

加快推进信息安全等级保护工作

■ 中国工程院院士 沈昌祥



信息系统安全等级划分与保护

2004年9月15日，公安部、国家保密局、国家密码管理局和国信办联合下发《关于信息安全等级保护工作的实施意见》（66号文件），明确实施等级保护的基本做法。

2007年6月22日，四部委又联合下发《信息安全等级保护管理办法》（43号文件），规范了信息安全等级保护的管理。去年6月份开始，全国范围内的重要信息系统普遍开展了信息安全等级保护定级工作，到现在为止定级工作基本上已经落实了。定级工作坚持自主定级、自主保护原则。根据信息系统在国家安全、经济建设、社会生活中的重要程度，以及系统遭受破坏后的危害程度等因素确定等级。通过信息系统的定级，国家掌握了重要信息系统在全国范围内的分布、使用情况以及其重要程度。经各大单位、行业提出，专家评审，公安部备案，定级工作已经基本结束。

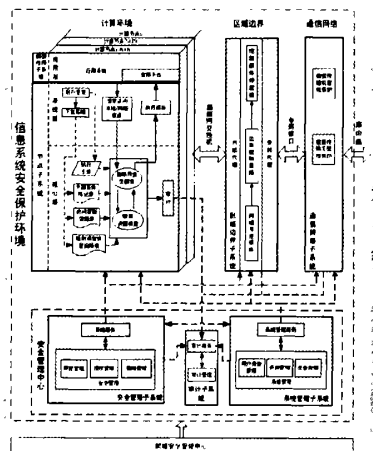
近期，国家网络与信息安全协调小组2008年工作要点已经确定：进一步推进信息安全等级保护工作，重点加强对第三级以上信息系统和涉及国家秘密信息系统的保护。

信息系统安全建设要点

1. 信息系统安全建设要特别重视安全保护环境的建设，正确构建安全保护环境框架非常重要。要构建安全管理中心支持高可信的计算环境，安全的区域边界和通信网络三重防御框架，如果不具有可信的保护环境作基础，很多安全设备、措施都将失效。譬如，通过使用防火墙、IDS、防病毒产品进行简单的技术上的堆砌，内部安全防护却是松松垮垮的，那么上述技术保护措施则起不到多大作用。打个比方，一个单位的安全首先要解决以办公室为主的安全，人员办公环境的安全。在信息系统当中，也要首先考虑计算环境的安全，这是安全保护的主体。但是，光里面安全了还不够，没有门卫站岗，门窗也不关还是不安全。所以第二道关就是边界的安全，没有经过授权和身份认证的不得“入内”。第三个是保障通信网络的安全，如防止信息被篡改和窃听。再打

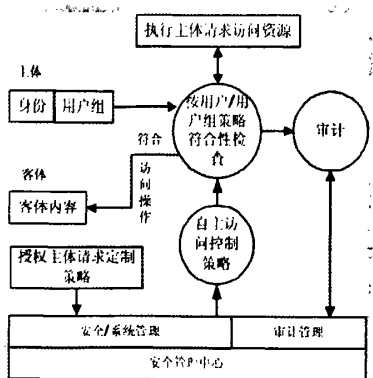
个比方，第一，单位或家里面，重要的东西该锁的锁，该放好的放好，小偷进来也摸不着，这是最重要的。第二，门窗关好，小偷不可以随便进来，进来以后也找不到想要的东西。第三，出门路上要小心携带东西别被偷了。另外，需要有管理平台，就是安全管理、系统管理、审计管理相互独立。这样系统安全是与日常的安全防护是相适应的，也是可理解和可管理的。这种结构与以往用物理层、网络层、系统层、应用层、数据层来描述系统安全相比，要更加科学合理。因为按层划分是描述开放互连网络的，不宜描述信息系统。

建设保护环境就是建设信息系统的TCB，即为信息系统建立基本的保护环境，并提供安全保护所要求的附加服务。下面以三级系统为例，展示了在安全管理中心支持下的计算环境、区域边界和通信网络三重安全防护结构框架，如右图所示：



安全防护结构框架图

2. 自主访问控制：第一级和第二级实行自主访问控制，允许命名用户以用户、用户组的身份控制客体的共享，阻止非授权用户读取敏感信息。其结构流程如右图所示：



自主访问控制结构流程图

3. 强制访问控制：第三级以上在进行自主访问控制基础上实行强制访问控制。

