马燕曹　周　湛　等编著

信息安全法规与标准

国家信息化安全教育认证(ISEC)系列教材

机械工业出版社
CHINA MACHINE PRESS

国家信息化安全教育认证(ISEC)系列教材

信息安全法规与标准

马燕曹　周　湛　等编著

信息系统一安全一标准
机械工业出版社

本书着重介绍了我国的信息安全立法情况，并对相关法规、条例进行了重点说明。书中系统、全面地介绍了国内外的信息安全标准和法规，并结合具体实例进行了分析。

本书不仅适合大专院校相关专业作为教材，对从事信息和网络安全方面的管理人员和技术人员也有参考价值。

图书在版编目(CIP)数据

信息安全法规与标准/马燕曹等编著. —北京：机械工业出版社，2004.4
(国家信息化安全教育认证(ISEC)系列教材)
ISBN 7-111-14171-7

Ⅰ.信… Ⅱ.马… Ⅲ.①信息系统—安全管理—法规—世界—资格考核—教材②信息系统—安全技术—标准—世界—资格考核—教材 Ⅳ.①D912.1②TP309-65

中国版本图书馆 CIP 数据核字(2004)第 019294 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)
责任编辑：李利健
责任印制：洪汉军

三河市宏达印刷有限公司印刷 ·新华书店北京发行所发行

2004 年 4 月第 1 版·第 1 次印刷
787mm×1092mm 1/16·11.75 印张·289 千字
0001—5000 册
定价：21.00 元

凡购本图书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话：(010)68993821、88379646
封面无防伪标均为盗版

出版说明

随着信息化在我国的不断深入和发展，信息技术和网络给社会的经济、科教、文化和管理等各个方面注入了新的活力。人们在感受它所带来的新体验、享受它为我们带来高效率的同时，也面临着日益突出的信息安全问题。党和国家领导人多次强调，必须充分认识到做好信息安全保障工作的重要性，大力搞好技术开发和人才培养。

对信息安全专业人才的需求是多层次的。从信息安全基础理论研究到新技术的开发利用，再到各级网络信息系统信息安全保障体系的建设、运行，需要根据不同要求有针对性的进行人才培养。

国家信息化安全教育认证(ISEC)项目是由信息产业部信息化推进司推出的信息安全领域的国家级认证体系。该项目由中国电子商务协会监督，由 ISEC 国家信息化安全教育认证管理中心统一管理与实施。ISEC 国家信息化安全教育认证管理中心以行业为基础、以技术为核心制定了一套面向应用的教育方案。根据工作性质的不同，教育对象被划分为规划决策层、管理运营层和操作层三个层次。认证体系的设计，课程内容及相应的教学考试大纲的编写和指定是针对三个层次人员对信息安全知识和技能的不同需求和理解程度的不同而制定的。确保不同层次，不同需求的各类人员从各自的角度充分掌握和理解信息安全的知识和技能。

本系列教材是在国家信息化安全教育认证(ISEC)专家组的指导下，由国家信息化安全教育认证(ISEC)教材编委会组织编写的。始终以 ISEC 国家信息化安全教育认证管理中心制订的各级考试大纲为依据，坚持面向行业用户的需求和侧重技术应用两个基本原则，全面地介绍了信息安全各种主流技术和管理规范，以帮助读者深入了解信息安全本质，并熟练掌握相应的技能，从而建立完备的信息安全观念。本系列教材包括：《网络安全基础》、《防火墙原理与技术》、《入侵检测技术》、《VPN 技术》、《PKI 技术》、《数据备份与灾难恢复》、《网络隔离与网闸》、《信息安全法规与标准》、《信息安全策略与机制》、《信息安全团队构建与管理》，共计 10 本。

在写作过程中，北京正阳天马信息技术有限公司为本系列教材的编写提供了很多宝贵的建议和支持。

前　言

随着计算机信息技术的普及，计算机作为信息收集、存储、加工和检索的工具得到了广泛的应用。但是，人们在利用网络信息技术不断改善、推进自己的工作与生活的同时，也切实感受到网上有害信息、网络病毒传播，以及黑客攻击所带来的恶劣影响与巨大的损失。信息安全已引起政府的高度重视，不断加强信息安全立法工作，加大执法力度。国内外相关部门也制定出了比较完整的信息安全标准体系，以指导网络信息系统用户的信息安全保障工作。

