文章编号：1005-8451（2015）02-0059-04

三级系统信息安全等级保护测评指标体系研究

姚洪磊，杨　文
（中国铁道科学研究院　电子计算技术研究所，北京　100081）

摘　要：依据《信息系统安全等级保护基本要求》中对三级系统的要求，本文建立了三级系统信息安全等级保护评价指标体系结构，并对三级信息系统各项测评指标进行了分解，使测评人员可以更有针对性地对信息系统标准符合性进行评价，依据分解后的指标体系，采用层次分析法和主观评价法确定了信息系统等级保护测评指标体系中各项指标所占的权重，得出更加精确的综合测评结果，为各行业的信息系统等级保护测评工作的开展提供参考。

关键词：信息安全；等级保护；测评指标
中图分类号：U29-39　　**文献标识码：**A

Evaluation index system of information security level protection for third-class system

YAO Honglei, YANG Wen
(Institute of Computing Technologies, China Academy of Railway Sciences, Beijing　100081, China)

Abstract: According to the requirements of “essential demand of information system security level protection” to third class system, the paper built the evaluation index system of information security level protection for third class system, further analyzed the evaluation index, made the personnel evaluate the standard compliance of information system with pertinence. According to the index system of decomposition, the weight of index in the System was determined by analytic hierarchy process and subjective estimate method, the integrated evaluation results were got more precise. It was provided reference for the evaluation work.

Key words: information security; level protection; evaluation index

伴随我国信息化程度的提高，信息安全等级保护测评逐渐成为各行业信息系统安全管理和安全技术的重要保障手段，通过测评结果可以体现出各类信息系统的安全程度。目前测评结果主要依据国家标准并通过人工经验分析得到，但由于标准的条款和指标较为宏观，无法对每一项指标进行细化和量化，导致测评过程中的人为主观判断影响较大，需要制定一个规范、客观的标准进行衡量，因此对信息系统等级保护测评的结果进行全面的量化是有必要的。

层次分析法是 T.L.Saaty 在 20 世纪 70 年代首次提出的[1~3]，它是将复杂问题分解成各个不同因素，按一定的支配关系形成递阶层次的结构，通过比较的方式，采用相对尺度的办法，减少性质不同的因素在比对过程中存在的问题和困难，综合人为判断，得出决策因素的重要性排序。

收稿日期：2014-10-08
作者简介：姚洪磊，助理研究员；杨　文，助理研究员。

本文根据信息系统等级保护的实际测评经验，开展了如下研究工作：（1）将《信息系统等级保护测评基本要求》[4] 中的测评指标按照技术类别进行重新分类，建立三级信息系统的等级保护测评指标体系，便于测评人员在实际测评过程中对各层面间的互补因素进行统筹和综合考虑，大大减轻了各层面间互补分析环节的工作量；(2) 在建立的体系基础上，对各项指标进行细化和分解，尽可能对各项指标要求进行量化，减少人为判断的主观影响；（3）采用层次分析法，确定三级信息系统等级保护测评指标中各项指标的权重，具有实用性，为继续开展等级保护测评研究打下了基础。

