信息安全技术丛书

信息系统安全等级保护实务

主　编　李　超
副主编　李秋香　何永忠

科学出版社

信息安全技术丛书

信息系统安全等级保护实务

主　编　李　超
副主编　李秋香　何永忠

科学出版社
北　京

内 容 简 介

本书系统、全面地介绍了信息系统安全等级保护的基本概念、实施流程和建设整改的方法。全书共15章，分为三个部分。第一部分简要介绍信息系统安全等级保护的基本概念，以及实施等级保护的全部流程；第二部分从信息系统安全等级保护建设者的角度对定级与备案、建设与整改、测评、检查等各环节的重点和难点进行了具体分析与论述，特别是从管理与技术两个方面详细讲解了信息系统安全等级保护建设、整改的具体实施方法；第三部分给出一个信息系统安全建设整改的实例，帮助读者实现从理论方法到具体实践的跨越。

本书适合作为信息系统安全等级保护设计、建设、运营和管理等相关专业人员的培训教材，也可作为信息安全专业安全等级保护类课程的教材。

图书在版编目（CIP）数据

信息系统安全等级保护实务/李超主编. —北京：科学出版社，2013
（信息安全技术丛书）
ISBN 978-7-03-035462-4

Ⅰ.①信… Ⅱ.①李… Ⅲ.①信息系统-安全技术 Ⅳ. ①TP309

中国版本图书馆CIP数据核字（2012）第205669号

责任编辑：张 濮 马晓晓/责任校对：刘小梅
责任印制：张 倩/封面设计：迷底书装

科学出版社出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com

骏走印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2013年3月第 一 版 开本：B5（720×1000）
2013年3月第一次印刷 印张：19
字数：383 000

定价：72.00元

（如有印装质量问题，我社负责调换）

编写委员会

主　编： 李　超

副主编： 李秋香　何永忠

成　员： 黎　琳　吴　薇　浮　欣　徐晓军
王海珍　吕　由　张彬彬　秦　超
湛高峰　刘志宇　沈孝东　印晓天
陈　思　程　楠　范　博　侯晓雄
于　灏　蒋　雯　崔宁宁　赵娉婷
王秋平　刘　军

序

随着科学技术特别是信息技术的突破式发展，社会信息化的速度也在飞速提升。然而，信息化在给人们带来极大便利与利益的同时，信息安全事件的频繁出现，越来越引起人们的严重关切。网络与信息安全不仅关系着国家安全和社会稳定，并且与人们日常生活息息相关。为有效应对网络和信息安全领域日益严峻的挑战，我国政府和社会各界已经并正在采取一系列重大措施。信息安全等级保护，就是我国为加强信息安全保障工作确立的一项基本制度和重要措施，它将政府部门监管与社会各界参与紧密联系起来，将信息安全管理与技术防范手段密切结合起来，将风险评估理论与持续改进的实践融合起来。近几年，网络和信息安全形势发生了重大变化：一方面，信息安全等级保护及相关一系列措施的实施，有效地加强和促进了我国的信息安全保障工作，有许多宝贵的经验值得总结；另一方面，由于国际上网络空间（cyber space）理论出台而引发的一系列新事态使信息安全形势愈加严峻，有不少迫切问题急需探索。这本书就是在这种新形势下应运而生的。

该书的编者都是我熟悉的教授、专家和研究人员，他们长期在信息安全领域进行着大量的理论研究和应用实践，掌握了信息安全领域的系统知识，有着丰富的实践经验。该书由浅入深系统地介绍了信息安全及信息系统安全等级保护工作的基本概念，信息安全相关法规制度与标准，结合具体实例介绍了等级保护工作实施流程以及工作中可能遇到的实际问题。该书还着重对信息系统运营、使用单位在信息系统定级、备案、等级测评、建设整改、监督检查等工作环节中的具体工作内容进行了阐述。该书后面给出了一个信息系统运营、使用单位开展信息安全等级保护工作的实例，对相关单位开展信息安全等级保护工作具有很好的借鉴意义。

