面向21世纪全国高职高专信息技术类规划教材

网络安全与防护基础教程

WANGLUO ANQUAN YU FANGHU JICHU JIAOCHENG

郎为民 雷承达 编著

北京大学出版社
PEKING UNIVERSITY PRESS

面向21世纪全国高职高专信息技术类规划教材

网络安全与防护基础教程

郎为民　雷承达　编著

北京大学出版社
PEKING UNIVERSITY PRESS

内 容 简 介

本书紧紧围绕计算机网络安全发展前沿的热点问题，比较全面和系统地介绍了网络与信息安全的基本理论和应用实践的最新成果。全书共分十章，包括绪论、密码学基础、系统攻击与防护、入侵检测系统、防火墙技术、虚拟专用网、恶意代码与计算机病毒、数据安全、网络安全和评估、网络安全的发展方向等内容。全书材料丰富，内容翔实，覆盖面广，可读性强，可作为从事国家安全和保密工作的人员在高新技术条件下做好工作、提高业务水平必备的实用工具书，也可作为国内网络安全、计算机安全和信息安全领域相关人员的技术培训教材。本书还可作为通信与电子系统、信号与信息处理、密码学等专业的本科生和大专生相关课程的教学参考书。

图书在版编目（CIP）数据

网络安全与防护基础教程/郎为民，雷承达编著. —北京：北京大学出版社，2005.7
（面向 21 世纪全国高职高专信息技术类规划教材）
ISBN 7-301-08850-7

I. 网… II. ①郎… ②雷… III. 计算机网络—安全技术—高等学校—教材
IV. TP393.08

中国版本图书馆 CIP 数据核字（2005）第 031070 号

书　　名：网络安全与防护基础教程
著作责任者：郎为民　雷承达　编著
责 任 编 辑：黄庆生　桂春
标 准 书 号：ISBN 7-301-08850-7/TP・0781
出　版　者：北京大学出版社
地　　址：北京市海淀区成府路 205 号　100871
电　　话：邮购部 62752015　发行部 62750672　编辑部 62765013
网　　址：http://cbs.pku.edu.cn
电 子 信 箱：xxjs@pup.pku.edu.cn
印　刷　者：河北滦县鑫华书刊印刷厂
发　行　者：北京大学出版社
经　销　者：新华书店
787 毫米×1092 毫米　16 开本　18.5 印张　404 千字
2005 年 7 月第 1 版　2005 年 7 月第 1 次印刷
定　　价：28.00 元

前　言

网络安全关系到国家安全，网络安全的理论及其应用技术的研究，不仅受到学术界以及工业界的关注，同时也受到各国政府的高度重视。随着网络经济和网络社会的到来，网络安全逐渐成为 Internet 及各项网络服务和应用进一步发展的关键问题，特别是 1993 年以后 Internet 开始商用化，加之 Internet/Intranet 技术日趋成熟，很多组织和企业都建立了自己的内部网络并将之与 Internet 联通。现代企业对信息的依赖越来越大，没有各种信息的支持，企业就不能生存和发展。信息已成为现代企业的一种重要资产，更需要加以妥善保护，否则，可能由于人为失误、敌方破坏、设备故障、系统缺陷和自然灾害等原因，使得信息资产被毁灭、消失、损坏、盗窃、贬值、转移，给企业带来致命的打击。由于计算机、通信、网络等现代化技术的普及应用和人员流动的频繁，信息受到的威胁更大。据统计，目前网络攻击手段有数千种之多，使网络安全问题变得极其严峻，据美国商业杂志《信息周刊》公布的一项调查报告称，黑客攻击和病毒等安全问题在 2000 年造成了上万亿美元的经济损失，在全球范围内每几秒钟就发生一起网络攻击事件。然而，由于种种原因，目前我国有关网络安全技术及其产品的研发与美国等西方发达国家相比尚有一定的距离。正因为如此，我们更应加倍努力，迎头赶上。

在这种背景下，为促进我国网络安全技术的进步，在国家自然科学基金和国家 863 高技术项目基金的资助下，笔者结合自己多年来在网络安全研究中的心得，特编拙著，以期抛砖引玉，为我国的网络安全事业尽一点微薄之力。

