信息安全等级保护攻略

谢冬青　黄　海/编著

科学出版社

信息安全等级保护攻略

谢冬青　黄　海　编著

科学出版社
北京

内 容 简 介

本书主要内容包括信息系统安全等级保护的定级备案、相关技术、等级保护实施、测评及应用实例等。以第三级系统安全保护为主线，从技术和管理方面介绍信息系统按照合理等级进行防护的方法、定级及备案方法、基本物理环境安全检测和评估方法、网络安全测评方法、主机和数据安全测评方法、应用系统安全测评方法、安全管理测评方法。同时，以第三级以上信息系统为例介绍渗透测试及渗透测试编制，并用具体的实例详细地阐述信息系统安全等级保护定级备案及测评的全过程。

本书适合高等院校信息安全专业研究生和高年级本科生阅读，也可供从事相关工作的技术人员和对信息安全感兴趣的读者阅读参考。

图书在版编目(CIP)数据

信息安全等级保护攻略 / 谢冬青，黄海编著. —北京：科学出版社，2016

ISBN 978-7-03-049026-1

Ⅰ. ①信… Ⅱ. ①谢…②黄… Ⅲ. ①信息系统-安全技术 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2016）第 141856 号

责任编辑：郭勇斌 邓新平 / 责任校对：彭 涛

责任印制：张 伟 / 封面设计：众轩企划

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

北京教图印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2016 年 6 月第 一 版 开本：720×1000 1/16

2016 年 6 月第一次印刷 印张：25

字数：504 000

定价：128.00 元

（如有印装质量问题，我社负责调换）

序　言

网络空间已成为国家继陆、海、空、天四个疆域之后的第五个疆域，网络空间安全是关系国家安全与社会发展的基础性、全局性、现实性和战略性的重大问题。没有网络安全就没有国家安全，加快网络安全和信息化事业发展，建设网络强国，是我国政府做出的重大战略部署。同时，计算机网络和“互联网+”在社会生产和服务信息化过程中呈现出巨大作用，已经成为当前知识经济和社会生活的基础设施，有力推动了企业信息化、新兴服务行业、信息产业的快速发展，带动了国民经济转型发展和社会进步。

由于网络系统的开放性，以及现有网络协议和软件系统固有的安全缺陷，任何一种网络系统都不可避免地、或多或少地存在一定的安全隐患和风险，使人们在享受网络所带来的方便和效益的同时，也面临网络安全提出的巨大挑战，如黑客攻击、病毒传播、非法联络、信息获取等，给网络信息安全带来严重的威胁。网络安全事件屡有发生，给国家安全、企业利益和个人权益带来极大的危害，并造成了巨大的经济损失。

近年来，随着信息化的发展，国内各行各业建设了大量的网络信息系统，信息安全问题变得日益突出。为了应对信息安全方面的挑战，国家相关部门制定了信息系统信息安全等级保护制度，要求关系国家命脉及重要基础行业的不涉及国家秘密的信息系统实行信息安全等级保护制度；涉及国家秘密的涉密信息系统实行分级保护制度，并制定了一系列相关技术标准和法律法规，推动了网络信息安全技术的发展，规范了网络信息系统建设和管理。

本书主要介绍信息系统安全等级保护的政策法规、等级保护的概念、原理和应用，包括信息系统安全等级保护的定级备案、相关技术、等级保护实施、测评及应用实例等，主要内容来源于信息系统安全等级保护相关标准。由于信息系统安全等级保护标准比较多，覆盖了等级保护的各个阶段，并且对每个保护等级都做了详细的规定和描述，学习起来难免有些眼花缭乱，不易理解和掌握。因此，本书对相关标准进行了梳理，主要以第三级系统安全保护为主线介绍等级保护的原理和方法，为进一步掌握和运用相关标准打下良好的基础。