网络与信息安全是一场持久、复杂的斗争，等级保护工作是一项基本制度，也是一项长期、艰巨的任务。希望和信息安全同事们一起，共同在阅读该书中获益，并不畏困难、不断探索，为国家信息安全保障工作做出新努力。

崔书昆

2013 年 3 月

前　言

目前，我国信息安全面临着非常严峻的形势。为了进一步提高信息安全的保障能力和防护水平，维护国家安全、公共利益和社会稳定，保障和促进信息化建设的健康发展，国务院发布的《中华人民共和国计算机信息系统安全保护条例》制定了“计算机信息系统实行安全等级保护”的政策，之后国家出台了一系列相关的法规、标准和指南，对等级保护工作的各个方面提出了具体要求。信息系统安全等级保护是能够有效保障我国信息系统安全的强制性制度安排，对提高我国信息安全保障水平、完善信息安全保障体系具有重要的意义。但由于相关文件体系复杂、内容较为抽象，如何在实践中准确理解等级保护的要求，并针对本单位的实际情况有效开展工作以满足等级保护的要求，存在很多现实的困难，并成为大家非常关注的问题。

1. 目标

本书是从信息系统建设与运营人员的实际需要出发，全面、系统介绍如何有效实施信息系统安全等级保护的实用教程，以从事信息系统安全设计、建设、运营工作的技术人员、运维人员和管理人员为读者对象，围绕为什么需要信息系统安全等级保护、实施安全等级保护的业务流程以及如何具体实施安全等级保护等问题展开论述。通过阅读本书，相关专业人员可以在对等级保护的整体实现、实施流程和具体方法有全面理解的基础上，针对实际系统需求，有效开展信息系统安全等级保护的设计、建设和运营工作。

2. 内容安排

全书共 15 章，分为三个部分。

第一部分包括第 1 章和第 2 章，简要介绍信息系统安全等级保护的基本概念，以及实施等级保护的全部流程。第 1 章对信息系统安全等级保护进行概述，主要介绍等级保护的目的、意义和相关法律法规，并简要说明等级测评的标准；第 2 章介绍等级保护的实施过程，从整体上说明信息安全工程等级保护的实施流程，包括系统定级与备案、总体规划、安全设计与实施、运行与维护等。

第二部分包括第 3～14 章，从信息系统安全等级保护建设者的角度对定级与备案、建设与整改、测评、检查等各环节的重点和难点进行具体分析与论述，特别是从管理与技术两个方面详细讲解了信息系统安全等级保护建设、整改的具体实施方法。第 3 章介绍信息系统的定级与备案，包括定级的原则、方法和备案的主要工作。第 4～12 章介绍信息系统安全等级保护建设整改阶段的主要实施方

法。第 4 章是方法论，介绍建设整改的分析与设计方法。第 5 章和第 6 章介绍等级保护管理建设方法，分别从组织结构、管理制度体系、人员安全管理方面介绍等级保护管理体系的建设，并从系统建设阶段和运维阶段的安全等级保护介绍信息系统生命周期的管理实务。第 7～11 章介绍等级保护技术建设方法：第 7 章介绍物理安全技术实施的内容，从环境物理安全建设、基本设备物理安全建设、智能设备物理安全建设三个层面出发来描述物理安全建设的完整过程；第 8 章介绍了以安全域划分为依托，访问控制、安全审计、入侵防范等为手段的网络安全技术，从各个层面来保障网络安全技术的实施；第 9 章针对主机安全技术的设计和实施做出了详细描述，着重从主机安全的各个层面进行介绍，并给出了具体设计的实例；第 10 章和第 11 章主要介绍应用安全和数据安全两方面内容，分别从各自的技术层面对它们所面临的风险、目标以及所对应的技术措施进行介绍。第 12 章分析了三级以上信息系统安全关键技术实施的难点，介绍了三级信息系统等级保护环境设计方法和基本模型。第二部分最后两章简单介绍了等级保护流程的测评与检查两个环节的工作实务：第 13 章介绍信息系统安全等级测评的发展过程、相关标准体系和测评工作内容，以及对信息系统进行风险评估的相关流程、分析方法和评估工具等；第 14 章介绍等级保护检查的相关方法和要求。

