信息系统等级保护与分级保护实施对比分析

郑见立 李亚子

（中国医学科学院医学信息研究所 北京 100020）

〔摘要〕 从适用范围、建设流程、系统定级、方案设计、系统实施、系统测评与检查、信息系统中止、招标采购方式等角度，对等级保护制度和分级保护制度在系统建设过程中的异同点进行详细对比分析，经比较这两种制度在实施客体、主管部门、建设流程、招标采购等多方面存在着不同点。

〔关键词〕 信息系统安全分级保护；信息系统安全等级保护；对比

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2015.10.005

Contrastive Analysis of Information System Grade Protection and Classified Protection

ZHENG Jian－li, LI Ya－zi, Institute of Medical Information, Chinese Academy of Medical Sciences, Beijing100020, China

〔**Abstract**〕 The paper makes detailed contrastive analysis of the grade protection system and classified protection system in the process of system construction from the applicable scope, construction procedure, system grading, schematic design, system implementation, system evaluation and inspection, information system halt, methods of bidding and purchasing, etc. By comparison, these two systems are different in the implementation object, competent department, construction procedure, bidding and purchasing, etc.

〔**Keywords**〕 Information system security classification protection; Information system security level protection; Comparison

1 引言

随着互联网和信息技术的快速发展，我国的信息化进程也在不断深入，与之而来的信息安全问题也日益凸显。为促进信息化建设的健康发展，我国政府分别于 2003 和 2004 年提出了涉密信息系统分级保护制度和信息系统安全等级保护制度，对建立国家信息安全保障体系有了明确的要求。分级保护制度和等级保护制度是两个既有联系又有区别的概念[1－2]，它们都是国家信息安全体系的重要组成部分，但二者在适用范围、建设过程、测评内容等方面又各自有侧重点，因此探讨等级保护制度和分级保护制度的关系有助于更好地理解国家信息安全体系，提高信息安全保障能力和水平，在维护国家安全和社会稳定、推进国家信息化建设中具有重要意义[3]。

2 资料与方法

2.1 资料

资料包括：《中华人民共和国保守国家秘密法》；《信息安全等级保护管理办法》；《中华人民共和国计算机信息系统安全保护条例》；《信息系统安全等级保护定级指南》；《信息系统安全等级保护基

〔修回日期〕 2015－05－06

〔作者简介〕 郑见立，硕士，实习研究员，发表论文 4 篇；李亚子，博士，副研究员，发表论文 30 余篇。

本要求》;《信息系统安全等级保护测评要求》;《信息系统安全等级保护实施指南》;《计算机信息系统安全等级保护工程管理要求》;《涉及国家秘密的信息系统分级保护技术要求》(BMB17—2006);《涉及国家秘密的信息系统工程监理规范》(BMB18—2006);《涉及国家秘密的信息系统分级保护管理规范》(BMB20—2007);《涉及国家秘密的信息系统分级保护测评指南》(BMB22—2007);《涉及国家秘密的信息系统分级保护方案设计指南》(BMB23—2008)。

2.2 方法

采用对比分析法,从适用范围、建设流程、系统定级、方案设计、系统实施、系统测评与检查、信息系统中止、招标采购方式等角度,对等级保护制度和分级保护制度在系统建设过程中进行对比分析。

3 分级保护和等级保护在系统建设中的对比分析

3.1 适用范围

《信息安全等级保护管理办法》第六条规定:信息系统安全等级保护的级别确定应当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,信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。因此,信息系统安全等级保护的客体包括。国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益。《中华人民共和国保守国家秘密法》第二十三条规定:涉及国家秘密的计算机信息系统应按照涉密程度实行分级保护。因此,信息系统安全等级保护的客体包括国家安全和利益。通过等级保护和分级保护的客体对比分析,可以发现:等级保护的范围比分级保护的适用范围更广,等级保护侧重于社会秩序、公共利益以及公民、法人、组织的合法权益,而分级保护则仅适用于国家安全和利益。

3.2 建设流程

3.2.1 *等级保护建设流程* 《信息安全技术信息系统安全等级保护实施指南》明确规定了信息系统安全等级保护实施的基本流程,主要包括信息系统定级、总体安全规划、安全设计与实施、安全运行与维护、信息系统中止 5 个步骤。根据《信息安全等级保护管理办法》,对已完成等级保护建设的信息系统,需进行等级测评,见图 1。

