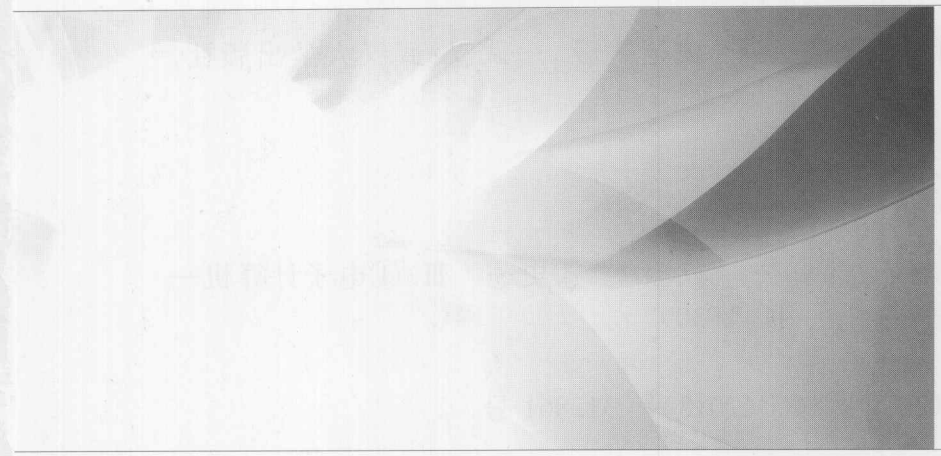
全国网络安全与执法专业丛书

访问控制

徐云峰 郭正彪 范平 史记 编著

WUHAN UNIVERSITY PRESS
武汉大学出版社

全国网络安全与执法专业丛书



访问控制

徐云峰 郭正彪 范平 史记 编著

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

访问控制/徐云峰,郭正彪,范平,史记编著.—武汉:武汉大学出版社,2014.2

全国网络安全与执法专业丛书

ISBN 978-7-307-12365-6

Ⅰ.访… Ⅱ.①徐… ②郭… ③范… ④史… Ⅲ.①电子计算机—安全技术—高等学校—教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2013)第 312861 号

责任编辑:刘 阳 责任校对:汪欣怡 版式设计:马 佳

出版发行:**武汉大学出版社** (430072 武昌 珞珈山)

(电子邮件:cbs22@whu.edu.cn 网址:www.wdp.whu.edu.cn)

印刷:武汉中科兴业印务有限公司

开本:787×1092 1/16 印张:20.75 字数:502 千字 插页:1

版次:2014 年 2 月第 1 版 2014 年 2 月第 1 次印刷

ISBN 978-7-307-12365-6 定价:45.00 元

前 言

当今世界，高新技术的竞争已经成为综合国力竞争胜负的关键。世界各国都在充分发展高新技术，争取最大限度地利用信息技术，特别是计算机技术和网络系统带来的巨大利益。1994 年 9 月，美国提出了建立全球信息基础设施计划的倡议，以进一步实现全球信息共享。这一举措尽管在一定程度上有利于加强国际间的经济、科技、教育合作和文化交流与合作，但同时也将成为美国等一些国家向世界各国进行经济扩张、政治渗透和文化入侵的最方便、快捷的途径。2010 年，美国举行第三次网络风暴演习，将网络安全提升到国家安全战略核心内容之一。2011 年 5 月，由奥巴马作序，美国发布具有划时代意义的《网络空间国际战略》，这标志着美国网络空间政策第一次有了顶层设计，向全世界宣示了其关于网络空间的核心利益。同年 7 月，美国国防部发布《网络空间行动战略》，将网络空间列为与陆、海、空、太空并列的“行动领域”，变被动防御为主动防御，将网络空间的威慑和攻击能力提升到更重要的位置。

网络安全关系国家安全，是我国信息化战略的七大要素之一。党的十八大报告中多次提及信息化与信息安全，明确把“信息化水平大幅提升”纳入全面建成小康社会的目标之一。在“推进经济结构战略性调整”中，强调“发展现代信息技术产业体系和健全信息安全保障体系”；在国防安全中，也要求“高度关注海洋、太空、网络空间安全”。互联网的开放性，给国家的信息安全带来了严重威胁。随着中国上网用户的增加，上网信息越来越多元化，不可避免地带来了泄密隐患，增加了国内信息网络被“入侵”、被窃密的概率和可能，因而我们必须提高认识，要从国家安全角度重视信息安全，以保证国家通信和计算机基础的安全。

