国家社会科学基金重点项目

信息安全管理论

XINXI ANQUAN GUANLILUN

王正德　杨世松　主编

军事科学出版社

国家社会科学基金重点项目

信息安全管理论

主　编：王正德　杨世松

副主编：祁建清　宋明武

马晓军　邵广纪

编　委：（以姓氏笔画为序）

丁　元　王朝阳　刘怀兴

刘丹凤　任晓华　陈文民

杜永英　张秀钢　张晓娟

张鸿雁　杨志强　杨国栋

宛东生　岳　磊　姜　华

周　林　周肖章　祝华杰

赵　涛　温建华　梁山华

袁巍伟　韩　东　翟　泽

军事科学出版社

图书在版编目（CIP）数据

信息安全管理论/王正德、杨世松主编．—北京：军事科学出版社，2009.7

ISBN 978-7-80237-262-7

Ⅰ.信… Ⅱ.①王…②杨… Ⅲ.信息系统—安全管理—研究—中国 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2009）第 112515 号

书　　名：信息安全管理论
主　　编：王正德　杨世松
责任编辑：张大禾
封面设计：刘　丹
出版发行：军事科学出版社（北京市海淀区青龙桥　100091）

标准书号：ISBN 978-7-80237-262-7
经 销 者：全国新华书店
印 刷 者：北京市毅峰迅捷印刷有限公司
开　　本：880 毫米×1230 毫米　A5
印　　张：13.5
字　　数：337 千字
版　　次：2009 年 7 月北京第 1 版
印　　次：2009 年 7 月第 1 次印刷
印　　数：1—3000 册
定　　价：22.00 元

销售热线：（010）62882626　66768547（兼传）
网　　址：http://www.jskxcbs.com
电子邮箱：jskxcbs@163.com

前　言

传统的信息安全研究，关注的焦点主要停留在技术层面上。国内外的不少机构和学者从技术层面对信息安全的基本概念、基本技术、体系结构以及发展战略等方面也进行了较为深入的研究，为信息安全工作奠定了很好的基础。但是，现实世界的任何系统都是由复杂的要素构成的，信息安全问题单纯依靠技术手段是解决不了的。信息安全建设应是一个系统工程，其主体应该是人（包括用户、团体、社会和国家），把信息安全管理与信息安全技术手段结合起来，对系统中的各个环节进行统一的规划和综合考虑，并要兼顾环境和系统内部不断发生的变化，建立系统化的管理体系。信息安全建设不仅是一个技术问题，更是一个管理问题。据有关机构统计表明：网络与信息安全事件大约有70%以上的问题是由管理因素造成的，诸如政策法规的不完善、管理制度的不健全、安全意识的淡薄和操作过程的失误等，这正应了十几年前国家863 CIMS专家组“三分技术，七分管理”的箴言。即便有好的安全设备、系统和技术，若没有有效地贯穿于信息流通与信息活动中的安全管理工作，也是无法真正实现信息安全的。因此，管理是贯穿信息安全整个过程的生命线。

信息安全管理不是一般性的管理问题，而是事关国家安全、经济发展、社会稳定和军事斗争成败的重大战略课题。信息安全管理不是一般管理手段的叠加，而是高度系统化的综合集成。信息安全管理作为信息安全建设的重要方面，国外的研究起步较早，主要的发达国家均出版有一些涉及信息安全管理内容的

颇具影响的著作，并确立了一些国际化的信息安全管理体系标准。我国也出台了不少关于信息安全和互联网安全的政策法规和国家标准。但是，国内外的信息安全管理研究包括其体系标准制定主要着眼于对策性和应用性，主要是将信息安全管理作为技术层面的补充，或仅局限于信息系统的安全管理技术，而从管理层面对信息安全管理进行系统研究的理论和论著尚未见到，国内这方面的研究也没有进入公共检索。这在客观上要求我们必须从更大的视野、更宽的角度、更广的领域，树立信息时代全新的信息安全管理观。

