网络信息安全工程技术与应用分析

潘 霄 葛维春 全成浩 胡 博 吴克河 潘明惠◎著

- 系统总结了最新**网络信息安全**工程理论和研究成果。
- 汇集了国家重大**科技攻关项目**与信息安全示范工程的经验
- 全面介绍了**信息安全**的基本理论、基础知识和发展趋势
- 包含**安全系统设计**、**安全防护体系**、**身份认证**与**授权管理**系统
- 介绍了**风险评估**方法、**数据备份**与**灾难恢复**、网络信息安全等级保护

清华大学出版社

网络信息安全工程技术与应用分析

潘 霄 葛维春 全成浩 胡 博 吴克河 潘明惠◎著

清华大学出版社
北 京

内 容 简 介

本书结合作者组织和参加国家重大科技攻关项目“电力系统信息安全示范工程”、国家863项目“电力二次系统安全防护体系研究”以及国网公司SG186、SG-ERP信息安全等级保护及保障体系工程的实践经验，本着力求反映信息安全技术的最新发展和理论与工程实践相结合的原则而编写。

全书共分为10章，主要内容包括国内外网络信息安全工程技术发展趋势、我国信息安全重大政策及发展方向、网络信息安全工程基本原理、网络信息安全工程技术领域基础知识及最新技术、网络信息安全风险评估方法与应用分析、网络信息安全系统设计与应用分析、网络信息安全防护体系及应用分析、网络信息安全身份认证与授权管理系统及应用分析、数据存储备份与灾难恢复技术及应用分析、网络信息安全等级保护及应用分析、互联网络空间安全战略与应用分析，以及在网络信息安全工程实践中成功的案例。

本书的突出特点是系统总结了运用最新网络信息安全工程理论和最新研究成果，组织和参加网络信息安全工程实践取得的成功案例。读者通过本书既可以学习网络信息安全工程理论和基础知识，互联网络空间安全战略及网络信息安全最新技术，也可以通过大量实例掌握网络信息安全工程组织、管理和技术实现方法。本书可作为高等院校、能源电力等行业的培训教材，也可以作为企事业单位从事信息安全工程工作的管理人员和工程技术人员的参考工具用书。

图书在版编目（CIP）数据

网络信息安全工程技术与应用分析 / 潘霄等著. —北京：清华大学出版社，2016
ISBN 978-7-302-43610-2

Ⅰ. ①网…　Ⅱ. ①潘…　Ⅲ. ①计算机网络–安全技术–研究　Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字（2016）第077561号

责任编辑：冯志强　薛　阳
封面设计：吕单单
责任校对：胡伟民
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn, http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：清华大学印刷厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　印　张：20.75　　插　页：1　　字　数：535千字
版　　次：2016年6月第1版　　印　次：2016年6月第1次印刷
印　　数：1～4000
定　　价：49.00元

产品编号：069001-01

This book is based on practical experience of organizing and participating in the major national scientific and technological project "Power System Information Security Demonstration project", the National 863 project "Power Secondary System Security Protection System Research" and the State Grid Corporation of SG186, SG-ERP of hierarchical protection of information security and the security system projects, and in principle of reflecting the latest development of information security technology and engineering practice.

This book contains 10 chapters. The main content is as follows: the domestic and international development trends of information security engineering technology, China's information security policy and the development direction of information security, the fundamental principle of information security engineering, the fundamental knowledge and the latest technology of information security engineering field, the design, application and analysis of information security system, identity authentication and authorization management system, data storage backup and disaster recovery system, network information security hierarchical protection, interconnection network space security strategy, and the successful cases in the network information security in engineering practice.

The outstanding feature of this book is to systematically summarize the application of the latest network information security engineering theory and the latest research results, and the successful cases from the personal organization and participation in network information security engineering practice. Readers can not only learn the network information security engineering theory and the fundamental knowledge, interconnection network space security strategy and the latest technology of network information security, but also grasp the method of organizing and managing the network information security engineering through a large number of practical examples. It is a valuable reference which elaborates network information security technology and engineering application analysis. It can be used as the textbook for institutions of higher learning or training materials for energy and electric power enterprises, or as the reference book for management and technical personnels of enterprises and institutions engaged in information security engineering.