访问控制技术是计算机科学与安全工程的结合体，也是保证网络安全的核心策略之一。它是针对越权使用资源的防御措施，是网络安全防范的主要策略，其主要任务是保证网络资源不被非法使用和非法访问。访问控制是一种重要的信息安全技术，是一种保障授权用户获取所需资源而拒绝非授权用户的安全机制，是保障现代信息系统安全不可缺少的一部分。访问控制是通过对访问的申请、批准和撤销的全过程进行有效的控制，从而确保只有合法用户的合法访问才能给予批准，而且相应的访问只能执行授权的操作。

本书共分为 10 个章节。第 1 章概述了信息安全，主要对信息安全的基本概念、体系结构、主要技术等作简要介绍，便于读者掌握访问控制技术的基本背景资料；第 2 章详细介绍了访问控制的基本概念，学习这些概念将有助于读者掌握在信息安全领域中，访问控制是如何发挥作用的；第 3 章主要介绍了访问控制的发展历史，以时间为主线，通过一些标志性的研究成果对访问控制的演进历史进行了系统呈现；第 4 章介绍了访问控制的策略，主要包括自主访问控制策略、强制访问控制策略、基于角色的访问控制策略；第 5 章主要介绍了访问控制的几种模型，包括状态机模型、信息流模型、Bell-LaPadula 模型、

Lattice 模型、Biba 模型、Clark-Wilson 模型等控制模型；第 6 章详述了访问控制机制，包括访问控制机制的理论基础以及访问控制的具体实现机制；第 7 章重点介绍了基于角色的访问控制，包括基于角色的访问控制实现的功能和标准以及具体实现模型等；第 8、9、10 三章分别介绍了基于多域的访问控制、基于信任管理的访问控制技术及访问控制应用。

在飞速发展的信息时代，信息的传播只需在瞬间就可完成，这种特性在给我们带来方便的同时也给国家层面的掌控带来了挑战。信息间的对抗无处不在，手段也是层出不穷。而访问控制作为信息安全的几大核心技术之一，在信息保护方面发挥着重要作用。因此，加强对访问控制技术的学习和研究，将极大地促进信息安全技术的发展。

本书的最大特点就是对访问控制的技术、策略、模型、实现机制及应用进行了系统的研究，并理论联系实际，使读者对访问控制有了深刻的了解。本书经过精心编排，内容上深入浅出，可作为高校及相关行业信息安全、计算机、通信、计算机网络、电子商务等专业本科生、研究生的教材或学习参考书，对相关专业领域研究人员和专业技术人员也具有一定的参考价值。

由于作者水平有限，书中可能会有不少谬误之处，敬请读者批评指正。

作　者

2013 年 8 月

http：//www. nirg. org

xu. lotus8340@ gmail. com

目 录

第1章 绪论 …… 1
1.1 信息安全的新特征 …… 1
1.2 信息安全基本概念 …… 4
1.3 信息系统安全介绍 …… 5
1.3.1 信息系统的安全评测准则 …… 5
1.3.2 OSI的安全体系结构 …… 9
1.3.3 OSI安全体系的管理 …… 14
1.4 信息安全的主要技术 …… 15
1.4.1 密码技术 …… 15
1.4.2 身份认证技术 …… 17
1.4.3 安全审计技术 …… 18
1.4.4 访问控制技术 …… 22
1.4.5 安全扫描技术 …… 24
1.4.6 防火墙技术 …… 27
1.4.7 入侵检测技术 …… 32
1.4.8 主机加固技术 …… 36
1.5 本章小结 …… 37
习题1 …… 37

第2章 访问控制的基本概念 …… 38
2.1 信息安全的三大风险 …… 38
2.2 常用的访问控制方式 …… 39
2.2.1 物理控制 …… 39
2.2.2 逻辑控制 …… 40
2.2.3 管理控制 …… 40
2.3 访问控制的目标 …… 41
2.4 认证和授权 …… 42
2.4.1 认证 …… 42
2.4.2 授权 …… 44
2.5 访问控制术语 …… 46
2.5.1 用户 …… 46
2.5.2 主体 …… 47

2.5.3 客体 …… 47
2.5.4 操作 …… 48
2.5.5 权限 …… 48
2.5.6 最小权限 …… 48
2.6 访问控制的策略、模型和机制 …… 49
2.6.1 访问控制策略 …… 49
2.6.2 访问控制模型 …… 55
2.6.3 访问控制机制 …… 66
2.6.4 策略、模型和机制的区别与联系 …… 73
2.7 本章小结 …… 74
习题2 …… 74

