XINXI ANQUAN BAOZHANG SHIWU

信息安全保障实务

冯前进 等◎编著

中国政法大学出版社

没有网络安全就没有国家安全

——习近平

信息安全保障实务

冯前进 等◎编著

中国政法大学出版社

2014·北京

图书在版编目（CIP）数据

信息安全保障实务/冯前进等编著. —北京：中国政法大学出版社，2014.8
ISBN 978-7-5620-5460-3

Ⅰ.①信… Ⅱ.①冯… Ⅲ.①信息安全－安全技术 Ⅳ.①TP309

中国版本图书馆CIP数据核字(2014)第162927号

出 版 者　中国政法大学出版社
地　　址　北京市海淀区西土城路25号
邮寄地址　北京100088信箱8034分箱　邮编100088
网　　址　http://www.cuplpress.com（网络实名：中国政法大学出版社）
电　　话　010-58908285(总编室)　58908334(邮购部)
承　　印　固安华明印业有限公司
开　　本　720mm×960mm　1/16
印　　张　23
字　　数　388千字
版　　次　2014年8月第1版
印　　次　2014年8月第1次印刷
定　　价　49.80元

前　言

随着信息技术的迅猛发展，计算机网络的应用领域已从传统的数学运算、文件处理、基于简单连接的内部网络业务处理、办公自动化等小型业务系统，逐渐向大型关键业务系统扩展。随着政府上网、企业上网、教育上网、家庭上网……互联网在经济、军事、文教、金融、商业等诸多领域得到广泛应用，可以说网络无处不在，它正在改变我们的工作方式和生活方式。计算机网络在给人们提供便利、带来效益的同时，也使信息安全面临着前所未有的巨大挑战，这就是信息安全问题。

党中央、国务院高度重视信息化及信息安全保障工作。江泽民同志多次强调，“四个现代化，哪一化也离不开信息化”。胡锦涛同志指出，“信息安全是个大问题。必须把安全问题放到至关重要的位置上，认真加以考虑和解决”。习近平总书记强调，“没有网络安全就没有国家安全”。2014 年 2 月 27 日，中央网络安全和信息化领导小组成立，习近平总书记亲自担任领导小组组长。由国家最高领导人担任主持网络安全和信息化工作的领导小组的组长，这在我国历史上还是第一次。

2003 年 7 月 22 日，国家信息化领导小组第三次会议在北京召开。会议讨论通过了我国信息安全保障工作的重要政策性指导文件——《关于加强信息安全保障工作的意见》（中办发［2003］27 号文），文中强调，要建立健全信息安全管理责任制，要始终坚持一手抓信息化发展，一手抓信息安全保障。文件明确提出了“积极防御、综合防范”的安全方针。

本书以信息安全保障为主线，分别从法律法规标准、管理、技术三个层面阐述如何构建信息安全保障体系。

本书由浙江警官职业学院冯前进副教授策划，并主持编著。全书框架和内容由冯前进制定、审核与修改。全书由冯前进统稿，由杭州电子科技大学赵泽茂教授主审。参加本书编著的有浙江警官职业学院冯前进、吕韩飞、孙

培梁、冯卓慧、郝晋霞，海南政法职业学院范一乐、郭毅，湖南安全技术职业学院匡芳君，河南职业技术学院王爱强，以及宁夏司法警官职业学院刘东昌等老师。浙江省公安厅网监总队总工程师蔡林教授对本书的编著提出了宝贵的意见和建议，在此谨表谢意。

各教学模块撰稿人分别是（以撰写学习单元先后为序）：

学习单元1～3：冯前进；　　学习单元4：刘东昌、冯前进；

学习单元5～6：孙培梁；　　学习单元7：王爱强；

学习单元8：范一乐；　　学习单元9：匡芳君；

学习单元10：郭毅；　　学习单元11：郝晋霞；

学习单元12～14：吕韩飞；　　学习单元15～16：冯卓慧。

由于作者水平有限，书中难免有疏漏和欠缺之处，敬请读者提出宝贵意见。

作　者

2014年5月

目　录

第一部分　信息安全保障概述

第二部分　信息安全标准与法律法规

第三部分　信息安全技术应用

第一部分　信息安全保障概述

学习单元1

信息化与信息安全

【学习目的与要求】

了解信息化的发展和信息安全现状，了解信息安全的概念。

第一节　信息化的发展和信息安全现状

21世纪，随着全球信息化趋势的不可避免，信息安全问题日渐成为世界各国所面临的主要问题之一。在我国接连发生了多起重大信息安全事件后，人们开始逐渐认识到国家的信息化程度越高，所面临的信息安全挑战也会越多。