本书编写人员

著者 潘霄 葛维春 全成浩 胡博 吴克河 潘明惠
前言 潘明惠
第 1 章 绪论 葛维春、刘 刚、周雨田、胡全贵
第 2 章 网络信息安全工程基本理论 全成浩、王漪、黎辉、杨大威、栾敬钊
第 3 章 网络信息安全工程基础知识 刘文娟、杨海峰、吴菲、陈力、王跃东
第 4 章 网络信息安全风险评估方法与应用分析 胡博、鲁顺、夏宗泽、祝榕岭
第 5 章 网络信息安全系统设计与应用分析 吴克河、李广野、潘洪建、苏畅、祁广源
第 6 章 网络信息安全防护体系及应用分析 孙 刚、刘国威、张松、高海波、戚欣革
第 7 章 身份认证与授权管理系统及应用分析 杨万清、王泽宁、雷振江、潘宁、隋佳新
第 8 章 数据存储备份与灾难恢复技术及应用分析 杨 轶、潘邈、吕旭明、张忠林、潘 琪
第 9 章 网络信息安全等级保护及应用分析 陈文康、尹晓华、刘永昌、刘坤、金星
第 10 章 网络空间信息安全战略及应用分析 潘霄、刘凯、金昱、周英杰、张凤军

前　言

人类先后经历了农业革命、工业革命、信息革命。每一次产业技术革命，都给人类的生产、生活带来了巨大而深刻的影响。现在，以互联网为代表的信息技术日新月异，引领了社会生产的新变革，创造了人类生活新空间，拓展了国家治理新领域，极大地提高了人类的认识水平，人们认识世界、改造世界的能力得到了极大提高。互联网作为20世纪最伟大的发明之一，把世界变成了“地球村”。全世界进入互联网3.0万物互联时代，2015年，全球网民数量已接近人口总数的一半。中国网民数量早在2008年就跃居全球第一，目前仍在快速增长中。截至2015年6月，中国网民规模已达6.68亿人，超过整个欧盟的总人口数量。互联网普及率为48.8%，其中，农村网民规模达1.86亿，与2014年年底相比增加800万。“十二五”期间，互联网经济在中国GDP中占比持续攀升，2014年达到7%，占比超过美国。

自2014年2月中央网络安全与信息化领导小组成立以来，习近平主席就网络安全与信息化重要性，多次强调指出“没有网络安全，就没有国家安全”、“没有信息化，就没有现代化”、“现在人类已经进入互联网时代这样一个历史阶段，这是一个世界潮流，而且这个互联网时代对人类的生活、生产、生产力的发展都具有很大的进步推动作用”、“网络信息是跨国界流动的，信息流引领技术流、资金流、人才流，信息资源日益成为重要生产要素和社会财富，信息掌握的多寡成为国家软实力和竞争力的重要标志”、“网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。做好网络安全和信息化工作，要处理好安全和发展的关系，做到协调一致、齐头并进，以安全保发展、以发展促安全，努力建久安之势、成长治之业”。

信息技术的发展拓展了人类感知、处理、存储、传递的能力，为人类开拓了崭新的生存空间。这种能力渗透到各行各业，显示了任何人，在任何地方，任何时间，高效高速地完成计算、通信、控制的潜能，使人类进入了无限遐想的信息革命时代。中国工程院沈昌祥院士，在谈到信息时代网络安全的重要性时强调：网络已经成为继陆、海、空、天之外的国家第5大主权空间。正如美国著名未来学家托夫勒所预言：“计算机网络的建立与普及将彻底地改变人类生存及生活的模式，而控制与掌握网络的人就是主宰。谁掌握了信息，控制了网络，谁就将拥有整个世界”。网络安全关系到国家安全，控制网络空间，就可以控制一个国家的经济命脉、政治导向和社会稳定。由于互联网信息技术以几何级数爆炸式增长、与相关领域快速融合和治理规范的缺失，在国内和国际层面上，网络虚拟空间都潜藏着诸多风险，包括网络恐怖主义在内的种种不法行为和有害信息，给各国的主权安全、民生经济等带来了严峻的现实挑战。信息是我们所处时代人类社会发展的主要战略资源，网络信息安全危及国家的政治、军事、经济、文化、社会生活的各个方面，已成为影响国家

