信息安全管理平台理论与实践

THE THEORY AND PRACTICE ON INFORMATION SECURITY MANAGEMENT PLATFORM

◆ 王代潮　曾德超　刘　岩 著

http://www.phei.com.cn

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

信息安全管理平台理论与实践

王代潮　曾德超　刘　岩　著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书遵循由一般到具体、由理论到实践的原则阐述了当前国内外信息安全领域的相关话题，探讨了信息安全平台建设的理论基础和设计思路，并从实际应用出发探讨如何切实地落实信息安全工作。本书有助于组织构建以风险管理为核心的保障体系，构建符合 ISO/IEC 15408 标准的系统，实现 ISO/IEC 27001 信息安全管理体系要求的控制措施，贯彻 ISSE 和 IATF 纵深防御的信息安全设计思路，从而能够实际强化信息安全意识，提高安全防护水平。

图书在版编目（CIP）数据

信息安全管理平台理论与实践/王代潮，曾德超，刘岩著. —北京：电子工业出版社，2007.5
ISBN 978-7-121-04313-0

Ⅰ. 信… Ⅱ. ①王… ②曾… ③刘… Ⅲ. 信息系统—安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2007）第 063459 号

责任编辑：刘文杰　沈桂晴
印　　刷：北京季蜂印刷有限公司
装　　订：三河市皇庄路通装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1 092　1/16　印张：23.75　字数：598 千字
印　　次：2007 年 5 月第 1 次印刷
印　　数：5 000 册　定价：40.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

作者简历

王代潮

籍贯河北，高级工程师，硕士，中国长城资产管理公司科技信息部总经理，从事多年技术及管理工作，先后主持完成若干重大科技项目，并获部级科技成果奖一次；在多种学术刊物（《中国金融电脑》、《金融电子化》、《网络安全技术与应用》、《信息安全与通信保密》等）上发表论文十余篇。出版专著《企业知识管理——理论与实务》。

曾德超

籍贯湖北，高级工程师，四川大学信息安全专业博士生，对计算机网络、信息安全理论研究较为深入，从事多年技术工作，参与若干重大科技项目，获部级科技成果奖一次；在国家级刊物（《计算机工程与应用》、《信息安全与通信保密》、《网络安全技术与应用》等）上发表论文十余篇；出版专著一本。

刘　岩

籍贯北京，荷兰TU/e硕士，现任atsec信息安全高级咨询顾问。对密码算法、协议和系统、黑客技术、相关国际法律法规有深入研究。致力于国际的安全标准的研究和应用，包括ISO/IEC 15408(CC)、27001、FIPS 140、PCI、数字权限管理等。发表论文《Common Criteria Certification in China: A comparison with the schemes of theCCRA》、《Protecting personal content on an OMA DRM platform (Philips Research technical report, Dec. 2005)》等。

序

信息是社会发展的重要战略资源，在信息技术广泛使用的今天，信息已渗入到社会生活的方方面面，谁掌握了信息，谁就掌握了主动权，信息的重要性被广泛接受。就宏观层面而言，国际上围绕信息的获取、使用和控制的斗争愈演愈烈，信息安全已成为亟待解决、影响国家大局和长远利益的重大关键问题。就微观层面而言，各类组织对信息系统的依赖与日俱增，信息安全已成为保障业务运作、获取收益、赢得机会的关键一环。因此，信息安全已成为各类组织信息工作的一个中心。

如何做好信息安全工作，是近几十年来众多专家学者和各类组织孜孜以求的目标。在这一过程中，人们对信息安全的认识从通信保密、计算机安全、信息安全到信息安全保障，取得了长足进步，并且创造出众多信息安全技术，典型的如防病毒、防火墙和入侵检测等。但传统的信息安全措施主要是堵漏洞、做高墙、防外攻等老三样，由于 PC 机体系结构等内在问题，仅凭老三样的不断堆砌无法从根本上解决信息安全问题。寻求积极、整体的安全保障体系，越来越成为业内人士的共识。

业界同仁要走出一条信息安全保障的新路子，不能仅仅局限于传统技术领域，要从更高、更宏观的角度来审视信息安全。从宏观上看，系统化地保障信息安全比信息安全产品的简单堆砌更重要，只有信息系统的整体安全才能构成真正意义上的安全。因此，从系统角度考虑信息安全将成为主流理念，其侧重点在于如何加强管理，所谓“三分技术、七分管理”。但要真正将管理理念融入到信息安全建设中，却是安全技术的软肋。例如，2006 年肆虐的熊猫烧香病毒，不是安全技术不够成熟，而是信息安全管理意识薄弱、管理体制不健全等造成了病毒的广泛传播。

近年来，国家积极推行信息等级保护制度，并发布了《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），强调实现信息安全等级保护制度，坚持统筹兼顾，突出重点，将管理思想融入到信息安全保障领域，体现了管理与技术并重的思想。

《信息安全管理平台的理论与实践》这本书以国家信息等级保护要求为切入点，在寻求管理与技术融合方面进行了深入探讨。该书在总结信息安全和信息安全管理理论的基础上，引入管理学中层次化组织结构思想，并将其应用到信息安全管理平台建设中，提出了信息安全管理平台框架，突出了信息安全管理的三个层次：一是安全决策，确定信息安全系统的安全框架与安全决策，体现等级保护思想；二是安全运营，确定信息安全的薄弱环节，向上汇总安全事件，向下反馈安全措施；三是安全实现，通过信息安全管理平台，及时把握系统的安全状况，统一调度安全产品，抵御各种攻击，保障信息安全。以上述思想为基础，作者从工程实践的角度，提出了信息安全管理平台的设计方法