一、信息化迅猛发展，信息技术广泛应用，我国步入信息化时代

据2014年1月中国互联网络信息中心（CNNIC）发布的《第33次中国互联网络发展状况统计报告》统计：截止到2013年12月31日，我国网民人数达到了6.18亿，互联网普及率为45.8%，网民规模为世界第一位；中国拥有的IPv4地址数达到3.30亿个，拥有IPv6地址16670块/32，排名世界第二；网站总数达到320万个，域名总数达到1844万个；网络国际出口带宽总量则达到3 406 824Mbps。

根据调查统计，有4.89亿人使用搜索引擎，有4.91亿人阅读网络新闻，有5.32亿人经常使用即时通信工具，3.38亿人经常参与网络游戏，2.59亿人经常使用电子邮件，4.37亿人拥有个人博客/个人空间，3.02亿人利用网络购物，2.50亿人使用网络银行，2.60亿人使用网上支付，这些数据表明互

联网已经深入到人们衣食住行的方方面面。[1]

另据《2013 年度中国电子商务市场数据监测报告》显示，2013 年中国电子商务市场交易额已达 10.2 万亿元，同比增长 29.9%；2013 年电子商务企业数量已达 29 303 家；2013 年个人网店的数量已经达到了 1120 万家；截至 2013 年 12 月，电子商务服务企业直接从业人员超过 235 万人。目前由电子商务间接带动的就业人数，已超过 1680 万人。

进入 21 世纪，中国的信息化步入快速发展的新阶段。国民经济与社会信息化水平不断提高，信息化在促进经济与社会协调、稳定、持续的发展过程中，发挥着越来越重要的作用。政府主导的人民网、新华网等新闻网站和新浪、搜狐等商业性综合网站的设立和稳步发展，在传播重要信息、反映社情民意、引导社会舆论等方面发挥了极其重要的影响和作用。信息化所带来的好处日益呈现，广大民众对信息化的前景和潜在价值的认识也越来越深刻。这些都充分说明，我国信息化建设已顺利迈入了一条适合本国国情、快速发展的道路，信息化进程良好，前景喜人。

互联网的飞速发展，改变了我们的生活、工作和学习方式，促进了经济和社会的发展，互联网在给人们带来了巨大的便利的同时，也使人类面临着信息安全方面的巨大挑战。近年来，网络安全隐患此起彼伏，计算机病毒和“黑客”攻击网络事件屡有发生，计算机（网络）犯罪也随之滋生，计算机犯罪不仅形式、手段新颖，而且发展速度迅猛、危害严重，从而对国家的主权、安全和社会稳定构成了威胁。

二、信息安全问题日益突出，信息安全现状面临严峻考验

据《2008 年全国信息网络安全状况与计算机病毒疫情调查分析报告》[2]，2008 年信息网络安全事件发生比例为 62.7%，计算机病毒感染率为 85.5%。而据 2011 年 7 月中国互联网络信息中心（CNNIC）发布的《第 28 次中国互联网络发展状况统计报告》统计，2011 年上半年，遇到过病毒或木马攻击的网民人数为 2.17 亿人，占网民总人数的 44.7%。有过账号或密码被盗经历的网民人数达到 1.21 亿人，占网民总人数的 24.9%，较 2010 年底增加了 3.1 个百分点。商务应用的发展也滋生了网上诈骗等问题，有 8% 的网民最近半年

〔1〕 数据来源：《CNNIC：第 33 次中国互联网络发展状况统计报告》。

〔2〕 调查内容为 2007 年 5 月至 2008 年 5 月我国联网单位发生网络安全事件以及计算机用户感染病毒情况。

在网上遇到过消费欺诈，该群体网民规模达到3880万。

所面临的信息安全问题，具体来说主要包括以下八个方面：

（一）网络安全事件屡屡发生，信息安全保障工作面临挑战

【案例1】跨行交易中断8小时

2006年4月20日上午10时56分，中国银联系统通信网络和主机出现故障，ATM机不能跨行取款，POS机不能刷卡消费，网上跨行交易无法顺利进行。

故障发生后，中国银联启动紧急应对预案，召集相关设备厂商共同努力。同时，银联及时告知各成员银行进展状况，通过全国分支机构和95516客服热线向商户和持卡人说明故障情况，并通过官方网站和新闻媒体通报事件与致歉。到下午5点左右，大部分机构和商户已基本恢复正常。晚8点，在银联与设备厂商的共同努力下，银联网络已经全面恢复正常。