鉴于信息安全管理在理论和实践上具有重要意义，着眼实现管理层面和技术层面的有机结合，该研究将信息安全与管理科学中的对策理论、控制理论、风险预测理论和决策分析等理论相结合，为构建新的交叉学科——信息安全管理学打下基础，初步形成了完整的信息安全管理理论体系，明确指出信息安全管理是保障我国信息安全乃至国家安全的基本途径。该课题研究，对于完善我国的国家信息安全管理体系、为确定国家信息安全战略和确保国家信息安全提供理论支持具有重要意义。但是，由于信息安全管理涉及的内容技术新、范围广、资料少，展开系统研究的难度非常大，有些研究还不够深入，特别是对信息安全管理体系结构的分析和效能评估尚处于探讨阶段，因此，本书的错误和不足之处在所难免，恳请广大读者和专家批评指正。

本书由王正德、杨世松主编，祁建清、宋明武、马晓军、邵广纪任副主编，参与本书编著工作的有丁元、王朝阳、刘怀兴、刘丹凤、任晓华、陈文民、杜永英、张秀钢、张晓娟、张鸿雁、杨志强、杨国栋、宛东生、岳磊、姜华、周林、周肖章、祝华杰、赵涛、温建华、梁山华、袁巍伟、韩东、翟泽。以上同志分别参加了各章节的撰写、研讨和修改工作，全书最后由主编、副主编统一修改及定稿。

本书在编著过程中，参考了不少有价值的书刊和专家学者的论文，主要参考文献都标注在每一章后面，谨表谢意；本课题鉴定专家组同志对研究成果提出了很好的修改意见，在此一并表示衷心感谢。

作　者

目　录

前　言 …… (1)
导　论 …… (1)
一、信息安全管理研究的时代背景 …… (1)
（一）信息安全管理是信息时代的必然产物 …… (1)
（二）国内外信息安全管理现状 …… (3)
（三）国内外信息安全管理的研究现状 …… (9)
二、信息安全管理研究的目的意义 …… (12)
（一）信息安全管理研究的目的 …… (12)
（二）信息安全管理研究的意义 …… (13)
三、信息安全管理研究的基本思路 …… (15)
（一）基本思路 …… (16)
（二）研究方法 …… (17)
第一章　信息安全管理概述 …… (22)
一、信息安全管理基本概念 …… (22)
（一）信息安全管理的内涵 …… (22)
（二）信息安全管理的特征 …… (25)
二、信息安全管理的发展规律与本质 …… (29)
（一）信息安全管理的发展规律 …… (30)
（二）信息安全管理的本质 …… (31)
三、信息安全管理研究对象 …… (31)
（一）信息安全管理的历史沿革 …… (32)
（二）信息安全管理的主要矛盾 …… (32)
（三）信息安全管理的基本原理 …… (32)

（四）信息安全管理的基本内容……（33）
四、信息安全管理的地位和作用 ……（38）
（一）信息安全管理是国家安全战略的
重要内容……（39）
（二）信息安全管理是综合国力竞争的
重要领域……（42）
（三）信息安全管理是军事斗争胜利的
重要保证……（43）
第二章 信息安全管理体制 ……（47）
一、信息安全管理体制概述 ……（47）
（一）美国信息安全管理体制概况……（48）
（二）我国信息安全管理体制现状……（53）
二、我国国家信息安全管理体制建设 ……（56）
（一）建设目标……（56）
（二）基本原则……（57）
三、我国国家信息安全管理机构框架 ……（60）
四、我国国家密码管理体制 ……（63）
（一）密码管理体制改革是信息化发展的
必然要求……（63）
（二）国家密码管理的基本原则……（64）
（三）国家密码管理机构和职能……（65）
（四）密码产品测评认证……（67）
五、我国国家信息安全监控管理体制 ……（68）
（一）国家信息安全监控的作用……（68）
（二）国家信息安全监控管理机构……（70）
六、我国国家信息安全科研与产业管理体制 ……（71）
（一）国家信息安全科研与产业管理原则……（71）
（二）国家信息安全科研与产业管理机构……（72）
七、我国国家信息安全测评认证管理体制 ……（72）

