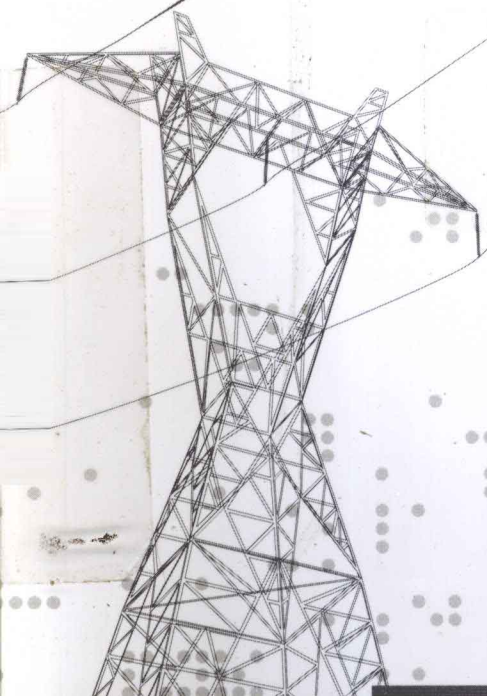
国家“十五”重大科技攻关项目
《电力系统信息安全示范工程》项目

成功实践经验 最新研究成果

网络信息安全工程

原理与应用

潘明惠 著



清华大学出版社

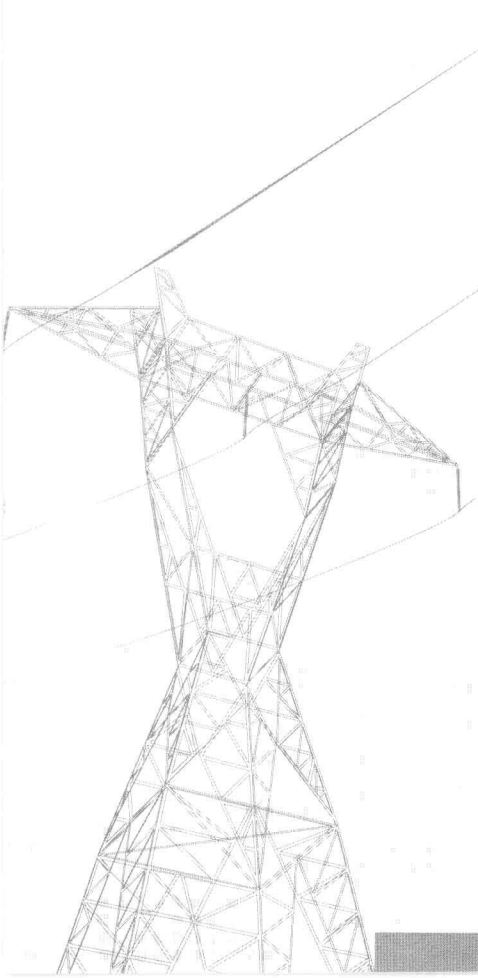
国家“十五”重大科技攻关项目
《电力系统信息安全示范工程》项目

成功实践经验 最新研究成果

网络信息安全工程

原理与应用

潘明惠 著



清华大学出版社
北 京

内 容 简 介

本书是作者在组织和主持国家“十五”重大科技攻关项目《电力系统信息安全示范工程》的实践中，运用社会发展系统动力学原理以及网络信息安全理论，指导大量网络信息安全工程实践取得成功经验，以及在应用工程理论和实践最新研究成果基础上编著的。

全书共分 9 章，第 1 章探讨网络信息安全与现代信息社会，信息安全工程主要研究方向以及云计算及云安全的现状及发展趋势。第 2 章介绍网络信息安全工程基本概念，网络信息安全工程有关基本原理，国际信息安全有关标准的研究与工程应用情况。第 3 章探讨网络信息安全总体框架、管理体系、技术体系的系统设计及应用实例。第 4 章探讨网络信息安全风险评估方法，风险评估目的及范围，安全风险评估及分析及应用实例。第 5 章探讨信息网络基础平台结构优化及应用实例。第 6 章探讨信息安全监视及管理平台的设计及应用实例。第 7 章探讨网络信息安全防护技术原理，网络信息安全防护体系的设计及应用实例。第 8 章探讨网络信息安全 PKI-CA/PMI 身份认证与授权管理系统及应用实例。第 9 章探讨数据存储备份与灾难恢复系统及应用实例。