第3章 访问控制的发展历史 …… 75
3.1 操作系统安全问题被提出和研究 …… 75
3.2 访问控制抽象:访问矩阵 …… 76
3.3 多级安全问题 …… 78
3.4 参考监控机和安全内核 …… 80
3.5 隐蔽通道概念 …… 81
3.6 BLP 模型 …… 84
3.6.1 BLP 模型的基本元素 …… 85
3.6.2 BLP 模型中的系统状态 …… 85
3.6.3 BLP 模型的安全特性 …… 85
3.6.4 BLP 模型的优点以及存在的问题 …… 86
3.7 HRU 模型 …… 87
3.8 自主访问控制和强制访问控制 …… 88
3.9 基于角色访问控制 …… 89
3.10 基于任务的访问控制 …… 91
3.11 基于对象的访问控制 …… 92
3.12 本章小结 …… 93
习题3 …… 93

第4章 访问控制策略 …… 94
4.1 自主访问控制策略 …… 94
4.1.1 自主访问控制策略的基本概念 …… 94
4.1.2 授权管理 …… 96
4.1.3 不足之处 …… 97
4.1.4 完善自主访问控制机制 …… 98
4.2 强制访问控制策略 …… 99
4.2.1 基本概念 …… 99

4.2.2 授权管理 …… 101
4.2.3 不足之处 …… 101
4.3 基于角色访问控制策略 …… 101
4.3.1 基本概念 …… 101
4.3.2 授权管理 …… 106
4.3.3 RBAC 的优势 …… 107
4.4 本章小结 …… 108
习题 4 …… 108

第 5 章 访问控制模型 …… 109
5.1 状态机模型 …… 109
5.2 信息流模型 …… 110
5.2.1 信息流模型的特点 …… 112
5.2.2 模型的缺点 …… 112
5.3 Bell-LaPadula 模型 …… 113
5.3.1 BLP 模型特征 …… 113
5.3.2 BLP 模型的访问控制原则 …… 114
5.3.3 BLP 模型的局限 …… 117
5.4 Lattice 模型 …… 118
5.5 Biba 模型 …… 119
5.6 Clark-Wilson 模型 …… 121
5.7 Chinese Wall 模型 …… 125
5.8 Domain-type Enforcement 模型 …… 129
5.9 Sutherland 模型 …… 131
5.10 Goguen-Meseguer 模型 …… 132
5.11 角色模型 …… 133
5.12 本章小结 …… 141
习题 5 …… 141

第 6 章 访问控制机制 …… 142
6.1 访问控制机制的理论基础 …… 142
6.2 访问控制机制的实现基础 …… 144
6.2.1 访问控制模型的实现机制 …… 144
6.2.2 访问控制模型的一般实现方法 …… 147
6.3 访问控制技术在操作系统中的实现 …… 149
6.3.1 Windows NT/2K 的安全访问控制 …… 149
6.3.2 Linux 的安全访问控制 …… 150
6.4 访问控制技术在数据库系统中的实现 …… 152
6.4.1 自主访问控制(DAC) …… 152

6.4.2 强制访问控制(MAC) …… 153
6.4.3 基于角色的访问控制(RBAC) …… 153
6.4.4 UCON 的提出 …… 154
6.4.5 DAC、MAC、RBAC、UCON 四种访问控制对比 …… 155
6.5 访问控制技术在网络中的实现 …… 156
6.5.1 网络访问控制 …… 156
6.5.2 分布式网络访问控制 …… 158
6.5.3 支持移动通信的访问控制 …… 159
6.5.4 可信网络访问控制 …… 159
6.6 访问控制技术在信息网格中的实现 …… 160
6.6.1 密码技术 …… 162
6.6.2 公钥基础设施 PKI …… 163
6.6.3 X.509 证书 …… 164
6.6.4 SSL 协议 …… 166
6.6.5 Kerberos 鉴别服务 …… 167
6.6.6 WS-Security …… 168
6.6.7 信息网格中访问控制过程的实现 …… 170
6.7 访问控制机制的分类 …… 170
6.7.1 基于进程的访问控制 …… 170
6.7.2 基于角色的访问控制 …… 172
6.7.3 基于上下文的访问控制 …… 173
6.7.4 通用的基于角色的访问控制 …… 175
6.7.5 基于组的访问控制 …… 176
6.7.6 基于任务的访问控制 …… 176
6.7.7 基于属性的访问控制 …… 180
6.7.8 非自主性访问控制 …… 182
6.7.9 基于信誉的访问控制 …… 183
6.7.10 委托授权问题 …… 183
6.8 本章小结 …… 184
习题 6 …… 184