本书共分十章。第 1 章主要讲述了网络安全的基本概念、主要目标和分类方法，列举了当前网络安全面临的主要威胁，建立了比较完整的网络安全体系，介绍了物理安全、网络安全、系统、信息和应用安全及安全管理的主要内容和相关对策。第 2 章主要讲述了数据加密技术的基本概念和分类方法，给出了对称密码体制、公钥密码体制、混合密码体制的信息处理流程和主要优缺点，介绍了数字签名的作用、特点和实现过程，概括了公钥基础设施的基本组成、主要功能，引入了密钥管理的基本概念和实现方法。第 3 章主要讲述了黑客与入侵者的基本概念，分析了系统攻击的三个阶段，列举了口令攻击、IP 欺骗、端口扫描、网络监听、电子邮件攻击的工作原理和相关技术，并给出了对应的防护措施。第 4 章给出了入侵检测的基本定义、主要任务和功能作用，概括了入侵检测系统的工作原理及分类，详细分析了基于主机、基于网络和基于分布式系统等三种入侵检测系统的工作原理及优缺点。第 5 章主要讲述了防火墙的相关概念、主要功能和局限性，分析了包过滤防火墙、应用代理防火墙、状态检测防火墙的基本原理和主要特点，并介绍了筛选路由器、

双宿主主机、屏蔽主机和屏蔽子网等四种防火墙的体系结构。第 6 章主要讲述了虚拟专用网的概念、功能、类型和优点，分析了 Access VPN、Intranet VPN、Extranet VPN 的基本原理及特点，概括了隧道技术、密码技术、身份认证技术、密钥管理技术的原理及应用，引入了第二层转发协议、点对点隧道协议、第二层隧道协议、SOCKSv5、IP 安全协议、通用路由封装协议的的相关知识。第 7 章主要讲述了恶意代码的基本概念、主要特点和清除方法，给出了计算机病毒的特征、分类、结构及传输方式，列举了病毒免疫技术、病毒检测技术、病毒预防技术和病毒消除技术的相关概念及实施方法。第 8 章主要讲述了数据完整性的基本概念，列举了提高数据完整性的主要方法，详细介绍了网络备份技术、归档技术、分级存储管理技术、容错与网络冗余技术、灾难恢复技术的原理和实现过程。第 9 章主要讲述了网络安全管理的基本概念、根本目标、面临的风险和构成框架，概括了制定信息安全管理策略应当遵循的基本原则，罗列了制定信息安全管理策略的方法，分析了信息安全管理标准 ISO 17799 的控制措施及其应用，介绍了安全评估的基本概念、主要过程、基本内容和关键技术，给出了可信计算机系统评估准则、计算机信息系统安全保护等级划分准则和通用安全评估准则三个信息安全评估标准。第 10 章主要分析了密码技术、入侵检测系统、防火墙和虚拟专用网的发展趋势。

本书由郎为民、雷承达担任主编，靳焰、王逢东、丁锐参与编写。在本书成稿过程中，得到了本人的导师、华中师范大学副校长杨宗凯教授的大力支持，华中科技大学电信系互联网技术研发中心的程文清副教授和谭运猛副教授对本书的初稿提出了很多宝贵的意见和建议，熊志强和付雄博士仔细阅读了本书有关章节，并更正了不少错误，作者向他们表示衷心的感谢。

北京大学出版社黄庆生主任作为本书的责任编辑，为本书的出版付出了辛勤的劳动，北京大学出版社对本书的出版给予了大力支持，在此我们一并表示感谢。

限于作者的水平，书中一定有不少缺点和错误，殷切期望广大读者批评指正。

郎为民

2005 年 1 月

目　录

第 1 章　绪论 1
1.1　网络安全概述 1
1.1.1　网络安全的基本概念 1
1.1.2　网络安全的目标 2
1.1.3　网络安全的分类 3
1.1.4　安全服务 4
1.1.5　安全机制 6
1.2　网络安全威胁 10
1.2.1　存在原因 10
1.2.2　威胁类别 12
1.2.3　防护措施 14
1.3　网络安全现状及对策 14
1.3.1　网络安全现状 14
1.3.2　主要的网络安全问题 16
1.3.3　网络安全策略 18
1.4　网络安全体系 20
1.4.1　物理安全 21
1.4.2　网络安全 22
1.4.3　系统、信息和应用安全 24
1.4.4　安全管理 25
1.5　思考题 26
第 2 章　密码学基础 27
2.1　数据加密技术 27
2.1.1　数据加密的基本概念 27
2.1.2　加密体制的分类 28
2.1.3　对称密码体制 30
2.1.4　公钥密码体制 31
2.1.5　混合密码体制 33
2.2　数字签名技术 33

