**第七章 信息安全策略**

**1．信息安全策略的制定过程是怎样的？**

**2．信息安全策略管理有哪些相关技术？这些技术的功能和作用分别是什么？**

**3．信息安全策略是什么？它有何特点？**

**4．如何进行信息安全策略的规划与实施？**

**5．信息安全策略使用了哪些主要技术？**

**6．什么是环境安全策略？环境安全策略包括哪些方面的内容？**

**7．系统安全策略的目标是什么？包括哪些内容？**

**8．病毒防护策略的功能有哪些？有什么要求？**

**9．什么是安全教育策略？**

1. **信息安全策略在实际网络管理中有哪些体现？**

1.当进行一项安全策略的制定工程时，可以用SDLC过程对其进行指导。SDLC（系统生命周期，系统生存周期）是软件产生直到报废的生命周期，是软件工程中的一种思想原则，即按部就班、逐步推进，每个阶段都要有定义、工作、审查、形成文档以供交流或备查，以提高软件的质量。制定流程可分为四个阶段：调查与分析阶段。设计阶段。实施阶段。维护阶段。

2.①LDAP协议：LDAP协议遵循X.500协议数据模式，实现PDP对目录服务器中策略信息的存取操作；LDAP协议中的数据是面向对象的，LDAP协议的模式规定了数据库的结构，而条目则是模式的实现，可以说，LDAP数据库就是由条目构成的。模式有两个重要的元素，属性类型和对象类，与对象类相关的还有内容规则、命名规则和结构规则等。可以认为对象类相当于C++中的类，而属性类型相当于类中的数据类型，条目就相当于类实例。

②COPS协议：COPS协议描述了一个基于信令协议的 QOS策略控制客户/服务器模型。COPS协议在PDP及其客户 （PEP）之间交换策略请求和决定信息。COPS协议具有可扩展性，可以支持其他类型的策略用户。在协议中没有对PDP的工作机制提出其他约束，只是要求在每个策略受控的管理域中，至少应该有一个PDP，而且PDP能够对策略请求做出决定并将其返回。COPS协议是简单而又可扩展的，采用了客户/服务器模型。在这个模型中，PEP发出策略请求、策略更新、策略删除的信息给远端PDP，PDP进行相应的决策，并将其决定返回给PEP。COPS协议使用 TCP作为传输层协议，可以提供可靠的报文交换。COPS提供了报文级的安全，可以进行确认、保护和维持报文的完整。COPS也能使用 IPSEC等已有协议来保证PDP和PEP间的认证和加密。COPS协议的一个重要特点就是策略请求/策略决定的当前状态为 PEP与PDP所共享，PEP发出的策略请求被PDP登记在案直到被PEP删除。

同时，对于已经被 PUP所登记的策略请求，PDP可以在任何时候异步的产生策略决定并将其下达给相关的PEP。

3.（1）信息安全策略从本质上来说是描述组织具有哪些重要信息资产，并说明这些信息资产如何被保护的一个计划。信息安全策略是进一步制定控制规则和安全程序的必要基础，其本质上是非形式化的，也可以是高度数学化的。（2）全面性、持久性、现实性、预见性、有效性。

4.具体步骤可分为：确定安全需求、制定可实现的安全目标、制订安全规划、制订系统的日常维护计划。

5.TCP/IP参考模型的安全协议分层；P2DR动态可适应安全模型；PDRR模型；WPDRRC模型等。

6.（1）物理和环境安全策略是指计算机信息和其他用于存储、处理或传输信息的物理设施，例如硬件、磁介质、电缆等，对于物理破坏来说是易受攻击的，同时也不可能完全消除这些风险。因此，应该将这些信息及物理设施放置于适当的环境中，并在物理上给予保护使之免受安全威胁和环境危害。（2）①安全区域②设备安全③物理访问控制④建筑和环境的安全管理⑤保密室、计算机房访问记录管理。

7.提供建立、实施、运作、监控、评审、维护和改进信息安全管理体系（ISMS）的规范实现信息安全的机密性、完整性和可用性。系统安全策略包括WWW访问策略、数据库系统安全策略、邮件系统安全策略、应用服务器系统安全策略、个人桌面系统安全策略、其他业务相关系统安全策略等。

8.病毒防范包括预防和检查病毒（包括实时扫描/过滤和定期检查），主要包括以下内容。（1）控制病毒入侵途径。（2）安装可靠的防病毒软件；病毒保护软件必须不能被禁用或被绕过；病毒保护软件的更改不能降低软件的有效性；不能为了降低病毒保护软件的自动更新频率而对其进行更改。（3）对系统进行实时监测和过滤。（4）定期杀毒。（5）及时更新病毒库。（6）及时上报。（7）详细记录。防病毒软件的安装和使用由信息安全管理部门专门的病毒防范管理员执行。严格控制盗版软件及其他第三方软件的使用，必要时，在运行前先对其进行病毒检查。内部工作人员因为上不安全的网站下载文件或其他方式导致中毒，造成的后果由其本人负责。

9.安全教育策略包括安全策略的发布宣传、执行效果的监督、安全机能的培训、安全意识的教育等。

10.（1）将网络的操作职责和计算机的操作职责分离。（2）制定了远程设备（包括用户区域的设备）的管理职责和程序。（3）采取了特殊的技术手段保护通过公共网络传送的数据的机密性和完整性，并保护连接的系统，采取了控制措施维护网络服务和所连接的计算机的可用性。（4）信息安全管理活动与技术控制措施协调一致，优化业务服务能力。（5）使用远程维护协议时，充分考虑其安全性。