第 7 章 基于角色的访问控制 …… 185
7.1 核心功能 …… 185
7.2 NIST 建议的 RBAC 标准 …… 188
7.2.1 RBAC0 模型 …… 188
7.2.2 RBAC1 模型 …… 189
7.2.3 RBAC2 模型 …… 190
7.2.4 RBAC3 模型 …… 190
7.3 角色分层 …… 191

7.4 责任分离 …… 193
7.5 ARBAC 基于角色的管理模型 …… 193
7.5.1 URA97 授权模型 …… 195
7.5.2 URA97 回收模型 …… 200
7.6 RBAC 的特点和优势 …… 202
7.6.1 RBAC 几大特点 …… 202
7.6.2 RBAC 应用优势 …… 202
7.7 RBAC 在企业中的运用 …… 202
7.7.1 在企业 IT 架构中集成 RBAC …… 203
7.7.2 使用 基于 X.509 属性证书的 RBAC 实企业访问控制框架 …… 209
7.7.3 RBAC 案例研究 …… 216
7.8 本章小结 …… 221
习题 7 …… 221

第 8 章 基于多域的访问控制 …… 222
8.1 基于角色映射的多域安全互操作 …… 222
8.1.1 多域安全互操作的应用背景 …… 222
8.1.2 角色映射技术 …… 223
8.1.3 建立角色映射的安全策略 …… 224
8.1.4 角色映射的维护 …… 225
8.1.5 角色映射的安全性分析 …… 225
8.2 动态结盟环境下基于角色访问控制 …… 226
8.2.1 动态结盟环境下的应用背景 …… 226
8.2.2 DRBAC 模型和理论 …… 227
8.2.3 基本指派模型的扩展 …… 233
8.2.4 DRBAC 模型实现的参考结构 …… 236
8.2.5 DRBAC 模型安全性分析 …… 238
8.3 多虚拟组织结盟的访问控制 …… 238
8.3.1 SVE 体系结构和基本组件 …… 239
8.3.2 应用实例分析 …… 239
8.3.3 SVE 的安全性分析 …… 241
8.4 结合 PKI 跨域的基于角色访问控制 …… 242
8.4.1 应用背景 …… 242
8.4.2 访问控制表和用户证书 …… 242
8.4.3 客户域内证书的撤销 …… 244
8.4.4 应用实例分析 …… 244
8.4.5 跨域的基于角色访问控制技术的安全性分析 …… 245
8.5 本章小结 …… 246
习题 8 …… 246

第9章 基于信任管理的访问控制技术 …… 247
9.1 信任管理的概念 …… 247
9.1.1 应用背景 …… 247
9.1.2 信任管理的基本概念 …… 248
9.1.3 信任管理的组件和框架 …… 250
9.1.4 信任管理技术的优点 …… 251
9.2 Police Maker 模型 …… 251
9.2.1 Police Maker 模型简介 …… 251
9.2.2 Police Maker 模型实例分析 …… 253
9.2.3 Police Maker 模型安全性分析 …… 254
9.2.4 Key Note 模型简介 …… 254
9.2.5 Key Note 模型安全性分析 …… 255
9.3 RT 模型 …… 255
9.3.1 应用背景 …… 255
9.3.2 基于属性的信任管理系统的基本概念 …… 256
9.3.3 RT 模型简介 …… 256
9.3.4 RT_0 模型基本组件 …… 256
9.3.5 RT_0 模型实例分析 …… 258
9.3.6 信任证的分布式存储和查找 …… 258
9.3.7 RT_0 模型的扩展 …… 259
9.3.8 RT 模型的安全性分析 …… 259
9.4 本章小结 …… 260
习题9 …… 260

