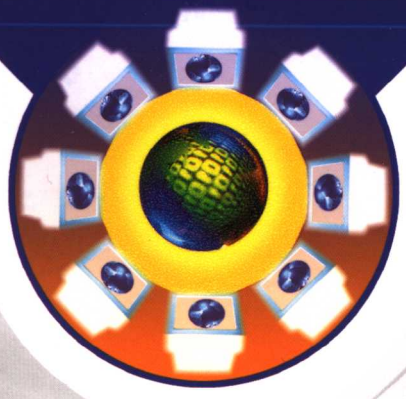
WANGLUO HUANJING XIA XINXI ANQUAN GUANLI TIXI YANJIU

◎唐珂 著

网络环境下信息安全管理体系研究



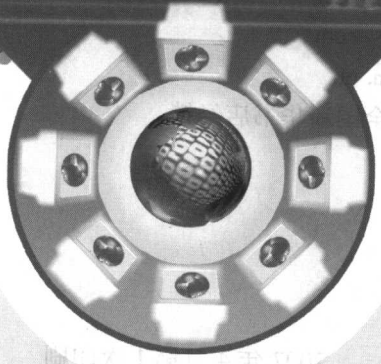
中国长安出版社

网络环境下信息安全

WANGLUO HUANJING XIA XINXI ANQUAN GUANLI TIXI YANJIU

◎唐珂 著

网络环境下信息安全管理体系研究



中国长安出版社

图书在版编目（CIP）数据

网络环境下信息安全管理体系研究／唐珂著．—北京：中国长安出版社，2007.3

ISBN 978-7-80175-564-3

Ⅰ．网… Ⅱ．唐… Ⅲ．计算机网络-信息管理-安全技术-研究 Ⅳ．TP393.08

中国版本图书馆 CIP 数据核字（2007）第 033747 号

网络环境下信息安全管理体系研究

唐 珂 著

出版：中国长安出版社

社址：北京市东城区北池子大街 14 号（100006）

网址：http://www.ccapress.com

邮箱：ccapress@yahoo.com.cn

发行：中国长安出版社 全国新华书店经销

电话：010-65281919

印刷：河北新华印刷一厂

开本：1/16

印张：20.75

字数：325 千字

版本：2007 年 4 月第 1 版 2007 年 4 月第 1 次印刷

书号：ISBN 978-7-80175-564-3

定价：45.00 元

作者简介

唐珂，1969年5月生，汉族，重庆市人，博士，副研究馆员，九届、十届全国青联委员。1984年就读四川大学历史系，1988年毕业分配至国家档案局工作。1994年—1999年任国家档案局、中央档案馆副处级、正处级职务；1999年—2005年，任中共中央办公厅副局级、正局级秘书。其间2000年—2002年在北京大学光华管理学院高级工商管理硕士班学习，获硕士学位；2002年—2005年考入中国人民大学信息资源管理学院攻读在职研究生，获管理学博士学位。2005年12月挂职任中共安徽省滁州市委常委、市政府副市长。曾发表各类文章数十篇，参与编撰著述十余部。

序

这本书是唐珂在他的博士学位论文基础上修改而成的。唐珂选择这个题目做论文、写专著显然很有意义，也很难做。

说这个题目有意义，是因为网络环境下的信息安全对于国家、各类社会组织和个人都很重要，都有很高的关联度，而且这种重要性和关联度将随着不可逆转的信息化进程而日益显著，以至于各行各业、各类人群都不能轻视它。2004 年 9 月 27 日，中共中央十六届四中全会通过的《中共中央关于加强党的执政能力建设的决定》中提出，要“坚决防范和打击各种敌对势力的渗透、颠覆和分裂活动，有效防范和应对来自国际经济领域的各种风险，确保国家的政治安全、经济安全、文化安全和信息安全”。在这里，党中央把信息安全作为国家安全的重要组成部分，与政治安全、经济安全和文化安全相提并论。事实上，信息安全还是其他领域国家安全的基础，因为在信息化进程中，社会生活各个方面的情况都会以各种形态的信息记录和反映出来，信息成为国家、社会组织和个人的资源、财富、创意和战略的承载。许多信息要通过网络进行定向和非定向的传递，如果网络环境中的信息防线漏洞百出或不堪一击，别有用意者的长驱直入就有了可以利用的便捷条件。因此，信息安全理所当然应该成为当今时代于国于民都十分重要的问题。