我们作为网络信息系统的建设者和使用者，也需要不断加强法律意识，掌握必要的技术管理要求，并把它们运用到现实工作中去。

为了使读者了解我国计算机信息安全的法律知识，为了更好地管理计算机信息系统，培养计算机信息管理的人才，保证信息和网络的安全，国家信息安全认证中心开始实施信息和网络安全方面的培训。《信息安全法规与标准》是安全培训中一项非常重要的内容，它是根据国家信息安全认证中心培训大纲要求编写的。

本书包括三部分共 9 章内容，其中：

第一部分（第 1～3 章）：在介绍法律和相关知识的基础上，通过实例分析了法律对信息安全的影响，及国内外现行的法律体系和信息系统安全的法律规范。

第二部分（第 4～7 章）：比较全面地介绍了我国《信息安全保护条例》和《信息安全管理办法》，同时还介绍了国际互联网的相关法规和其他有关信息安全的法规。

第三部分（第 8～9 章）：比较详细地介绍了我国有关信息安全的标准和国外关于信息安全管理的标准 ISO/IEC17799。

本书在系统和全面介绍信息安全法规与标准的同时，还结合具体实例进行了具有针对性的分析。除用于教育、培训认证外，本书对从事信息和网络安全方面的管理人员和技术人员都有实际的参考价值。

本书在编写过程中，参考了大量资料，并得到多位同行的大力支持和帮助，在此一并表示感谢。除封面署名外，参加本书编写工作的还有周知平、张宏、赵正仪、徐容磊等，彭澎对全书进行了审阅和修改。

由于时间紧迫，书中难免存在错漏之处，敬请读者批评指正。

编　者

目　录

第二部分　法 律 法 规

第三部分 标 准

第一部分　总　　论

第1章　信息安全对法律的需求

本章导读：

本章介绍了计算机犯罪界定、计算机犯罪的各种形式、计算机犯罪常使用的方法以及因计算机犯罪所引发的各种问题。要求大家了解在使用计算机时什么能做，什么不能做。重点掌握计算机犯罪界定。

信息安全主要包括系统安全、系统中的信息安全和管理安全三方面内容。信息安全的基本属性主要包括：可靠性、完整性、保密性、可用性、可控性、不可否认性等。要保证系统和信息的安全就需要有相应的法律来保障，这就是信息安全对法律的需求。

1.1　犯罪

1. 犯罪的概念

犯罪给信息系统的安全和保密措施带来了巨大的威胁，它是信息安全和保密要防范的重点。《中华人民共和国刑法》第二章第十三条对犯罪作了如下定义：一切危害国家主权、领土完整和安全、分裂国家、颠覆人民民主专政的政权和推翻社会主义制度，破坏社会秩序和经济秩序，侵犯国有财产或者劳动群众集体所有的财产，侵犯公民私人所有的财产，侵犯公民的人身权利、民主权利和其他权利，以及其他危害社会的行为，依照法律应当受刑罚处罚的，都属于犯罪，但是情节显著轻微且危害不大的，不认为是犯罪。

犯罪有故意犯罪和过失犯罪两种主要类型。

2. 计算机犯罪

计算机犯罪(Computer Crime)是指行为人通过计算机操作所实施的危害计算机信息系统(包括内存数据及程序)安全以及其他严重危害社会的并应当处以刑罚的行为。计算机犯罪产生于20世纪60年代，到了本世纪初已呈猖獗之势，并逐渐被各国所重视。计算机犯罪的实质特征主要表现在：

1) 计算机本身的不可或缺性和不可替代性。

2) 在某种意义上作为犯罪对象出现的特性。

3) 明确了计算机犯罪侵犯的客体。

随着科技的进步，作为高科技、高智能且表现形式多种多样的计算机犯罪大致可分为两大类型：一类是行为人利用计算机操作实施的非法侵入或破坏计算机信息系统(包括内存数据及程序)安全，从而给社会造成严重危害的并应当处以刑罚的行为；另一类是行为人利用计算机操作实施的除非法侵入或破坏计算机信息系统安全以外的其他严重危害社会的并应当处以刑罚的行为。

新刑法中第285～287条是关于计算机犯罪条款的规定，其中：

- 第285条：非法侵入国家计算机信息系统罪；
- 第286条：破坏计算机信息系统罪；
- 第287条：利用计算机犯罪。

其中第285、286条采用列举式，是新刑法新增加的罪名，并规定了相应的刑罚。而第287条是对以计算机为犯罪工具的原则性规定，是指那些以计算机为犯罪工具，通过输入指令而获取非法利益和机密的犯罪行为，其刑罚由其他相关的条款规定。