1　测评指标体系结构

依据《信息系统安全等级保护基本要求》，将三级系统中的技术安全指标按照技术类别进行了重新划分，形成了三级信息系统等级保护测评指标体系，

如图 1 所示。

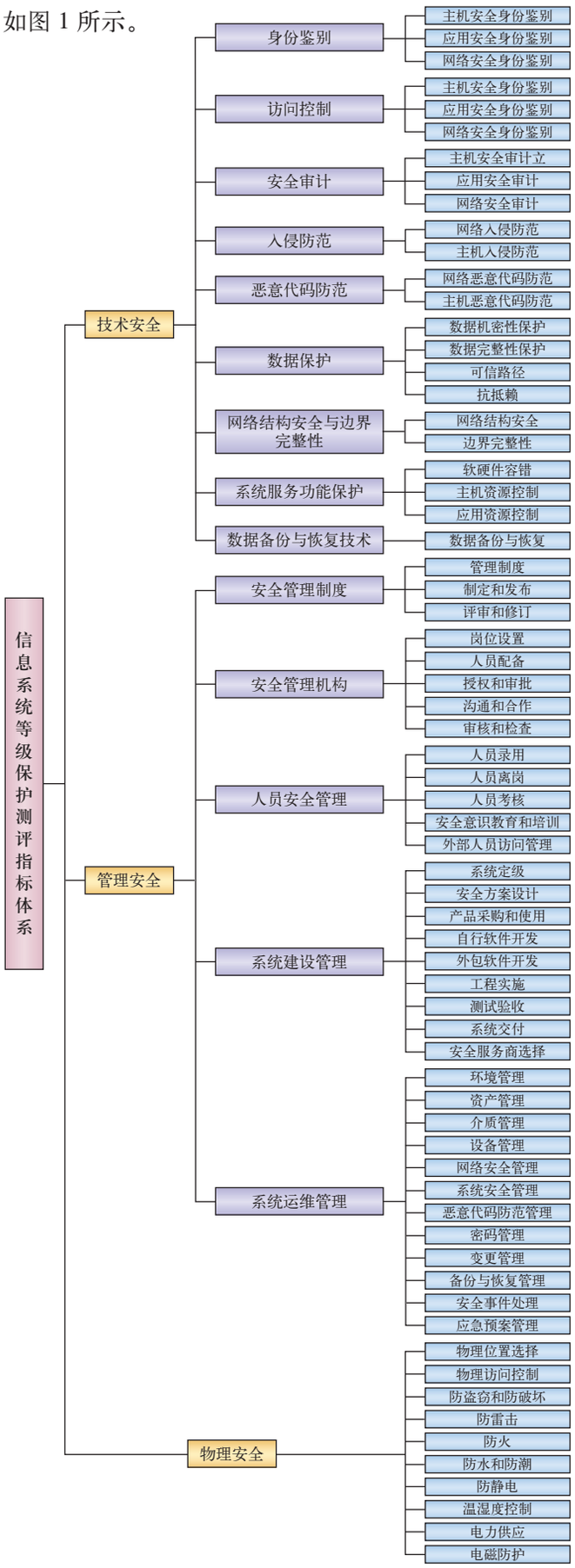

图1 三级信息系统等级保护测评指标体系

2 测评指标及要求

本文将测评指标中的安全技术划分为 9 类，以身份鉴别技术为例，对身份鉴别技术进行指标分解，如表 1 所示。

表1 身份鉴别技术指标及要求

测评指标	测评项	测评指标分解
主机安全身份鉴别	身份标识和鉴别措施	标识：操作系统给每个用户命名一个不重复的用户名和 SID 来作为身份标识
		鉴别：给每个用户设置口令即密码
	用户名 / 口令强度要求	密码复杂度：密码设置要求至少有一个数字、一个字母和一个上档键符号
		密码长度：密码设置为 8 位以上
		密码更换周期：不大于 3 个月
		弱口令：不采用典型弱口令如 123、abc 等，尤其是不采用账户默认口令即空口令
	登录失败处理	非法登录次数：建议 3~5 次
		账户锁定时间：≤ 30 min
	鉴别信息传输安全（防窃听）	加密传输：采用 SSH 加密的远程管理软件，对用户名和口令进行传输
	操作系统用户唯一	用户名唯一：操作系统内用户名不存在重名
	组合鉴别技术	鉴别方式：除用户名口令外还需增加至少以下一种鉴别技术，包括：挑战应答、动态口令、物理设备和生物识别技术
应用系统身份鉴别	登录控制	应用系统提供专用的登录控制模块
		具体采取的鉴别措施是什么
		是否有添加、删除用户和修改用户权限的操作规程及记录
	组合鉴别	组合的鉴别技术实现用户身份鉴别
	身份标识和鉴别	鉴别信息复杂度
		应用系统对用户标识是否具有唯一性
		系统采取何种措施防止身份鉴别信息被冒用
	登陆失败处理	应用系统是否具有登录失败处理功能
	功能启用	身份标识和鉴别功能是否有效
		登录失败处理功能是否有效
		根据安全策略配置相关参数
		身份标识和鉴别功能不存在明显的弱点
网络设备身份鉴别	设备安全防护措施	边界和网络设备的防护措施设置
		配置边界和网络设备的登录和验证方式
		网络特权用户的权限如何分配
	地址限制	管理员登录地址进行限制
	用户标识	设备用户的标识唯一
	组合鉴别	同一用户具有两种或两种以上组合的鉴别技术进行身份鉴别
	鉴别信息保护	鉴别信息不易被冒用
		口令设置有复杂度和定期修改要求
		网络设备的口令策略
		配置对设备远程管理所产生的鉴别信息进行保护的功能
	鉴别失败	鉴别失败处理措施
	防止窃听	防止鉴别信息被窃听的保护措施
	权限分离	特权用户的权限分离