本书的突出特点是系统总结了运用信息安全基本理论和作者最新研究成果，读者通过本书可以学习网络信息安全基本理论、掌握网络信息安全工程组织、管理和应用工程实践方法及系统应用实例。

图书在版编目（CIP）数据

网络信息安全工程原理与应用 / 潘明惠著. —北京：清华大学出版社，2011.6
ISBN 978-7-302-25517-8

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

中国版本图书馆 CIP 数据核字（2011）第 076969 号

责任编辑：冯志强
责任校对：徐俊伟
责任印制：李红英
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京鑫丰华彩印有限公司
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：185×260　**印　张**：18.25　**插　页**：1　**字　数**：459 千字
版　　次：2011 年 6 月第 1 版　　**印　　次**：2011 年 6 月第1 次印刷
印　　数：1～5000
定　　价：45.00 元

产品编号：041969-01

前　言

信息化正在不断地推动着社会变革的进程和改变着人们的生产方式和生活方式。信息交换和共享推动了人类历史发展和社会进步。利用先进的信息技术、实现企业信息化、提高企业生存和发展能力以及企业市场竞争能力是现代化企业发展的必由之路。通过企业信息化，不断优化组织结构，调整企业管理体制和运行机制，建设流程型现代企业，实现信息和知识资源的共享，共享程度越高，信息和知识作为生产要素的价值越高，解放和提高生产力的能力就越大。

信息化以通信和计算机为技术基础，以数字化和网络化为技术特点。它有别于传统方式的信息获取、储存、处理、传输、使用，从而也给现代社会的正常发展带来了一系列的前所未有的风险和威胁。人们对信息安全的需求随着时代发展而不断地提高。信息化的现代文明使人类在知识经济的概念下，推动社会发展与进步的趋势已不可逆转，但与此同时“信息战”的阴影也已隐约升空。信息安全对现代社会健康有序发展，保障国家安全、社会稳定起着不可或缺的重要作用，对信息革命的成败有着关键的影响。不是在信息化中安全生存发展，就是在信息化中衰亡——美好和严酷就这样摆在我们的面前。

电力工业是国民经济的基础产业和公用事业。电力系统的安全稳定运行，关系到整个社会的各个行业和千家万户。电力系统的生产、经营和管理中，电网实时信息、企业经营管理等信息系统的安全直接关系到电力系统的安全稳定运行，关系到社会的稳定，关系到用户的安全供电、企业生存和发展的重大问题。在信息网络环境下，信息获取、储存、处理、传输、使用的保密性、完整性、不可否认性、可用性和可控性问题目前没有系统解决。电力系统信息安全是保证电力系统安全运行和对社会可靠供电十分重要的课题，是一项涉及面广，技术及管理复杂的系统工程。随着应用需求的不断提升，信息网络规模的不断扩大，网络及信息安全问题更为突出。

作者在组织和主持国家“十五”重大科技攻关项目《电力系统信息安全示范工程》子课题《辽宁电力系统信息安全示范工程》的实践中，运用社会发展系统动力学原理以及信息安全理论，探讨网络信息安全工程有关基本原理，国际信息安全有关标准的研究与工程应用情况，提出网络信息安全三大支柱的概念，即网络及信息安全防护体系——解决网络安全问题；身份认证与授权管理体系（PKI—CA/PMI）——解决信息交换与共享安全问题；数据备份及灾难恢复体系——解决数据备份、存储与恢复安全问题。组织实施了建立网络信息安全总体框架、管理体系、技术体系，网络信息安全风险评估分析，信息网络基础平台结构优化工程，构建网络信息安全监视及管理平台，建立完善的网络信息安全 PKI-CA/PMI 身份认证与授权管理系统和存储网络与备份容灾及灾难恢复系统并在工程实践中应用。

