<<信息安全等级保护基本要求培训>>

图书基本信息

书名：<<信息安全等级保护基本要求培训教程>>

13位ISBN编号：9787121115479

10位ISBN编号：7121115476

出版时间：2010-9

出版时间：电子工业出版社

作者：陆宝华

页数：335

前言

随着我国各行各业信息化的快速发展，人们的工作、生活和各项社会活动越来越多地依赖于网络和计算机系统，为信息化保驾护航的信息安全越来越受到普遍关注。
我国正在实行的信息安全等级保护制度，对于信息化状态下的国家安全、社会稳定、经济发展和人民财产保护具有十分重要的意义和作用。
与国外普遍采用的以风险管理方法来控制信息系统的安全不同，我国采用等级管理方法来控制信息系统的安全。
风险管理方法的基本思想是在信息系统生存周期的各个阶段，采用风险分析的方法，分析和评估信息系统的风险，并根据风险情况对信息系统的安全措施进行相应调整，使其安全性达到所需的要求。
等级管理方法的基本思想是在信息系统生存周期的不同阶段，通过确定信息系统的安全保护等级，并按照确定的安全保护等级的要求进行信息系统安全的设计、实现、运行控制和维护，使其安全性达到确定安全保护等级的安全目标。
我国当前实施的信息安全等级保护制度属于等级管理方法，其出发点是“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”。

内容概要

《信息安全等级保护基本要求》是目前在信息系统等级确定以后，对信息系统进行安全改造、改建、加固的依据，也是测评机构对信息系统进行安全测评及国家信息安全监管部门进行监督、检查、指导的依据。
本书对《信息安全等级保护基本要求》中所涉及的标准、安全模型、安全功能等知识进行了较为系统的分类介绍，并着重介绍了技术要求中的网络安全、主机安全、应用安全及数据安全方面的要求。而且对一些基本要求中的条款进行解释和说明，有的地方还提出了应该采用技术的建议。
本书对国家标准《信息安全等级保护基本要求》进行了原理性分析，具有很高的实用价值，解决了目前绝大多数相关人员读不懂标准的难题，是落实等级保护制度的必读之作。
本书适合从事信息保障的各类技术人员、管理人员及大专院校相关专业的师生阅读。