3. 计算机犯罪的主要表现形式

计算机犯罪的表现形式主要有：

(1) 非法侵入计算机信息系统罪

在《中华人民共和国计算机信息系统安全保护条例》中，对计算机信息系统作如下定义：计算机信息系统是指由计算机及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标的规则对信息进行采集、加工、存储、传输、检索等处理的人和系统。

我国新刑法的第285条对非法侵入计算机信息系统罪作了较为详尽的规定：违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下的有期徒刑或者拘役。

通常侵入计算机信息系统的方法有：技术攻击、通过后门进行非法入侵、通过陷阱门进行非法入侵以及非法的用户冒充合法的用户进入计算机信息系统等。

(2) 破坏计算机信息系统罪

我国新刑法第286条对此项罪名作了如下规定："违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上的有期徒刑。违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加，后果严重的，依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。"此项罪名可以分解为破坏计算机信息系统功能罪、破坏计算机信息系统数据和应用程序罪、制作并传播破坏性程序罪。常见的手段有计算机病毒、数据欺骗等等。

4. 计算机犯罪常使用的方法

计算机犯罪常使用的方法有：

1) 计算机犯罪常使用的方法和手段是以合法手段为掩护，查寻计算机信息系统中不允许访问的文件，或者侵入重要领域的计算机信息系统。

2) 用某种方法紧跟享有特权的用户，侵入重要的计算机信息系统，破坏或者窃取计算机信息系统中的重要数据或程序文件；有意设置并插入某种程序编码，并设定这些编码在某一特定条件下自动执行，删除数据文件或者破坏系统功能，使整个系统处于瘫痪。

3) 在数据传输或者输入过程中，对数据的内容进行修改，干扰计算机信息系统。

4) 未经计算机软件著作权人授权，复制、发行他人的软件作品和制作、传播计算机病毒等。

1.2　民事问题

在计算机安全使用等方面，不仅存在犯罪问题，也存在民事问题。任何人都可以对任何人任何事提起民事诉讼。下面通过一个简单的例子来说明有关民事问题。

例如：A 公司为建立大型的 B2C 类电子商务网站，注册了 www.abc.com，www.abc.net 等相关域名，对 abc.com 进行了全方位保护。而 A 公司的域名与 B 企业的域名相同，不仅如此，在网站正式开通后，发现技术人员误将学习使用的页面传到了 Internet 网上，而学习所使用的网页页面又恰恰是 B 企业的页面。发现问题后，A 公司立即将误传的页面全部撤下。此后不久，B 企业通过召开各大新闻单位和媒体记者的新闻发布会等方式，单方面对 A 公司进行了一系列的抨击。A 公司的相关电子邮箱遭到了垃圾邮件的攻击，致使邮箱不能正常使用。

此事件说明网络管理方面的漏洞和人为的误操作对网络安全所造成的影响。

1.3　隐私问题

隐私问题是信息安全和保密中所涉及到的非常重要的一个问题，隐私问题在个人、组织中都存在。利用法律手段有效地保护组织和个人的隐私具有非常重要的意义。

例如：美国即将对有意滥用别人住处者处以最高 250000 美元的罚金和最多 10 年的监禁。

另一则来自国外网站的消息：英国一位 21 岁的年轻黑客，由于前女友的移情别恋，愤而将与前女友做爱的照片及录像“大白于天下”，张贴在被其黑掉的站点上，因此被法院判了五个月的牢狱。

这位黑客名叫菲利普诺斯，日前黑掉了前女友注册的一个交友网站。他将前女友的资料肆意篡改，并把与其做爱的照片张贴在被黑的交友网站上。据英国当地法院透露，诺斯通过他在移动电话公司的朋友获得前女友的相关信息，然后侵入她的邮件账号，并打印了 50 份有关两人做爱的海报，准备在这位 19 岁的前女友家乡 Epsom 到处张贴。

目前他已被控犯有非法盗取私人数据、非法篡改计算机程序及虐待罪。诺斯的前女友对所发生的一切表示非常难过、羞辱，对诺斯的行为表示震惊和悲哀。

据此案件的律师 Michael Spong 称，诺斯使用前女友的账号及密码登录交友网站，修改资料。而且把两人亲昵的照片放在网上。甚至还与美国的一家公司联系打算以诺斯前女友的名字创建一个色情站点。