本书是在国家“十五”重大科技攻关项目《电力系统信息安全示范工程》子课题《辽宁电力系统信息安全示范工程》全面验收并获得国家、电力行业及国家电网公司科技进

步奖后2005年开始编写的。信息化工程是一项涉及面广、复杂的系统工程。网络信息安全工程是涉及面更广、更为复杂的系统工程。作者给出8年信息化工程及网络信息安全工程应用理论和实践的成果，包括经验与教训供大家借鉴。在编写过程中作者2006年初调任省农电局负责安全工作副局长，328次深入县（郊区）农电局调研，对安全工作在理论和实践有了更深刻的理解。2008年初调任省公司信息通信公司副总经理兼总工程师，负责计划和安全工作，并负责组织和主持省公司ERP成熟套装软件项目实施与应用工作，对大型企业ERP系统信息安全重要性有更新的认识，2010年8月调任省公司科技信息部兼智能电网部负责公司信息化工作，更感到信息安全工作的紧迫性，因此抓紧整理编著此书。为读者在今后的理论研究和工程实践提供借鉴。本书可供企业领导、信息化及信息安全工程技术及管理人员，用于指导信息系统建设、管理与应用工作；也可供IT厂商了解企业信息化及信息安全工程建设与应用的实际需求，有针对性的服务；对于大学教师和科研人员可以作为供信息化建设与应用的教学与科研参考用书。

全书共分9章，第1章探讨网络信息安全与现代信息社会，信息安全工程主要研究方向以及云计算及云安全的现状及发展趋势。第2章介绍网络信息安全工程基本概念，网络信息安全工程有关基本原理，国际信息安全有关标准的研究与工程应用情况。第3章探讨网络信息安全总体框架、管理体系、技术体系的系统设计及应用实例。第4章探讨网络信息安全风险评估方法，风险评估目的及范围，安全风险评估及分析及应用实例。第5章探讨信息网络基础平台结构优化及应用实例。第6章探讨信息安全监视及管理平台的设计及应用实例。第7章探讨网络信息安全防护技术原理，网络信息安全防护体系的设计及应用实例。第8章探讨网络信息安全PKI-CA/PMI身份认证与授权管理系统及应用实例。第9章探讨数据存储备份与灾难恢复系统及应用实例。

本书的编著出版，感谢国家电力公司科技信息部、信息中心、辽宁省电力有限公司领导和各部门、基层单位同志们的大力支持；感谢科技部及国密办组织专家、教授指导和帮助；感谢中国电力科学研究院、哈尔滨工业大学，中国科学院计算技术研究所、吉大正元公司、北京东华合创数码公司、辽宁傲联通公司工程技术人员的长期合作及共同辛勤工作。由于本人水平有限，书中的内容难免有不足之处，敬请读者批评与指教。

潘明惠

2011年1月于沈阳

个 人 简 介

潘明惠，1955 年出生，毕业于哈尔滨工业大学电力系统及自动化专业，工学博士学位，教授级高级工程师，高级企业信息管理师，哈尔滨工业大学兼职教授。长期从事电力系统自动化、信息化应用研究与工程实践，是辽宁省政府信息化专家委员会成员，国家重大科技攻关项目专家组成员，组织和主持了多项国家、省部级科技攻关课题研究与开发和重大自动化、信息化工程。获得国家科技进步一等奖 1 项，二等奖 1 项；省、部级科技进步奖 11 项，被国务院授予《政府特殊津贴专家》、辽宁省委、辽宁省人民政府授予《辽宁省优秀专家》称号，先后发表科技论文 36 篇，其中：《电力信息化工程的理论与应用研究》在中国电机工程协会组织的《中国电机工程学报》百篇杰出学术论文评选中，被评选为杰出学术论文，出版了《信息化工程原理与应用》、《信息化工程技术问答 200 题》、《计算机及信息网络基础知识》等著作。