（一）国家信息安全测评认证管理原则……（73）
（二）国家信息安全测评认证管理机构……（74）
（三）国家信息安全测评认证管理过程……（76）
第三章　信息安全资产管理……（78）
一、信息安全投资管理……（78）
二、信息安全设备管理……（80）
三、信息安全人力资源管理……（81）
（一）信息安全人才培养……（81）
（二）信息安全人才使用和筛选制度……（84）
（三）积极参与国际信息安全人才争夺……（87）
第四章　信息安全技术与产业管理……（89）
一、我国信息安全技术与产业的发展战略……（89）
二、我国信息安全技术与产业发展现状……（90）
（一）信息安全关键技术受制于人……（90）
（二）信息安全产业缺乏核心竞争力……（91）
三、发展国家信息安全技术与产业战略举措……（92）
（一）战略原则……（92）
（二）战略举措……（93）
四、信息安全基本技术管理……（97）
（一）防病毒技术管理……（98）
（二）防火墙技术管理……（100）
（三）入侵检测技术管理……（101）
（四）虚拟专用网（VPN）技术的管理……（106）
（五）补丁技术管理……（108）
（六）数据恢复技术管理……（113）
第五章　信息安全法规管理……（119）
一、信息安全法规的地位与作用……（119）
（一）信息安全法规的内涵……（119）
（二）信息安全法规在法律体系中的地位……（121）

（三）信息安全法规的作用 …… （123）
二、国外信息安全法规建设概况 …… （125）
（一）美国 …… （125）
（二）俄罗斯 …… （128）
（三）日本 …… （129）
（四）欧盟 …… （130）
三、我国信息安全政策法规发展现状 …… （132）
四、研究制定我国信息安全政策法规 …… （135）
（一）研究制定我国信息安全政策法规的原则 …… （136）
（二）信息安全政策法规管理的主要内容 …… （137）
第六章 信息安全风险管理 …… （141）
一、信息安全风险管理概述 …… （141）
（一）风险和信息安全风险 …… （141）
（二）信息安全风险的相关要素 …… （142）
（三）信息安全风险管理 …… （144）
二、信息安全风险要素的识别与分析 …… （146）
（一）资产的识别与分析 …… （146）
（二）威胁的识别与分析 …… （148）
（三）薄弱点的识别与分析 …… （152）
三、信息安全风险评估 …… （157）
（一）信息安全风险评估概述 …… （157）
（二）信息安全风险评估的实施流程 …… （159）
（三）信息安全风险的评估算法 …… （160）
四、信息安全风险控制 …… （167）
（一）风险控制的基本原则 …… （167）
（二）风险控制的具体措施 …… （170）
（三）持续性控制风险的对策 …… （171）
第七章 信息安全预警与应急响应管理 …… （175）
一、信息安全预警与应急响应概述 …… （175）

（一）预警与应急响应的目标与对象 …… （175）
（二）预警与应急响应的技术体系 …… （177）
二、美国国家信息安全应急响应体系发展状况 …… （179）
三、我国信息安全预警与应急响应发展历程 …… （185）
四、我国国家信息安全预警与应急响应
体系的构想 …… （188）
（一）建立信息安全预警与应急响应组织机构 …… （189）
（二）建立信息安全预警与应急响应
基础设施 …… （192）
（三）构建适合我国国情的预警与应急
响应机制 …… （201）
第八章　信息安全测评认证管理 …… （210）
一、信息安全测评认证概念 …… （210）
二、信息安全测评认证的标准与内容 …… （212）
（一）国外测评认证标准 …… （213）
（二）我国测评认证标准 …… （218）
（三）信息安全测评认证的业务内容 …… （221）
（四）信息安全产品体系 …… （222）
三、信息安全测评认证的程序 …… （227）
（一）程序执行过程 …… （228）
（二）程序执行时间安排 …… （231）
四、信息安全测评认证的实施 …… （231）
五、我国的信息安全测评认证体系 …… （233）
六、信息技术安全评估通用标准 …… （236）
（一）信息技术安全评估通用标准（CC） …… （239）
（二）信息技术安全通用评估方法（CEM） …… （248）
第九章　信息安全等级管理 …… （252）
一、信息安全等级保护管理制度的形成 …… （252）
（一）信息安全与等级保护 …… （252）