2.2.1 散列算法 34
2.2.2 数字签名的基本概念 34
2.2.3 数字签名的特点 36
2.2.4 数字签名的实现过程 37
2.3 公钥基础设施 39
2.3.1 PKI 的基本组成 39
2.3.2 PKI 的主要功能 42
2.3.3 认证中心 43
2.3.4 数字证书 48
2.4 密钥管理 51
2.4.1 密钥管理的基本概念 52
2.4.2 密钥管理的实现方法 52
2.4.3 密钥的生成 53
2.4.4 密钥的分配 53
2.4.5 密钥的备份与恢复 54
2.4.6 密钥的更新和销毁 55
2.5 思考题 55
第 3 章 系统攻击与防护 56
3.1 系统攻击概述 56
3.1.1 黑客与入侵者 56
3.1.2 系统攻击的三个阶段 57
3.1.3 网络入侵的对象 58
3.2 口令攻击 60
3.2.1 口令认证的过程 60
3.2.2 破解口令的方法 61
3.2.3 创建安全口令 64
3.3 IP 欺骗 65
3.3.1 IP 欺骗的原理 66
3.3.2 IP 欺骗的基本形式 67
3.3.3 IP 欺骗攻击的防护 69
3.4 端口扫描 70
3.4.1 端口扫描的基本概念 71
3.4.2 端口扫描技术 72
3.4.3 端口扫描的防御技术 74
3.5 网络监听 75

3.5.1 网络监听的原理 75
3.5.2 网络监听的检测技术 77
3.5.3 网络监听的防御技术 79
3.6 电子邮件攻击 80
3.6.1 电子邮件的工作原理 80
3.6.2 电子邮件面临的主要威胁 81
3.6.3 电子邮件攻击方法 83
3.6.4 电子邮件防护措施 84
3.7 思考题 86
第 4 章 入侵检测系统 87
4.1 入侵检测 87
4.1.1 入侵检测概述 87
4.1.2 入侵检测的主要任务和作用 91
4.1.3 入侵检测系统的基本结构 92
4.1.4 入侵检测系统的工作原理 93
4.1.5 入侵检测系统的分类 95
4.1.6 入侵检测系统的局限性 96
4.2 入侵检测系统的分析方式 97
4.2.1 异常检测技术 97
4.2.2 误用检测技术 100
4.2.3 异常检测技术和误用检测技术的比较 102
4.2.4 其他入侵检测技术的研究 103
4.3 入侵检测系统的结构 103
4.3.1 基于网络的入侵检测系统 103
4.3.2 基于主机的入侵检测系统 108
4.3.3 基于分布式系统的入侵检测技术 111
4.4 思考题 112
第 5 章 防火墙技术 113
5.1 防火墙概述 113
5.1.1 防火墙的定义和相关概念 113
5.1.2 防火墙的功能 116
5.1.3 防火墙的安全策略 118
5.1.4 防火墙的局限性 119
5.2 防火墙的种类 120
5.2.1 包过滤防火墙 120

5.2.2 应用代理过滤防火墙 124
5.2.3 状态检测防火墙 128
5.3 防火墙的体系结构 131
5.3.1 筛选路由器 131
5.3.2 双宿主主机结构 133
5.3.3 屏蔽主机结构 135
5.3.4 屏蔽子网结构 137
5.4 思考题 140
第 6 章 虚拟专用网 141
6.1 虚拟专用网概述 141
6.1.1 虚拟专用网的概念 141
6.1.2 虚拟专用网的功能 143
6.1.3 虚拟专用网的类型 144
6.1.4 虚拟专用网的优点 149
6.1.5 虚拟专用网的原理 150
6.2 虚拟专用网技术 152
6.2.1 隧道技术 152
6.2.2 密码技术 154
6.2.3 身份认证技术 154
6.2.4 密钥管理技术 155
6.3 隧道协议 156
6.3.1 隧道协议的基本概念 156
6.3.2 第二层隧道协议 157
6.3.3 第三层隧道协议 163
6.4 思考题 167
第 7 章 恶意代码与计算机病毒 168
7.1 恶意代码 168
7.1.1 恶意代码的基本概念 168
7.1.2 恶意代码的特点和分类 169
7.1.3 恶意代码的清除 171
7.2 计算机病毒 172
7.2.1 计算机病毒的概念 172
7.2.2 计算机病毒的特征 175
7.2.3 计算机病毒的分类 176
7.2.4 计算机病毒的结构 179