大局和长远利益的重大战略问题。网络信息安全保障能力是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，是世界各国在奋力攀登的制高点。

本书结合作者组织和参加国家重大科技攻关项目“电力系统信息安全示范工程”、国家863项目“电力二次系统安全防护体系研究”以及国家电网公司SG186、SG-ERP信息安全等级保护及保障体系工程的实践经验，本着力求反映信息安全技术的最新发展成果，以及理论与工程实践相结合的原则而编写。全书共分为10章：第1章分析国内外网络信息安全工程技术发展趋势，我国信息安全重大政策及发展方向；第2、3章介绍网络信息安全工程技术基本理论、信息安全工程技术领域基础知识及最新技术；第4章 探讨网络信息安全系统设计与应用分析；第5章阐述网络信息安全风险评估方法与应用分析； 第6章分析网络信息安全防护体系与应用；第7章探讨网络信息安全身份认证与授权管理系统与应用分析；第8章介绍数据存储备份与灾难恢复系统与应用分析；第9章 阐述网络信息安全等级保护与应用分析；第10章分析互联网络空间安全战略与应用；并介绍了在网络信息安全工程实践中成功的案例。

近年来，互联网信息技术飞速发展，在人们面前展示出一幅美好的画卷，同时，网络空间信息安全也受到严重的威胁，党中央和国务院已将网络空间安全与信息化同时提升到国家战略。作者长期从事信息化与网络信息安全工程研究，在国内外发表过大量文章、报告和培训讲课，深深地感到我们与先进国家相比还有一定差距，挑战与机遇并存，希望与困难同在，我们必须抓住机遇迎接挑战，满怀希望战胜困难。

本书的突出特点是系统总结了最新网络信息安全工程理论和最新研究成果，运用社会发展系统动力学原理，组织和参加网络信息安全工程实践取得的成功案例。读者通过本书既可以学习网络信息安全工程理论和基础知识，互联网络空间安全战略及网络信息安全最新技术，也可以通过大量实例掌握网络信息安全工程组织、管理和技术实现方法，是一本网络信息安全工程技术与应用分析的工具书。可作为高等院校、能源电力等行业培训教材，也可以供企事业单位从事信息安全工程相关工作的管理人员和工程技术人员参考。

本书编著出版，衷心感谢国家电网公司吴玉生总信息师、李向荣副总工程师、刘建明主任、王继业主任、吴杏平主任，中国电力科学研究院周孝信院士、于尔铿老师、刘广一博士、赵君总经理、哈尔滨工业大学徐殿国院长、陈学允老师、柳焯老师、李志民老师，中国科学院沈阳计算技术研究所李彤、王素香研究员等人多年来的关心帮助与支持。衷心感谢辽宁省电力有限公司有关部门、基层单位同志们的大力支持，感谢国家科技部及国家商用密码管理办公室组织专家、教授的指导和帮助，感谢辽宁省电力有限公司经济技术研究院、华北电力大学电力信息技术工程研究中心、为本书编辑出版发行给予的大力支持和帮助。由于时间仓促，作者水平有限，书中的内容难免有疏漏或不妥之处，敬请读者批评与指教。

潘明惠

2016年1月16日于沈阳

目　录

第1章 绪 论

信息技术的发展，以其拓展人类感知、处理、存储、传递的能力，为人类开拓出崭新的生存空间。网络已经成为继陆、海、空、天之外的国家第5大主权空间。习近平主席关于“没有网络安全，就没有国家安全”，“没有信息化，就没有现代化”的科学论断，揭示了网络安全及信息化在国家战略中的重要地位和作用。