（二）信息系统安全等级与信息安全技术等级 …… (256)
（三）信息安全等级保护的特征 …… (257)
（四）信息和信息系统安全等级体系结构 …… (258)
二、信息系统安全等级保护标准体系 …… (261)
（一）标准体系的组成及相互关系 …… (262)
（二）标准体系的主要特点 …… (264)
三、按数据分类分区域分等级 …… (265)
四、信息安全等级保护工作的组织实施 …… (271)
五、等级保护、风险评估、安全测评的
联系和区别 …… (272)
（一）三者关系的基本判断 …… (272)
（二）等级保护与风险评估的关系 …… (273)
（三）等级保护与系统测评的关系 …… (274)
（四）风险评估与系统测评的关系 …… (274)
第十章 密码与密钥管理 …… (276)
一、密码技术概述 …… (276)
（一）密码与密码技术 …… (277)
（二）密码技术体制 …… (278)
（三）标准化及其组织机构 …… (283)
（四）中国信息安全的国际标准 …… (286)
二、密钥分配与托管 …… (288)
（一）密钥分配 …… (288)
（二）公开密钥体系结构 …… (289)
（三）密钥托管技术 …… (302)
三、密码管理 …… (304)
（一）信任服务体系管理 …… (304)
（二）网络信任体系管理 …… (309)
第十一章 军事信息安全管理 …… (314)
一、军事信息安全概述 …… (314)

（一）军事信息安全的定义 …… （314）
（二）军事信息安全等级 …… （315）
（三）军事信息安全环境 …… （317）
（四）信息战与信息安全 …… （320）
二、军事信息安全防护 …… （322）
（一）军用计算机网络安全防护 …… （322）
（二）军用数据库安全防护 …… （326）
（三）电磁辐射防护 …… （330）
（四）军事信息失窃防护 …… （333）
三、军事信息安全管理 …… （337）
（一）军事信息安全管理原则 …… （337）
（二）军事信息安全防护体系 …… （339）
（三）军事信息安全管理制度 …… （344）
（四）组建军队信息安全力量 …… （346）
（五）信息作战中的信息安全管理 …… （349）
第十二章　信息安全管理效能评估 …… （356）
一、信息安全管理效能基本概念 …… （356）
（一）基于信息安全风险评估的管理效能分析模型 …… （357）
（二）基于灰色关联的风险评估模型 …… （359）
二、信息安全管理能力评估模型 …… （360）
（一）信息安全管理能力的分析指标体系 …… （360）
（二）基于模糊层次法的管理能力评估模型 …… （365）
（三）基于 AHP 模型的信息安全管理效能评估 …… （368）
三、信息安全系统效能评估方法 …… （380）
（一）入侵检测系统工作性能分析 …… （381）
（二）入侵检测系统效能分析 …… （382）
（三）网络攻击条件下入侵检测系统效能评估模型 …… （384）

第十三章　我国信息安全管理战略对策 …… (390)
一、加强信息安全管理基础建设 …… (390)
（一）健全国家信息安全管理体制 …… (390)
（二）完善国家信息安全管理机制 …… (392)
（三）营造信息安全管理良好氛围 …… (393)
（四）规划信息安全基础设施建设 …… (396)
二、推动信息安全管理人才队伍培养 …… (398)
（一）信息安全管理人才培养的紧迫性 …… (398)
（二）信息安全管理人才培养的举措 …… (399)
三、加快发展信息安全科研与产业 …… (400)
（一）抓好信息安全科研规划 …… (401)
（二）着眼重点和前沿项目 …… (401)
（三）加快信息技术的自主化进程 …… (402)
（四）重点发展信息安全保密技术和产品 …… (403)
（五）建立国家统一的信息安全技术平台 …… (404)
（六）发展产学研一体化信息安全产业 …… (404)
四、强化信息安全法规管理 …… (405)
（一）构建完善的信息安全法规体系 …… (405)
（二）依据法规进行信息安全管理 …… (407)
五、开展信息安全的国际合作 …… (410)
（一）信息安全国际合作的必要性 …… (411)
（二）信息安全国际合作的可行性 …… (412)
（三）国际信息安全合作的进展 …… (415)

导 论

信息化是一把“双刃剑”，在为人类社会提供着各种便利的同时，也带来了信息安全风险。随着社会秩序、组织关系和个体行为的不断变化调整，以及信息技术的飞速发展，信息安全成为国家安全领域新的最严峻的挑战。《孙子兵法》云：“先为不可胜，然后可以为胜。”只有先将己方的信息安全防线筑牢，才能全力以赴地对敌发起攻击。“千里之堤，溃于蚁穴”，信息安全管理方面的小小疏漏都可能导致全盘皆输。因此，信息时代的信息安全管理研究，对于国家安全具有先决性和全局性的意义。