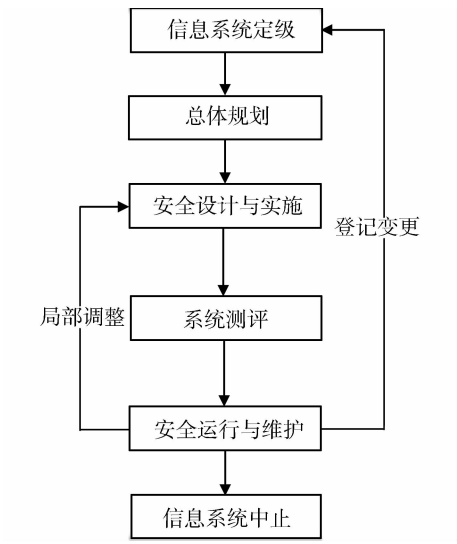

图 1 信息系统安全等级保护实施的基本流程

在安全运行与维护阶段,因需求的局部调整或发生重大调整,系统实施流程需重新回到安全设计或系统定级阶段。

3.2.2 *分级保护建设流程* 信息系统安全分级保护实施的一般流程包括系统定级、方案设计、项目预评测、项目招投标、工程实施、系统测评、系统审批、日常管理、测试与检查、系统废止等步骤,见图 2。