7.2.5 计算机病毒的传播方式 180
7.3 计算机病毒的防治技术 182
7.3.1 病毒免疫技术 182
7.3.2 病毒检测技术 185
7.3.3 病毒预防技术 188
7.3.4 病毒消除技术 189
7.4 思考题 191
第 8 章 数据安全 192
8.1 数据完整性 192
8.1.1 数据完整性 192
8.1.2 提高数据完整性的办法 194
8.2 网络备份技术 195
8.2.1 网络备份的种类 195
8.2.2 备份恢复的种类 196
8.2.3 网络备份系统的组成 197
8.2.4 备份和恢复的设备与介质 199
8.2.5 提高备份性能的技术 200
8.3 归档 201
8.3.1 归档的基本概念 201
8.3.2 归档的方法 202
8.3.3 归档中的介质与冗余 204
8.4 分级存储管理 205
8.4.1 分级存储管理的功能组件 205
8.4.2 分级存储管理的工作过程 206
8.5 容错与网络冗余 207
8.5.1 容错技术的分类 207
8.5.2 容错系统实现方法 208
8.5.3 网络冗余 211
8.6 灾难恢复技术 212
8.6.1 灾难恢复前的准备 212
8.6.2 灾难恢复过程 213
8.7 思考题 217
第 9 章 网络安全管理和评估 218
9.1 网络安全管理 218
9.1.1 网络安全管理的概念 218

9.1.2 网络安全管理面临的风险 220
9.1.3 网络安全管理的目标 221
9.1.4 网络安全管理系统的构成 222
9.1.5 网络安全管理的措施 224
9.2 信息安全管理策略 226
9.2.1 制定信息安全管理策略的原则 226
9.2.2 信息安全管理策略的基本内容 226
9.3 信息安全管理标准 229
9.3.1 ISO 17799 标准简介 229
9.3.2 ISO 17799 标准控制措施 230
9.3.3 ISO 17799 标准的应用 234
9.4 安全评估 235
9.4.1 安全评估的过程 235
9.4.2 安全评估的主要内容 237
9.4.3 安全评估的基本技术 238
9.5 安全评估准则 241
9.5.1 可信计算机系统评估准则 241
9.5.2 计算机信息系统安全保护等级划分准则 242
9.5.3 通用安全评估准则 245
9.6 思考题 247
第 10 章 网络安全的发展方向 248
10.1 密码技术的发展方向 248
10.1.1 密码专用芯片集成技术 248
10.1.2 椭圆曲线加密技术 248
10.1.3 量子加密技术 249
10.1.4 混沌加密技术 250
10.1.5 生物特征加密技术 251
10.2 入侵检测系统的发展方向 254
10.2.1 分布式入侵检测技术 255
10.2.2 智能化入侵检测 256
10.2.3 入侵预防技术 258
10.2.4 全面的安全防御技术 259
10.3 防火墙技术的发展方向 261
10.3.1 性能方面的发展趋势 262
10.3.2 体系结构的发展趋势 265

10.3.3 系统管理的发展趋势 270
10.4 虚拟专用网的发展趋势 270
10.4.1 IPSec VPN 271
10.4.2 MPLS VPN 273
10.5 思考题 275
附录 英文缩略词 276
参考文献 282

第1章 绪 论

1.1 网络安全概述

随着经济信息化的迅速发展，计算机网络对安全要求越来越高，尤其是 Internet/Intranet 迅猛发展和广泛应用以来，网络信息安全问题涉及到国家主权和社会公共安全等许多重大问题。世界各国已经认识到信息安全涉及重大国家利益，是互联网经济的制高点，也是推动互联网发展、电子政务和电子商务的关键，发展信息安全技术是目前面临的迫切要求。

伴随着黑客工具和攻击技术的日益发展，使用这些工具所需具备的各种技巧和知识在不断减少，从而造成全球范围内黑客行为的泛滥，导致了一个全新战争形式的出现，即网络安全技术的大战。

1.1.1 网络安全的基本概念

“安全”一词在字典中被定义为“远离危险的状态或特性”和“为防范间谍活动或蓄意破坏、犯罪、攻击或逃跑而采取的措施”。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、数论和信息论等多种学科的综合性学科。它关系到国家安全和主权、社会稳定、民族文化的继承和发扬，其重要性正伴随着全球信息化步伐的加快而日益凸现出来。

从本质上来讲，网络安全就是网络上的信息安全，它涉及的领域相当广泛。这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。从狭义的保护角度来看，计算机网络安全是指计算机及其网络信息资源不受自然和人为因素的威胁或危害。

