山东政法学院学术文库·管理学
Shandongzhengfaxueyuanxueshuwenku Guanlixue

山东省社会科学规划研究项目文丛·重点项目

◎ 王海军 著

网络信息安全管理研究

Wangluoxinxi
AnquanguanliYanjiu

山东大学出版社

山东政法学院学术文库·管理学
山东省社会科学规划研究项目文丛·重点项目

网络信息安全管理研究

王海军　著

山东大学出版社

图书在版编目(CIP)数据

网络信息安全管理研究/王海军著. —济南：
山东大学出版社，2010.8
ISBN 978-7-5607-4178-9

Ⅰ. ①网...
Ⅱ. ①王...
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(2010)第 169610 号

山东大学出版社出版发行
(山东省济南市山大南路 27 号　邮政编码：250100)
山 东 省 新 华 书 店 经 销
济南景升印业有限公司印刷
880×1230 毫米　1/32　8.75 印张　242 千字
2010 年 8 月第 1 版　2010 年 8 月第 1 次印刷
定价：20.00 元

学术、学问与学术传统（总序）

所谓学术，据《辞海》解释，是指较为专门、有系统的学问。而学问则是学习、问难。[①] 做学问、搞学术是一个艰苦的过程，它既要有努力的学习又要有潜心的沉思，来不得半点马虎，几乎没有任何捷径可走。严格说来学问与学术还是有一些区别的。何怀宏说："学术是大家的，学术乃天下之公器，有规有界。学问是个人的，学问乃自我之心得，无端无涯。"[②] 对大部分人文学科的学者来说，做学问主要是在书斋里面，得耐得住寂寞。虽然学者们要面对现实，但只有经得起冷板凳的磨练才能产出真正的学术。做学问讲究个人的修养，是把思想变成文字的过程。思想一旦变成用文字表述的作品，学问就成了学术成果。创新性的学术成果就是书斋里的革命，而"革命"性的学术是促使社会进步的精神力量。然而，学问是怎样产生，又是如何变成学术的呢？

梁启超先生认为，将世界纷繁复杂的东西作为做学问的资料进行疏理分类、归纳整理，这就是能力。有了这种能力，"思想乃起，有思想故，斯有议论，有议论故，斯有学问"，"则凡学术关于有形实物者，其基础可知耳，何也？学固以实验为本，而所谓实验者，自有一定之界，苟不驰于此界之外，则其实验乃可信凭。界者何？物之现象是也。若贸然自以为能讲求庶物之本相者，则非复学术之

① 参见《辞海》，上海辞书出版社 1999 年版，第 3193、3194 页。

② 何怀宏：《问题意识》，山东友谊出版社 2005 年版，第 1 页。

界矣”[①]。梁治平在总结他的学术经验时也讲到，当以学术的方式来审视自己的感受和结论的时候，就必须达到一种理性的自觉，要向自己，同时也向所有其他人，提供一些经得起检验的论据，并且公开自己的论证方式。自己承担了依靠理性去证明的义务，那就不仅要公开，而且要忠实和公正。古人说，学术乃天下公器，同样包含这一层道理。自己依此去做，实际是在尽学者的本分。结论其实并不重要，要紧的是隐藏在结论后面的东西。[②] 确实，这里面既有学术意境，也有学术方法，更重要的还可能在于学术的创新。学问与学术的真谛在于不断地创新，为社会不断地补充精神食粮。

学术创新是当下学界最重要的理念。然而，要真正对学术有所贡献则需要诸多的条件，起码对一个学者来说，要切实领悟学术的价值；要具备良好的学术意境和深厚的文化底蕴；要有正确的逻辑思维方法；在某种意义上还要有学术系谱的传承。邓正来在《深度研究与自主发展》一文中介绍说：美国著名文化人类学家吉尔兹遵循韦伯比较行为与行动的理路，对“眼皮痉挛”（行为）与“递眼色”（行动）作比较所得出的结论：前者只是动作，而后者却是有意义的动作。文章还介绍了 F. Crews 为西方反实证主义的知识运动的检讨对我们的启示：“一个优秀学者最重要的标志就是对先验结论‘抱有一种本能的警觉，换句话就是，对任何未经检验得出的、貌似权威的结论、理论体系或者其他一般论点一概持怀疑态度’。”[③] 我认为，这种观点对于当下各大学中正在寻究大学精神和探求学术创新路径的学者而言，“不能不说是知识活动的一个尺度”。学术创新不应是“眼皮痉挛”，起码应该是“递眼色”。学术是指那些对社会产生一定影响的学问。