Author Introduction

Pan Minghui, born in 1955, graduated from Harbin Institute of Technology Power Systems and Automation with Ph.D of Engineering, Professor level senior engineer, senior information official of enterprise, and adjunct professor of Harbin Institute of Technology. Mr. Pan has been engaged in power system automation, information technology application research and engineering practice for a long time. He is also appointed member of Liaoning Provincial Committee of Experts on information technology, of Experts on major National Scientific and Technological Project, and organized and chaired countable numbers of national, provincial and ministerial scientific and technological issues of major research and development and automation, and information technology projects. He is awarded first prize once and second prize once in National Scientific and Technological Progress Award, eleven Provincial and ministerial level scientific and technological progress awards. Mr. Pan was awarded "Special Allowance from Chinese government" given by State Council, title of "Outstanding experts in Liaoning Province" awarded by Liaoning Provincial Committee, Liaoning Provincial People's Government. He has published 36 scientific papers, in which "Theory and Application of Electric Power Information Engineering" was selected as outstanding paper among "one hundred outstanding academic selection" organized by CSEE by Chinese Electrical Engineering Committee. Mr. Pan also published several books including "Principles and Applications of information technology projects", "200 Questions and Answers on information engineering", "Basic knowledge of computer and information networks".

目　录

第1章 绪 论

1.1 背景及意义

随着计算机及信息网络技术的飞速发展，信息和网络已经成为人类进步和社会发展的重要基础。信息与网络涉及国家的政府、军事、科技、文教、企业等诸多领域，在计算机信息网络中存储、传输和处理的信息有许多是政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要信息，其中有很多是敏感信息甚至是国家机密，所以难免会吸引来自世界各地的各种人为攻击（例如，信息泄露、信息窃取、数据删除与添加、计算机病毒等）。因此计算机网络信息安全是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬、企业生存和发展等的重大问题，重要性正随着全球信息化步伐的加快而变得越来越重要。

从世界范围来看，黑色产业链越来越成为焦点，黑客的技术炫耀开始与经济利益越绑越紧；与此相对应，僵尸网络、木马等变得越来越活跃，而一般性质的蠕虫，尤其是大规模蠕虫则相比过去发生多种变异；由于几乎没有遇到太多法律上的对抗，导致黑客对网页的攻击越来越泛化，例如，钓鱼网站因域名劫持等手段的越来越高超而变得防不胜防。

随着网络的发展，技术的进步，信息安全面临的挑战也在增大。一方面对网络的攻击方式层出不穷，每两年间增加了十几倍，攻击方式的增加意味着对网络威胁的增大。随着硬件技术和并行技术的发展，计算机的计算能力迅速提高，针对安全通信措施的攻击也不断增大。另一方面网络应用范围的不断扩大，使人们对网络依赖的程度增大，对网络的破坏造成的损失和混乱会比以往任何时候都大。这些对网络信息安全保护提出了更高的要求，也使网络信息安全学科的地位显得更加重要，网络信息安全必然随着网络应用的发展而不断发展。网络信息安全工程既是一个理论问题，又是一个工程实践问题，是一项庞大和复杂的系统工程，探讨和研究网络信息安全理论与应用，指导工程实践是一个必须面对和急待解决的问题。

1.2 网络信息安全与现代信息社会

生产力的革命促进了人类的生存与发展。几千年的人类历史上，发生过三次伟大的生产力革命。

第一次是农业革命，它使人类从原始部落的游猎为生转化为依靠土地，男耕女织，

以解决赖以为生的衣食问题。

第二次是工业革命，它使人类不但能够利用物质，而且学会利用能源。煤、油、电以及利用能源的机械大大延拓了人类劳动的器官，创造了空前的财富，带来了人类的现代文明。反映在自然科学上的成就是人类认识自然规律的研究能力超过了以往的几千年，数学、物理、化学的经典研究奠定了现代科学的基础。反映在人类的生产活动的成就是使人们创造财富和抵御自然灾害的能力大大增强。通过车（汽车、火车）船、飞机、电报、电话、电，人们的交往空间和时效大大提高，人类解决衣、食、住、行、用的能力超过以往任何时代，自然的人向自主的人大大迈进了一步。

第三次是信息革命，20 世纪的科学技术发展，特别是信息科学技术的发展，带来了生产力的又一次革命。这场革命早在工业化进程中就开始孕育。20 世纪 50 年代前的电报电话等通信技术的基础和计算机技术的出现，为 20 世纪 60 年代计算机联网实验提供了最初的条件，20 世纪 70 年代半导体微电子技术的飞跃，数字化技术的成熟，为计算机网络走出军事的封闭环境和研究所以及校园的象牙之塔奠定了技术基础。

