信息系统安全集成

张启浩◆编著

信息化、信息安全工程建设指导类书籍
法律、法规、规范、标准于一体
网络安全、信息保密于一体
设计、施工、质量控制于一体
技术手段、管理措施于一体

中国建筑工业出版社

信息系统安全集成

张启浩　编著

中国建筑工业出版社

图书在版编目(CIP)数据

信息系统安全集成/张启浩编著．—北京：中国建筑工业出版社，2015.12

ISBN 978-7-112-18781-2

Ⅰ.①信… Ⅱ.①张… Ⅲ.①信息系统-安全技术 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字(2015)第 284608 号

该书分为六章，第一章信息安全概述，第二章信息安全集成准备，第三章信息系统安全方案设计，第四章安全设备测试，第五章工程实施，第六章信息安全管理。该书从信息安全相关法律、法规，到等级保护、分级保护规范标准；从信息安全的需求分析、方案设计，到工程施工组织管理、系统测试、质量控制；从技术保护措施，到安全管理保障措施，全面系统分析了信息系统安全建设工作涉及的各个方面。

该书为信息化、信息安全工程建设指导类书籍，可以作为信息系统安全保障工程师培训教材，也可作为信息系统安全工程专业教材使用。

* * *

责任编辑：张 磊

责任设计：董建平

责任校对：陈晶晶 关 健

信息系统安全集成

张启浩 编著

*

中国建筑工业出版社出版、发行（北京西郊百万庄）

各地新华书店、建筑书店经销

北京红光制版公司制版

北京同文印刷有限责任公司印刷

*

开本：787×1092 毫米 1/16 印张：23¼ 字数：580 千字

2016 年 4 月第一版 2016 年 4 月第一次印刷

定价：**55.00** 元

ISBN 978-7-112-18781-2

(27916)

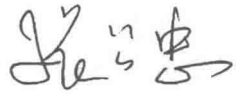
序

张启浩同志编著的《信息系统安全集成》是一部信息化、信息安全工程建设指导类书籍，该书的内容全面论述和系统分析了计算机信息系统如何开展信息安全保护建设和实现信息安全目标，是一部将信息系统安全相关法律、法规、政策、保护制度、信息安全等级保护系列规范、涉及国家秘密信息系统分级保护建设规范、安全技术措施、安全管理措施融于一体的工程建设指导书，是一部理论性与实践性相结合的好书，对我国信息化和信息安全建设实践将发挥着重要指导作用。

该书围绕信息系统实现信息安全目标，将国家法律、法规、信息安全建设规范、涉密信息系统技术规范等要求，全面落实在需求分析、方案设计、工程施工管理与组织、工程质量管理、信息安全管理等信息化系统建设过程的各个环节。与其他相关专业书刊内容对比，该书最显著特点是，把有关信息安全与保密建设的相关法律、法规、政策、规范标准、安全技术、安全管理、工程建设管理与施工管理等涉及信息化工程建设的各个方面均进行了全面论述，对信息化工程设计者、工程实施者都有指导意义。该书基本涵盖了信息化建设涉及的法律、法规、建设规范、涉及信息系统规范及政策等的强制性规定和一般性规定等内容，对建设管理者来说，阅读该书基本上就能够了解信息化建设应当建设什么，遵循的标准是什么，怎样组织建设和管理工程施工；对施工者来说，知道工程项目设计施工中国家强制性和一般性要求是什么，国家颁布的信息系统安全技术标准和安全管理要求是什么，如何通过具体安全技术措施和管理手段实现国家规范要求；对施工管理者来说，怎样进行施工管理，保证工程质量，从而保证信息安全目标的实现，保证项目实施符合国家相关规范。同时，该书对编制申报信息安全集成服务资质和培训信息安全保障工程师也具有很好的指导意义。

当前全球和全国都在高度关注网络和信息安全的背景下，出版发行该书，对于贯彻习近平总书记的“没有网络安全就没有国家安全，没有信息化就没有现代化”的重要思想，具有直接的积极意义。