说这个题目难做有很多原因，一方面，信息安全的概念和范围处于动态的扩展之中，以至于我们的认识和对策也需要不断地随之调整。最初的信息安全主要是面向单机、面向数据，20 世纪 90 年代以后，则扩展到鉴别、授权、访问控制、抗否认性、可服务性以及基于内容的个人隐私、知识产权等方面的系统保护。以保护信息完整性、可用性、保密性和可靠性为宗旨的信息安全逐步延长了它的战线，扩大了它的阵地，成为一个涉及面很广的综合性问题，需要全面管理和多种技术的高度联动。另一方面，这是一场魔高一尺、道高一丈的较量，问题与技术

的不断出新，攻击与反攻击能力的螺旋式提升，使得信息安全概念的相对性日益明显，涉足这一领域就如同穿上红舞鞋一样无法停下旋转的舞步，总有新的难题牵引着研究者的注意力和研究方向。

关注信息安全问题的人并不少，唐珂在这本书中要做的事情，是针对信息安全问题的综合性特征，在已有的研究和实践基础上搭建一个网络环境下的信息安全管理体系。于是，作者着眼于总体，着眼于层次和结构，详细分析了信息安全的相关要素，其中以安全风险评估、网络信任体系、网络安全防御体系等子系统为重点。作者根据网络环境下信息安全管理的需求，对通用的信息安全管理体系模型作了细化和改造，使其成为更适合我国实际情况的网络环境下信息安全管理理论参考模型。这个参考模型尽可能周全地综合了信息安全领域的诸多要素，具有较好的可实现性和可操作性，可以为信息安全保障体系的建设提供宏观、全面的框架思路。

从博士论文的写作到书稿完成，几年来唐珂紧紧跟踪国内外信息安全领域的动态，一直没有间断。这本书不仅对国内外信息安全领域的最新理论作出阐释，选取最近的实践案例进行分析，对国际国内最新颁布的相关标准加以介绍，还融入了作者对该领域的不断思考和研究成果。可以说，本书是作者近年来对信息安全领域持续关注与研究的结晶。

这本书是唐珂在紧张、繁忙的工作之余完成的，长期在综合性岗位上处理综合性事务的经历培养了他捕捉新问题的敏锐、驾驭复杂问题的自如和逻辑思维的缜密。工作中不可推卸的责任增加了他写作过程的艰辛，也使他从中受益。信息安全的研究领域既宽广又纵深，在信息化进程中，新防线和新隐患相生相伴，没有止境。因此，我希望唐珂和更多的人在这一领域不断探索跋涉，不断有所建树。

中国人民大学副校长、博士生导师

冯惠玲

二〇〇七年一月

前 言

当今世界，科技进步日新月异，信息和网络技术飞速发展，对人类生活和经济社会的各个层面产生了广泛而深刻的影响，也带来了新的活力与动力，推动了整个社会的信息化进程。与此同时，网络的安全性也日益引起人们的重视，信息安全越来越成为信息化建设中备受关注的重要问题。为什么要选择这样一个课题进行研究，考虑初衷和来龙去脉何在，其重要性和现实意义在哪里。扪心自问，其实这方面想法由来已久，有三个方面的因素促使我最终选定这个课题。

