E-Crime and Computer Forensics

信息犯罪与计算机取证

王永全　唐　玲　刘三满◎主编

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

E-Crime and Computer Forensics

信息犯罪与计算机取证

王永全　唐　玲　刘三满◎主编

人民邮电出版社

北　京

图书在版编目（CIP）数据

信息犯罪与计算机取证 / 王永全，唐玲，刘三满主编. -- 北京 : 人民邮电出版社，2018.2
ISBN 978-7-115-47398-1

Ⅰ. ①信… Ⅱ. ①王… ②唐… ③刘… Ⅲ. ①计算机犯罪－研究②计算机犯罪－证据－调查 Ⅳ. ①D914.04 ②D918

中国版本图书馆CIP数据核字(2017)第316729号

内 容 提 要

本书以新的视角，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、法律和管理等问题进行了全面、系统的梳理。融信息安全、信息犯罪、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空间安全预防、监控和打击的“前、中、后”思想。主要包括：信息安全，信息犯罪，计算机取证理论、技术、工具及相关标准规范等基本内容；以及电子数据证据的发现与收集，电子数据证据固定与保全，电子数据恢复，电子数据证据归档、分析与评估，计算机司法鉴定，云计算与大数据时代计算机取证面临的新技术与新问题等具体内容；另外，还选取了部分与网络空间安全和信息犯罪紧密相关的法律法规和规章制度作为附录，以适应当前相关课程的前瞻性教学要求和“计算机”与“法律”复合应用型人才培养的迫切需要。结合本书相关内容的学习和实践需要，还编写了配套实训用书《信息犯罪与计算机取证实训教程》，以进一步增强实践性环节的教学需要。

本书适用于计算机、信息安全、通信电子、网络安全与执法、法学、公安学等相关学科专业的本科生高年级学生以及相关专业研究生、企事业单位及公检法司等部门工作人员作为教材或参考书使用。

◆ 主　　编　王永全　唐　玲　刘三满
责任编辑　邢建春
责任印制　彭志环
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京市艺辉印刷有限公司印刷
◆ 开本：787×1092　1/16
印张：20.5　　2018 年 2 月第 1 版
字数：499 千字　　2018 年 2 月北京第 1 次印刷

定价：88.00 元

读者服务热线：（010）81055488　印装质量热线：（010）81055316
反盗版热线：（010）81055315

本书编委会

主　编　王永全　唐　玲　刘三满

副主编　涂　敏　廖根为　徐玉麟　王　弈

委　员（以撰写章节为序）

王　弈　李　玮　廖根为　刘　琴

王永全　唐　玲　赵　庸　徐志强

徐玉麟　刘三满　程　燕　涂　敏

李　毅　焦　娜　刘　洋

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和源泉。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，特别是云计算、大数据、移动互联网、物联网和人工智能等新一代信息技术的推进，人类社会已从农业经济、工业经济、知识经济时代向信息经济和智能经济时代转变。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和智能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和信息革命的飞速发展，互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成的网络空间已成为继“陆、海、空、天”之外的“第五类疆域”，正在全面改变人们的生产生活方式，深刻影响人类社会历史发展进程。下一代互联网技术和通信技术的迅速发展，互联网的普及和应用已涉及生活与工作的方方面面，特别是我国“互联网+”行动计划、中国制造 2025、促进大数据发展行动纲要、国家网络空间安全战略和新一代人工智能发展规划等国家战略规划的制定与实施，电子商务与电子政务的发展壮大，智慧城市建设的开展，使我国新一代信息技术的应用与发展日益深入。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。在移动互联是“新渠道”、大数据是“新石油”、智慧城市是“新要地”、云计算是“新能力”、物联网和人工智能是“新未来”的网络时代，必须维护网络空间主权、安全和发展利益，网络空间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，也是各国奋力攀登的制高点。因此，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、文化和社会生活的各方面，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，扩展到信息基础设施、信息运行系统的保护，即从信息载体或信息基础设施、信息运行、信息内容、信息价值角度进行保护，任何以信息载体或信息基础设施、信息运行、信息内容、信息价值为对象和工具实施的严重危害社会的信息犯罪行为均应受到处罚。