一、信息安全管理研究的时代背景

面对复杂、严峻的信息安全管理形势，根据信息安全风险的来源和层次，有针对性地采取技术、管理和法律等措施，谋求构建立体的、全面的信息安全管理体系，已逐渐成为共识。了解信息安全威胁及与之针锋相对的信息安全管理的发展动因、轨迹、趋势及其研究现状，是深入进行信息安全管理研究的理论基石和实践源泉。

（一）信息安全管理是信息时代的必然产物

信息安全是信息化发展的必然产物。随着信息技术的发展及其广泛应用，国家的国防、通信、能源、交通、航空、救灾、消防、金融等基础设施系统越来越多地利用网络传输数据和进

行管理。信息安全已经成为一个关系到国家安危、国民经济、人民生活、社会安定等诸多方面的重大现实问题。没有信息安全，也就没有真正的政治安全、军事安全和经济安全，也就没有完全意义上的国家安全。信息疆域改变了由领土、领海、领空构成的国家空间的结构，使得国家主权有了新的内涵；维护信息疆域的安全，也成了维护国家主权完整的核心内容之一。

随着人类信息化进程的不断推进，以及围绕信息获取、利用和控制的斗争日趋激烈，信息安全面临的问题越来越复杂，信息安全保障的难度也越来越大。如何以新的思路、新的机制和新的方法加强信息安全工作，除应着力在寻求信息安全技术上新的突破外，加强信息安全管理是当前切实保障信息安全的根本途径。

我国《2006—2020年国家信息化发展战略》中明确指出，大量层出不穷的信息安全事件表明，信息安全管理水平低下和信息安全管理意识薄弱是导致信息不安全现象的主要原因。越来越多的人认识到单纯依赖技术及防护设备是不可能带来真正意义上的信息安全的，过去人们忽视了信息安全管理是当前切实保证信息安全的根本途径，不知道信息安全管理是什么？如何实施有效的信息安全管理？即对信息安全管理的相关理论与方法没有清楚的认识与掌握，以致对信息安全管理理解片面或者混淆于其他领域的安全管理观念。

无数事实证明，信息化水平越高，对信息安全管理的依赖性就越强，信息安全问题也就越突出。在体系对抗的大环节下，某个单位出了问题、某个环节存有漏洞，都可能导致整个信息系统出现危机。从作战的角度来看，特别是未来的信息化作战，既需要锐利的“矛”，更需要坚固的“盾”，信息安全管理是全员工程和系统工程，更是信息时代现实的战斗力，以及国家安全的重要组成要素。

（二）国内外信息安全管理现状

与民族分裂、跨国犯罪、恐怖主义等非传统安全问题一样，信息安全也呈现出全球性、突发性、扩散性等特点。但它又是一个全新的领域，是一个多维、多因素、多层次、多目标的系统，其复杂性、跨国性、不可控性更为突出。信息及网络技术的全球性、互联性、开放性、信息资源和数据共享性、通信信道共用性等，又使其本身极易受攻击，攻击的不可预测性、危害的连锁扩散性大大增强了信息安全问题造成的危害。西方发达国家很早就认识到了信息安全不同于其他安全领域的特性，以及与国家整体利益和国防的紧密联系问题，高度重视自身的信息安全问题，同时采取了一系列措施来加强其信息产业在全球的垄断地位，政府部门甚至还通过对信息产业实行严格的控制，对其他国家的信息安全带来很大威胁。对于绝大多数发展中国家和欠发达国家而言，当前信息疆域的安全普遍面临着内外双重威胁。内部威胁主要来自信息化程度不高，信息安全意识不强，经验不足，经费投入有限，信息安全难以保证。外部威胁主要来自发达国家对信息的控制与垄断。信息安全管理面临的形势更加复杂和严峻。

1. 美国信息安全管理概况。美国作为世界上信息化程度最高的国家，在信息技术的主导权和网络上的话语权等方面总是占据先天优势，因此，他们在信息安全管理相关研究和管理实践方面也一直走在前列，具体表现在：一是制定了军政部门、公共部门和私营领域的风险管理政策和指南；二是形成了军、政、学、商分工协作的信息安全管理体系；三是国防部、商务部、审计署、预算管理等部门各司其职，形成了较为完整的信息安全管理工作机制。[1]

众所周知，美国国防部（DOD）作为信息安全管理领域的领路者，其所作出的积极探索可以说几乎影响着全世界信息安