【案例2】民航离港系统瘫痪

2006年10月10日，北京，一连串急促的电话声打破了中国民航信息网络股份公司（简称“中航信”）的平静：首都机场，13时28分起，由于离港系统的主机文件损坏，造成操作系统的核心文件无法使用，机场和航空公司无法在前端提取旅客信息数据，导致33个航班延误，近千名旅客滞留。

然而，受影响的机场并没有止步于首都机场。13时33分起，深圳宝安机场离港系统瘫痪44分钟，25个航班不能正常办理登机手续；13时35分起，广州新白云机场离港系统瘫痪45分钟，7个航班直接受影响，乘机手续只能改为手工办理……

【案例3】证券交易系统大面积拥堵

2007年1月15日，申银万国公司交易系统全线拥堵；1月17日，建设银行一个营业部基金销售系统发生瘫痪；1月18日，招商证券交易系统发生瘫痪；1月19日，光大银行在销售国投瑞银基金公司基金时，注册登记系统陷入瘫痪。随着牛市的来临，网络梗阻、系统罢工、电话无效导致的大面积“堵单”事件让股民忧心，更让券商面临严峻的考验。

【案例4】最高人民检察院举报网站开通首日因点击率过高遭瘫痪

检察机关全国统一举报电话“12309”自2009年6月22日起在最高人民检察院和部分省级检察院正式投入使用，其余省份将在年内陆续开通。同时，为方便群众记忆和使用，最高检举报网站的新域名

www. 12309. gov. cn 于 6 月 22 日起正式启用。但因点击率过高，最高检举报网站开通首日就遭瘫痪。

【案例 5】国防部网站开通首月遭 230 多万次攻击

2009 年 8 月 20 日零时，中国国防部网站上线试运行，开通第一日点击量达 7000 多万，第二天就冲到 1. 3 亿，网站试运行 3 个月以来总点击量已经达到 12. 5 亿次。而开通首月，网站受到的攻击达 230 多万次。

（二）网络犯罪形势严峻

根据公安部统计，1988 年～1989 年，仅发生计算机犯罪案件 9 起，1989 年～1990 年发生计算机犯罪案件上百起，1993 年发生计算机犯罪案件 1000 多起，1994 年为 1450 起，2000 年公安机关立案侦查的计算机违法犯罪案件达到 2700 余起，2001 年又涨到 4500 余起，2003 年高达 10 000 多起，到了 2005 年，又上升至 21 000 余起。由此可以看出，计算机犯罪的发案率呈直线上升趋势。如何有效地发现、打击和预防计算机犯罪，成为公安、司法机关在新世纪亟待解决的重大课题。

尤其是我国网络金融安全隐患巨大，我国银行网络每年因安全问题，包括外部攻击、内外勾结、内部人员违法犯罪和技术缺陷，引起的经济损失数以亿计。

【案例 6】 1986 年 7 月，中国银行深圳市蛇口支行电脑主管陈新义伙同苏庆忠通过计算机骗取银行巨款，共计人民币 2 万余元，港币 3 万元，成为中国大陆第一例计算机犯罪案件。

【案例 7】 1995 年 6 月，桂林市工商银行解东办事处微机操作员李波擅自修改计算机程序和数据，将储户存入的款项改存到自己的账号上，先后作案 6 起，总金额达到人民币 2110 万元，成为我国国内涉案金额最大的一起计算机犯罪。

【案例 8】 2004 年 9 月 5 日，我国首例利用木马程序犯罪案在江西省南昌市中级人民法院开庭审理。公诉机关指控，三名被告张勇、王浩、邹亮（“黑客”）以自己制作的仿冒网站为平台，利用木马程序非法窃取了全国各地 50 多名股民的股票账号与密码，在不到 2 个月的时间里，盗买、盗卖价值 1141. 9 万元的股票，非法获利 38. 6 万元。9 月 9 日下