本书未对相关的信息安全技术做详细的介绍，建议读者同时学习掌握一定的信息安全基础知识，这样有助于理解和掌握本书的内容。

全书分为10章，第1章为信息安全等级保护政策法规，介绍信息安全相关国家标准、信息安全相关法律法规、等级保护政策法规的落实；第2章为信息安全等级保护技术，介绍信息安全等级保护涉及相关技术基础；第3章为信息安全等级保护实施，主要介绍按照等级保护基本要求及其标准，如何从技术及管理方面去实现信息系统按照合理等级进行防护，使信息安全等级保护相关要求能够落地；第4章为信息安全等级保护定级备案，详细介绍按照等级保护定级指南该如何对信息系统进行定级和向相关部门备案；第5章为物理安全测评，介绍如何按照等级保护测评指南对信息系统的基本物理环境进行安全检测和评估；第6章为网络安全测评，介绍如何进行信息系统网络安全的测评，包括交换机、路由器及安全设备测评等内容；第7章为主机与数据库安全测评，介绍操作系统及数据库的安全测评指南；第8章为应用安全测评，介绍如何进行应用系统安全测评，并阐述综合分析和评估方法；第9章为管理安全测评，详细阐述安全管理机构、安全管理制度、人员安全管理、系统建设管理、运维安全管理等方面的测评指导；第10章为工具测试内容，主要介绍第三级以上信息系统如何进行渗透测试，以及如何进行渗透测试报告编制，同时用一个具体的实例详细阐述信息系统安全等级保护定级备案及测评的全过程。

本书主要内容来源于国家相关标准，在此谨向相关标准制定者表示敬意和感谢。如果本书能够对信息系统安全等级保护制度的推广应用及人才培养起到有益的作用，则作者的目的便达到了。

作　者

2016年1月

目　录

第1章　信息安全等级保护政策法规

信息系统安全等级保护是近年来国家重点开展的工作之一，公安部根据《中华人民共和国计算机信息系统保护条例》，会同国家保密局、国家密码管理局、国务院、国家发展和改革委员会出台的相关文件，对信息系统安全等级保护给出了相关的指导意见和规范，这一系列的文件初步构成了信息安全等级保护的政策法规，本章主要对其中的一些重要文件进行介绍。

§1.1　信息安全等级保护基本要求

《信息系统安全等级保护基本要求》规定了安全保护等级信息系统的基本保护要求，包括基本技术要求和基本管理要求，适用于指导分等级的信息系统的安全建设和监督管理。

§1.1.1　信息系统安全保护等级

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，由低到高划分为五级。

同等级的信息系统应具备的基本安全保护能力如下。

第一级安全保护能力：应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的关键资源损害，在系统遭到损害后，能够恢复部分功能。

第二级安全保护能力：应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。

第三级安全保护能力：应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难，以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全

事件，在系统遭到损害后，能够较快恢复绝大部分功能。

第四级安全保护能力：应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难，以及其他相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。

第五级安全保护能力：本级的计算机信息系统可信计算基满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算基在其构造时，排除对实施安全策略并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最低程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。

§1.1.2 基本技术要求和基本管理要求

信息系统安全等级保护应依据信息系统的安全保护等级情况保证它们具有相应等级的基本安全保护能力，不同安全保护等级的信息系统要求具有不同的安全保护能力。

基本安全要求是针对不同安全保护等级信息系统应该具有的基本安全保护能力提出的，根据实现方式的不同，基本安全要求分为基本技术要求和基本管理要求两大类。基本技术要求与信息系统提供的技术安全机制有关，主要通过在信息系统中部署软硬件并正确地配置其安全功能来实现；基本管理要求与信息系统中各种角色参与的活动有关，主要通过控制各种角色的活动，从政策、制度、规范、流程及记录等方面做出规定来实现。

基本技术要求从物理安全、网络安全、主机安全、应用安全和数据安全几个层面提出；基本管理要求从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理几个方面提出；基本技术要求和基本管理要求是确保信息系统安全不可分割的两个部分。

基本安全要求从各个层面或方面提出了系统的每个组件应该满足的安全要求，信息系统具有的整体安全保护能力是通过不同组件实现基本安全要求来保证。除了保证系统的每个组件满足基本安全要求，还要考虑组件之间的相互关系，以保证信息系统的整体安全保护能力。

对于涉及国家秘密的信息系统，应按照国家保密工作部门的相关规定和标准进行保护。对于涉及密码的使用和管理，应按照国家密码管理的相关规定和标准实施。

根据保护侧重点的不同，技术类安全要求进一步细分为：保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改的信息安全类要求（简记为 S）；保护系统连续正常地运行，免受对系统的未授权修改、破坏而导致系统不可用的服务保证类要求（简记为 A）；通用安全保护类要求（简记为 G）。

