**第四章 信息安全等级保护**

**1．什么是信息安全等级保护，为什么要实行信息安全等级保护？**

**2．简述信息安全等级保护准则的发展历程？**

**3．简要介绍TCSEC准则和CC准则中的安全级别？**

**4．信息安全等级保护的原则是什么？**

**5．信息安全等级保护技术基本要求和管理基本要求中包括那些内容？**

**6．什么是安全域，如何划分一个安全域？**

**7．简述边界保护中边界的具体含义？**

**8．网络安全保护包含哪些内容？**

**9．我国信息系统安全等级是如何划分的，简述每一级的内容？**

**10．简要概述信息安全定级步骤？**

1.（1）信息安全等级保护是指对涉及国计民生的基础信息网络和重要信息系统按其重要程度及实际安全需求，合理投入，分级进行保护，分类指导，分阶段实施。（2）保障信息系统安全正常运行，提高信息安全综合防护能力，能够保障国家安全，维护社会秩序和稳定，保障并促进信息化建设健康发展，拉动信息安全和基础信息科学技术发展与产业化，进而牵动经济发展，提高综合国力。

2. 信息安全等级保护在国际上得到了广泛的认可，其思想源头可以追溯到美国的军事保密制度。自20世纪60年代以来，这一思想不断发展、完善。等级保护思想第一个比较成熟并且具有重大影响的是1985年发布的《可信计算机系统评估准则》（TCSEC），该准则是当时美国国防部为适应军事计算机的保密需要，针对没有外部连接的多用户系统提出的。

受美国等级保护思想的影响，欧盟和加拿大也分别制定了自己的等级保护评估准则。英、法、德、荷等四国于1991年提出了包含保密性、完整性、可用性等概念的《信息技术安全评估准则》（ITSEC）。ITSEC作为多国安全评估标准的综合产物，适用于军队、政府和商业部门。1993年加拿大公布《可信计算机产品评估准则》（CTCPEC）3.0版本。CTCPEC作为TCSEC和ITSEC的结合，将安全分为功能性要求和保证性要求两部分。功能性要求分为机密性、完整性、可用性、可控性等四个大类。

为解决原各自标准中出现的概念和技术上的差异，1996年美国、欧盟、加拿大联合起来将各自评估准则整合，形成评估通用准则CC（Common Criteria）。1999年出台的CC2.1版本被ISO采纳，作为ISO15408发布。在CC中定义的评估信息技术产品和系统安全性所需要的基础准则，是度量信息技术安全性的基准。

3.TCSEC安全级别

|  |  |  |  |
| --- | --- | --- | --- |
| 类别 | 级别 | 名称 | 主要特征 |
| D | D1 | 低级保护 | 本地操作系统，或者是一个完全没有保护的网络 |
| C | C1 | 主存取控制 | 可信任运算基础体制，所有文档都具有相同的机密性 |
| C2 | 自主存取控制 | 单独的可追究性，加强了可调的审慎控制 |

续表

|  |  |  |  |
| --- | --- | --- | --- |
| 类别 | 级别 | 名称 | 主要特征 |
| B | B1 | 强制存取保护 | 强迫访问控制，使用灵敏度标记 |
| B2 | 结构化保护 | 可信任运算基础体制，隐通信约束 |
| B3 | 安全区域 | 建立安全审计跟踪，支持独立的安全管理 |
| A | A1 | 形式化认证 | 按正式的设计规范分析系统，确保系统符合设计规范 |

CC安全级别

|  |  |  |
| --- | --- | --- |
| 级别 | 名称 | 主要特征 |
| EAL1 | 功能测试 | 不满足品质 |
| EAL2 | 结构测试 | 测试 |
| EAL3 | 方法测试和检验 | 配置控制和可控的分析 |
| EAL4 | 方法设计、测试和评审 | 访问详细设计和源码 |
| EAL5 | 半形式化设计和测试 | 详细的脆弱性分析 |
| EAL6 | 半形式化验证设计和测试 | 设计与源码对应 |
| EAL7 | 形式化验证设计和测试 | 形式化设计 |