第10章 访问控制应用 …… 261
10.1 Windows Server 中的访问控制简介 …… 261
10.1.1 权限 …… 262
10.1.2 查看文件和文件夹上的有效权限 …… 263
10.1.3 管理对象所有权 …… 265
10.1.4 取得文件或文件夹的所有权 …… 265
10.1.5 安全管理审核 …… 266
10.1.6 授权管理器 …… 273
10.2 包过滤访问控制的实现 …… 277
10.2.1 包过滤技术简介 …… 278
10.2.2 截获网络封装包 …… 280
10.2.3 驱动程序和应用程序间的通信 …… 281
10.2.4 过滤规则设置 …… 281
10.2.5 记录和报警 …… 282
10.3 代理服务器的访问控制 …… 282

10.3.1　代理服务器的功能 …… 282
10.3.2　代理服务器的分类及特点 …… 283
10.3.3　各种代理服务器的比较 …… 285
10.3.4　Linux 下安装配置 squid Proxy Server …… 285
10.4　应用强制访问控制管理网络服务 …… 301
10.4.1　强制访问控制机制简介 …… 301
10.4.2　如何启动和关闭 SELinux …… 301
10.4.3　使用 SELinux 策略目录 …… 303
10.4.4　管理网络服务的文件系统访问权限 …… 304
10.5　通过静态路由实现网络访问控制 …… 306
10.5.1　路由表生成机制的分类 …… 307
10.5.2　实现网络路由的控制 …… 308
10.6　本章小结 …… 309
习题 10 …… 309

附录 1　计算机信息系统安全保护等级划分准则 GB 17859-1999 …… 310

附录 2　中华人民共和国计算机信息系统安全保护条例 …… 318

参考文献 …… 321

第1章 绪 论

“谁掌握了信息，谁就掌握了权力。”——Zbigniew Brzenzinski，美国前国家安全顾问。

进入21世纪后，全球信息化引发了世界范围的深刻变革，大部分国家的国民经济和社会发展对信息技术的依赖达到了前所未有的程度，这也使得信息安全发展成为涉及各个领域，不仅影响公民个人权益，更关乎国家安全、经济发展、公众利益的重大战略问题。本章主要对信息安全的基本概念、体系结构、主要技术等作简要介绍，以便于使读者掌握访问控制技术的基本背景资料。

1.1 信息安全的新特征

自1999年的梅丽莎病毒大爆发以来，电子邮件所携带的病毒在2000年以ILOVEYOU的面貌达到了一个爆发高峰，该病毒在5个小时里就阻塞了全球范围内的E-mail服务器。

俄罗斯在2000年成立了联邦信息安全管理机构，负责去统一领导和协调国家信息安全防范信息作战。

2000年2月7日上午10：15分至下午1：25分，Yahoo网站被黑客攻击，该网站自设立以来破天荒头一次中断服务长达3个小时之久。一星期后，美国CNN、亚马逊、eBay、BUY. COM等商业网站都遭到了类似攻击，致使eBay、BUY等网站被迫关闭。

2000年2月8日下午到2月9日上午，新浪声称遭到了黑客长达18小时的攻击，致使电子邮箱系统完全瘫痪。

2002年10月21日下午5时左右，国际互联网系统的核心，位于美国、瑞典、英国、日本等国家和地区的13个根域名服务器，遭受了有史以来规模最大、最复杂的一次攻击。整个袭击横跨全世界，规模巨大，并持续了1小时左右。

2003年1月25日，互联网遭遇到全球性的蠕虫病毒（Win32. SQLExp. Worm）攻击，导致全球范围内的互联网瘫痪，全世界范围内经济损失额高达12亿美元。8月11日，一种名为“冲击波”（WORM_ MSBlast. A）的新型蠕虫病毒开始在网络上广泛传播，对计算机正常使用和网络运行造成严重影响。

2004年，腾讯、江民、新浪等国内知名网站也陆续被有组织的黑客入侵或遭受严重的攻击，遭受重大损失。

2005年，间谍软件、网络钓鱼严重威胁信息安全。在2005年有将近90%以上的消费者个人电脑受到某种形式的间谍软件侵袭，网络钓鱼的攻击方式以平均每月73%的比例向上增加。

美国自2006年，决定由国土安全部每两年举行一次代号“网络风暴”的多部门联合

网络攻防演习。

2006 年 12 月 26 日，由于我国南海海域地震引发台湾以南 15 公里海底光缆断裂，造成国际港澳台通信线路大量中断，互联网访问质量受到严重影响。

2008 年初香港娱乐圈爆出“艳照门”事件，由于个人隐私数据的外泄，给个人和企业带来严重的负面影响和经济损失。

美国在 2008 年联合了 10 多个国家，在 2010 年联合了 20 多个国家进行了演练。在演习中，主要以能源、公共服务、铁路运输、物流服务、金融服务作为模拟目标，重点放在检验和提高网络应急演练和恢复能力上。