第一是工作的需要。在我近20年职业生涯中，有机会接触到档案、密码、通信、党政专网、电子政务、电子党务等方面事务，涉及到信息安全及相关工作领域，能够了解到有关的现行政策、措施方略与发展动态。我们已经认识到，信息是重要的生产要素和战略资源，信息安全则要求使信息避免一系列威胁，它决定要保护哪些对象，为什么要保护这些对象，应该从哪些方面进行保护，以保障业务的连续性，最大限度地减少业务的损失，最大限度地获取投资的回报，等等。信息安全涉及的是机密性、完整性、可用性、身份认证、授权管理和责任认定。由于互联网具有高度开放性特点、局域网具有资源共享性特点，尽管网络建设中有物理隔绝等防范措施，也容易招致来自外部或内部的各种攻击，包括黑客组织、犯罪集团或信息战对抗等攻击行为，同时网上大量有害及违法信息也呈泛滥趋势，危害日益严重，防不胜防。在实际工作中我们强调要处理好安全与效率、安全与发展、安全与畅通的关系，也就是说效率、发展、畅通必须以安全为前提，否则就会失去意义。目前信息安全是“点击率”很高的热点、难点问题，对于信息化建设来说，这一问题如果解决得好，可以收到事半功倍之效，如果解决得不好，必然成为发展的瓶颈，甚至造成颠覆性的后果。事实表明，如果缺乏正确的引导和科学的管理，网络信息极易使一些局部问题扩大为全局性问题，一般问题演变成社会和政治问题，甚至引起突发性、群体性事件。打一个形象的比

方，就像美国科学家洛伦兹提出的“蝴蝶效应”理论，巴西亚马逊流域热带雨林中的一只蝴蝶轻轻扇动其翅膀，其能量和威力借助多米诺骨牌效应逐渐放大并传播开来，传递到远方，有可能会在美国的德克萨斯州引发一场龙卷风和暴风骤雨。同样，黑客及别有用心之人，在网络上布设程序陷阱、发布电脑病毒，传播开来，可以引起信息系统故障，造成工作停顿、秩序混乱甚至大面积瘫痪，产生难以挽回的严重影响和无可弥补的重大损失。这方面的案例触目惊心、不胜枚举，正说明道高一尺、魔高一丈的道理。当前国内外形势正在发生深刻变化，窃密与反窃密的斗争尖锐复杂，尤以网络基础设施和电子数据为重点，我们亟须增强忧患意识、危机意识和防范意识。信息安全及保守秘密，过去战争年代是保生命保胜利，和平建设时期是保安全保发展，当前已逐渐成为各方面争夺技术制高点的焦点与核心，成为实力的象征和成败的关键，并且上升为关系国家安全、发展全局和根本利益的重大问题。

第二是专家学者们的支持、鼓励和指导，使我有信心针对这个热点问题展开研究。实践表明，随着人们对信息安全的认识不断深化，这个课题有极大的研究价值和研究空间，非常值得深入钻研。网络的作用和价值不言而喻，它应用之广泛，影响之深远，已成为人们赖以生存的工作和生活方式，须臾不可分离的必要工具和手段。网络环境下信息安全的重要性突出表现在，网络已经完全渗透到社会生活的各个层面，网络无孔不入、无处不在、无时不有、无所不包，网络让人们成为地球村、信息站中的一员，使人们联络方便、沟通迅捷、效率提高，许多人离不开网络，许多事缺不了网络，在某种程度上人们已经依附于网络，成为网络世界的一分子、一部分。各种信息系统、电子政务、网上医疗、电子商务、网上支付、远程教育等，前景不可低估不容小觑，说离开网络寸步难行一事无成可能有点言过其实；但假若现实中没有了网络，人们的工作效率、生产能力、生活质量、研究水平则可能大打折扣大受影响。信息化建设项目追求易学好用、操作简便、省事高效，通过人性化设计、个性化服务，人人均可熟练操作运用。然而这种人与机器的关系，是建立在可信性和可靠性的基础之上的。所以信息安全问题的实质不仅是技术问题，更是一个管理问题。现代管理学的一条著名的经典定律——“墨菲定律”认为，如果错误有可能发生，不管这种可能性有多小，它总