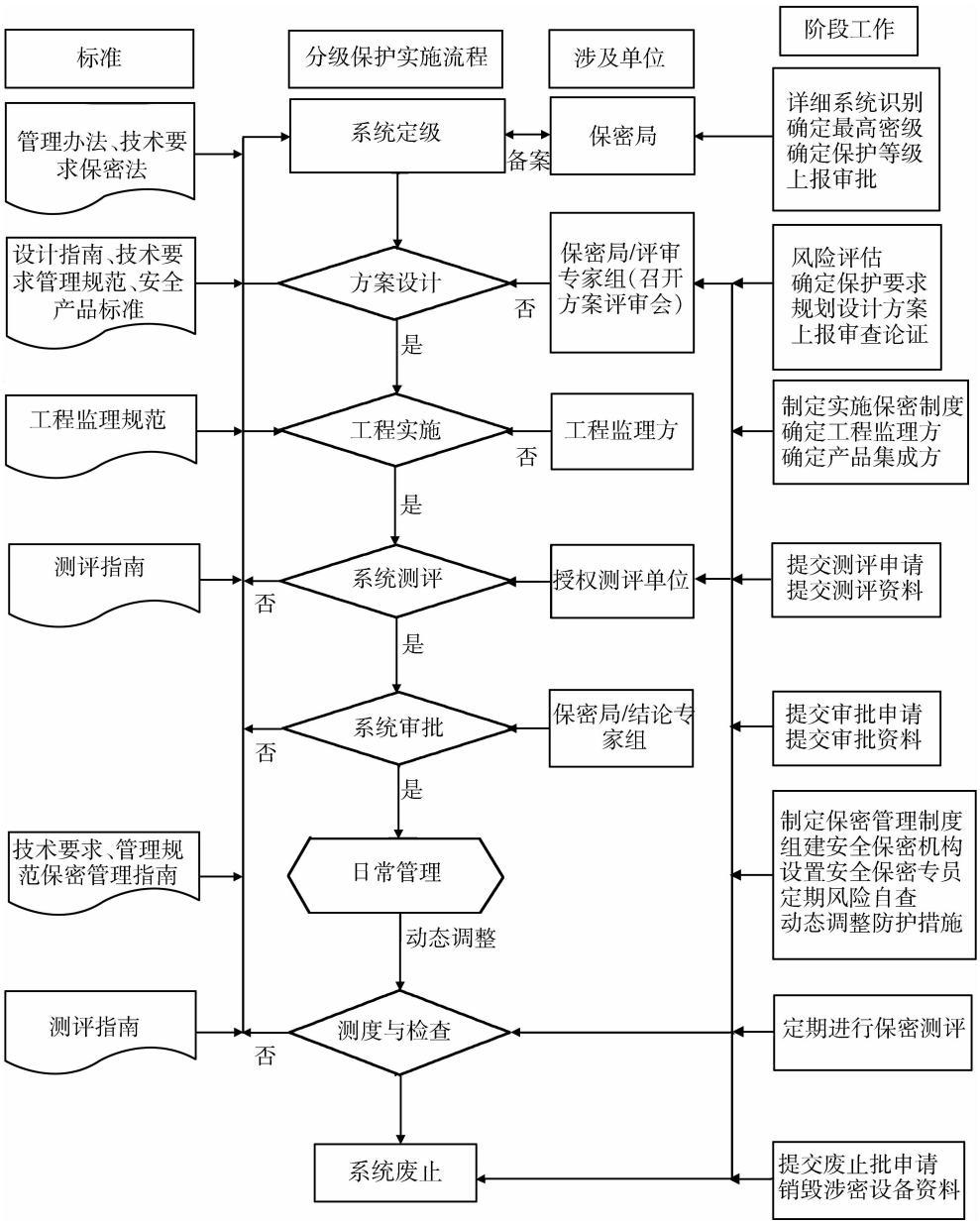

图 2 信息系统安全分级保护实施的基本流程

通过等级保护和分级保护的实施流程对比分析，可以发现：二者的实施基本流程大体相同，均包括系统定级、方案设计（总体规划，安全设计）、实施、测评、审批、运行、测试、系统废止等步骤；不同的是：信息系统等级保护的定级和测评方为公安部门，而信息系统分级保护的定级和测评方为国家保密局。

3.3 系统定级

主要从备案部门、定级阶段、定级要素、客体、级别、等级变更等方面，对等级保护和分级保护的系统定级对比分析，见表 1。

表 1 等级保护和分级保护的系统定级对比分析

项目	等级保护	分级保护
报备部门	公安部门	国家保密局
定级阶段	在方案设计前	在方案设计前
定级要素	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。	分级保护对象的客体受到侵害的程度
客体	(1) 公民、法人和其他组织的合法权益； (2) 社会秩序、公共利益； (3) 国家安全	国家安全和利益
级别	信息系统安全等级保护等级分 5 级： 第 1 级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益； 第 2 级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全； 第 3 级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害； 第 4 级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害； 第 5 级，信息系统受到破坏后，会对国家安全造成特别严重损害	国家秘密的密级分为绝密、机密、秘密 3 级。绝密级国家秘密是最重要的国家秘密，泄露会使国家安全和利益遭受特别严重的损害；机密级国家秘密是重要的国家秘密，泄露会使国家安全和利益遭受严重的损害；秘密级国家秘密是一般的国家秘密，泄露会使国家安全和利益遭受损害
等级变更	有	有

3.4 方案设计

信息系统安全等级保护的总体安全规划和安全方案设计包括安全需求分析、总体安全设计、安全建设项目规划和安全方案设计。信息系统安全分级保护的方案设计包括选择方案设计方、系统风险评估、确定保护要求、规划设计方案和设计方案论证。通过以上内容对比分析，可以发现：总体安全规划或方案设计总体相同，区别在：(1) 依据的标准规范不同，等级保护依据《信息系统安全等级保护实施指南》，分级保护依据《涉及国家秘密的信息系统分级保护方案设计指南》(BMB23—2008)；(2) 分级保护，需要上报信息系统安全保障体系详细设计方案到保密部门，并组织评审专家进行论证；(3) 选择的方案设计方的资质不一样，等级保护对设计方资质没有特殊要求，分保系统的方案设计方需满足涉密信息系统甲 (乙) 级资质或单项资质。

3.5 系统实施

等级保护的系统实施包括管理措施的实施和技术措施的实施。管理措施包括管理机构和人员、管理制度、人员安全培训、安全实施过程管理；技术措施包括信息安全产品采购、安全控制开发、安全控制集成、系统验收。分保系统的系统实施，主要依据《涉及国家秘密的信息系统分级保护技术要求》(BMB17—2006)、《涉及国家秘密的信息系统分级保护管理规范》(BMB20—2007)、《涉及国家秘密的信息系统工程监理规范》(BMB18—2006) 和系统设计方案进行开发。等级保护和分级保护在系统实施方面的对比分析：(1) 系统实施方资质，分级保护的实施方需具备涉密信息系统相应的资质。等级保护的实施方需要根据安全保护级别，具备不同等级的系统集成资质。(2) 依据的标准规范不同。