2008 年 8 月，在俄罗斯向格鲁吉亚发动战争前，俄格爆发了大规模网络战，格鲁吉亚政府网站也遭到了黑客攻击，格总统萨卡什维利的个人主页被人篡改；与此同时，俄方的新闻机构也受到严重攻击。

美国于 2009 年 6 月组建了网络空间司令部，任命亚历山大·吉斯上将为司令官。重点发展全球网络空间态势感知能力，以及对国家和政府部门的技术支援能力。2009 年 12 月，美国政府成立了网络安全办公室，任命霍华德·施密特为主任。

2009 年 6 月 12 日，伊朗举行第 10 届总统大选，Twitter 等社交网站成为策划、煽动伊朗社会动荡的重要推手，成为一种强有力的政治工具，被奥巴马政府喻为“箭袋中的一支新箭”。

2010 年 1 月 12 日晨 7 时起，百度因 www. baidu. com 的域名在美国域名注册商处被非法篡改，导致全球多处用户不能正常访问百度。

网络泛化的现状使得网络与信息安全问题越来越突出，而网络安全问题也已经成为了事关每一个国家政治安全、经济安全、社会稳定及决定战争胜负的至关重要的问题。

现如今的互联网发展趋势为：宽带化、无线化、智能化。除此之外，物联网的发展同样也是一个热点问题。随着现代互联网络的发展，我们现在更加强调在“任何时间、任何地点，为任何人连接任何物”，因此诞生了泛在网这个概念。“人、机、物”新三网融合的情况，也成为网络发展的新远景。在网络发展的同时，信息安全事件也在不断增多。

近年来出现的这些信息安全事件，引起了人们对信息安全问题的深刻思考，信息安全已然成为了决定信息化成败，关乎政治安全与稳定、经济发展乃至国家安全的重要课题。

2008 年，美国方面提出了网域空间（SyberSpace）的概念，把由计算机控制的网络、关键产业设备还有系统中的嵌入式处理器以及控制器都纳入了这一范畴，让传统网络的内涵由通信网络、计算机的网络扩展到陆、海、空、天等所有的信息环境，从计算机和网络的设备扩展到了各种嵌入式处理器和控制器，从物理设施一直扩展到了人类活动的各个方面。可以这样说，网域空间的概念充分地体现出了网络与信息技术的渗透性、衍生性、普适性。

总结这些信息安全事件，可以看到信息安全呈现出一些新的特征：

一是信息安全威胁来源呈现出多元化的趋势。这些安全威胁可能来自信息战部队、情报机构、国内外敌对势力和政治团体、恐怖分子、工业间谍、犯罪团伙、职业型黑客或娱乐型黑客，但任何一种危害都不容忽视。

二是信息安全威胁复杂化，这些威胁的目标已经不再单单是破坏计算机和网络，而是逐渐转向经济利益方面。各类和经济相关的数据和信息都成为了攻击者的目标。

三是攻防的非对称性。这种非对称性体现在攻防技术的非对称（如大量自动化攻击工具使得入侵网络与信息系统的门槛降到极低）、攻防成本的非对称（如一个1500元的DDOS攻击软件能使一个电子商务网站损失几百至几千万的营业额）和攻防主体的非对称（如弱国、政治团体甚至个人都能向强国发起攻击）。

四是影响的广泛性。首先体现在影响的人群十分广泛，如海底光缆断裂事件，据一些网站调查显示超过半数以上的人认为生活和工作受到了严重影响。其次体现为扩散性极强，如2000年的ILOVEYOU电子邮件病毒，仅5个小时就阻塞了全球范围内的E-mail服务器。再次体现了连锁反应突出，由于各类信息网络的基础设施之间有着极强的互依赖性，一个局部系统的攻击最终可能造成国家范围内的大规模基础设施灾难。

五是后果的严重性。国家已经全面建立在网络和信息系统的支持之上，信息安全事件动辄影响社稷安危。后果一，推翻国家政权，1991年的海湾战争中，美军利用信息战致使伊拉克的防空系统陷入瘫痪。后果二，瘫痪国家基础设施，2003年美国及加拿大南部由于软件错误导致大规模停电事故。后果三，造成巨大经济损失。2011年，瑞士银行一名员工因违规交易导致该行亏损20亿美元。后果四，引发公共安全灾难。2000年，澳大利亚昆士兰州马鲁奇郡的污水管理系统被攻击，导致数百万升未经处理的污水倾倒进当地的公园和河流中，致使水生动物大量死亡，人们生活受到极大困扰。