1.4　习题

一、选择题：

1. 下列哪些不是计算机犯罪的特征。

A. 计算机本身的不可或缺性和不可替代性

B. 在某种意义上作为犯罪对象出现的特性

C. 行凶所使用的凶器

D. 明确了计算机犯罪侵犯的客体

2. 在新刑法中,下列哪条犯罪不是计算机犯罪。

A. 利用计算机犯罪　　B. 故意伤害罪

C. 破坏计算机信息系统罪　　D. 非法侵入国家计算机信息系统罪

3. 对犯有新刑法第285条规定的非法侵入计算机信息系统罪可处_____。

A. 三年以下的有期徒刑或者拘役　　B. 1000元罚款

C. 三年以上五年以下的有期徒刑　　D. 10000元罚款

4. 行为人通过计算机操作所实施的危害计算机信息系统(包括内存数据及程序)安全以及其他严重危害社会的并应当处以刑罚的行为是_____。

A. 破坏公共财物　　B. 破坏他人财产

C. 计算机犯罪　　D. 故意伤害他人

5. 计算机犯罪主要涉及刑事问题、民事问题和_____。

A. 隐私问题　　B. 民生问题

C. 人际关系问题　　D. 上述所有问题

二、简答题:

1. 简述什么是侵入计算机信息系统罪。

2. 简述什么是破坏计算机信息系统罪。

3. 简述计算机犯罪的实质特征。

4. 计算机犯罪除了引起刑事问题外,还会引起什么问题?

第2章　立法、司法和执法组织

本章导读：

本章包括立法、司法和执法三方面的内容，简单介绍了国内外的立法权、立法程序及法律文本的确定，国内外司法、执法组织和司法、执法程序。重点掌握我国的司法、执法程序，以便当计算机安全受到威胁时知道如何应对。

依照我国的法律体系立法过程包括：

立法组织：提出立法议案并组织有关人员编写法律条款，报请有关部门（最高立法权利部门是全国人民代表大会）批准，由国家行政机关颁布实施。

执法过程：由执法组织依法执法。

司法过程：司法部门根据证据对当事人依法进行审判。

2.1　立法

2.1.1　立法权

立法权是一定的国家机关依法享有的制定、修改、废止法律等规范性文件的权力，是国家权力体系中最重要的核心的权力。

在我国根据享有立法权主体和形式的不同，立法权可以划分为国家立法权、地方立法权、行政立法权、授权立法权等。

2.1.2　立法组织与立法程序

1. 立法组织

享有立法权的组织是立法组织。例如：在我国，国务院、全国和各地区人大是立法组织。其中，全国人大常委会是最高立法组织。

2. 立法程序

目前，我国法律的制定程序主要有以下四个步骤：

(1) 法律方案的提出

下列个人和组织享有向最高国家权力机关提出法律议案的提案权：

1) 全国人大代表和全国人大常委会的组成人员。

2) 全国人大主席团、全国人大常委会可以向全国人大提出法律议案。

3) 国务院、最高人民法院、最高人民检察院可以向全国人大或全国人大常委会提出法律议案。

(2) 法律草案的审议

审议是指立法机关对已经列入议事日程的法律草案正式进行审查和讨论。

(3) 法律草案的表决和通过

法律草案的表决和通过是立法机关以法定多数人对法律草案表示最终的赞同,从而使法律草案成为法律。

(4) 法律的公布

法律的公布是指立法机关或国家元首将已通过的法律以一定的形式予以公布,以便全社会遵守执行。

我国宪法规定,中华人民共和国主席根据全国人民代表大会的决定和全国人民代表大会常务委员会的决定,公布法律。

2.1.3 立法权等级

立法权是有级别的,不同级别立法的内容,所立法律的适用范围是不同的。

1. 国家立法权

国家立法权是由一定的中央国家权力机关行使,用以调整基本的、带全局性的社会关系,在立法体系中居于基础和主导地位的最高立法权。

1) 1994 年 2 月 18 日,国务院发布《中华人民共和国计算机信息系统安全保护条例》。

第二十条 违反本条例的规定,有下列行为之一的,由公安机关处以警告或者停机整顿:

- 违反计算机信息系统安全等级保护制度,危害计算机信息系统安全的;
- 违反计算机信息系统国际联网备案制度的;
- 不按照规定时间报告计算机信息系统中发生的案件的;
- 接到公安机关要求改进安全状况的通知后,在限期内拒不改进的;
- 有危害计算机信息系统安全的其他行为的。