第三部分是第 15 章，给出一个信息系统安全建设整改的实例，帮助读者实现从理论方法到具体实践的跨越。

3. 本书特色

在撰写本书过程中，我们力求做到以下几点。

（1）内容全面，重点突出：在论述等级保护整个过程的同时，根据读者实际需要，着重介绍定级备案、建设整改等内容。

（2）语言通俗，图文并茂：书中采用大量表格和流程图，使内容更加清晰、易懂。

（3）面向实践，实例丰富：包括各种大小实例，与实践紧密结合，生动且便于理解。

4. 阅读建议

建议读者可以按以下顺序安排阅读。不了解等级保护背景、基本流程的读者，首先需要通读第 1 章和第 2 章的内容。其他章节的内容可根据实际工作需要阅读。各章内容相对独立，阅读的顺序不会影响对相关章节的理解。其中，第 4 章是建设整改的方法论，第 12 章是难点问题分析，等级保护的系统设计者应详细阅读；第 13 章是等级保护测评工作的简单介绍，等级保护的建设人员只需要了解即可；第 15 章是实例，可以结合前面各章节的内容阅读。

本书由李超担任主编，李秋香、何永忠担任副主编。参与本书资料搜集整理和写作的人员还有黎琳、蒋雯、赵娉婷、崔宁宁、刘军、王秋平等同志。感谢所

有为本书的写作提供帮助的人员，特别要感谢赵战生教授、刘海峰同志、王新杰同志、侯晓雄同志和北京益安信息安全技术培训中心，他们在本书写作过程中多次给予具体指导，提出了很多宝贵的意见。本书的编写和出版还得到国家发展和改革委员会信息安全服务专项“重要信息系统安全测评与评估服务”项目和“重要信息系统等级保护专业化服务”项目的支持，在此表示感谢！

由于作者水平有限，书中难免有疏漏之处，恳请广大读者批评指正。

作　者

2012 年 12 月

目　录

第1章 概 论

1.1 等级保护的目的和意义

近年来，随着我国经济的持续发展和国际地位的不断提高，国民经济和社会发展的信息化进程全面加快，信息网络覆盖率越来越高，网络的利用率也稳步提高。在关系国计民生的重要领域，信息系统已经成为国家的关键基础设施，这对我国信息化建设提出了新要求。

根据《2011年中国互联网网络安全态势报告》，基础网络防护能力虽然明显提升，但安全隐患仍不容忽视。例如，涉及基础电信运营企业的信息安全漏洞数量较多。据国家信息安全漏洞共享平台(China National Vulnerability Database，CNVD)统计，2011年发现涉及电信运营企业网络设备(如路由器、交换机等)的漏洞203个，其中高危漏洞73个；发现直接面向公众服务的零日DNS漏洞23个，应用广泛的域名解析服务器软件BIND9漏洞7个。这些数据表明，涉及基础电信运营企业的攻击形势依然严峻。另据国家计算机网络应急技术处理协调中心(National Computer Network Emergency Response Technical，CNCERT)监测，2011年每天发生的分布式拒绝服务(Distributed Denial of Service，DDoS)攻击事件中，平均约7%的事件涉及基础电信运营企业的域名系统或服务。根据调查和研究发现，我国部分网站的用户信息仍采用明文的方式存储，相关漏洞修补不及时，安全防护水平较低。此外，我国遭受境外的网络攻击持续增多，网上银行面临的钓鱼威胁愈演愈烈，手机恶意程序呈现多发态势，木马和僵尸网络活动越发猖獗，应用软件漏洞呈现迅猛增长趋势，DDoS攻击仍然呈现频率高、规模大和转嫁攻击的特点。360安全中心发布的研究数据表明，2011年我国受恶意程序攻击的电脑数量呈上升趋势，如图1-1所示。