会发生，并将会引起最大可能的损失。此定律提醒我们：解决问题的手段越高明，我们将要面临的麻烦就越严重。同时，“墨菲定律”忠告人们，面对人类的自身缺陷，我们最好还是想得更周到和全面一些，采取多种保险措施，防止偶然发生的人为失误导致灾难和损失。针对网络环境下日益突出日益重要的信息安全问题，有人认为诸多问题应归因于“三分技术七分管理”，只有将技术与管理很好地、完美地结合起来，防止两张皮，相互脱节，才能有效防范和杜绝各种危险、危机与潜在的威胁，才能解决好日趋严重的信息安全问题。从目前的状况看，现有的解决方案和尝试各有优缺点，应该适应实际需要，从技术与管理相结合的角度，进行综合研究。而这正是本课题想要做的工作。

第三是前些年因工作关系有机会参访了一些国家，注意到不少西方国家很早就开始关注这方面问题，并就信息安全、个人信息保护、技术标准等问题制定规定，采取相应措施。而我对此问题产生兴趣，最早可追溯至1997年5至7月的赴美学习。当时在马里兰大学人文历史学院学习研讨了美国对信息资源的管理方法、制度和法律法规，诸如《信息自由法》和《隐私法》等，参观考察了许多联邦机构，包括白宫、国会大厦、最高法院、五角大楼、国家档案与文件管理署等，亲身体验到他们对信息资源极高的重视程度和非常到位的分级管理措施，深感值得我们学习、思考和借鉴，以致回国后连续写了20篇系列文章发表见报。在美国社会，“信息公开是原则，不公开是例外”作为一种理念早就深入人心。一方面访客可以随便参观各种权威机构，任意查阅大量信息资料；另一方面又利用“特例”实行非常严格的管理，让局外人接触不到极小部分最核心的机密信息。总之，把各种信息资源管理得井井有条，该开放的完全放开，该保密的坚决保住，使信息得其所用，用其所长。而作为组织内的个人来说，其思想观念和行为举止都能自觉按照规章制度，依法办事。很具体的一个事例，比如单位、公司的计算机坏了，决不会拿到外面去修，一定是搬回公司总部去处理。也就是说，全社会人人都有比较强的信息安全意识，对信息的保护、管理、使用非常精心，恰到好处并用法律法规加以固定，十分严格、十分规范。美国人强烈的信息安全意识，严格规范的制度和管理，给我留下了深刻印象。回国后我一直在思考，我们对待信息资源的态度，是否符合与遵循信息工作的客观规律？为了保密保险起

见，达到万无一失的目的，人为地划分范围过宽、密级过高，甚至奉行一把锁主义，束之高阁，把信息资源看得过紧，拒人于千里之外，以为这样就安全了保密了，殊不知过犹不及，安全是安全了，但信息资源的利用效率与我们的投入相比是不成正比的，是不平衡的。而在网络信息技术高速发展的今天，又滋生出一种有密难保和无密可保的悲观情绪，认为信息安全问题难以对付，无法解决。这两种观点都是偏激的、不可取的。《庄子·应帝王》中有一则寓言讲得好，“南海之帝为儵，北海之帝为忽，中央之帝为浑沌。与忽时相与遇于浑沌之地，浑沌待之甚善。与忽谋报浑沌之德，曰：‘人皆有七窍以视听食息，此独无有，尝试凿之。’日凿一窍，七日而浑沌死。”两者好心好意去帮忙，结果却办了坏事，使中央之帝七窍流血而死。这告诉我们凡事要尊重客观规律、顺应自然，因地制宜、因势利导，实事求是、一切从实际出发，科学认真对待、避免想当然滥用人为。应该认识到，在信息安全问题上，我们与西方发达国家的差距，不仅体现在科技上，还体现在管理上，更重要的是安全意识不强，同时技术上的大量引进也使我们在关键技术上受制于人。信息技术的发展已充分证明，信息安全的管理是提高效率和应用水平的重要方面。