第二十三条 故意输入计算机病毒以及其他有害数据,危害计算机信息系统安全的,或者未经许可出售计算机信息系统安全专用产品的,由公安机关处以警告或者对个人处以 5000 元以下的罚款、对单位处以 15000 元以下的罚款;有违法所得的,除予以没收外,可以处以违法所得 1~3 倍的罚款。

第二十四条 违反本条例的规定,构成违反治安管理行为的,依照《中华人民共和国治安管理处罚条例》的有关规定处罚;构成犯罪的,依法追究刑事责任。

第二十五条 任何组织或者个人违反本条例的规定,给国家、集体或者他人财产造成损失的,应当依法承担民事责任。

2) 1997 年 3 月 15 日,全国人民代表大会通过《中华人民共和国刑法》。

第二百八十五条 违反国家规定,侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的,处三年以下有期徒刑或者拘役。

第二百八十六条 违反国家规定,对计算机信息系统功能进行删除、修改、增加、干扰,造成计算机信息系统不能正常运行,后果严重的,处五年以下有期徒刑或者拘役;后果特别严重的,处五年以上有期徒刑。

违反国家规定,对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作,后果严重的,依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序,影响计算机系统正常运行,后果严重的,依照第一款的规定处罚。

第二百八十七条　利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

2. 地方立法权

地方立法权是由有权的地方国家权力机关行使的立法权。享有地方立法权的地方权力机关可以是单一层次的，也可以是多层次的。

2001年11月16日，由于近期广州市连续发生多起国际互联网网站被攻击、黑客夺取系统管理员权限，以及盗用用户电子邮箱密码的恶性案件，造成大量信息泄漏的严重后果，市有关部门日前向广州地区各有关单位的计算机安全领导小组发出了《关于加强网站安全防范黑客攻击的紧急通知》。通知要求包括：

- 凡涉及敏感信息的内部计算机网络一律不得与国际互联网联网，确需与国际互联网联网的计算机要彻底清除其中的敏感信息。内部网的计算机要严格限制使用外来程序和磁盘。
- 严格限制FTP、Telnet等登录账号权限，关闭服务器、路由器上不必要的服务功能和端口，安装系统最新补丁程序，定期更改系统密码。
- 凡安装、使用计算机安全专用产品的，该产品必须持有公安部颁发的计算机安全专用产品许可销售标志，未有该标志的产品一律不得销售和使用。
- 一旦发现制作、传播计算机病毒和非法侵入计算机信息系统等网上违法犯罪活动的，请及时向广州市公安局计算机管理监察处报告。

广东省将于2003年6月1日起实施《广东省计算机信息系统安全保护管理规定》，这是该省首次出台的计算机信息系统安全保护管理规章。

广东此次出台的该项规定全文共有二十八条，包括安全保护制度及技术措施、重点安全保护单位范围、法律责任等多个部分，如规定公安机关、国家安全机关为保护信息系统安全，在紧急情况下，可采取暂停服务、暂时停机、暂停联网等紧急措施；各市公安局设立报警处置中心，负责受理网上发生的案件和指导处置重大安全事故等。

3. 行政立法权

行政立法权是源于宪法、由国家行政机关依法行使的、低于国家立法权的一种独立的立法权，包括中央行政立法权和地方行政立法权。地方行政立法权又可分为不同的层次。

1）1996年4月，原邮电部颁布《中国公用计算机互连网国际联网管理办法》。

第八条　接入单位负责对其接入网内用户的管理，并按照规定与用户签定协议，明确双方的权利、义务和责任。

第九条　接入单位和用户应遵守国家法律、法规，加强信息安全教育，严格执行国家保密制度，并对所提供的信息内容负责。

第十条　任何组织或个人，不得利用计算机国际联网从事危害国家安全，泄露国家秘密等犯罪活动；不得利用计算机国际联网查阅、复制、制造和传播危害国家安全，妨碍社会治安和淫秽色情的信息；发现上述违法犯罪行为和有害信息，应及时向有关主管机关报告。

第十一条　任何组织或个人，不得利用计算机国际联网从事危害他人信息系统和网络安全，侵犯他人合法权益的活动。

第十五条　违反本办法第九条、第十条和第十一条规定的，由邮电部或邮电管理局给予警