美国著名的未来学家 Alvin Toffler 很早就预感到信息革命的巨大影响，出版了他的《第三次浪潮》等系列名著。他深刻地指出：电脑网络的建立与普及将彻底地改变人类的生存及生活模式，而控制与掌握网络的人就是人类未来命运的主宰。谁掌握了信息，控制了网络，谁就拥有整个世界。

信息是资源，它与物质、能源一起构成人类生存发展的三大支柱，是我们所处时代最重要、最主要的资源，已经成为越来越多的人们的共识。信息社会对人类的满足已经从物质生活的衣、食、住、行、用拓宽到深层精神生活的听、看、想、说、研。现代化的信息手段对于人类的社会管理、生产活动、经济贸易、科学研究、学校教育、文化生活、医疗保健以致战争方式都产生了空前深刻的巨大影响。

人类社会是一个有序运作的实体，理想、信念、道德、法规从不同层面维系社会秩序。传统的一切准则在电子信息环境中如何体现与维护，到现在为止并没有根本解决。理念、法规和技术都在发展完善的过程之中。信息化以通信和计算机为技术基础，以数字化和网络化为技术特点。它有别于传统方式的信息获取、储存、处理、传输、使用，从而也给现代社会的正常发展带来了一系列的前所未有的风险和威胁。

从 Internet 国际互联网的发展来看，它最初是美国军方出于预防核战争对军事指挥系统的毁灭性打击提出的研究课题，之后将其军事用途分离出去，并在科研、教育的校园环境中进一步完善，就变成了解决互连、互通、互操作的技术课题。校园环境理想的技术、信息共享使 Internet 的发展忽略了安全问题。20 世纪 90 年代后它从校园环境走上了社会应用，商业应用的需要使人们意识到了忽视安全的危害。尽管校园环境的孩子们涉世不深，缺乏社会责任感，但其中许多对计算机游戏钟爱至深，有相当一批后来成了技艺超群的电脑玩家（早年的黑客），有的成为当今社会信息产业界的开拓先驱，而有的则成为害群之马。他们的继承者越来越多，在网上存在利益的今天，他们的行为从另一个方面向人们揭示了信息系统的脆弱性，引起人们对信息安全的空前重视。

人们对信息安全的需求随着时代发展而不断地提高。首先人们意识到的是信息保密。在近代历史上已成为战争的情报军事手段和政府专用技术。在传统信息环境中，普

通人通过邮政系统发送信件，为了个人隐私还要装上个信封。可是到了使用数字化电子信息的今天，以 0、1 比特串编码在网上传来传去，连个“信封”都没有，我们发的电子邮件都是“明信片”，那还有什么秘密可讲！因此就提出了信息安全中的保密性需求。

在传统社会中，不相识的人们相互建立信任需要介绍信，并且在上面签上名，盖上章。那么在电子信息环境中应如何签名盖章，怎么知道信息真实的发送者和接收者，怎么知道信息是真实的，并且在法律意义上做到责任的不可抵赖，等等，为此，人们归纳信息安全时提出了完整性和不可否认性的需求。

人们还意识到信息和信息系统都是它的所有者花费了代价建设起来的。但是，存在着由于计算机病毒或其他人为的原因可能造成的对主人的拒绝服务，被他人滥用机密或信息的情况。因而，又提出了信息安全中的可用性需求。

由于社会中存在不法分子，地球上各国之间还时有由于意识形态和利益冲突造成的敌对行为，政府对社会的监控管理行为（如搭线监听犯罪分子的通信）在社会广泛使用信息安全设施和装置时可能受到严重影响，以至不能实施，因而就出现了信息安全中的可控性需求。

信息化的现代文明使人类在知识经济的概念下推动社会发展与进步的趋势已初见端倪，但与此同时，“信息战”的阴影也已隐约升空。信息安全对现代社会健康有序发展，保障国家安全、社会稳定肩负着不可或缺的重要作用，对信息革命的成败有着关键的影响。不是在数字化中安全生存，就是在数字化中衰亡——美好和严酷就这样摆在我们的面前。