从广义来说，凡是涉及到网络信息保密性、完整性、可用性、真实性、可控性的相关技术和理论都是网络安全的研究领域。下面给出一个网络安全的通用定义：网络安全是指网络系统的硬件、软件及其系统中的数据得到有效的保护，不会由于偶然的或者恶意的原因而遭到破坏、更改和泄露，系统能够连续可靠正常地运行，且能保证网络服务不中断。

网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。技术方面主要侧重于防范外部非法用户的攻击，管理方面则侧重于内部人为因素的管理。如何更有效地保护重要的信息数据、提高计算机网络系统的安全性已经成为所有计算机网络应用必须考虑和解决的一个重要问题。

1.1.2 网络安全的目标

通俗地说，网络信息安全与保密主要是指保护网络信息系统，使其没有危险、不受威胁、不出事故。从技术角度来说，网络信息安全与保密的目标主要表现在系统的可靠性、可用性、保密性、完整性、不可抵赖性和可控性等方面。

1. 可靠性

可靠性是指网络信息系统能够在规定条件下和规定时间内完成规定功能的特性。可靠性是系统安全最基本要求之一，是所有网络信息系统建设和运行的目标。网络信息系统的可靠性测度方法主要有三种：抗毁性、生存性和有效性。可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性和环境可靠性等方面。

2. 可用性

可用性是指网络信息可被授权实体访问并按需求使用的特性，即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。网络信息系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的，甚至还有时间限制。可用性一般用系统正常使用时间和整个工作时间之比来度量。可用性应当满足以下要求：身份识别与确认、访问控制、业务流控制、路由选择控制和审计跟踪。

3. 保密性

保密性是指网络信息不泄露给非授权用户、实体或不供其使用的特性，即信息只为授权用户服务，并防止泄漏给非授权个人或实体的特性。保密性建立在可靠性和可用性的基础之上，是保障网络信息安全的重要手段。

常用的保密技术包括：防侦收（使攻击者侦收不到有用的信息）、防辐射（防止有用信息以各种途径辐射出去）、信息加密（在密钥的控制下，用加密算法对信息进行加密处理，即使攻击者得到了加密后的信息也会因为没有密钥而无法读懂有效信息）、物理保密（利用各种物理方法，如限制、隔离、掩蔽和控制等措施，保护信息不被泄露）。

4. 完整性

完整性是指网络信息未经授权不能进行改变的特性，即网络信息在存储或传输过程中，能够确保不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和正确传输。

完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因的破坏。影响网络信息完整性的主要因素有：设备故障、误码（传输、

处理、存储过程中产生的误码；定时的稳定度和精度降低造成的误码；各种干扰源造成的误码)、人为攻击和计算机病毒等。

保障网络信息完整性的主要方法有：

（1）协议：通过各种安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段。

（2）纠错编码方法：用以完成检错和纠错功能，最简单和常用的纠错编码方法是奇偶校验法。

（3）密码校验和方法：它是抗篡改和传输失败的重要手段。

（4）数字签名：保障信息的真实性。

（5）公证：请求网络管理或中介机构证明信息的真实性。

5. 不可抵赖性

不可抵赖性，也称不可否认性，是指在网络系统信息的交互过程中，能够确信参与者的真实同一性的特性，即所有参与者都不能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止接收方事后否认已经接收的信息。

6. 可控性

可控性是指对网络信息的传播及内容具有控制能力的特性。概括地说，网络信息安全与保密的核心是通过计算机、网络、密码技术和安全技术，保护在公用网络信息系统中传输、交换和存储消息的可靠性、可用性、真实性、保密性、完整性和不可抵赖性等。

1.1.3 网络安全的分类

根据应用环境的不同，网络安全可分为运行系统安全、网络信息安全、信息传输安全和信息内容安全四类，如图 1-1 所示。

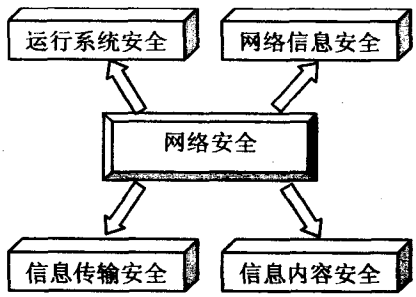

图 1-1　网络安全的分类

1. 运行系统安全

运行系统安全用于保证信息处理和传输系统的安全，侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁泄漏而产生信息泄露，干扰他人或受他人干扰。

2. 网络信息安全

网络信息安全包括用户口令鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，安全问题跟踪，计算机病毒防治和数据加密。