---

① 梁启超：《饮冰室合集》（二），文集之十三，中华书局 1989 年版，第 52、56 页。

② 参见《学术思想评论》第 3 辑，辽宁大学出版社 1998 年版，第 541 页。

③ 《学术思想评论》第 2 辑，辽宁大学出版社 1997 年版，第 39、47 页。

凡办得好的大学，都有一种良好的学术氛围与传统。徐显明说："学术传统是一所大学所拥有的最有价值的无形资产，它比起那些有形的资产更加珍贵。"他认为，需要代代传承的学术系统主要有四个方面：一则，养涵崇高，襟怀宏伟的大家气度。视学术犹如生命，具有对学问的虔诚敬畏之风气和孜孜不倦地探求之良俗。在科学的道路上，百折而又不挠，宽容而又大气，兼蓄而无门户之见，从而造就一批历久弥新的传世之作。二则，开拓创新，研故出新，有敢为天下先的学术追求。学者们都以学问的拓荒者为荣。他们的头脑不但专为学问而准备，也有着对时代变迁、学术更替的足够敏感。高文典册成就于启例发凡的学术努力之中。三则，沉潜学问，厚积薄发的精品意识。学者们恪守"板凳要坐十年冷，文章不写半句空"的信条，深知做学问要耐得住寂寞，避免浅薄浮躁，急功近利。"根本固者，华实必茂，源流深者，光澜必章"是他们追求的学问境界。四则，崇争尚辩，追求学术自由的治学精神。学者们对"知出乎争"这一儒家遗训深信不疑。[①] 我想，这些良好的学术传统既已成为名牌大学的灵魂依然散发着光彩，那么，对于苦苦寻找发展之路的新兴大学来讲，确应视为楷模而效之。

山东政法学院推出这套"学术文库"，将分不同学科陆续出版。这不仅是该院专家学者们多年来精心研究所取得的成果的展示，更重要的在于通过这种学术作品的出版，历练学术意境，提升学术水平，进而在不断努力的基础上形成自己的学术传统。

是为序。

山东大学教授
博士生导师　陈金钊

2006 年 8 月

① 参见《山东大学百年学术精粹·总序》，山东大学出版社 2001 年版。

前　言

本书内容

计算机信息安全问题涉及到每一位网络用户，需要大家共同参与并了解，做好防御工作。保护信息安全除了需要先进的技术（设备）之外，更需要相关的技术管理和安全的组织行政管理，而后者应该是重中之重。

网络安全管理正逐渐成为网络管理技术中的一个重要分支，使得网络安全管理系统呈现出从通常网管系统中分离出来的趋势。在构建安全的网络环境之前，必须清楚网络信息安全的需求。网络人员应该对信息安全的业务需求进行深入了解，清楚一个安全的计划是机构综合管理的必要组成部分，要洞察常见的信息安全威胁和攻击手段。

当然，安全需求要经过系统地评估安全风险才能得到确认。对网络信息安全要进行风险分析、评估。

目前威胁主流系统的安全漏洞已经数以千计。即使在一个小型的企业网当中，也难以对每个可能发生安全问题的地方进行监控，而在浩瀚的互联网世界，更是有无以计数的危险。因此网络与信息安全将呈现以下发展趋势：(1) 安全需求呈现多样化趋势；(2) 技术发展两极分化：专一和融合，无疑将增强防御能力；(3) 安全管理体系化，使防御系统更容易建立。

信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。本身包括的范围很大，大到国家军事政治等机密安全，小到如防范商业企业机密泄露、防范青少年对不良信息的浏览、个人

信息的泄露等。

本书正是从以上两方面进行分析研究，总结近年来的管理经验、技术进步，并分别进行了详细介绍，以期对从事网络安全研究或网络活动的人士提供有益的帮助，并对网络安全的前沿研究起到推动作用。

读者对象

本书是从事网络安全工作人员不可多得的参考书，也适合大中专院校师生阅读。对那些还没引起重视或忽略网络安全的读者来说，本书将起到很好的帮助作用，建议这些读者先读第一部分内容，然后再学习技术部分。