4.（1）自主保护原则

信息系统运营、使用单位及其主管部门按照国家相关法规和标准，自主确定信息系统的安全保护等级，自行组织实施安全保护。

（2）重点保护原则

根据信息系统的重要程度、业务特点，通过划分不同安全保护等级的信息系统，实现不同强度的安全保护，集中资源优先保护涉及核心业务或关键信息资产的信息系统。

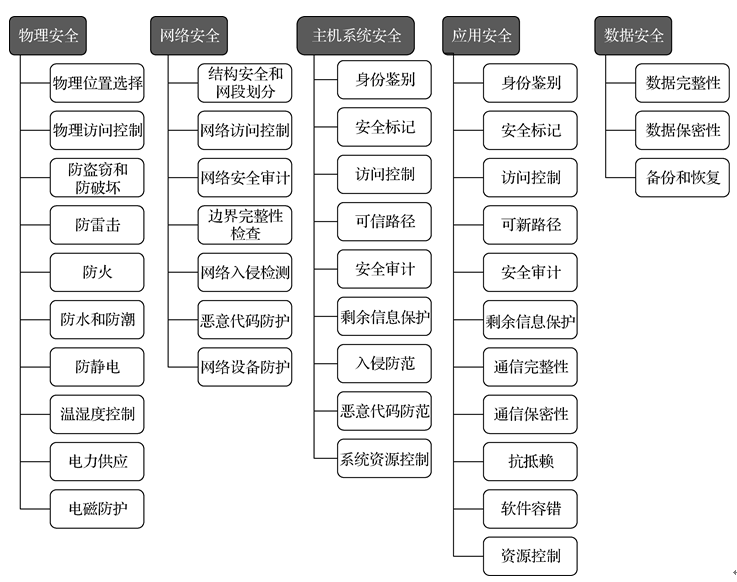
（3）同步建设原则

信息系统在新建、改建、扩建时应当同步规划和设计安全方案，投入一定比例的资金建设信息安全设施，使得保障信息安全与信息化建设相适应。

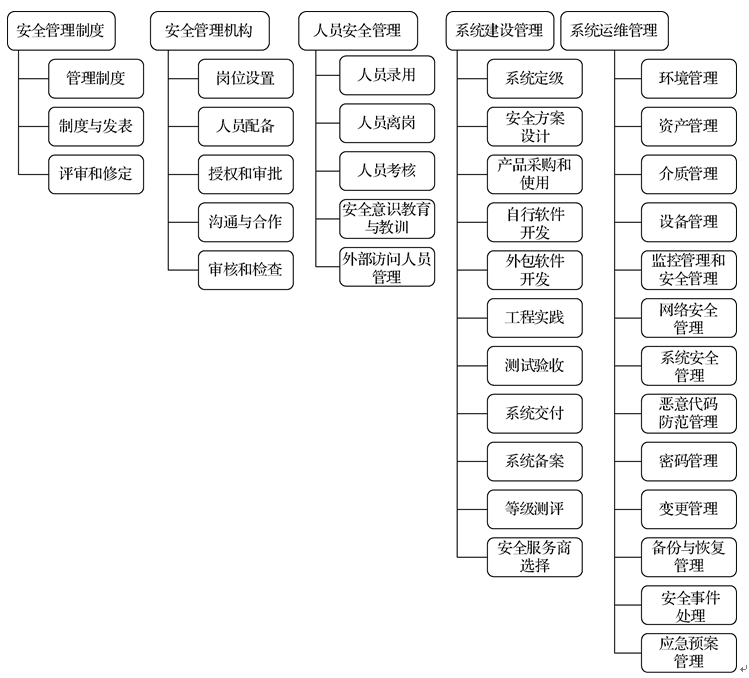
（4）动态调整原则

要跟据信息系统的变化情况，随时调整安全保护措施。由于信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级，根据信息系统安全保护等级的调整情况，重新实施安全保护。

5.（1）技术基本要求



（2）管理基本要求



6.（1）安全域是指同一系统内根据信息的性质、使用主体、安全目标和策略等元素的不同来划分的不同逻辑子网或网络，每一个逻辑区域有相同的安全保护需求，具有相同的安全访问控制和边界控制策略，区域间具有相互信任关系，而且相同的网络安全域共享同样的安全策略。(2)①查看网络上承载的业务系统的访问终端与业务主机的访问关系以及业务主机之间的访问关系，若业务主机之间没有任何访问关系则单独考虑各业务系统安全域的划分；若业务主机之间有访问关系，则将这几个业务系统统筹到一起考虑安全域。②划分安全计算域：根据业务系统的业务功能实现机制、保护等级程度进行安全计算域的划分，一般分为核心处理域和访问域，其中数据库服务器等后台处理设备归入核心处理域，前台直接面对用户的应用服务器归入访问域；局域网访问域可以有多种类型，如开发区、测试区、数据共享区、数据交换区、第三方维护管理区、VPN接入区等；局域网的内部核心处理域包括：数据库、安全控制管理、后台维护区（网管工作区）等，核心处理域应具有隔离设备对该区域进行安全隔离，如防火墙，路由器（使用ACL），交换机（使用VLAN）等。③划分安全用户域：根据业务系统的访问用户分类进行安全用户域的划分，访问同类数据的用户终端，需要进行相同级别保护划为一类安全用户域，一般分为管理用户域、内部用户域、外部用户域；④划分安全网络域：安全网络域是由具有相同安全等级的计算域和用户域连接组成的网络域。网络域的安全等级的确定与网络所连接的安全用户域和（或）安全计算域的安全等级有关。一般同一网络内化分三种安全域：外部域、接入域、内部域。