清华大学教授、国家住建部建筑智能化技术专家委员会副主任张公忠于北京清华园



2015.8.8

前　言

中共中央总书记、国家主席习近平同志指出："没有网络安全就没有国家安全，没有信息化就没有现代化。"习主席高度概括了信息化和网络安全对国家发展和安全的重要作用和战略地位，要求我们既要高度重视信息化建设，也要高度重视网络安全建设。

随着信息技术的快速发展和广泛应用，网络连接全世界，有网络的地方就有信息化应用，人们通过网络获取大量的有用信息，包括政治、经济、军事、科技、贸易、教育、工业、农业等方面的信息，特别是行业纵向专网，如国家电子政务内网、银行专网、电信网、电力网等行业网络，利用信息化开展社会管理、依法行政、行业的职能业务管理和生产等。互联网、物联网给人们的生产、生活带来极大方便，信息的交流快捷、高效、便利、内容丰富。网络把全国性的集团变成了一个小单元，互联网把全球变成了地球村。网络对人类社会、经济的发展起到了积极的促进作用，网络给人类社会带来日新月异的变化。同时，随之而来的是无形的、看不见摸不着的信息安全威胁、安全风险，它涉及到每个局域网，每个应用系统，每台个人应用终端。国家的信息安全保密，企业的信息安全，公民的个人信息安全，各行业的信息安全都受到威胁和挑战。因此，人们对网络信息安全保护的需求日益迫切。

信息安全是通过技术手段、管理制度建设，通过法律保护，行政管理等手段，保障计算机信息系统不被破坏，系统不被非法侵入、非法登录，信息不被篡改、窃取，国家秘密不被泄露，保障网络系统正常运行。

为了实现信息安全目标，国家已经建立了系列的法律、法规、监管体制和制度，颁布了信息系统安全等级保护系列标准。我们在信息化建设过程中，如何正确理解和落实这些法律、法规和技术规范，在实际工作中如何开展涉密信息系统分级保护建设，非涉密信息系统等级保护建设，使建设的系统符合等级保护、分级保护建设规范，是我们应当认真研究的课题。

另外，作者在参与大量的《信息系统安全集成服务资质》审核工作中，发现绝大多数申报企业对信息系统安全集成的过程管理、制度建设、安全集成实现方法、施工质量管理、安全系统测试不熟悉，这不仅影响申报工作的进行，更影响具体项目的施工质量。

作者撰写《信息系统安全集成》的目的，是为了指导信息化建设单位规划自己的信息系统安全建设，指导从事计算机信息系统集成公司，如何按照法律、法规、信息系统安全等级保护、涉密信息系统分级保护相关的规范和标准，开展计算机信息系统项目的需求调研、方案设计、施工管理，保证工程施工质量，使信息系统项目建设符合国家颁布的涉密信息系统和非涉密信息系统的建设规范和标准，实现信息安全保密建设目标；指导信息化建设和应用的管理者，组织本单位的信息化系统建设、施工管理、运行管理，保证信息系统安全、保密、稳定、可靠；对编制信息系统安全集成服务资质申报材料，编制工程实施方案、投标文件中的技术方案，提高投标书的质量，增强市场竞争力都有指导意义；该书

是一部信集化、信息安全工程建设指导类书籍，可以作为信息系统安全保障工程师培训教材，作为信息系统安全工程专业教材使用。

该书分为六章，第一章信息安全概述，第二章信息安全集成准备，第三章信息系统安全方案设计，第四章安全设备测试，第五章工程实施，第六章信息安全管理。该书从信息安全相关法律、法规，到等级保护、分级保护规范标准；从信息安全的需求分析、方案设计，到工程施工组织管理、系统测试、质量控制；从技术保护措施，到安全管理保障措施，全面系统分析了信息系统安全建设工作涉及的方方面面。