本书特点

1. 可以像工具书一样查看，可以像技术资料一样使用，可以像教材一样学习。在讲解过程中由浅入深、由易到难、循序渐进，并结合相关技术的实用示例，使读者全面了解网络安全的内容及技术，帮助读者快速熟悉网络安全。

2. 以实用技术为中心，以提高读者的网络安全意识、技术开发能力为宗旨，通过类比和实际应用分析，力求让读者抓住事物本质，迅速掌握相关技术。

3. 系统地介绍了网络安全管理、网络安全攻击手段和防御技术，通过学习，读者可以快速领悟网络安全的方方面面，了解各种防御技术，增强自己或单位的网络安全。

著　者

2010 年 3 月 3 日

目 录

上篇　网络信息安全管理

网络信息安全不仅仅是技术部门的事情！

随着计算机信息安全问题的日益增加，对该问题的解决应该从全方位来考虑。当今我们每个人都处于网络的包围当中，因此安全问题涉及每一个人，需要网络上的每个人都参与，共同防护我们的网络信息安全。信息安全除了需要先进的技术（设备）之外，还需要安全的技术管理和安全的组织行政管理，后者更应该是重中之重。

网络管理从功能上一般包括配置管理、性能管理、安全管理、故障管理等。由于网络安全对网络信息系统的性能、管理的关联及影响越来越复杂和严重，因此网络安全管理已成为网络管理技术中的一个重要分支，正受到业界及用户的广泛关注。可能也正是由于网络安全管理技术要解决的问题的突出性和特殊性，使得网络安全管理系统呈现出从通常网管系统中分离出来的趋势。

为了网络的安全，必须设计一个工作安全计划，然后需要一个管理模型来执行和维护这个计划。应创建安全框架，制定信息安全蓝图。安全模型一般是由服务机构提供的通用蓝图。

在构建安全的网络环境之前，我们必须清楚网络信息安全的需求。信息安全的主要任务是确定系统及其内容不被非法访问和泄漏。随着攻击手段的日益复杂，信息安全的需求也在不断增加。网络人员应该对信息安全的业务需求进行深入了解，清楚一个安全的计划是机构综合管理的必要组成部分，要洞察常见的信息安全威胁和攻击手段。

信息安全包括对数据和物理信息资产的保护。物理安全是设

计、实现和维护机构物理资源的措施。如果攻击者获得被控制设备的物理访问权，就可以绕过对此设备的大多数基于技术的安全控制。因此制定信息安全计划时，物理安全应得到与逻辑安全一样的关注。安全的网络环境同样需要人员操作的安全管理，主要包括操作权限管理、责任管理、信息监控管理和灾难恢复管理等。文件的严格管理也是要讨论的内容之一，文件要按密级分档、及时登记，过时的文件要及时销毁等，从上到下都要做好这方面的工作。

当然，安全需求要经过系统地评估安全风险才能得到确认。对网络信息安全要进行风险分析、评估。风险评估可以在整个机构或机构的一部分、单个信息系统、某个系统部件或服务上实行，只要是可行的、现实的和有益的就可以了。

第1章　网络信息安全管理概述

网络信息安全随着网络的普及和人们生活对网络的依赖而提到日程上来，而且成为一个越来越重要的问题。对于这个问题，我们首先必须搞明白如下问题：

☆什么是安全？

☆什么是网络？

☆什么是网络安全？

☆网络安全的内涵是什么？

20世纪90年代以来，以网络技术及服务为代表的“第二次信息革命”浪潮席卷全球，迅速渗透到政府、企业、经济等各个领域。互联网恰如一柄“双刃剑”，为人们工作带来便利的同时，也伴随着日趋严重的网络入侵安全问题。如政府公用站点，既要访问Internet的共享信息资源，又要把Intranet的一部分信息对外提供服务，资源共享的同时也带来了安全问题。如何保护网络的信息安全，防范来自外部网络的黑客和非法入侵者的攻击，建立起强健的网络信息安全防范系统，在某种程度上决定着一个国家信息化建设的成败。

在当前复杂的网络应用环境下，任何单一的防护产品都无法满足保障用户网络系统、信息资源的安全。据美国《金融时报》报道，现在平均每10秒就发生一次入侵计算机网络的事件，超过1/3的互联网防火墙被攻破。2006年4月7日，美国联邦调查局(FBI)和计算机安全机构(CSI)公布的计算机犯罪和安全的最新统计结果显示，美国企业和政府机构因重要信息被窃取所造成的损失，超过了其他对计算机系统攻击所造成的损失。网络信息安全的重要性可见一斑。