鉴于计算机网络与信息安全的脆弱性，近年来，危害计算机网络与信息安全的事件（纠纷）或违法犯罪行为的案件越来越多，为此，人们对计算机网络与信息安全以及相关违法犯

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）及其相关设备以及数字产品中的数据进行收集、固定、分析，从而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供，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，保障网络空间安全，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，吸引了计算机科学与技术、网络空间安全、法学和公安学等学科领域专家的极大重视和关注，并成为上述所涉及学科的交叉研究前沿领域。

根据以上思考和认识，我们认为，构建具有自主知识产权的网络空间安全防御体系，不仅需要先进的技术和装备作为坚实的基础，而且还需要有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，许多高校的计算机、信息安全、通信、公安技术、法学和公安学等相关学科专业，根据这类复合应用型人才培养对学生应具备的知识和技能要求，已为本科生高年级和研究生开设了相关必修或选修课程，如“信息犯罪与计算机取证”“电子数据取证与司法鉴定”等。为满足这类课程的教学需要，我们从相关课程的具体教学目标及其实现出发，组织具有丰富教学经验的教师，根据信息技术的发展变化，特别是新一代信息技术的深入应用和网络空间安全的法治化建设情况，以新的视角，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、法律与管理等问题进行了梳理，重新编写了“信息犯罪与计算机取证”这本教材，以适应当前相关课程的前瞻性教学要求和复合应用型人才培养的迫切需要。

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，从信息犯罪的防控和打击等方面所涉及的技术、法律和管理问题展开，介绍了信息安全，信息犯罪，计算机取证理论、技术、工具及相关标准规范等方面的基本内容；为切合发生信息犯罪（信息安全事件）后的侦查（调查）取证与鉴定等司法运用实际需要，还较为全面、系统地介绍了电子数据证据的发现与收集，电子数据证据固定与保全，电子数据恢复，电子数据证据归档、分析与评估，计算机司法鉴定以及云计算与大数据时代计算机取证面临的新技术与新问题等具体内容；另外，还选取了部分与网络空间安全和信息犯罪紧密相关的法律法规和规章作为附录。结合本书相关内容的学习和实践需要，还编写了配套实训用书《信息犯罪与计算机取证实训教程》，以进一步增强实践性环节的教学需要。

作为计算机科学与技术、网络空间安全、公安技术、法学与公安学等学科交叉研究和融合的前沿领域知识，本书可作为计算机、信息安全、通信、公安技术以及法学和公安学等相关学科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、技术和管理人员，以及公检法司等领域工作者参考和使用。

本书特色体现在以下方面。

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空间安全预防、监控和打击的“前、中、后”思想，有利于读者

以技术、法律与管理为视角，较为全面、系统地认识和把握网络空间安全问题的体系框架。

2. 交叉性和融合性

本书在参考国内外学者相关研究成果和资料的基础上，结合作者自身所承担的交叉科研课题及其成果，进行了有机的融合。这对计算机科学与技术、网络空间安全与法学和公安学等学科知识交叉融合以及相关专业人才的培养具有重要意义。

3. 实践性和应用性

本书结构清晰、内容简洁、重点突出、编排合理、衔接自然、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、唐玲和刘三满任主编，涂敏、廖根为、徐玉麟和王弈任副主编。王永全和唐玲拟定编写大纲并统稿。统稿人在统稿和审阅全书过程中，对一些章节的内容进行了合理的修改、完善和整合处理。

本书撰写人员的分工如下（以撰写章节为序）：王弈第 1 章，李玮第 1 章，廖根为第 2~6 章、第 12 章、第 13 章、附录，刘琴第 7 章，王永全第 8 章、第 12 章、第 13 章、第 14 章、附录，唐玲第 8 章、第 9 章、第 14 章，赵庸第 8 章、第 9 章，徐志强第 8 章、第 9 章、第 11 章，徐玉麟第 8 章、第 11 章，刘三满第 9 章、附录，程燕第 10 章，涂敏第 11 章、附录，李毅第 11 章、第 13 章，焦娜第 14 章，刘洋第 14 章。