与要点，并结合在自行建设信息安全管理平台中的经验，提供了一个实用的、管理与技术并重的信息安全管理平台应用案例。

一个好的信息安全管理系统是简洁的，易于控制和管理的，该书通过理论梳理与实践探索，提出的信息安全管理平台体现了易实现、易管理、参照性强的特点，是对信息安全管理理论和实践的有益探索。

信息安全管理是一个动态的、全方位的、不断变化的过程，不可能一蹴而就，需要在不断探索实践的基础上提高完善。从这个意义上讲，《信息安全管理平台的理论与实践》的出版对于推动中国信息安全管理的健康发展也是十分有益的。同时，该书给出的案例具有很好的参考作用，我衷心希望此书能成为从事信息安全管理工作的各界人士的有益参考。

中国工程院院士 沈昌祥

2007 年 3 月

前言

随着信息化的飞速发展，信息安全技术和管理都受到了广泛的关注。信息安全管理体系和标准特别强调，信息安全不仅强调技术，还应重视管理，要做到二者有机结合。如何体系化、流程化、平台化地进行信息安全平台的建设，是当前业界不断讨论和完善的重要话题之一。

信息安全平台涵盖了广泛的信息安全技术和管理理念。机构资产的梳理、防火墙的配置、入侵检测系统的事件分析甚至整个信息系统的脆弱性和威胁分析等等，单一的因素都不能构成完整的信息安全。机构的信息安全不仅仅要求技术人员对于细节的关注，更需要管理者宏观地对整体的安全现状和态势进行了解和把握，果断有效地传达旨意采取措施。所以信息安全平台建设的重要价值就是通过技术的实现手段加强对安全管理的关注。

本书将通过信息安全平台建设理论与实践的方方面面，阐述信息安全的理论基础和设计思路，并从实际应用出发探讨如何切实地落实信息安全工作。

本书将以信息安全平台的建设理论和实践为引线，分为三大部分：理论篇、设计篇和应用篇。

第一部分阐述了信息安全的理论基础。此部分涉及广泛的安全概念和技术知识，从信息安全的发展和未来趋势谈起，涉及诸多的安全技术，如防火墙、入侵检测、防病毒等等；并涵盖目前流行的安全理论基础，如可信计算理论、信息安全服务模型、风险管理等等；并且涉及国际国内的信息安全现状和趋势，所遵从的信息安全相关标准和规范体系，如 ISO/IEC 15408（Common Criteria）、FIPS 140-2、ISO/IEC 27001（原 BS7799）的安全要求，以及国内的标准现状、等级保护要求等。

第二部分从设计的角度出发，阐述了平台建设的设计理念。首先从平台的基础体系入手，介绍体系架构和开发环境；然后探讨平台涉及的接口协议和格式，中间件概念及设计思路；安全域的网络设计和平台的结合；随后探讨平台的保障功能设计，如身份认证；并着重以模块的形式探讨信息安全平台的设计思路和技术细节，并提出相关的增强辅助模块设计，如自身安全考虑等。

第三部分阐述了信息安全平台建设的实践和应用。首先给出某机构实现信息安全管理平台的实例描述；之后从目前应用面最广泛的微软产品线入手，介绍信息安全建设的应用模型和实例；从行业发展来看，政府、电力、通信、军工军队、金融，各个领域对于信息安全的要求不断增加，具有其共同点又存在差异。金融机构从网络基础建设、数据大集中以来，安全建设将是重中之重。中国的信息安全起步和发展都处于世界前列，特别是在金融领域，2000 年以来信息安全的技术和管理层面都已经做了大量的工作。本部分将对各行业的信息安全势态进行分析和介绍，并着重于金融行业信息安全，分析其如何为金融客户

提供高可靠、高质量的服务，使得金融机构稳步健康地发展。最后在本部分中，针对平台相关的标准应用进行分析和介绍，如等级保护的实践。

本书将以信息安全平台建设为出发点，谈及了如何切实地落实信息安全工作，特别是从安全管理理念考虑。平台的建设是整个信息安全管理体系（ISMS）PDCA 过程的重要的工作，各机构在信息安全建设中，应配合其实施和应用，加强安全策略的制定、资产的梳理、风险评估工作、安全域的划分、安全意识和培训、建立应急响应等等安全工作，从而将安全管理与技术手段有效地结合。

在本书的编写过程中，我们获得了业界专家和同仁的巨大帮助。在此我们特别感谢潘柱廷、肖立昕、赵呈东、徐刚、吴茂标、任平为本书提供宝贵的思路和参考资料；感谢郭斌、马丹、杨帆在编写过程中的帮助；感谢白海蔚、刘辉对本书进行审核；感谢所有为本书的出版做出贡献的人。

本书内容深入浅出，涵盖信息安全建设的各个方面，特别是从管理的角度探讨信息安全并致力于技术实现。本书适用于广泛的读者群体，包括但不限于各行业机构的 IT 管理者、机构高层决策者、信息安全专家、研究学者、产品开发者等。我们希望和各方面的信息安全参与者共同研究，提高整体信息安全的管理和技术水平。

作　者

2007 年 3 月

反侵权盗版声明

目 录

上篇（理论篇）

中篇（设计篇）