1.1 背景及意义

互联网是20世纪最伟大的发明之一，自从1994年我国首次全功能接入互联网，中国互联网已经过二十多年的发展，网民规模迅速扩大。截至2015年6月，中国网民已达6.68亿人，超过整个欧盟的总人口数量。随着现代信息和网络技术的不断发展和广泛应用，国际信息化浪潮更加深刻地影响和改变着人们的生产方式、生活方式、工作方式，不断推出的各种网络接入更加便捷，应用更加多样，内容极大丰富，网络已经变得“无处不在、无时不在、无所不包”，极大地促进了国家经济、政治、文化、社会等各个方面的发展。信息已经成为人类社会发展的重要战略资源。对中国而言，网络空间最大限度地激发了信息化高速发展的活力，蕴含着新一轮技术革命的丰厚能量，网络技术的迭代式发展和互联网公司的创新应用，让互联网经济成为拉动消费需求的重要力量。网络空间为维护、延长中国的战略机遇期赢得了新的发展机会，又为中国开拓新的发展空间创造了历史条件。但与此同时，网络和业务发展过程中也出现了许多新情况、新问题、新挑战，世界各国对信息安全的重视程度不断提高，国际信息安全领域动作频繁，各国政府、军队、相关企业成为该领域的主角。美国著名未来学家托夫勒所预言：“计算机网络的建立与普及将彻底地改变人类生存及生活的模式，而控制与掌握网络的人就是主宰。谁掌握了信息，控制了网络，谁就将拥有整个世界”。网络信息安全已经成为国家战略重点。云计算、云安全、大数据、物联网、智慧地球、智能化安全产品、网络战等新概念、新技术和新产品层出不穷，国际信息安全领域的发展呈现出一些新特点和新趋势。发展信息安全工程技术已成为世界各国信息化建设的重要任务，信息安全已成为维护国家安全和社会稳定的重要基石。

2000年初，国家启动了“十五”重大科技攻关项目“国家信息安全应用示范工程”，国家电力公司承担电力系统信息安全示范工程项目。辽宁省电力有限公司成为电力系统信息安全示范工程试点单位，全面组织“辽宁电力系统信息安全应用示范工程”。2002年启动了国家“863”项目“国家电网调度中心安全防护体系研究及示范工程”，提出了我国电力系统信息安全防护总体策略：“安全分区、网络专用、横向隔离、纵向认证”，由此形成

了以边界防护为要点、多道防线构成的纵深防护体系。2006 年，国家电网公司实施了信息化 SG186 工程，全面建设一体化企业级信息集成平台，人、财、物等 8 大类业务应用，技术、标准、安全防护等 6 个保障体系，大力推进集团企业的信息化建设，推动信息化向集中统一和优化整合方向发展。2011 年，国家电网公司在 SG186 工程的基础上，全面启动了“覆盖面更广、集成度更深、智能化更高、安全性更强、互动性更好、可视化更优”的信息化 SG-ERP 工程建设，根据电网信息安全防护特点，建设电网信息安全三道防线以实现网络纵深防御，进一步提升了信息系统的安全保障能力，我国电力信息安全达到国际一流水平。

2014 年 2 月 27 日，中央网络安全与信息化领导小组成立，由中共中央总书记、国家主席习近平担任组长，李克强总理担任第一副组长，统筹协调各个领域的网络安全和信息化重大问题，制定实施国家网络安全和信息化发展战略、宏观规划和重大政策，不断增强安全保障能力。习近平主席关于“没有网络安全，就没有国家安全”，“没有信息化，就没有现代化”的科学论断，将网络安全及信息化国家战略提高到前所未有的高度，预示着中国在打一场网络安全和信息化的翻身仗方面，也将迎来新的历史突破。强化网络信息安全，并与国家信息化整体战略双轮驱动，对中华民族伟大复兴，实现两个一百年奋斗目标具有重大战略意义。

1.2 国内外网络信息安全发展简述

1.2.1 国际网络信息安全工程技术发展历程

第一个时期是通信安全时期，以 1949 年香农发表的《保密通信的信息理论》为里程碑，主要研究对称密码算法和分析。在这个时期通信技术还不发达，计算机只是零散地位于不同的地点，信息系统的安全仅限于保证计算机的物理安全以及通过密码（主要是序列密码）解决通信安全的保密问题。把计算机安置在相对安全的地点，不容许非授权用户接近，就基本可以保证数据的安全性了。这个时期的安全性是指信息的保密性，对安全理论和技术的研究也仅限于密码学。这一阶段的信息安全可以简称为通信安全，它侧重于保证数据在从一地传送到另一地时的安全性。