这里不妨引用一些事例和数据。回顾历史，古时候有“烽火戏诸侯”的故事，假信息的传递最终导致亡国。上世纪“二战”中的太平洋战争，由于盟军一再破译日本的密码，掌握了战事主动权，并将日军联合舰队司令山本五十六的座机击落。现代有电脑千年虫病毒发作，给全球的经济社会造成惨重损失。在2000年2月的“黑客事件”中，雅虎、亚马逊等世界著名国际互联网网络遭黑客攻击而几乎全面瘫痪，据统计，三天的直接经济损失超过10亿美元。2001年7月，“红色代码”病毒仅在13小时内就攻击了全球范围内的36万台主机，造成26亿美元的经济损失。随着网络技术和信息化的快速发展，给社会生活带来了巨大的变革，网络在给人们带来方便快捷高效的同时，也潜伏着危机和隐患，就像任何事物都存在多面性一样，网络也是一柄双刃剑，对个人对群体乃至对国家都是这个道理。当前，网上信息良莠不齐，滥竽充数，假冒伪劣，鱼目混珠，泥沙俱下。从个人来说，网络在把人们紧密联系在一起的同时，也侵袭着个人的隐私、秘密，给居心叵测的人大开方便之门，给人们带来损失造成伤害，让人惊呼“网

络可怕”、“信息失控”；从国家来说，涉密信息的妥善保护和安全管理形势严峻，能否拓展“信息疆域”，保卫“信息边疆”，加强国家信息安全的保障能力，构筑起强有力的信息安全保障体系，已成为“国之大事”。信息安全出现了各种各样过去没有出现的新情况新课题，如系统漏洞、网络窃密、计算机病毒、网络攻击、垃圾电子邮件、虚假有害信息内容和网络违法犯罪等。据我国计算机病毒应急处理中心统计，2003 年我国 85．6%的计算机遭受过病毒感染，2004 年的感染率达 87．9%。据计算机事件应急响应组织（CERT）的统计，2002 年报告的攻击事件为 82094 起，2003 年上升到 137529 起，网络攻击的目标更大多地集中到银行证券和各种网络交易系统。国外某权威专业杂志的调查表明，2003 年全球范围内的电子犯罪上升趋势明显，犯罪活动给被调查对象造成了高达 6．66 亿美元的损失。根据公安部的统计，2004 年我国查处的信息网络违法犯罪案件达 13650 起，比上年上升 18%。由此可见，网络信息安全这种非传统性安全问题日益凸现，已成为影响政治、经济、军事、文化安全以及社会稳定的重大问题，成为国家安全的重大组成部分，也成为国际性的技术问题、社会问题和各国面临的共同挑战。党的十六届四中全会作出的《关于加强党的执政能力建设的决定》，针对传统安全威胁和非传统安全威胁的因素相互交织的新情况，强调要“确保国家的政治安全、经济安全、文化安全和信息安全。”

关于加强信息安全管理的重要性，这个问题应该放到国家的整个发展战略中去考察，认清信息安全问题在国家现代化建设大局中的位置。所谓不谋全局者不足以谋一域，不谋长远者不足以谋一时，就是这个道理。信息化是 21 世纪的重要特征，随着经济全球化深入发展，国际间生产要素和产业转移加快，信息作为重要的生产要素，成为推动社会发展的最主要动力之一，信息产业已成为当今中国第一大产业。信息化作为当今世界发展的大趋势，也是我们面临的重大发展机遇。大力推进信息化，以信息化带动工业化，以工业化促进信息化，走新型工业化道路，是我国全面建设小康社会、加快社会主义现代化建设的必然选择。本世纪头 20 年，是我国改革发展的重要战略机遇期。能否抓住、抓紧、用好这一不可多得并且可以大有作为的历史机遇，关系到改革开放和现代化建设的顺利进行，关系到中国特色社会主义事业发展的全局，关系到全面建设小康社会和构建