2011年，国内外发生的安全事件引起了广泛的关注，造成了很大的影响。例如，国内多家银行网银用户遭到大规模钓鱼攻击，损失巨大；RSA遭黑客攻击，主流身份认证产品SecureID的重要信息泄露，导致美国多家军工企业信息系统受到严重威胁；LulzSec成功袭击了美国中央情报局、美国参议院、任天堂、索尼等多家机构，引起国际社会广泛关注；DigiNotar、Comodo等多家证书机构遭到攻击，攻击者得以伪造Google、Live、Gmail、Skype等多家知名网站证书，使互联网安全遭遇严重威胁，导致DigiNotar公司宣布破产；韩国农协银行遭遇攻击，导致系统长时间瘫痪和大量交易数据丢失；腾讯网大面积访问异

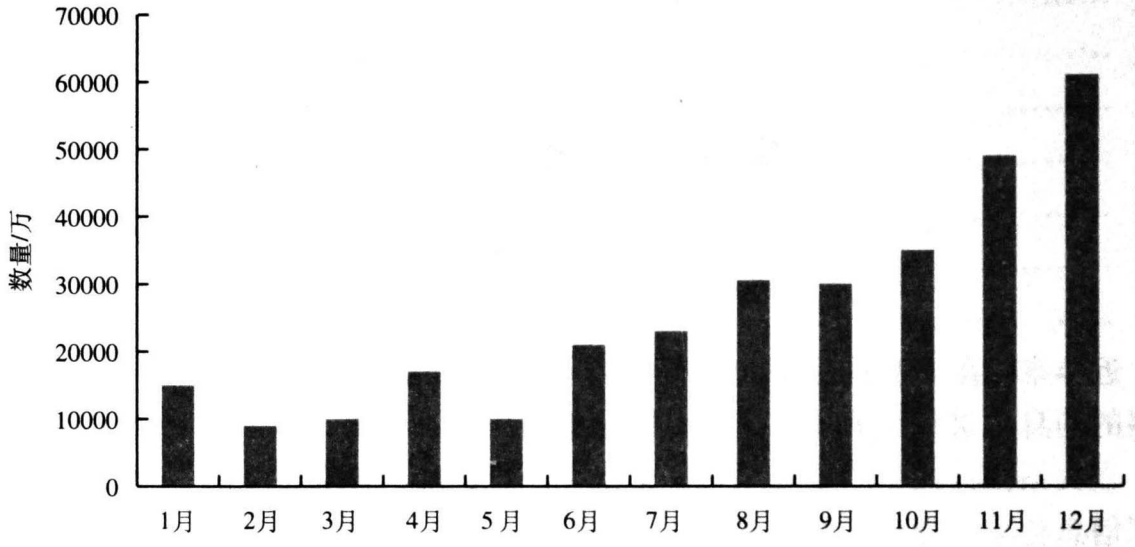

图 1-1 2011 年受恶意程序攻击的电脑数量

常；新浪微博病毒大范围传播；花旗银行网站遭遇黑客，20 万信用卡用户信息被盗；维基泄密事件中加密数据包密钥意外泄露，导致大量情报人员身份泄露等。信息安全事件的不断发生，凸显了信息安全的重要性。从最高层次来讲，信息安全关系到国家的安全；对组织机构来说，信息安全关系到组织机构的正常运作和持续发展；就个人而言，信息安全是保护个人隐私和财产的必然要求。

从总体上看，我国基础信息网络和重要信息系统安全面临的形势十分严峻，既有外部威胁，又存在自身的脆弱性和薄弱环节，威胁分类如图 1-2 所示。例如，不法分子利用一些安全漏洞，使用病毒、木马、网络钓鱼等技术进行网络盗窃、网络诈骗等违法犯罪活动，对我国的经济秩序、社会管理秩序和公民的合法权益造成严重侵害。由于我国的信息安全保障工作尚处于起步阶段，很多基础信息网络和重要信息系统的核心设备、技术和高端服务主要依赖国外进口，在很多技术方面不能实现自主控制，这就造成了基础信息网络和重要信息系统安全技术隐患。此外，我国在信息安全保障工作方面本身基础还很薄弱，信息安全意识和安全防范能力薄弱，信息系统安全建设和监管缺乏依据和标准，安全保护措施和安全制度不落实，监管措施不够到位。因此，进一步加强信息安全保护工作不仅是实现国家对重要信息系统重点保护的重大措施，也是一项事关国家安全和社会稳定的政治任务。