第一章概述，分为四节进行分析。第一节对信息安全的基本概念进行了分析，包括信息安全面临的威胁，信息安全含义，信息安全特征，信息安全内容、信息安全实现方法；第二节为信息安全的法律保障，分析国家颁布的保护信息安全的法律、法规、管理制度、体制等；第三节为分级保护制度与等级保护制度，分析我国现行的涉及国家秘密信息系统分级保护建设制度，非涉密信息系统信息安全等级保护制度，等级保护基本框架。对信息安全等级保护标准体系、保护管理体系、保护技术体系、保护等级的定义、保护原则要求、保护等级的适用性等进行了全面分析。第四节为确定安全保护等级，分析国家颁布的信息安全等级保护定级原则和定级指南，指导等级保护建设项目实施前的定级工作，确定建设项目的信息安全等级。

第二章为信息安全集成准备。该章分为两节，系统论述了信息安全需求分析的基本概念，阐述了信息化建设基本情况分析，法律、法规和规范性文件的适用性分析；国家颁布保密、安全相关规范和标准的适用性分析；建设单位的上级主管部门，本地区的信息安全、保密主管部门的分级保护、等级保护建设规划；本级信息化发展规划的安全需求等。

第三章为信息系统安全方案设计。根据 GB 22239—2008《信息系统安全等级保护基本要求》中的技术要求，叙述每一条具体的技术规定，使读者明确国家颁布的信息安全等级保护的基本技术要求内容是什么。针对这些原则性要求，重点分析和论述在项目设计中采取具体安全措施，保证《基本要求》中条款的原则性规定的落实，运用成熟技术手段实现规范条款的原则性规定。文章结构采取陈述《信息安全等级保护基本要求》技术要求条款，与实现这些原则性要求所采取的安全技术措施，对应性进行陈述，使读者更容易理解和执行国家规范的具体技术要求。信息系统安全设计，包括物理安全、网络安全、主机安全、应用安全、操作系统与数据库安全、数据备份与恢复、信任体系等方面。

该章还对信息系统安全方案设计原则，设计文书的编制方法，设计方案的论证评审程序进行了分析。

第四章为安全设备测试。为了使读者了解信息安全设备的评价标准和测试方法，在工程建设中正确选择、检测安全设备，保证信息安全项目建设工程质量，本章分为三节分别对信息安全的常用设备——防火墙、入侵检测系统、安全审计系统的评价与测试方法及内容进行分析和介绍，对建设单位正确选择信息安全设备，施工单位检验施工质量和设备质量，编制设计方案中的测试模板等都有指导意义。

第五章为工程实施。该章分为五节，第一节工程施工管理与组织，系统分析了工程项目施工的组织机构，项目管理制度，施工进度计划等。第二节为施工质量管理，包括信息系统安全集成项目质量管理的概念和影响工程质量的决定因素；质量管理程序；工程质量管理体系，包括质量管理机构，质量管理岗位责任制。第三节质量保证措施，从质量管理

规范性文件、质量保证措施运行、各施工阶段质量保证措施、工序质量控制措施、单项工艺质量控制措施、隐蔽工程质量保证措施、设备材料质量保证措施、工程资料管理质量保证措施等八个方面进行了详细论述。

在信息安全项目的方案设计阶段、工程实施阶段，产生、收集、整理的资料，即工程施工中的质量证明材料，是证明项目实施是否到达工程质量标准，实现信息系统安全目标的主要证据。收集证据证明安全项目建设目标已经实现，是“安全保障阶段”工程施工资料管理的重要任务。对典型资料的编写内容提出了具体要求。

第四节为国际市场产品安全准入与认证。该节通过对全球国际市场公认的产品安全准入制度的分析，了解什么是强制性认证，什么是自愿性认证；介绍世界各国和中国的电气、电子类产品认证标志的含义和认证机构，使读者知晓进口到中国的电气、电子产品是否获得了国际组织认证、国家之间认可的合规的认证，是否符合中国的强制认证。了解国际和国家产品安全准入制度，对正确判断市场化产品质量，正确选择信息系统工程建设中的设备和器材，保证工程质量，具有重要意义。