本书在撰写过程中，作为上海市教育委员会 2013 年度本科重点专业（特色）核心课程建设项目的成果之一，得到了华东政法大学以及各参加编写人员所在单位或部门领导的关心、帮助和鼓励，在此表示衷心感谢！同时，本书的撰写，还参考引用了相关学者的资料或研究成果，但难免挂一漏万，在此，表示衷心感谢！此外，还要感谢赵帅、陈贵峰、田晶林、邢华蓉、吕凡、王淼、徐利等为本书部分书稿的校对工作所付出的辛勤劳动。另外，本书的编辑出版，还得到了 2014 年国家社会科学基金重大项目（第二批）“涉信息网络违法犯罪行为法律规制研究”（No.14ZDB147）和“山西省‘1331 工程’重点学科建设计划”的支持，在此，一并表示衷心感谢！

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

作 者

2017 年 10 月

目　录

第1章 信息安全

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

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，理解节点安全与通信安全的联系与区别，及其在整个信息系统中安全的地位与作用。

1.1 信息安全概述

在信息高速发展的今天，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消失殆尽。

随着互联网的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和破坏程度提高的特点。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节点安全到节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。

1.1.1 信息安全的含义

提到安全，人们总会联想到保护有价值的东西。一件物品或东西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

1 http://www.cert.org.

息记录在纸张上，或者写在某件东西上，那么通过传统的物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、U 盘等磁性介质到计算机网络上的节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才能达到期望的效果[2]。例如，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，还要制订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。这些都是构成一个安全信息系统需要考虑的因素。

信息安全是安全研究领域的一个子集，是由信息系统、信息技术产生的相关安全问题的集合。它包括物理安全、数据安全、网络安全、信息基础设施安全、信息资产安全、金融安全、个人权益安全、企业生存安全、社会稳定和国家信息利益安全[3]。信息安全与其他领域的安全问题相比，在问题出现、发展、更替的速度上更快，时效性更强，有极大的挑战性，需要从技术、管理和法律三个层面共同解决。下面给出几个具有代表性的信息安全的定义[4]。

1. 国际标准化组织 ISO 的定义

为数据处理系统建立和采取的技术和管理的安全保护。保护计算机硬件、软件、数据不因偶尔的或恶意的原因而受到破坏、更改、泄露。

2. 欧盟的定义

欧盟在“Information Technology Security Evaluation Criteria”（Version 1.2, Officer for Offical Publication of the European Communities, June, 1991）中将信息安全定义为：在既定的密级条件下，网络与信息系统抵御意外或恶意行为的能力。这些事件和行为将威胁所存储或传输的数据以及经由这些网络和系统所提供服务的可用性、真实性、完整性和机密性。

3. 美国的定义

美国的不同部门对信息安全的定义也略有差异，美国国家安全电信和信息系统安全委员会（NSTISSC）从技术和管理措施角度对信息安全的定义是：对信息、系统以及使用、存储和传输的硬件的保护，是所采取的相关政策、认识、培训和教育以及技术等必要的手段。

从信息安全涉及的内容而言，信息安全是指：确保存储或传送中的数据，不被他人有意或无意地窃取与破坏。包括：

（1）信息设施及环境安全，包括建筑物与周遭环境的安全；

（2）数据安全，确保数据不会被非法入侵者读取或破坏；

（3）程序安全，重视软件开发过程的品质及维护；

（4）系统安全，维护计算机系统正常运作。

而美国军方对信息安全的理解与上述表述有所不同，他们将信息安全问题抽象为一个由信息系统、信息内容、信息系统的所有者和运营者、信息安全规则等多个因素构成的多维空间。

---

2 应用密码学手册 Handbook of Applied Cryptography. [加] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, 著. 胡磊，王鹏, 等, 译. 电子工业出版社，北京：2005 年，p2。

3 张显龙, 编著. 《全球视野下的中国信息安全战略》，清华大学出版社，p33。

4 http://www.iso27001.org.cn/iso27001/biaozhun/show_170.html, 2015 年 12 月 11 日。