信息安全保护工作必须符合社会的发展规律。例如，各企事业单位的信息系统是根据社会发展、社会生活和工作的需要而设计和建立的，是社会发展的重要战略资源，是社会构成、行政组织体系的反映。这种体系是分层次和分级别的，与其对应的各种信息系统在社会和经济价值方面也具有不同的等级，客观上体现为系统基础资源和信息资源的价值大小、用户访问权限的大小、大系统中各子系

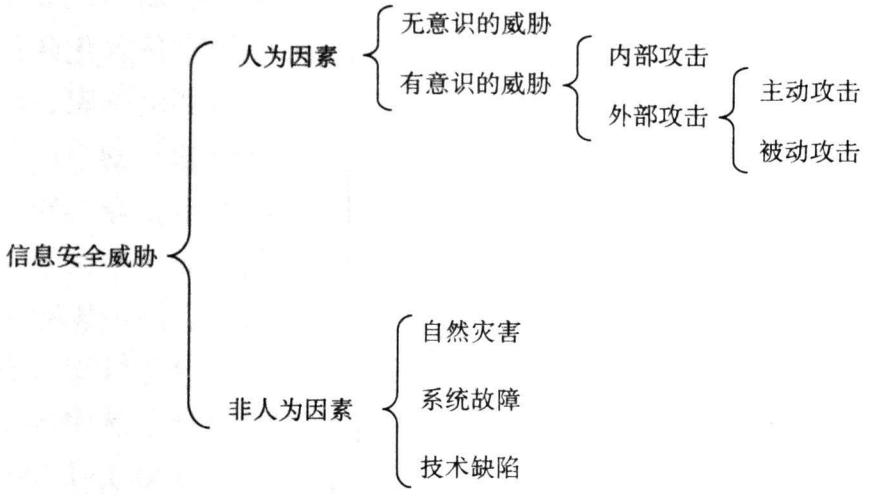

图 1-2 信息安全威胁的分类

统重要程度的区别等表现因素。可见，科学的分级、分区域、分类和分阶段的开展信息安全保护工作符合社会发展的客观规律。

近年来，党中央、国务院对信息安全高度重视，在各有关方面的共同努力下，我国的信息安全工作取得了很大进展。随着以互联网为代表的信息技术逐渐融入社会生活的各个方面，并在全球范围内产生越来越深远的影响，信息安全也逐渐受到国家的重视。国务院常务会议中，讨论通过了《关于大力推进信息化发展和切实保障信息安全的若干意见》，确定了多项重要信息化工作，其中就包括健全信息安全防护与管理等内容。会议的成功召开，使信息安全问题再次成为社会各界关注的焦点，构建自主可控的信息安全保障体系已迫在眉睫。当前，我国政府负责安全工作的部门对于密码、涉密网络与公共网络隔离、信息化安全技术、产品和服务进行测评认证和市场准入，这些措施实质上是代表国家提出的安全要求。

为进一步提高信息安全保障能力和防护水平，维护国家安全、公共利益和社会稳定，保障和促进信息化建设的健康发展，国家出台了一系列的政策措施。1994 年，国务院颁布的《中华人民共和国计算机信息系统安全保护条例》(国务院 147 号令)中规定，“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”；2003 年，中央办公厅、国务院办公厅转发的《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27 号)明确指出，“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”；2004 年，由公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合转发的《关于信息安全等级保护工作的实施意见》(公通字[2004]66 号)中再次强调，“信息安全等级保