第五节为项目实施中的保密管理。该节针对具体信息系统安全集成项目实施过程中参与人员的保密管理，保证施工方人员了解、接触和知悉建设单位的国家秘密和工作秘密的保密安全。通过分析保密管理、保密制度建设、保密责任落实等，使读者明确施工过程中的保密管理工作。

第六章为信息安全管理。包括信息安全管理制度建设、安全管理机构、系统建设安全管理和运行管理。按照《信息安全等级保护基本要求》对安全管理的规定逐条进行分析，并结合实际工作提出具体措施要求。在系统建设安全管理中，对项目施工主体资格问题进行了分析，介绍国家现行工程资质种类、承担的工程能力范围，以及从事信息系统安全等级保护、涉密信息系统分级保护工程项目应当具备的资质条件。项目方案设计管理，介绍涉密信息系统、非涉密信息系统方案设计审查方法、流程、法规的强制性规定，介绍信息安全产品选择的强制性规定等。掌握这些知识，这对建设单位组织信息安全项目建设，施工主体开展项目施工都有着积极的意义。

由于该书涉及内容广泛，加之本人水平有限，难免存在错误之处，敬请读者谅解。

张启浩个人简介

张启浩，现任成都市人民检察院技术处正处级检察员、三级高级检察官、高级工程师、成都理工大研究生导师、四川省评标专家库专家、四川省政府采购专家库专家、北京市评标专家库专家、西藏自治区检察院两房建设和信息化专家、最高人民检察院信息人才库专家，中国建筑业协会智能建筑分会第三、四、五届专家工作委员会专家（国家级），国家级刊物《智能建筑》编委会委员，四川省计算机集成行业协会副理事长、专家委主任，中国信息安全认证中心资质评审专家，成都市电子政务内网专家组专家。

在工作中充分发挥自己的技术优势，创新工作机制，推动信息化发展，使成都市检察院信息化建设得到了很大的发展。经过几年的努力，成都市检察院所取得的成绩和经验得到了高检院的充分肯定，多次向全国检察机关转发推广。贾春旺检察长07年5月视察成都市检察院时，高度评价“成都市检察院的信息化工作走在全国检察机关前列”、“达到全国一流”。2011年曹建民视察成都时评价“成都市检察院推行网上办案、绩效量化考核，对推动执法规范化建设具有积极意义，值得借鉴”。

1997年研制成功了寻呼机信息拦截系统，为检察机关的侦查现代化做出了贡献。1999年由青海人民出版社出版的《国魂——跨世纪中华兴国精英大典》一书收编了本人的业绩。

2000年负责规划设计、施工管理本院新办公楼智能化大厦系统。该系统造价近两千万元，是当时西南地区智能化系统规模最大、系统最完善、功能最强大的系统集成。同时负责中央空调、暖通、配电、消防自动报警系统等技术工作。通过对设备配置大量的分析和市场研究，对系统配置进行了调整，重新招标，为检察院挽回资金470万元。

善于研究，把实际工作整理提升撰写成理论文章。近几年来，先后在国家级刊物发表论文42篇，高检院内部刊物转发信息化工作经验、理论文章20多篇，20多篇论文被收集到《中文科技论文数据库》，4条信息化工作经验写进了《全国检察机关信息化发展纲要》，4次在全国性行业发展论坛会上发表学术演讲。编写《全国检察机关会议系统技术培训教材》并授课，参加撰写并出版《智能建筑行业发展报告》一书，2009年获得“美国西蒙杯论文大赛”中国区一等奖，免费前往印尼参加亚太地区国际学术交流。