本书中对基本安全要求使用了标记，其中的字母表示安全要求的类型，数字表示适用的安全保护等级。

§1.1.3 信息系统的基本要求

以第三级系统（S3A3G3）为例，具体要求如下。

1. *物理安全*

1）物理位置的选择（G3）

本项要求包括：

（1）机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内。

（2）机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。

2）物理访问控制（G3）

本项要求包括：

（1）机房出入口应安排专人值守，控制、鉴别和记录进入的人员。

（2）需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。

（3）应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装过渡区域。

（4）重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

3）防盗窃和防破坏（G3）

本项要求包括：

（1）应将主要设备放置在机房内。

（2）应将设备或主要部件进行固定，并设置明显的不易除去的标记。

（3）应将通信线缆铺设在隐蔽处，可铺设在地下或管道中。

（4）应对介质分类标识，存储在介质库或档案室中。

（5）应利用光、电等技术设置机房防盗报警系统。

（6）应对机房设置监控报警系统。

4）防雷击（G3）

本项要求包括：

（1）机房建筑应设置避雷装置。

（2）应设置防雷保安器，防止感应雷。

（3）机房应设置交流电源地线。

5）防火（G3）

本项要求包括：

（1）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。

（2）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

（3）机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

6）防水和防潮（G3）

本项要求包括：

（1）水管安装，不得穿过机房屋顶和活动地板。

（2）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

（3）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

（4）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

7）防静电（G3）

本项要求包括：

（1）主要设备应采取必要的接地防静电措施。

（2）机房应采用防静电地板。

8）温湿度控制（G3）

机房应设置温度、湿度自动调节设施，使机房温度、湿度的变化在设备运行所允许的范围之内。

9）电力供应（A3）

本项要求包括：

（1）应在机房供电线路上配置稳压器和过电压防护设备。

（2）应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求。

（3）应设置冗余或并行的电力电缆线路为计算机系统供电。

（4）应建立备用供电系统。

10）电磁防护（S3）

本项要求包括：

（1）应采用接地方式防止外界电磁干扰和设备寄生耦合干扰。

（2）电源线和通信线缆应隔离铺设，避免互相干扰。

（3）应对关键设备和磁介质实施电磁屏蔽。

2. 网络安全

1）结构安全（G3）

本项要求包括：

（1）应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要。

（2）应保证网络各个部分的带宽满足业务高峰期需要。

（3）应在业务终端与业务服务器之间进行路由控制建立安全的访问路径。

（4）应绘制与当前运行情况相符的网络拓扑结构图。

（5）应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

（6）应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段。

（7）应按照对业务服务的重要次序指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。

2）访问控制（G3）

本项要求包括：

（1）应在网络边界部署访问控制设备，启用访问控制功能。

（2）应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级。

（3）应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制。

（4）应在会话处于非活跃一定时间或会话结束后终止网络连接。

（5）应限制网络最大流量数及网络连接数。

（6）重要网段应采取技术手段防止地址欺骗。

（7）应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户。

（8）应限制具有拨号访问权限的用户数量。

3）安全审计（G3）

本项要求包括：

（1）应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。

（2）审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

（3）应能够根据记录数据进行分析，并生成审计报表。

（4）应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

4）边界完整性检查（S3）

本项要求包括：

（1）应能够对非授权设备私自连到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

（2）应能够对内部网络用户私自连到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

5）入侵防范（G3）

本项要求包括：

（1）应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等。

（2）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

6）恶意代码防范（G3）

本项要求包括：

（1）应在网络边界处对恶意代码进行检测和清除。

（2）应维护恶意代码库的升级和检测系统的更新。

7）网络设备防护（G3）

本项要求包括：

（1）应对登录网络设备的用户进行身份鉴别。

（2）应对网络设备的管理员登录地址进行限制。

（3）网络设备用户的标识应唯一。

（4）主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术进行身份鉴别。

（5）身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

（6）应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。

（7）当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

（8）应实现设备特权用户的权限分离。

3. 主机安全

1）身份鉴别（S3）

本项要求包括：

（1）应对登录操作系统和数据库系统的用户进行身份标识和鉴别。

（2）操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。

（3）应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

（4）当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

（5）应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。

（6）应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

2）访问控制（S3）

本项要求包括：

（1）应启用访问控制功能，依据安全策略控制用户对资源的访问。

（2）应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。

（3）应实现操作系统和数据库系统特权用户的权限分离。

（4）应严格限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令。

（5）应及时删除多余的、过期的账户，避免共享账户的存在。

（6）应对重要信息资源设置敏感标记。

（7）应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

3）安全审计（G3）

本项要求包括：

（1）审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户。

（2）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件。

（3）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。

（4）应能够根据记录数据进行分析，并生成审计报表。

（5）应保护审计进程，避免受到未预期的中断。

（6）应保护审计记录，避免受到未预期的删除、修改或覆盖等。

4）剩余信息保护（S3）

本项要求包括：

（1）应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘，还是存放在内存。