本章将对网络信息安全及其管理进行简单的阐述，从安全入手，分析自安全问题出现到现在的安全形势，提出领导与管理的方法及其重要作用，最后是建立网络信息安全管理的一个模型。

1.1 信息安全

在《汉语大词典》里“安全”的解释是：“平安无危险，保护、保全。”当进入信息时代时，就会遇到信息安全的问题。网络迅速发展的今天，网络信息安全又成了令人瞩目的问题。关于信息安全的定义，还没有统一的标准，以下是一些有代表性的定义方式。

1.1.1 信息安全的概念

国内学者给出的定义是：“信息安全保密内容分为：实体安全、运行安全、数据安全和管理安全四个方面。”

我国计算机信息系统安全专用产品分类原则给出的定义是：“涉及实体安全、运行安全和信息安全三个方面。”

我国相关立法给出的定义是：“保障计算机及其相关的和配套的设备、设施（网络）的安全、运行环境的安全，保障信息安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全。”这里面涉及了物理安全、运行安全与信息安全三个层面。

国家信息安全重点实验室给出的定义是：“信息安全涉及信息的机密性、完整性、可用性、可控性。综合起来说，就是要保障电子信息的有效性。”

英国 BS7799 信息安全管理标准给出的定义是：“信息安全是使信息避免一系列威胁，保障商务的连续性，最大限度地减少商务的损失，最大限度地获取投资和商务的回报，涉及的是机密性、完整性、可用性。”

美国国家安全局信息保障主任给出的定义是：“因为术语‘信息安全’一直仅表示信息的机密性，在国防部我们用‘信息保障’来描述

信息安全，也叫‘IA’。它包含5种安全服务，包括机密性、完整性、可用性、真实性和不可抵赖性。”

国际标准化委员会给出的定义是：“为数据处理系统而采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露。”这里面既包含了层面的概念，其中计算机硬件可以看作是物理层面，软件可以看作是运行层面，再就是数据层面；又包含了属性的概念，其中破坏涉及的是可用性，更改涉及的是完整性，显露涉及的是机密性。

综观从不同的角度对信息安全的不同描述，可以理解为：一种是从信息安全所涉及层面的角度进行描述，大体上涉及了实体（物理）安全、运行安全、数据（信息）安全；一种是从信息安全所涉及的安全属性的角度进行描述，大体上涉及了机密性、完整性、可用性。

这里把网络安全简单定义为计算机网络环境下的信息安全，即网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。所以网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

网络安全的具体含义会随着“角度”的变化而变化。比如：从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私、访问和破坏。

从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。

对安全保密部门来说，他们希望对非法的、有害的或涉及国家机

密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失。

从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

关于安全的定义，下面的解释就更容易让我们理解了：

“如果把一封信锁在保险柜中，把保险柜藏起来，然后告诉你去看这封信，这并不是安全，而是隐藏；相反，如果把一封信锁在保险柜中，然后把保险柜及其设计规范和许多同样的保险柜给你，以便你和世界上最好的开保险柜的专家能够研究锁的装置，而你还是无法打开保险柜去读这封信，这才是安全……”

——Bruce Schneier

以下是一些关于网络安全重要性的描述：

“谁掌握了信息，控制了网络，谁将拥有整个世界。”

——美国著名未来学家阿尔温·托尔勒

“今后的时代，控制世界的国家将不是靠军事，而是信息能力走在前面的国家。” ——美国前总统克林顿

“信息时代的出现，将从根本上改变战争的进行方式。”

——美国前陆军参谋长沙利文上将

“0、1 所构成的电子脉搏维系着我们的生存，瞬间即达的在线商务滋养着我们的生活，数字的流动就像血液，在我们的大众文化和集体意识的动脉中流淌。然而，我们必须痛苦地指出，这些动脉在今日因特网的战场上伤痕累累，更令我们痛苦的是，每日在网络丛林中的数以百万计的人们对这些伤口不以为然或熟视无睹。”

We will dem that 62% of all systems can be penetrated in less than 30 minutes.

More than half of all attacks will come from inside your own organization.

——from tnn. com

美国中央情报局 CIA 大厅的石墙上刻着一段话：你应当了解真相，真相会使你自由。