定了整个系统的安全强度，而物理安全是信息安全的基础，当这层根基不稳

① 参见〔美〕Harold F. Tipton, Micki Krause 主编：《信息安全管理手册》（卷 III）（第四版），电子工业出版社 2004 年版，第 420 页。

试读结束，需要全本PDF请购买 www.ertongbook.com