3.6 系统测评与检查对比

3.6.1 测评机构不同 信息系统安全等级保护的系统测评机构是公安部门，信息系统安全分级保护的系统测评机构是保密局。

3.6.2 测评依据不同 信息系统安全等级保护的测评依据是《信息系统安全等级保护测评要求》，信息系统安全分级保护的测评依据是《涉及国家秘密的信息系统分级保护测评指南》(BMB22—2007)。

3.6.3 测评流程对比 等保系统和分保系统的测评流程见图 3、图 4。

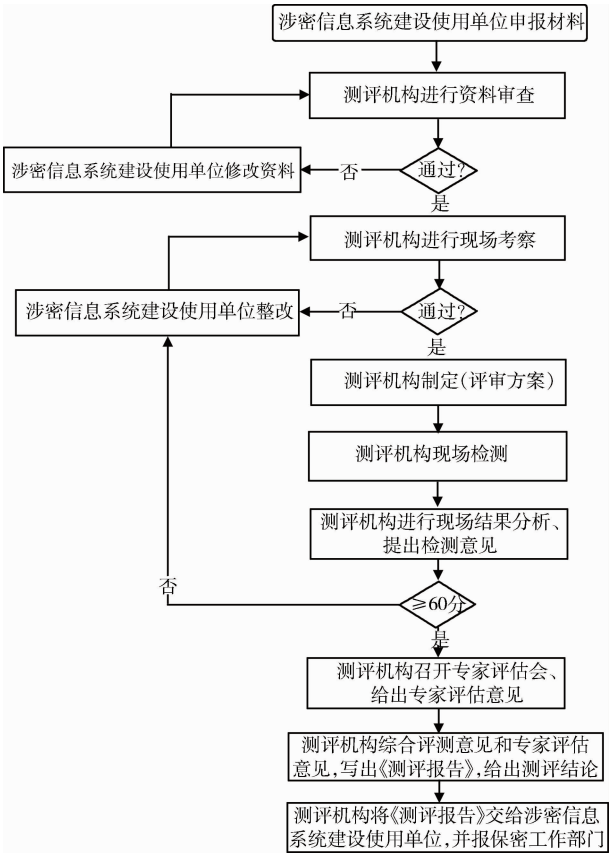

图 3 分级保护制度测评流程[4]

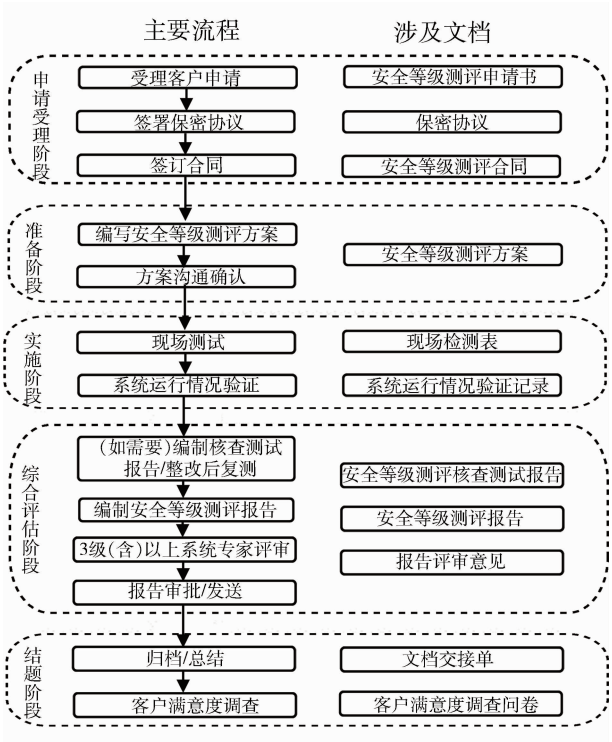

图 4 等级保护的测评流程[5]

3.6.4 测评要求不同 等级保护制度和分级保护制度的测评要求对比分析，见表 2。

表 2 等保系统和分保系统的测评要求对比

项目	等级保护	分级保护
测评内容	包括单元测评和整体测评。单元测评包括：安全技术测评和安全管理测评；整体测评包括安全控制点间测评、层面间测评、区域间测评、系统结构安全测评	分保系统的测评包括技术部分和管理部分的测评。技术部分测评内容的满分定为 70 分，管理部分测评内容的满分定为 30 分。技术部分包括基本技术要求、物理安全、运行安全和信息安全保密。管理部分包括过程管理、基本管理要求和其他管理内容
测评方法	测评的方法包括访谈、检查和测试	资料检查、现场考察、测试、专家评估
基本测评项	没有	基本测评项 15 项，可一票否决
评审或检查频次	第 3 级信息系统应当每年至少进行一次等级测评，第 4 级信息系统应当每半年至少进行一次等级测评，第 5 级信息系统应当依据特殊安全需求进行等级测评	分保系统上线运行后，根据国家保密部门要求秘密、机密级信息系统每两年进行一次安全保密检查，绝密级信息系统每一年进行一次安全保密检查

