“十二五”
国家重点图书出版规划项目

学术中国 · 院士系列

未来网络创新技术研究系列

信息系统安全等级化保护原理与实践

沈昌祥　张鹏　李挥　刘敦伟　赵林欣　刘京京　刘冶　编著

Principles and Practices of Classified Protection of Information System Security

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS

"十二五"
国家重点图书出版规划项目

学术中国 · 院士系列

未来网络创新技术研究系列

信息系统安全等级化保护原理与实践

■ 沈昌祥 张鹏 李挥 刘敦伟 赵林欣 刘京京 刘冶 编著

Principles and Practices of Classified Protection of Information System Security

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

信息系统安全等级化保护原理与实践 / 沈昌祥等编著. -- 北京 : 人民邮电出版社, 2017.3
（学术中国. 院士系列. 未来网络创新技术研究系列）
ISBN 978-7-115-45012-8

Ⅰ. ①信… Ⅱ. ①沈… Ⅲ. ①信息系统－系统安全性－研究 Ⅳ. ①G202

中国版本图书馆CIP数据核字(2017)第075493号

内 容 提 要

本书从等级化管理的历史出发，描述了等级化保护的现状以及今后的发展方向：随后从等级化安全保障体系和等级保护对象两个角度分别进行阐述。具体解析了等级化安全保障体系的结构以及框架，探讨了等级保护安全体系设计的方法原则，并详细介绍了安全组织体系设计；同时，对保护对象的分类和如何保护进行了详细说明；接着，从等级保护的策略体系、技术体系以及运作体系3个方面分别着手，介绍了3种体系的主要内容、设计方法以及具体流程。

◆ 编　著　沈昌祥　张　鹏　李　挥　刘敦伟
　　赵林欣　刘京京　刘　治
责任编辑　代晓丽
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
固安县铭成印刷有限公司印刷

◆ 开本：700×1000　1/16
印张：　22.5　　2017年 3月第 1版
字数：　441千字　　2017年 3月河北第1次印刷

定价：128.00元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

前 言

为什么要写这本书？

随着通信技术、计算机技术和网络的发展，网络用户与日俱增，且全球数据量呈现爆炸式增长。而信息化蓬勃发展的同时信息安全问题也越来越严重。在信息全球化的世界，信息安全已经成为国家安全的一个非常重要的组成部分，并占有举足轻重的战略地位，对国家经济安全、金融安全、国防安全、政治安全和文化安全都起到了重要作用。

等级保护是国家信息安全保障体系中的一项基础性、制度性工作。自《国家信息化领导小组关于加强信息安全保障工作的意见》明确提出“实行信息安全等级保护”制度以来，国家主管部门陆续发布了一系列相关政策法规，推进信息安全等级保护工作的落实。

但是，等级保护的概念自 20 世纪 90 年代被提出以后，一直未能得到有效实行。其中的一个主要原因是等级保护的概念和安全要求复杂，如果没有专业的安全知识和能力，用户很难将其执行，这就造成了等级保护存在很高的技术门槛，难以在普通用户中推广实现。

在传统的安全保障体系设计中，重点强调两个方面：一是强调安全保障的深度；二是强调安全保障过程的完整性。依据这两种模型所构建的安全保障体系都能够实现对信息系统的保护，但是这些模型都存在一个重要问题，就是安全保障体系的设计仅针对防护措施构建，而没有考虑到保护对象对安全措施的需求，重要信息系统和一般信息系统在安全保障上如何区别实现。那么怎样才能将这两点与等级保护更好地结合在一起呢？如果等级保护和这两个模型不能有机地结合，不但不能做到安全的差异性和针对性保护，实现安全的精细化管理，反而会给网络信息资源和信息安全带来巨大的灾难。

信息系统的差异性，使其安全要求的属性和强度存在较大差异性；又出于经济性的考虑，需要考虑信息安全要求与资金人力投入的平衡。设计安全保障措施时不能“一刀切”，必须考虑差异性和经济性。一个信息系统需要安全措施的强度，与该系统所承担的业务职能和系统的重要性有关。因此，将保护对象的重要程度

纳入安全保障体系设计，通过定义信息系统的安全等级、相应安全措施的等级，构建等级化安全体系，是完善信息安全保障体系设计的一种有效方法。

在等级化信息安全保障体系中，依据等级保护方法给信息系统划分系统安全等级，再根据安全等级确定适当等级的安全措施，达到适度安全，才能真正做到合理的安全防护。这里面，分级分类是等级保护中的关键，如果分级分类不科学，就不可能采取适度安全的保障措施，有可能盲目地浪费资源，也有可能达不到目的。等级保护体系又是一个循环的过程，在建立起一个有效的、持续性的验证方法后，确保信息系统在不断发展的同时保障安全等级要求，并且通过进行不断检查，反复验证安全的可靠性。

当前，到了信息安全等级保护 2.0 的时代，等级保护理论和实践有了重大突破和进展，特别是云计算和大数据的兴起对等级保护的实施提出了新的要求和挑战，我们要进一步了解网络空间的新特点和新趋势，从而更好地做好信息系统的等级保护工作。

作为一名信息安全领域的专家，一直希望能为信息安全等级保护的实施做些有意义的工作，为贯彻落实等级化保护制度提供一些理论方面的分析和实践方面的指导。

这本书到底写了什么？

本书内容从等级化管理的历史出发，描述了等级化保护的现状以及今后的发展方向，说明了等级保护已经从一种专门用于军事领域的技术思想发展为现在几乎贯穿了信息安全保障方方面面的制度。随后从等级化安全保障体系和等级保护对象两个角度分别进行阐述，具体解析了等级化安全保障体系的结构以及框架，探讨了等级保护安全体系设计的方法原则，并详细介绍了安全组织体系设计，同时也对保护对象的分类和如何保护进行了详细说明。接着，本书从等级保护的策略体系、技术体系以及运作体系 3 个方面分别着手，介绍了 3 种体系的主要内容、设计方法以及具体流程。

等级化保护要立足于需求和现状来实现。于是本书从国家对信息安全等级保护的基本要求和规范着手，详细解读了国家在这方面的要求，帮助读者更好地理解国家信息安全等级保护策略。接着研究了综合评价指标体系建立的基本原则和一般流程，结合了定性定量两种方法，把各种要素有机融合，给出了一个系统定级量化计算方法。

接着对信息安全等级保护风险分与评估的各方面内容进行了分析，结合《信息安全技术信息系统安全等级保护基本要求》(GBT 22239-2008)、《信息安全技术信息系统安全等级保护测评要求》、《信息安全技术信息系统安全等级保护测评过程指南》等指南对测评指标体系进行了进一步的延伸和优化。然后介绍了等级化管理实施的基本流程，并对各个阶段进行了深入探讨。

从理论上具体论述了等级化保护之后，本书提供了一个实例。通过运用前文提出的测评指标体系与综合评价方法，对一个省级电信计费系统的安全等级值进行了计算，从而验证了本书定级方法的可行性与有效性。

随后本书针对当前的新形势，对等级保护进行了创新与发展，提出了一个三重保护结构，又对云计算下的等级保护进行了一个较为直观和全面的介绍，并将其纳入了等级保护体系的保护范围内。

对于如何落实等级保护的实施，本书最后提出设计一个等级化安全管理支撑平台的方法来具体落实，并从设计目标、架构等方面来介绍平台的组成和功能以及系统的设计。

作　者

2016 年 12 月

目 录