3. 信息传输安全

信息传输安全地保证信息传输后果的安全，包括信息过滤等。它侧重于防止和控制非法、有害的信息进行传输后的后果，避免公用网络上大量自由传输的信息失控。

4. 信息内容安全

信息内容安全侧重于提供信息的保密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。它本质上是保护用户的利益和隐私。

1.1.4 安全服务

在计算机网络中，安全服务通常包括安全风险评估服务、安全顾问服务、安全培训服务、电子商务安全服务、管理防火墙和虚拟专用网服务、防黑客服务、实时监控服务和防病毒服务等内容。

1. 安全风险评估服务

安全风险评估服务的内容包括：使用自动缺陷扫描工具对目标信息系统进行扫描以发现目标系统中所存在的技术缺陷和设置错误；结合目标信息系统的应用需求和安全需求对缺陷扫描的结果进行分析，得出目标系统缺陷评估结论和目标系统加固建议报告书；通过对客户的安全管理策略、信息系统结构、网络、系统、数据库和业务应用等方面进行安全风险评估，确定所存在的安全隐患及安全事故对客户整体可能造成的损失程度和风险大小，帮助客户确定对各部分的网络安全投资预算。

在目标信息系统被可靠加固的基础上，根据其应用需求和安全需求，在目标系统中所应用的技术被发现存在新的缺陷或者出现必要的更新时，对目标用户进行主动提醒并为目标用户提供具体的修改或更新建议及详细的操作规程。在目标信息系统的应用需求和安全需求发生变化时，响应目标用户的要求，对这些变化进行评估并为目标用户提供具体的建议和详细的操作规程。

2. 安全顾问服务

安全顾问服务是指对客户的互联网关键业务应用系统进行调研，结合国内外最新的网络安全技术，为托管客户提供符合自身实际情况的网络安全解决方案和安全体系设计方案。

根据目标系统缺陷评估结论和目标系统加固建议报告书的要求，制定各种子系统的加

固说明和详细加固规程。同时，根据目标用户的要求，对目标信息系统的加固、安全方案的部署、安全设备的配置、管理以及安全事件的分析处理提供远程或现场技术支持和操作。

3. 安全培训服务

通过与国内外著名网络安全公司的合作和技术交流以及数据中心安全服务的经验积累，为客户提供各种安全培训，主要内容包括互联网安全的最新进展和发展趋势、网络安全技术和产品及安全管理制度等。安全教育和培训要求毫无保留地提供信息系统安全管理和技术方面的信息，其中包括具体的操作方法和步骤。信息系统用户通过培训了解信息系统的安全知识，并且能够自主地将这些安全知识应用到信息系统中去，采取具有成本效益的安全解决方案以全面、有效地提高信息系统的整体安全防护水平。

4. 电子商务安全服务

为从事电子商务服务的托管客户提供全面的用户管理、访问控制、目录服务、审计服务、CA 证书和数字签名、网上支付等配套技术服务。根据目标信息系统的应用需求和安全需求，结合目标用户的具体要求、行业特点和市场当前所具备的产品等情况提出目标系统的技术解决方案。

5. 管理防火墙和虚拟专用网服务

为托管客户提供集中监控和安全策略配置的防火墙及虚拟专用网（Virtual Private Network，简称 VPN）设施。客户可以选择适合自身需要的防火墙和 VPN，接受防火墙和 VPN 的状态监控、故障重启、升级、策略配置等技术服务。

6. 防黑客服务和实时监控服务

通过对托管客户的网络、主机、数据库和通用网关接口（Common Gateway Interface，简称 CGI）程序的安全漏洞扫描，优化系统配置和及时更新补丁，最大限度地弥补最新的安全漏洞和消除安全隐患。同时，通过在客户的网络和主机上安装入侵检测探头，将黑客入侵迹象实时记录并上报给安全监控中心，由安全服务工程师进行记录、分析和处理。对于严重的黑客入侵行为，将启动二线的安全专家进行紧急响应，及时阻断入侵和恢复网络系统，并根据客户要求提供法律诉讼所需要的黑客入侵证据。

7. 防病毒服务

与国内外著名的防病毒技术厂商合作，通过在托管客户的防火墙和网关部署网络防毒系统，定期升级网络杀毒软件和病毒标志，并采用多层过滤等方式，在第一时间杀除最新已知的互联网病毒，包括电子邮件及附件、压缩文件中隐藏的病毒、非法程序和代码等。防病毒服务包括无毒托管主机、无毒邮箱和针对企业内部办公网络病毒防治的办公室医生服务。