2005－2006年被最高人民检察院聘请为建筑智能化专家，参加国家重点过程－最高人民检察院办公大楼智能化系统工程建设，从事智能化系统（造价6000万）的规划、设计、编制招标文件、施工管理等，同时还负责配电、暖通系统的技术工作，为高检院大楼建设做出了很大贡献，受到最高检察院张耕常务副检察长和胡克惠副检察长等领导高度评价，受到最高检察院贾春旺检察长的亲切接见。

2006年至08年，组织研发《集中式检察业务综合应用动态管理系统》（办案软件）、《检务保障软件》、《综合绩效考核软件》，这些软件的研发和推广应用，极大地推动了成都市检察机关信息化的发展。

近几年，先后指导最高人民检察院、贵州省院、西藏自治区院、四川省院、江苏省院、武汉市院、长春市院、云南省院等十多个省检察院新办公大楼智能化建设；作为四川省评标专家和政府采购评审专家，参加全省工程项目评标上两百多次；参加国家大型重点工程——北京奥运会、广州亚运会、海南博鳌国际论坛等国家大型工程建设项目的论证、评审。

自 2008 年以来被“中国建筑业协会智能建筑专业委员会”选拔为第三、四、五届专家工作委员会专家，信息网络专业组副组长。该专家组是我国建筑智能化行业最高权威机构，是住房与城市建设部的智囊团，为国家制定工程技术标准，规划、指导、咨询国家重点工程建设，开展学术交流。2008 年以来连续四届被国家级刊物——《智能建筑》出版社聘为编委会委员。

2006 年参加全国检察机关信息化该系统建设规范的制定，2009 参与国家标准—《智能建筑工程施工规范》，2014 年参加四川省《智能建筑设计规程》、《智能建筑施工工艺规程》制定工作。

自转业以来，五年被评为先进工作者、优秀公务员、人民满意检察官，4 次被评为优秀党员，荣立三等功一次。集体三等功一次，2009 年 10 月获得“第四届美国西蒙杯论文大赛一等奖”前往印尼参加亚太地区国际学术交流。2009 年 12 月获得《智能建筑》优秀论文奖。2012 年被评为成都市“十佳检察干警”，2013 年被授予“中国智能建筑行业突出贡献专家”（全国共 30 名）。

联系电话：13908017943　028-87782109
地　　址：成都市菊乐路 216 号成都市人民检察院技术处

目　录

第一章 概 述

第一节 信息安全的基本概念

随着信息技术的发展和广泛应用，人们通过网络获取大量的有用信息，包括政治、经济、军事、科技、贸易、教育与学习、工业、农业，特别是行业纵向网络，通过信息化的应用开展行业的业务生产。互联网、物联网给人们的生产生活带来极大方便，快捷、高效和便利。网络把全国性的集团变成了一个小单元，互联网把全球变成了地球村。网络给人们学习、生产、生活带来便利，对人类经济、社会的发展起到了积极的促进作用。网络在给人类社会带来日新月异变化的同时，也正面临着越来越多的安全问题。

随之而来的无形的安全威胁、安全风险涉及每个局域网、每个应用系统、每台个人应用终端。国家的信息安全保密，企业的信息安全，公民的个人信息安全，各行业的信息都受到威胁和挑战。因此，人们不得不重视网络信息安全。

一、信息安全面临的威胁[1]

根据国家互联网应急中心（以下简称 CNCERT/CC）发布的 2014 年、2015 年《中国互联网发展状况与安全报告》指出，当前对主要网站的网页篡改、网站后门、拒绝服务攻击等进行全面的监测，并且对漏洞、仿冒等网站信息系统和网站用户造成高风险威胁的情况进行检测。从监测整体情况看，针对网站攻击仍然是当前黑客主要攻击目标。2012 年以来，互联网黑客地下产业仍然较为活跃，针对中国互联网站的篡改、后门攻击事件数量呈现逐年上升趋势，政府网站是攻击的重要目标。黑客地下产业以获取利益为目的特点日趋明显，以网络欺诈、讹诈为代表的拒绝服务攻击以及仿冒网站的行为是黑客重要的得利渠道。信息系统漏洞，特别是高危漏洞呈现逐年递增趋势，这给黑客发起大规模网络攻击或针对重要价值目标发起攻击提供了便利条件。网站信息系统所承载的数据机密性、服务可用性、信息完整性受到严重的威胁，影响到网站的服务体验和用户上网安全。具体的攻击行为、特点、数量、来源分析如下：