午，南昌市中级人民法院一审以盗窃罪判处张勇无期徒刑，王浩、邹亮分别被判13年和12年有期徒刑。

【案例9】2005年9月，天津市商学院校园发生银行卡盗窃案。经查该校在学生入学时统一为学生办理了农业银行信用卡，反映失窃的学生均为该校03级高职学生，共有50多人，共失窃10余万元。专案组确定应为嫌疑人窃取了受害人的银行卡资料后，用互联网上淘宝网下属的“支付宝公司（网上银行代理）”采用支取、转账或购物的方式盗取银行卡内现金。在犯罪嫌疑人宗徽辉（浙江东阳人）作案的3天里，共窃取42名学生信用卡内人民币71000元，并先后72次转账至其在“支付宝”上申请的7个账户内，后被法院以盗窃罪依法判处有期徒刑7年，并处罚金人民币1万元；本案另一犯罪嫌疑人邹磊（03级工业设计专业学生，20岁，安徽人）系该校校园网站负责人，警方将其抓获后在其宿舍起获了“代如亮”等5张身份证、10余张银行卡，以及用赃款购置的笔记本电脑、MP3等，涉及金额1.6万余元。

（三）网上有害信息污染严重

计算机有害信息主要是指计算机网络及计算机信息系统及其存储介质中存在、出现的，以计算机程序、图像、文字、声音等多种形式表示的，含有攻击人民民主专政、社会主义制度，攻击党和国家领导人，破坏民族团结等危害国家安全内容的信息；含有宣扬封建迷信、淫秽色情、凶杀、教唆犯罪等危害社会治安秩序内容的信息，以及危害计算机信息系统运行和计算机功能发挥，影响应用软件的数据可靠性、完整性和保密性，用于违法活动的计算机程序（含计算机病毒）。

有害信息在网络上传播的主要表现形式有：

1. 在校园网电子公告栏、留言板、聊天室、QQ等交互式栏目和一些网站、网页、个人主页中张贴、传播有害信息。

2. 通过电子邮件和短信息服务发送有害信息及网上泄密等。

3. 境外敌对势力、民族分裂势力、宗教极端势力、“法轮功”邪教和“民运”组织等网站和论坛。

4. 在互联网上下载、传播含有色情、赌博、暴力、封建迷信等的不健康信息。

5. 制造计算机病毒并将其在互联网上传播，且计算机病毒已经严重威胁人们正常的工作与生活。

据公安部统计，仅2007年1月1日~5月15日，全国各地共清理、删除网上淫秽色情信息等有害信息16万余条，其中淫秽色情信息9万余条，诈骗、六合彩赌博和销售违禁品等有害信息7万余条；关闭违法网站和网上信息服务栏目4800余个；各级公安机关立案侦查网络淫秽色情违法犯罪案件1170余起，侦破案件244起，抓获涉案违法犯罪嫌疑人270余名。

（四）网络黑客无孔不入

2007年，在地下黑色产业链的推动下，网络犯罪行为趋利性表现得更加明显，追求经济利益依然是其主要目标。黑客往往利用仿冒网站（俗称网络钓鱼）、伪造邮件、盗号木马、后门病毒等方式，并结合社会工程学，窃取大量用户数据牟取暴利。用户数据包括网游账号、网银账号和密码、网银数字证书等。木马、病毒等恶意程序的制作与传播、窃取用户信息、第三方平台销赃、洗钱等各环节的流水作业构成了完善的地下黑色产业链条，为各种网络犯罪行为带来了利益驱动，加之黑客攻击手法隐蔽性更强，使得对这些网络犯罪行为的取证、追查和打击都非常困难。

2010年CNCERT共接到网页仿冒事件报告1566起，其中被仿冒的大多是电子商务网站、金融机构网站、第三方在线支付站点、社区交友网站等。表1-1列出了CNCERT又称CNCERT/CC接收到的按事件次数排名的前十位被仿冒网站。

表1-1　2010年CNCERT接收到被仿冒网站TOP10

被仿冒网站	次数
bbva. com（毕尔巴鄂比斯开银行）	170
ebay. com（美国电子商务网站）	134
bradesco. com. br（巴西布拉德斯科银行）	127
hsbc. com. cn（中国香港汇丰银行）	115
irs. gov（美国国家税务局）	73
wachovia. com（美国瓦霍维亚银行）	71
alliance - leicester. co. uk（英国联合莱斯特银行）	57
icbc. com. cn（中国工商银行）	51
cctv. com（中国中央电视台）	51
ceca. es（西班牙储蓄银行联盟）	37