7. 边界安全保护

|  |  |  |  |
| --- | --- | --- | --- |
| 边界类型 | 边界说明 | 主要控制实施 | 产品实现 |
| 外网第三方边界 | 外网与互联网的边界及其他单位通过拨号连接所形成的网络边界 | 网络访问控制；流量及连接数控制；内容过滤；对外服务安全；入侵检测 | 防火墙；统一威胁管理（UTM）；入侵检测/防护系统（IDS/IPS）；虚拟专用网络（VPN） |
| 内网第三方边界 | 内网与企业业务合作伙伴等第三方网络专线连接所形成的边界，如银行 | 网络访问控制；流量及连接数控制；入侵检测 | 防火墙；入侵检测/防护系统（IDS/IPS） |
| 内外网边界 | 信息内网与信息外网连接的边界 | 逻辑强隔离 | 专用逻辑强隔离 |
| 纵向边界 | 信息内网纵向上下级单位网络连接的边界以及平级单位间连接的边界 | 网络访问控制；入侵检测 | 防火墙；入侵检测/防护系统（IDS/IPS） |
| 横向域间边界 | 各安全域间的互访边界 | 域间访问控制；边界入侵检测 | 防火墙；入侵检测/防护系统（IDS/IPS）；WLAN；ACL |

8. 网络安全防护主要包含以下5个方面的内容。

（1）物理安全策略

物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害及人为破坏；验证用户的身份和使用权限、防止用户越权操作；确保计算机系统有一个良好的电磁兼容工作环境；建立完备的安全管理制度，防止非法进入计算机控制和各种偷窃、破坏活动的发生。

（2）访问控制策略

访问控制策略是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和访问。它也是维护网络系统安全，保护网络资源的重要手段之一。

（3）防火墙控制

防火墙是用以阻止网络中的黑客访问某个机构网络的一道屏障，也可以称之为控制进、出两个方向通信的门槛。在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻挡外部网络的入侵。

（4）信息加密策略

信息加密的目的是保护网内的数据、文件、口令、控制信息，以及网上传输的数据。

（5）网络安全管理策略

在网络安全中，除了采取上述技术措施之外，加强网络的安全管理，制定合理的规章制度，对于确保网络安全、可靠地运行，能够起到十分关键的作用。网络的安全管理策略包括确定安全管理等级和安全管理范围，制定有关网络操作使用规程和人员出入机房管理的制度，制定网络系统的维护制度和应急措施。

9.（1）信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。（2）①第一级用户自主保护级：本级的计算机信息系统可信计算基通过隔离用户与数据，使用户具备自主安全保护的能力。②第二级系统审计保护级：与用户自主保护级相比，本级的计算机信息系统可信计算基实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。③第三级安全标记保护级：本级的计算机信息系统可信计算基具有系统审计保护级所有功能。此外，还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出信息的能力；消除通过测试发现的任何错误。④第四级结构化保护级：本级的计算机信息系统可信计算基建立于一个明确定义的形式化安全策略模型之上，它要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。⑤第五级访问验证保护级：本级的计算机信息系统可信计算基满足访问监控器的需求，访问监控器仲裁主体对客体的全部访问。

10. ①确定定级对象：按如下原则确定定级对象：承载相对独立或单一业务应用的信息系统；信息系统的信息安全由本单位主管；具有信息系统的基本要素。②初步确定信息系统等级：信息系统安全包括业务信息安全和系统服务安全，与之相关的受侵害客体和对客体的侵害程度可能不同，因此，信息系统定级也应由业务信息安全和系统服务安全两方面确定。从业务信息安全角度反映的信息系统安全保护等级称为业务信息安全等级；从系统服务安全角度反映的信息系统安全保护等级称为系统服务安全等级。③信息系统等级评审：在信息系统安全保护等级确定过程中，也可以聘请专家进行咨询评审，并出具定级评审意见。④信息系统等级的最终确定与审批：信息系统运营使用单位参考专家定级评审意见，最终确定信息系统等级，形成《定级报告》。