3.7 信息系统中止

分保系统不再使用时，使用单位应向保密工作部门提交系统废止申请备案，并依据保密规定对涉密设备、产品妥善退密处理，销毁涉密介质，确保泄密事件不发生。等级保护信息系统不再使用时，应对系统的信息进行转移、暂存和清除；对设备进行迁移或废弃；对存储介质进行清除或销毁。分级保护和等级保护的信息系统中止基本相同，区别在于分级保护系统不再使用时，需向保密工作部门提交系统废止申请备案。

3.8 招标采购方式

（下转第 33 页）

管理及其信息化工作得到来自医院管理、临床、护理、患者等多方面的好评，在促进医疗工作的同时，起到提高住院患者医疗安全的作用。医嘱闭环管理既是新一代临床信息管理基础，也为病人医疗保障建设指明方向，是现代智能性数字化医院建设的重要内容，对医院临床信息化发展具有重要意义。

参考文献

1 郑西川，孙宇，郝安琪，等. 新一代临床护理信息系统建设与应用实践［J］. 中国医院杂志，2015，19（3）：64－66.

2 郑西川，孙宇，郝安琪，等. 基于标准化信息集成的新一代移动护理系统技术实现与应用分析［J］. 中国卫生信息管理杂志，2015，12（1）：83－88.

3 胡彬，马俊，许燕玲，等. 面向临床路径应用的护理决策信息系统应用实践［J］. 医疗卫生装备，2013，34（6）：44－46.

4 胡彬，郑西川，孙宇，等. 支持临床决策的电子护理记录架构设计［J］. 中国数字医学，2013，8（5）：31－33.

5 郑西川. 基于物联网的智慧医疗信息化 10 大关键技术研究［J］. 医学信息学杂志，2013，34（1）：10－14，34.

6 马俊，谭申生，郑西川，等. RFID 技术在手术医疗器械质量追溯管理中的应用［J］. 中国医院管理杂志，2013，33（10）：59－60.

7 马俊，许燕玲，孙宇，等. 医疗物联网技术及其在临床手术灭菌器械追溯管理中的应用［J］. 中国数字医学，2013，8（4）：59－62.

（上接第 29 页）

根据《涉及国家秘密的信息系统分级保护管理规范》（BMB20－2007）规定，涉密信息系统的集成与系统服务、安全保密产品的采购不得进行公开招标，应在具有资质的单位和经国家主管部门批准的范围内，采取邀标、竞争性谈判、单一来源采购和询价的方式进行。而信息系统安全等级保护对招标采购的方式没有限制。

4 结语

对比分析发现，信息系统安全等级保护和信息系统分级保护在实施客体、主管部门、建设流程等方面存在着各自的特点。梳理和总结这些异同点将有助于更加深入地理解这两项基本制度，为以后信息系统筹建方在信息系统安全制度的选择、系统定级、招标方式等系统建设流程方面起到一定的借鉴作用，为信息系统建设方的系统方案设计、系统建设、系统测评、系统中止等方面提供一定的参考作用。

参考文献

1 丁全和. 浅析信息安全中的等级保护与分级保护［J］. 网络安全技术与应用，2014，（7）：121－123.

2 苏乃锋，刘洪雷. 信息安全中的等级保护与分级保护初探［J］. 网络与信息，2011，（12）：58.

3 杨治华. 关于信息系统等级保护实施的几点思考［C］. 合肥：第二届全国信息安全等级保护技术大会，2013.

4 孔斌，杜虹，马朝斌. 涉密信息系统的分级保护测评［C］. 重庆：第十七届全国信息保密学术会议，2007.

5 信息系统安全等级测评［EB/OL］.［2014－12－09］. http：//www.bjtec.org.cn/cenep/html/00000000000000001264/160020/ejaqcp.html.