（一）篡改网站攻击行为数量逐年增长

据中国互联网应急监测中心报告，截止 2014 年底中国的互联网站总数达到 364.7 万个，中国网站遭受篡改攻击数量逐年增多，2013 年被篡改的中国网站数量为 2.4034 万个，比上年度增长 46.7%。被篡改的中国网站，商业机构的网站（.com）最多，占 67.2%；其次是政府类（.gov.cn）网站和网络组织类（.net）网站，分别占 10.1%和 6.4%；非盈利组织类（.org）网站和教育机构类（.edu.cn）网站分别占 1.9%和 0.4%。

2014 年我国境内被篡改网站的数量为 3.6969 万个，较 2013 年大幅增长 53.8%，其中政府网站 1763 个，较 2013 年下降 27.4%。对政府网站实施篡改攻击后，除植入异常页面破坏政府形象或植入暗链进行广告推广以外，还出现了一些植入钓鱼页面的现象。

政府网站受到暗链植入攻击威胁较大。2013 年中国政府网站被篡改的数量达到 2430 个，较上年度增长 34.9%，占 CNCERT/CC 监测的政府网站类别总数的 4.0%。2013 年我国境内被篡改的政府网站中，以植入暗链方式被攻击的占 57%，被篡改的 41.8%。政府网站更容易遭受植入暗链的攻击。

（二）安全漏洞是诱发篡改网站和后门攻击的原因

1. 系统漏洞是诱发网站被篡改和后门攻击的主要原因

大多数针对网站的篡改和后门攻击等网络安全威胁都是由网站信息系统所存在的安全漏洞诱发的，漏洞数量呈逐年递增态势。

由 CNCERT/CC 主办的国家信息漏洞共享平台收录信息系统安全新增漏洞数量，近三年来年均增长率在 15%～25%之间。2013 年 7854 个，2014 年 9163 个，平均每月新增收录漏洞 763 个。其中高危漏洞 2394 个，占 26.1%，可诱发“零日攻击”的漏洞（即披露时厂商未提供补丁）3229 个，占 35.2%。

2. 应用软件和 WEB 应用漏洞占较大比例

应用程序类漏洞占 68.5%，WEB 应用漏洞占 16.1%，网络设备漏洞占 6.0%。涵盖 Microsoft、IBM、Apple、WordPress、Adobe、Cisco、Mozilla、Novell、Google、Oracle 等厂商的产品。

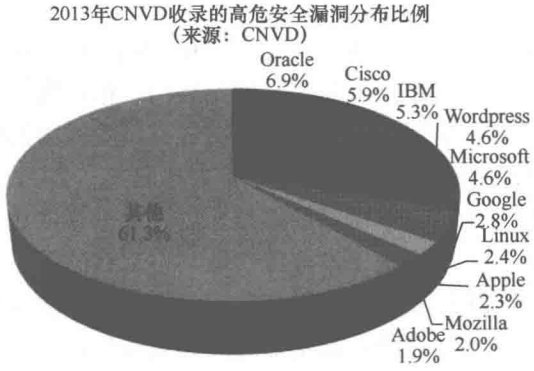


图 1-1 2013 年收录的高危安全漏洞分布各企业占比情况图

各厂商产品中高危漏洞的分布情况如图 1-1 所示，可以看出，涉及 Oracle 产品的高危漏洞最多，占全部高危漏洞的 6.9%。

2014 年国家信息安全漏洞共享平台共向政府机构和重要信息系统部门通报漏洞事件 9068 起，向软硬件厂商通报处置通用漏洞事件 714 起，为漏洞防护发挥了一定的作用。

