网络信息安全等级保护制度

信息网络的全球化使得信息网络的安全问题也全球化起来，任何与互联网相连接的信息系统都必须面对世界范围内的网络攻击、数据窃取、身份假冒等安全问题。发达国家普遍发生的有关利用计算机进行犯罪的案件，绝大部分已经在我国出现。

目前，我国进口的计算机系统产品，其安全功能基本上是最低层次的，我国尚没有自己的配套安全技术产品，使用的微机和网络产品从硬件、固件到软件，基本没有安全保障功 能，在建的一些重要信息系统，也缺乏安全技术防范措施。这些问题若不加紧解决，会影响国家主权和安全、信息化社会的政治安定和社会稳定、经济和现代化建设顺利发展。

但是，当前计算机信息系统的建设者、管理者和使用者都面临着一个共同的问题，就是他们建设、管理或使用的信息系统是否是安全的？如何评价系统的安全性？这就需要有一整套用于规范计算机信息系统安全建设和使用的标准和管理办法。

一、等级保护制度的意义

1994 年，国务院发布了《中华人民共和国计算机信息系统安全保护条例》（以下简称《条例》），该条例是计算机信息系统安全保护的法律基础。其中第九条规定计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。公安部在《条例》发布实施后便着手开始了计算机信息系统安全等级保护的研究和准备工作。等级管理的思想和方法具有科学、合理、规范、便于理解、掌握和运用等优点，因此，对计算机信息系统实行安全等级保护制度，是我国计算机信息系统安全保护工作的重要发展思路，对于正在发展中的信息系统安全保护工作更有着十分重要的意义。

为切实加强重要领域信息系统安全的规范化建设和管理，全面提高国家信息系统安全保护的整体水平，使公安机关公共信息网络安全监察工作更加科学、规范，指导工作更具体、明确，公安部组织制订了《计算机信息系统安全保护等级划分准则》（以下简称《准则》）国家标准，并于 1999 年 9 月 13 日由国家质量技术监督局审查通过并正式批准发布，已于 2001 年 1 月 1 日执行。该准则的发布为计算机信息系统安全法规和配套标准的制定和执法部门的监督检查提供了依据，为安全产品的研制提供了技术支持，为安全系统的建设和管理提供了技术指导，是我国计算机信息系统安全保护等级工作的基础。

二、国外等级保护的发展历程

美国国防部早在 80 年代就针对国防部门的计算机安全保密开展了一系列有影响的工作，后来成立了所属的机构--国家计算机安全中心（NCSC）继续进行有关工作。1983 年他们公布了可信计算机系统评估准则（TCSEC-TrustedComputerSystemEvaluationCriteria, 俗称橘皮书），橘皮书中使用了可信计算基础（TrustedComputingBase,TCB）这一概念，即计算机硬件与支持不可信应用及不可信用户的操作系统的组合体。在 TCSEC 的评价准则中，从 B 级开始就要求具有强制存取控制和形式化模型技术的应用。橘皮书论述的重点是通用的操作系统，为了使它的评判方法适用于网络，NCSC 于 1987 年出版了一

系列有关可信计算机数据库、可信计算机网络等的指南等（俗称彩虹系列）。该书从网络安全的角度出发，解释了准则中的观点，从用户登录、授权管理、访问控制、审计跟踪、隐通道分析、可信通道建立、安全检测、生命周期保障、文本写作、用户指南均提出了规范性要求，并根据所采用的安全策略、系统所具备的安全功能将系统分为四类七个安全级别。将计算机系统的可信程度划分为 D、C1、C2、B1、B2、B3 和 A1 七个层次。

TCSEC 带动了国际计算机安全的评估研究，90 年代西欧四国（英、法、荷、德）联合提出了信息技术安全评估标准（ITSEC），ITSEC（又称欧洲白皮书）除了吸收 TCSEC 的成功经验外，首次提出了信息安全的保密性、完整性、可用性的概念，把可信计算机的概念提高到可信信息技术的高度上来认识。他们的工作成为欧共体信息安全计划的基础，并对国际信息安全的研究、实施带来深刻的影响。