六是事件的突发性。各类信息安全威胁往往具有潜伏性和不可预测性，对被攻击方呈现出极强的突发性，为信息安全事件处置带来了极大的难度和挑战。

信息网络中的安全问题是各国信息化发展过程中所面临的一个共同挑战。在如此严峻的条件下很多国家已经通过各种举措展开了应对。

在国际上大部分国家都持有这样的观点：网络和信息化程度越高，其复杂度也越高。与此同时安全问题的影响也就越突出。部分国家也在推行以防范网络威胁、维护网络主导权为主的网络安全战略。在这些国家中，北约、欧盟将网上的政治、经济间谍活动明确视为最重大威胁，他们表示将会投入大量资源以防止大规模网络攻击，要制定新的战略构想，更加积极地采取行动。美国总统奥巴马曾经这样说道："网络空间的发展直接影响到美国的繁荣"。网络安全问题已经成为当前美国所面对的最严峻的挑战。要像拥有军事优势那样对网络空间完全控制，最终达到太空、核、网络三位一体的新型威慑形势。为此，美国正在着手进行基于网域空间突击力、防御力、信息力三大力量的建设。

虽然我国在近年来非常重视网络安全的发展，"十五"以来相继完成了一系列重大工程并且在网络安全领域发挥了重大的作用。但是由于国际形势复杂多变导致我们所面临的局势依然严峻，这主要体现在：（1）国外着力于训练网络空间作战能力，其中以美国为代表的国家积极采取各种手段加强网络空间作战能力。（2）境外敌对势力利用网络空间对我国实施渗透破坏，他们利用境外情报机构对我国进行窃密，并在网络上和我国进行对抗。此外，以美国为首的西方国家利用网络和信息技术方面的优势，对我国进行技术遏制，利用垄断地位和相关标准迫使我国继续对其技术、服务和应用的依赖。

面对日趋复杂的网络安全新形势，如何维护网络信息安全成为了一大主要任务。网络安全是信息化背景下一个不可回避的问题，同时也是一个长期而复杂的系统工程。坚持以发展保安全；以安全促发展的方针。提高信息化水平的同时，在以下方面还要增强网络与信息安全保障的能力：（1）从战略高度提高我国网络空间防护能力。网络空间防护是我

国战略发展的重要组成部分，也关系到我国的核心利益。我们必须从国家安全的角度来看待网络空间的安全战略，将网络空间防护能力建设纳入国家中长期战略规划。（2）加强对网络和信息的安全管理。强化全民的信息安全意识；加快信息安全的相关立法；在信息网络科学变革性突破的时候，指定相应的国家发展规划，努力在相关领域取得重要突破技术专项发展规划，努力在核心芯片、基础软件、关键应用等科学技术领域取得重要或重大突破。

1.2 信息安全基本概念

信息安全的概念随着信息技术的发展而不断演变。

早在20世纪初期，通信技术水平比较低，电话、电报、传真等信息交换过程中存在着各种各样的安全隐患问题，对于信息，人们强调的主要是它的保密性和安全性，对安全理论和技术的研究侧重于密码学，这一阶段的信息安全可以简单称为通信安全。

20世纪60年代后，半导体和集成电路技术的飞速发展带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，人们对信息的安全已经逐渐扩展为以保密性、完整性和可用性为目标的信息安全阶段。美国在《联邦信息安全管理法案》（FISMA，2002年3月通过）中，将信息安全定义为“保护信息和信息系统以避免未授权的访问、使用、泄露、破坏、修改或者销毁，以确保信息的完整性、保密性和可用性”。其中完整性是指防止不恰当的信息篡改和破坏，也包括确保信息的不可否认性和可认证性；保密性是指对信息访问和公开的权限设置，包括对个人隐私的保护；可用性是指对信息的及时和可靠的访问。这种定义也被称为“信息安全的金三角”（见图1-1）。