2014 年“心脏滴血”“破壳”等漏洞先后爆发，其所涉及的均为互联网基础应用或协议，范围十分广泛，因此漏洞危害级别非常高，影响范围波及整个互联网。如 2014 年 9 月 25 日，GNU Bash 组件被披露存在远程代码执行漏洞，该组件是一个命令解释器，广泛应用于目前所有主流 UNIX/Linux 操作系统平台以及 OpenSSH、Apache、DHCP 和其他使用 Bash 作为解释器的应用。我国直接受到上述漏洞影响的服务器数以万计，影响数万甚至上亿数量级用户。

（三）被置入后门的网站数量比例很大

网站后门是黑客成功入侵网站服务器后设置的后门程序。通过在网站的特定目录中上

传远程控制页面，黑客能够暗中对网站服务器进行远程控制，窃取、查看、修改、删除网站服务器上的文件，读取并修改网站数据库的数据，甚至能够直接在网站服务器上运行系统命令。

1. 被植入后门网站数量2013年大幅上升，2014年有所下降

CNCERT/CC共监测到境内中国网站被植入网站后门的数量很大，2013年7.616万个，较上年大幅增长46%，其中政府网站有2425个。2014年为4万余个，较2013年下降47.2%，其中政府网站为1529个，较2013年下降36.9%。从域名类型来看，2013年被植入后门的网站中，商业机构类的网站（.com）最多，占61.46%；其次是网络组织类网站（.net）占5.87%；政府类（.gov.cn）网站占5.76%。

2. 黑客攻击呈现组织性和计划性，采用方式较多的仍然是网页篡改和植入后门

2014年1.9万余个境外IP地址通过植入后门对境内3.3万余个网站实施远程控制，境外控制端IP地址和所控制境内网站数量分别较2013年下降37.8%和45.3%。2014年我国政府网站频繁遭受黑客组织攻击，从攻击方式来看，黑客组织采用较多的仍然是网页篡改和植入后门，并体现了黑客攻击的组织性和计划性。另外还存在其他的特点，2014年出现针对政府网站的拒绝服务攻击、窃取并公布网站信息等攻击，影响网站正常运行，造成网站信息泄露，对政府网站的攻击方式日趋多样化复杂化；此外，从一些黑客组织公布的信息来看，不仅攻击目标的URL链接，还包括网站服务器类型、服务器IP地址等信息。

3. 后门攻击源主要来自境外IP

根据CNCERT/CC监测，2013年向中国网站实施植入后门攻击的IP地址中，有3万余个位于境外，其中，位于美国的6215个IP地址（20.2%）共向我国境内1.5349万个网站植入了后门程序，侵入网站数量居首位。其次是印尼（11.4%）和韩国（6.5%）等国家和地区。2014年监测的数据，后门植入数量4万余个，位于美国的4761个IP地址通过植入后门控制了我国境内5580个网站，入侵网站数量居首位。

具体分布情况如图1-2所示。

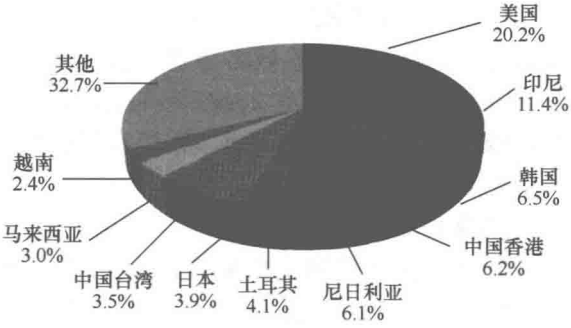


图1-2　2013年向中国网站植入后门的境外IP地址分布图

（四）黑客攻击网站的行为形成地下产业

目前针对网站的大规模攻击情况主要有拒绝服务攻击、扫描探测攻击等。拒绝服务攻击主要目的是瘫痪网站服务，造成对业务可用性的影响，主要手段是通过构造大流量或特定结构的网络数据包消耗目标主机系统或网络资源；扫描探测攻击主要是指黑客在窃取信息或其他攻击目的而进行的前期信息收集或发现漏洞发起针对特定目标或互联网大规模目标的攻击行为。