美国为了保持他们在制定准则方面的优势，不甘心 TCSEC 的影响被 ITSEC 取代，他们采取联合其他国家共同提出新评估准则的办法体现他们的领导作用。1991 年 1 月宣布了制定通用安全评估准则（CC）的计划。1996 年 1 月出版了 1.0 版。它的基础是欧洲的 ITSEC，美国的包括 TCSEC 在内的新的联邦评估标准，加拿大的 CTCPEC，以及国际标准化组织 ISO：SC27WG3 的安全评估标准。CC 标准吸收了各先进国家对现代信息系统信息安全的经验与知识，将会对未来信息安全的研究与应用带来重大影响。

三、中国的等级保护体系

由于对信息系统和安全产品的安全性评估事关国家安全和社会安全，任何国家不会轻易相信和接受由别的国家所作的评估结果，为保险起见，要通过本国标准的测试才认为可靠。因此，没有一个国家会把事关国家安全利益的信息安全产品和系统的安全可信性建立在别人的评估标准、评估体系和评估结果的基础上。而是在充分借鉴国际标准的前提下，制定自己的安全评估标准。1989 年公安部开始设计起草法律和标准，在起草过程中经过长期的对国内外广泛的调查和研究，特别是对国外的法律法规、政府政策、标准和计算机犯罪的研究，使我们认识到要从法律、管理和技术三个方面着手；采取的措施要从国家制度的角度来看问题，对信息安全要实行等级保护制度。

国家标准《准则》就是要从安全整体上进行保护，从整体上、根本上、基础上来解决等级保护问题。要建立良好的国家整体保护制度，标准体系是基础。由国家的统一标准要求对系统进行评估，《准则》的配套标准分两类：一是《计算机信息系统安全保护等级划分准则应用指南》，它包括技术指南、建设指南和管理指南；二是《计算机信息系统安全保护等级评估准则》，它包括安全操作系统、安全数据库、网关、防火墙、路由器和身份认证管理等。目前，国家正在组织有关单位完善信息系统安全等级保护制度的标准体系。

《准则》对计算机信息系统安全保护能力划分了五个等级，计算机信息系统安全保护能力随着安全保护等级的增高，逐渐增强。高级别的安全要求是低级别要求的超集。

《准则》将计算机安全保护划分为以下五个级别：

第一级：用户自主保护级。它的安全保护机制使用户具备自主安全保护的能力，保护用户的信息免受非法的读写破坏。

第二级：系统审计保护级。除具备第一级所有的安全保护功能外，要求创建和维护访问的审计跟踪记录，是所有的用户对自己行为的合法性负责。

第三级：安全标记保护级。除继承前一个级别的安全功能外，还要求以访问对象标记的安全级别限制访问者的访问权限，实现对访问对象的强制访问。

第四级：结构化保护级。在继承前面安全级别安全功能的基础上，将安全保护机制划分为关键部分和非关键部分，对关键部分直接控制访问者对访问对象的存取，从而加强系统的抗渗透能力。

第五级：访问验证保护级。这一个级别特别增设了访问验证功能，负责仲裁访问者对访问对象的所有访问活动。

需要实施安全等级保护的信息系统为：

- 党政系统(党委、政府)；
- 金融系统(银行、保险、证券)；
- 财税系统(财政、税务、工商)；
- 经贸系统(商业贸易、海关)；
- 电信系统(邮电、电信、广播、电视)；
- 能源系统(电力、热力、燃气、煤炭、油料)；
- 交通运输系统(航空、航天、铁路、公路、水运、海运)；
- 供水系统(水利及水源供给)；
- 社会应急服务系统(医疗、消防、紧急救援)；
- 教育科研系统(教育、科研、尖端科技)；
- 国防建设系统。

四、等级保护制度建设

国家实行计算机信息系统安全等级保护制度建设主要由以下几部分构成：

1.计算机信息系统安全等级保护标准体系。

2.计算机信息系统安全等级保护管理的行政法规体系。

3.信息系统安全等级保护所需的系统设备技术体系。

4.安全等级系统的建设和管理机制。

5.计算机信息系统安全监督管理体系。

建立计算机信息系统安全等级保护制度，是我国计算机信息系统安全保护工作中的一件大事，它直接关系到各行各业的计算机信息系统建设和管理，是一项复杂的社会化的系统工程，需要社会各界的共同参与。在当前全社会信息化发展达到一定水平和阶段的情况下，虽然存在一些客观困难，但只要我们抓住机遇，下大力气，采取有力措施，就一定能够在不太长的时间内，将我国的计算机信息系统安全保护的整体水平迅速提高。