和谐社会的进程，关系到党和国家的兴旺发达、长治久安和中华民族的伟大复兴。以胡锦涛同志为总书记的新一届党中央领导集体，审时度势，提出要坚持以人为本，全面、协调、可持续的科学发展观，强调以科学发展观统领经济社会发展全局，牢固树立并切实把科学发展观贯穿于经济社会发展的全过程、落实到经济社会发展的各个环节，使经济社会与人口、资源、环境有机统一起来，使物质文明、政治文明、精神文明建设有机统一起来，使经济发展、政治发展、社会发展和人的全面发展有机统一起来。党的十六届四中全会根据新世纪新阶段我国经济社会发展的新要求和我国社会出现的新趋势新特点，提出了构建社会主义和谐社会的重大战略举措，使我国社会主义现代化建设的总体布局调整为社会主义经济建设、政治建设、文化建设、社会建设四位一体。信息安全对这一战略举措的成功与否有着密切联系，因为在信息化时代的今天，信息安全直接影响着政治、经济、军事、社会和文化等各个领域的安全，成为关系到经济发展、社会稳定和国家安全的重大战略问题，保障信息安全的能力已是综合国力、经济竞争力和民族生存能力的重要组成部分，是各国奋力攀登的制高点。可以说，没有国家的信息安全，就没有真正意义上的经济、政治、文化和国防安全。然而我国信息安全工作中存在的一些亟待解决的问题不容忽视：网络与信息系统的防护水平不高，应急处理能力不强；信息安全的管理和技术人才缺乏，信息安全关键技术整体上比较落后，信息安全产业缺乏核心竞争力；信息安全法律法规和标准不完善；全社会的信息安全意识不强，信息安全管理薄弱。与此同时，网上有害信息传播、病毒传播和网络攻击日趋严重，网络失泄密事件屡有发生，网络犯罪呈快速上升趋势，境内外敌对势力针对信息网络的破坏活动和利用信息网络进行的反动宣传活动日益猖獗，严重危害公众和国家利益，影响信息化建设的健康发展。从我国国情来说，做好信息安全保障工作，是促进信息化发展、加强法制建设、推动依法治国的有效途径，是巩固党的执政基础和执政地位、提高党的执政能力与执政水平的必然要求和重要内容，同时也是构建社会主义和谐社会的题中应有之义。

综观上述，信息安全战略不仅对个人、企业、团体、单位有重要意义，而且对强化执政理念，维护国家民族整体利益均有重要意义。信息安全是一项长期、复杂的系统工程，是一个多层次、多因素、多目标的复合系统。客观地说，安全

只是相对而言，绝对安全的网络是不存在的。对于一个网络的安全性来说，不仅要看它所采取的防范措施，而且还要看它的管理措施。网络提供的服务功能是否强大与网络是否安全总是一对矛盾，信息安全技术正是在不断解决这对矛盾中向前发展的。对待网络环境下的信息安全问题，构建信息安全管理体系，我们要实事求是，客观分析，要兴利除弊、趋利避害，确保信息安全和网络畅通，最大限度地发挥信息网络的作用和优势。信息安全战略内容丰富，包罗万象，除了信息安全管理体系的建设外，还有建立健全信息安全领导体制与机构，制定完善信息安全法律法规，实现信息安全设备自主化计划，组建信息安全执法队伍，建立信息作战攻防队伍，培养信息技术和信息安全技术人才，加强信息安全教育，等等。本课题题目不用“战略”而用“问题”，正是力图想以一篇论文解决“战略”中的一点问题而已。

目 录