拒绝服务攻击的危害有三大特点：

一是黑客形成地下产业化。产业化的主要表现为黑客开发的大规模部署的攻击工具，

有目的、有手段、有计划地开展攻击活动，这比个体黑客的单个攻击行为危害更大。2013年，CNCERT/CC监测到活跃的典型DDoS工具攻击事件控制服务器IP数量为11650个，其中位于我国境内的IP数量为3607个，约占全部控制服务器的31%，位于美国和韩国的控制服务器IP地址数量分别居第2、3位。

二是发起攻击的数据量特别大。根据CNCERT/CC抽样监测数据显示，2013年平均每天发生攻击流量超过1Gbit/s的攻击事件1802起，较2012年增长76%。

三是漏洞成为发起网站攻击的直接“导火索”。针对漏洞攻击情况，CNCERT/CC联合知道创宇、安全宝、奇虎360等国内安全企业，对各企业建立的网站服务平台的网站攻击情况进行了监测。360网站卫士共拦截各类网站漏洞攻击1.21亿次，平均每天拦截35万次；知道创宇公司2013年通过加速乐平台检测到受攻击的平台用户站点数量为7万多个，其中攻击次数为7000多万次，其中境外攻击次数占比93.4%；安全宝公司2013年共拦截针对安全宝网站服务平台用户网站的攻击近3亿次。

（五）网络欺骗行为——网络钓鱼对社会的危害更大

网页仿冒俗称网络钓鱼（Phishing），是一种利用社会工程学及互联网技术，旨在窃取上网用户的身份信息、银行账号密码、虚拟财产账户等信息的网络欺骗行为。网页仿冒具有很强的欺骗性，上网用户一旦受骗，损失很大，对社会的影响也很大。储蓄用户受骗会使自己蒙受重大经济损失，影响社会稳定和银行的信誉。假冒中央电视台会使公民遭受经济和其他损失，同时损害中央电视台名誉。

1. 大多数仿冒网站服务器位于境外

2013年，CNCERT/CC共监测发现仿冒中国网站的仿冒页面URL地址3万余个，涉及域名1.8万个，这些域名分别解析到境内外4240个IP地址，有90.2%位于境外，其中IP地址位于美国的有2043个，占总量53.4%。从钓鱼站点使用域名的顶级域分布来看，以“.COM”最多，占51.1%，其次是“.TK”和“.NET”，分别占16.8%和8.3%。

2. 仿冒页面数高速增长

2014年国家互联网应急中心监测发现针对我国境内网站的仿冒页面（URL链接）99409个，较2013年增长2.3倍，涉及IP地址6844个，较2013年增长61.4%，平均每个IP地址承载约14个仿冒页面。国家互联网应急中心全年接收到网页仿冒类事件举报17873起、处置事件17926起。

3. 金融、传媒和支付类网站成为仿冒重点目标

仿冒网站给境内用户带来经济上的重大损失，其中一些仿冒网站抓住用户的侥幸心理，以利诱方式诱惑互联网用户。知名度较大的传媒、金融、支付类机构容易成为仿冒网站仿冒的目标，针对第三方支付机构的仿冒页面最多。网页仿冒与移动应用越来越紧密，2014年发生多起仿冒网银、微信等移动应用（APP）的事件，这些仿冒应用内嵌钓鱼网站，欺骗用户提交银行卡号、有效期、CVV码、身份证号等关键信息，同时还可拦截用户短信，窃取网银交易或支付验证码信息，导致用户资金损失。

被仿冒次数超过百次的有：中央电视台、中国工商银行、中国银行、中国建设银行、招商银行、中国农业银行、中国邮政储蓄银行、腾讯公司等机构的网站。2013年这些机