<<信息安全等级保护基本要求培训>>

书籍目录

第1章　等级保护基本要求概述　1.1　等级保护基本要求背景及作用　1.1.1　信息系统安全等级保护的基本内容　1.1.2　主要作用及特点　1.2　不同安全等级的安全保护能力　1.2.1　对抗能力　1.2.2　恢复能力　1.2.3　保护能力要求　1.3　基本要求的思想　1.3.1　逐级增强原则　1.3.2　控制点逐级增加　1.3.3　要求项逐级增加　1.3.4　控制强度逐级增强　1.4　与其他标准的关系　1.4.1　标准间的承接关系　1.4.2　技术标准第2章　基本要求与安全保障模型　2.1　与PPDRR模型的关系　2.1.1　PPDRR模型介绍　2.1.2　等级保护基本要求与PPDRR模型的关系　2.2　基本要求与IATF的关系　2.2.1　IATF简介　2.2.2　等级保护基本要求与IATF的关系　2.3　基本要求与能力成熟度模型(CMM)的关系　第3章　安全技术和安全管理基本要求　3.1　基本要求的框架结构　3.2　安全技术基本要求　3.2.1　安全技术基本要求的三种类型　3.2.2　标记说明　3.2.3　技术要求的分层描述　3.3　管理要求　3.3.1　安全管理制度　3.3.2　安全管理机构　3.3.3　人员安全管理　3.3.4　系统建设管理　3.3.5　系统运维管理第4章　身份鉴别　4.1　身份鉴别机制　4.1.1　标识与鉴别的概念　4.1.2　鉴别技术　4.1.3　与鉴别有关的安全机制　4.1.4　CC的标识与鉴别要求　4.2　主机与应用安全中身份鉴别的基本要求　4.2.1　主机身份鉴别的要求　4.2.2　应用中的身份鉴别要求　4.3　网络设备身份鉴别要求　4.3.1　第一级网络设备防护要求(G1)　4.3.2　第二级信息系统的网络设备防护要求(G2)　4.3.3　第三级网络设备防护(G3)　4.3.4　第四级网络设备防护(G4)　第5章　自主访问控制　5.1　访问控制的一般概念　5.1.1　访问控制的一般原理　5.1.2　访问控制过程　5.1.3　访问控制类型　5.1.4　访问控制信息　5.1.5　访问控制模型　5.2　自主访问控制　5.2.1　保护位(ProtectionBit)机制　5.2.2　访问控制表(ACL)机制　5.2.3　访问许可权与访问操作权　5.3　自主访问控制要求　5.3.1　第一、第二级的主机访问控制要求(S1)(S2)　5.3.2　第一、第二级应用安全的访问控制要求(S1)(S2)　5.3.3　网络访问控制(G1)(G2)　第6章　标记与强制访问控制(MAC)　6.1　标记　6.1.1　标记的作用与要求　6.1.2　CC中的标记要求　6.2　强制访问控制　6.2.1　MAC机制的实现方法　6.2.2　支持MAC的措施　6.3　基于角色的访问控制(RBAC)　6.3.1　RBAC的基本概念　6.3.2　IlBAC96模型　6.3.3　RBAC97模型(AdministrationRBACModel)　6.3.4　NISTRBAC建议标准　6.3.5　RBAC的特点　6.4　新型访问控制　6.4.1　基于任务的访问控制(TBAC)　6.4.2　基于对象的访问控制(OBAC)　6.5　高等级信息系统的强制访问控制要求　6.5.1　主机及应用安全第三、第四级的强制访问控制要求　6.5.2　网络访问控制　第7章　安全审计　7.1　安全审计的概念　7.1.1　定义　7.1.2　审计的目的与基本要求　7.1.3　审计事件　7.2　审计系统的实现　7.2.1　审计实现的一般方法　7.2.2　主机环境下审计的实现　7.2.3　分布式环境下的审计　7.3　审计信息的浏览　7.3.1　审计信息的浏览技术　7.3.2　审计信息的无害化处理　7.4　审计的基本要求　7.4.1　主机及应用程序的审计要求　7.4.2　网络安全审计　第8章　入侵防范　8.1　入侵行为概述　8.1.1　攻击的分类　8.1.2　攻击步骤　8.1.3　黑客攻击的常用手段　8.1.4　攻击的发展　8.2　IPV4协议的缺陷及导致的攻击　8.2.1　网络层协议的缺陷与可能导致的攻击　8.2.2　传输层存在的安全问题　8.2.3　高层协议的安全问题　8.3　主机系统及应用软件脆弱性　8.3.1　系统漏洞简介　8.3.2　操作系统的部分漏洞举例　8.3.3　数据库部分漏洞举例　8.3.4　应用程序的漏洞　8.4　入侵防范的基本要求　8.4.1　网络的入侵防范　8.4.2　主机入侵防护基本要求　第9章　恶意代码防范　9.1　恶意代码介绍　9.1.1　计算机病毒　9.1.2　蠕虫　9.1.3　陷门　9.1.4　特洛伊木马　9.1.5　逻辑炸弹　9.1.6　流氓软件　9.1.7　僵尸网络　9.2　恶意代码防范的基本要求　9.2.1　网络恶意代码防范　9.2.2　主机恶意代码防范的基本要求　第10章　数据保护　10.1　用户数据的保护　10.1.1　用户数据的机密性保护　10.1.2　用户数据的完整性保护　10.2　TSF数据的保护　10.3　数据保护基本要求　10.3.1　数据的机密性保护要求　10.3.2　数据的完整性要求　10.3.3　可信路径的意义与要求　10.4　抗抵赖　10.4.1　抗抵赖功能　10.4.2　抗抵赖要求　第11章　网络结构安全及边界完整性　11.1　网络结构安全　11.1.1　安全域划分　11.1.2　子系统划分　11.1.3　网络结构安全基本要求　11.2　网络边界的完整性保护　11.2.1　边界完整性保护要求　11.2.2　边界完整性检查方法与技术介绍　第12章　系统服务功能保护的基本要求　12.1　容错

、备份与恢复技术　12.1.1　检验技术原理　12.1.2　硬件容错系统介绍　12.1.3　软件容错系统介绍　12.1.4　数据容错　12.1.5　可信恢复　12.1.6　容错、备份与恢复的基本要求　12.2　资源控制　12.2.1　主机资源的控制基本要求　12.2.2　应用安全中的资源控制基本要求　第13章　信息安全管理体系　13.1　信息安全管理体系概述　13.2　信息安全管理体系原理　13.3　信息安全管理体系标准　第14章　管理要求　14.1　安全管理制度　14.1.1　管理制度　14.1.2　制定和发布　14.1.3　评审和修订　14.2　安全管理机构　14.2.1　岗位设置　14.2.2　人员配备　14.2.3　授权和审批　14.2.4　沟通和合作　14.2.5　审核和检查　……

章节摘录

插图：《基本要求》，是各等级信息系统安全达标要求的基本尺度。
各等级信息系统均应该依据自身的保护目标达到《基本要求》中所给出的相应等级及相应需求的规定。
1.1.1 信息系统安全等级保护的基本内容66号文中规定了信息安全等级保护的基本内容：“ 是指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。
”等级保护的核心是信息系统的分等级保护。
信息系统根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高划分为以下五级。
第一级信息系统，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。
信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行自主保护。

编辑推荐

《信息安全等级保护基本要求培训教程》：安全技术大系·国家信息安全等级保护系列丛书

版权说明