1.3　从密码技术发展历程认识信息安全的重要性

密码技术的发展大致可分为 3 个阶段：1949 年之前为第一个阶段，在这一阶段，密码学并不是一门科学，而被更多地视作一门艺术。1949～1976 年为第二个阶段，1949 年 Shannon 发表的“保密通信的信息理论”将密码学的研究纳入了科学的轨道。在这一阶段，密码学的发展很慢，公开的文献也很少。1976 年至今为第三个阶段，1976 年 Diffie 和 Hellman 发表的“密码学的新方向”提出了一种崭新的密码体制，冲破了长期以来一直沿用的单钥密码体制。新的双钥（公钥）密码体制可使通信双方之间无须事先交换密钥就可建立起保密通信。在这一阶段，密码技术的发展非常迅速。1977 年美国国家标准局（NBS）公布了数据加密标准（DES）。1993 年美国政府宣布了一项新的建议——Clipper 建议，该建议规定使用专门授权制造的且算法不予以公布的 Clipper 芯片实施商用加密。

密码技术是网络信息安全技术中的核心技术，它主要由密码编码技术和密码分析技术两个分支组成。密码编码技术的主要任务是寻求产生安全性高的有效密码算法，以满足对消息进行加密或认证的要求。密码分析技术的主要任务是破译密码或伪造认证码，实现窃取机密信息或进行诈骗破坏活动。这两个分支既相互对立，又相互依存。信息的安全性主要包括两个方面，即信息的保密性和信息的认证性。保密的目的是防止敌手破译系统中的机密信息。认证的目的有两个：一是验证信息的发送者是真正的，而不是冒

充的；二是验证信息的完整性，即验证信息在传送或存储过程中未被窜改、重放或延迟等。信息的保密性和信息的认证性是信息的安全性的两个不同方面，认证不能自动地提供保密性，而保密也不能自然地提供认证功能。在用密码技术保护的现代信息系统的安全性主要取决于对密钥的保护，而不是对算法或硬件本身的保护，即密码算法的安全性完全寓于密钥之中。可见，密钥的保护和管理在数据系统安全中是极为重要的。

1.4 网络信息安全存在的主要问题

网络信息安全主要涉及网络信息的安全和网络系统本身的安全。在信息网络中存在着各种资源设施，随时存储和传输的大量数据，这些设施可能遭到攻击和破坏，数据在存储和传输过程中可能被盗用、暴露或篡改。另外，信息网络本身可能存在某些不完善之处，网络软件也有可能遭受恶意程序的攻击而使整个网络陷于瘫痪。同时网络实体还要经受诸如水灾、火灾、地震、电磁辐射等方面的考验。

1.4.1 影响计算机信息网络安全的因素

随着计算机信息网络技术的发展和应用，一方面网络提供了信息资源共享性、系统的可靠性、工作的效率和系统的可扩充性；同时也正是这些特点，增加了网络安全的脆弱性和复杂性，资源共享和分布增加了网络受威胁和攻击的可能性。对信息网络的威胁，主要有以下 4 个方面。

（1）信息网络硬件设备和线路的安全问题。例如：Internet 的脆弱性；电磁泄露；搭线窃听；非法终端；非法入侵；注入非法信息；线路干扰；意外原因；病毒入侵；黑客攻击等。

（2）信息网络系统和软件的安全问题。例如：网络软件的漏洞及缺陷；网络软件安全功能不健全或被安装了“特洛伊木马”；应加安全措施的软件未给予标识和保护；未对用户进行等级分类和标识；错误地进行路由选择；拒绝服务；信息重播；软件缺陷；没有正确的安全策略和安全机制；缺乏先进的安全工具和手段；程序版本错误等。

（3）信息网络管理人员的安全意识问题。例如：保密观念不强或不懂保密规则；操作失误；规章制度不健全；明知故犯或有意破坏网络系统和设备；身份证被窃取；否认或冒充；系统操作的人员以超越权限的非法行为来获取或篡改信息等。

（4）环境的安全因素。环境因素威胁着网络的安全，如地震、火灾、水灾、风灾等自然灾害或掉电、停电等事故。

从以上 4 个方面来看，影响网络安全的因素主要有以下几个方面。

① 局域网存在的缺陷和 Internet 的脆弱性。

② 网络软件的缺陷和 Internet 服务中的漏洞。

③ 薄弱的网络认证环节。

④ 没有正确的安全策略和安全机制。