第二个时期为计算机安全时期，在 20 世纪 60 年代后，半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，计算机和网络技术的应用进入了实用化和规模化阶段，数据的传输已经可以通过计算机网络来完成。这时候的信息已经分成静态信息和动态信息。1969 年，美国兰德公司给美国国防部的报告中指出“计算机太脆弱了，有安全问题”——这是首次公开提到计算机安全。在当时和其后的相当一段时间，“计算机安全”的内涵主要是指实体安全，即物理安全。

1976 年，现代密码学时代，以提出非对称（公钥）密码思想为标志，非对称密码体制及相关技术迅速发展。1977 年美国国家标准局（NBS）公布的国家数据加密标准（DES）

和1983年美国国防部公布的可信计算机系统评价准则（TCSEC-Trusted Computer System Evaluation Criteria，俗称橘皮书，1985年再版）标志着解决计算机信息系统保密性问题的研究和应用迈上了历史的新台阶。到了20世纪80年代后期，“网络安全”和“信息安全”才开始逐步被广泛采用。

第三个时期是在20世纪90年代兴起的网络时代。从20世纪90年代开始，由于互联网技术的飞速发展，信息无论是企业内部还是外部都得到了极大的开放，而由此产生的信息安全问题跨越了时间和空间，信息安全的焦点已经从传统的保密性、完整性和可用性三个原则衍生为诸如可控性、抗抵赖性、真实性等其他的原则和目标。

第四个时期是进入21世纪的信息安全保障时代，其主要标志是《信息保障技术框架》（IATF）。如果说对信息的保护，主要还是处于从传统安全理念到信息化安全理念的转变过程中，那么面向业务的安全保障，就完全是从信息化的角度来考虑信息的安全了。体系性的安全保障理念，不仅是关注系统的漏洞，而且是从业务的生命周期着手，对业务流程进行分析，找出流程中的关键控制点，从安全事件出现的前、中、后三个阶段进行安全保障。面向业务的安全保障不是只建立防护屏障，而是建立一个“深度防御体系”，通过更多的技术手段把安全管理与技术防护联系起来，不再是被动地保护自己，而是主动地防御攻击。也就是说，面向业务的安全防护已经从被动走向主动，安全保障理念从风险承受模式走向安全保障模式。信息安全阶段也转化为从整体角度考虑其体系建设的信息安全保障时代。

1.2.2 我国网络信息安全发展历程及趋势

我国网络信息安全工程技术发展经历了以下5个阶段。

第一阶段：20世纪80年代末之前。1986年，中国计算机学会计算机安全专业委员会正式开始活动，以及1987年国家信息中心成立第一个专门安全机构，从一个侧面反映了中国计算机安全事业的起步。这个阶段的典型特征是国家尚没有相关的法律法规，没有较完整意义的专门针对计算机系统安全方面的规章，安全标准也少，谈不上国家的统一管理，只是在物理安全及保密通信等个别环节上有些规定，广大应用部门也基本上没有意识到计算机安全的重要性，只有个别部门和少数有计算机安全意识的人们开始在实际工作中进行摸索。在此阶段，计算机安全的主要内容就是实体安全，20世纪80年代后期开始了防计算机病毒及计算机犯罪的工作，但都没有形成规模。

第二阶段：20世纪80年代末至20世纪90年代末。20世纪80年代末，随着我国计算机应用的迅速拓展，各个行业、企业的安全需求也开始显现。除了此前已经出现的病毒问题，内部信息泄漏和系统宕机等成为企业不可忽视的问题。此外，20世纪90年代初，世界信息技术革命使许多国家把信息化作为国策，美国“信息高速公路”等政策也让中国意识到了信息化的重要性，在此背景下我国信息化开始进入较快发展期，中国的计算机安全事业也开始起步。

在这个阶段，一个典型的标志就是关于计算机安全的法律法规开始出现——1994年，公安部颁布了“中华人民共和国计算机信息系统安全保护条例”，这是我国第一个计算机安