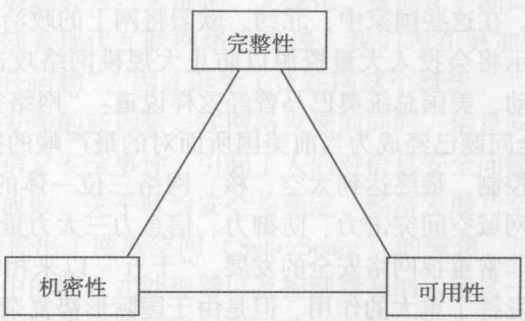


图1-1 信息安全的金三角

20世纪80年代开始，由于互联网技术的飞速发展，信息无论是对内还是对外都得到空前开放，由此产生的信息安全问题跨越了时间和空间，信息安全的中心已经不再是传统的三个原则了，而是衍生出了诸如可控性、抗抵赖性、真实性等其他的原则和目标，信息安全也转化为从整体角度考虑其体系建设的信息保障阶段。以美国为例，1998年5月，克林顿政府发布第63号总统令《克林顿政府对关键基础设施保护的政策》（PDD-63），指定中央情报局、商务部、国防部、能源部、司法部、联邦调查局、交通部、财政部、联邦紧急事务处理局、国家安全局等关键部门作为实施信息安全保护计划的第一批部门，实

现信息安全保障。2000年1月，美国政府制定了《信息系统保护国家计划》，要求在2000年12月前建立一个具备初步运作能力的关键信息系统防备体系。2001年1月，布什总统签署第13231号行政令《信息时代的关键基础设施保护》，授权成立一项旨在通过不断努力来保护关键基础设施中的信息系统的保护项目，包括对应急战备通信设施及其相关的物理设施进行保护。“911”事件后，美军参谋机构发行的《2010年联战远景》白皮书中写道：“鉴于现代计算机网络、通信系统及电子数据库重要性的日益提升，将信息完全纳入国家整体安全政策中仍属必要。在平时，信息战有助于预防冲突发生，或应对危机及公开敌意行为。在危险爆发时，信息战可以用来解决纷争、增强吓阻，或准备应对公开冲突。在战时，信息战则可以直接达成战略、作战及战术目标，或强化其他用于达成这些目标的方法”。2003年2月发布的《保护网络空间的国家战略》进一步指出：“美国的政策是通过保护关键基础设施，防止信息系统的运行遭到破坏，从而保护美国的人民、美国的经济及国家的安全”，并明确规定国土安全部将成为联邦政府确保网络安全的核心部门，并且在确保网络安全方面充当联邦政府与各州、地方政府和非政府组织，即公共部门、私营部门和研究机构之间的指挥中枢。由此可见，信息安全已经发展成为影响公民个人权益、关乎国家安全、经济发展、公众利益的重大战略问题，许多国家在此共识上形成了新的信息安全观。2005年4月，美国政府公布了美国总统IT咨询委员会向总统布什提交的《网络空间安全：迫在眉睫的危机》的紧急报告，对美国2003年的信息安全战略提出不同看法，指出过去十年中美国保护国家信息技术基础建设工作是失败的。2006年10月，俄罗斯联合中国等国向联合国提交了《从国际安全角度来看信息和电信领域的发展》的决议草案，信息安全被定义为“保护个人、社会和国家在信息领域的根本利益”。该草案在联合国会议上获得高票通过，这标志着国际社会对当前信息安全基本概念的认识达成了一致。

网络信息安全涉及国家的各个部门和组织、机构，也涉及经济活动的方方面面。虽然各个部门在网络与信息安全中的任务和义务不同，但是最终的目的都是一致的。网络安全需要多方协同，优势互补，加快提升我国的网络与信息安全整体水平。

1.3 信息系统安全介绍

在飞速发展的信息时代，信息的传播只需要在瞬间就可以完成，这种特性在带来方便的同时也给国家层面的管控带来了挑战。管控不当会造成重要的信息泄露，因此信息安全问题已经成为国家安全所面临的重要威胁。在我国，三大因素造成了互联网领域的国家信息安全问题：一是用户快速增长，这对于社会和经济的影响力空前增大。二是Web2.0时代高速发展，各种新类型应用层出不断。互联网中的自组织不断增加并逐渐趋于主流。三是区别于传统范畴的硬件、软件、黑客等领域的信息安全问题，与互联网新运用、新趋势、新特征相关的一系列新信息安全问题日益突出。

1.3.1 信息系统的安全评测准则

20世纪80年代中期，美国国防部为了对军事计算机采取更好的保密措施，制订了“可信计算机系统安全评价准则”（TCSEC），其后又对网络系统、数据库等方面做出了安