3　测评指标计算

3.1　测评指标的权重

测评指标的权重反映了对应的指标在信息系统测试要求中所占的比重大小，本文以某个三级信息系统测评结果为例，说明如何采用层次分析法来量化信息系统等级保护测评指标和权重，如表 2 所示。

表2　层次分析法对三级信息系统测评指标评分

测评类	权重	测评层	权重	测评指标	权重	某信息点评分
技术要求	0.314 9	身份鉴别	0.042	主机安全身份鉴别	0.014	90
				…	…	…
		访问控制	0.035	主机安全访问控制	0.011	88
				…	…	…
		安全审计	0.016	主机安全审计	0.005 3	96
				…	…	…
		入侵防范	0.011	主机入侵防范	0.005 5	90
				…	…	…
		恶意代码防范	0.035	网络恶意代码防范	0.017 5	80
				…	…	…
		数据保护	0.045	数据机密性保护	0.011	80
				…	…	…
		网络结构安全与边界完整性	0.021	网络结构安全	0.01	80
				…	…	…
		系统服务功能保护	0.054	软硬件容错	0.018	80
				…	…	…
		数据备份与恢复技术	0.056	数据备份与恢复	0.056	60
管理要求	0.54	安全管理制度	0.108 2	确立管理制度	0.046 2	85
				…	…	…
		安全管理机构	0.132 2	岗位设置	0.042 7	73
				…	…	…
		人员安全管理	0.132 2	人员录用	0.037 1	100
				…	…	…
		系统建设管理	0.088 6	系统定级	0.011 4	100
				…	…	…
物理安全	0.135 1	物理安全	0.135 1	物理位置的选择	0.020 1	100
				…	…	…

3.2　测评指标的计算

3.2.1　判断测评点指标得分

依据《信息系统安全等级保护基本要求》，被测信息系统各项指标的符合程度可以划分为“符合”、“基本符合”、“一般符合”、“基本不中符合”、“不符合”5 种类型，根据实践经验，5 个符合程度的判别依据及其赋值如表 3 所示。

表3　测评点标准符合程度判别依据及赋值

判断条件	F_i（第 i 项测评点）	标准符合度
结果中不存在不符合条件，或不符合条件在此信息系统中面临的风险非常低	$F_i \geqslant 90$	符合
结果中存在不符合条件，同时不符合条件面临的风险很低	$80 \leqslant F_i<90$	基本符合
结果中存在不符合条件，同时不符合条件面临的风险较低	$70 \leqslant F_i<80$	一般符合
结果中存在不符合条件，同时不符合条件面临的风险较高	$70 \leqslant F_i<60$	基本不符合
结果中存在不符合条件，同时不符合条件面临的风险很高	$F_i<60$	不符合

3.2.2　综合测评指标计算

综合测评指标 [5] 是用于反映当前信息系统的安全程度，是评价和描述信息系统安全标准符合性的综合性指标，计算公式为：

$$P=\sum_{i=1}^{n} F_i \cdot Q_i \qquad (1)$$

式（1）中，P 为综合测评指标，Q_i 为第 i 项测评点的权重，F_i 为第 i 项测评点指标评分值，n 为测评点指标的项目总数。综合测评指标与测评体系标准符合程度和对应关系如表 4 所示。

表4　综合测评指标与测评体系标准符合程度和对应关系

P	符合程度
$P \geqslant 90$	符合
$80 \leqslant P<90$	基本符合
$70 \leqslant P<80$	一般符合
$70 \leqslant P<60$	基本不符合
$P<60$	不符合

以某个第 3 级信息系统等级保护测评结果为例，根据表 2 得到 F_i、Q_i 的值，应用公式（1）可得 P 值：

$$P=0.014\times90+0.014\times88+0.014\times70+\cdots\cdots+0.0122\times98=87.3056 \qquad (2)$$

对照表 4，P 的值在 $80 \leqslant P< 90$ 间，三级信息系统符合《信息系统安全等级保护基本要求》中的要求。

4　结束语

本文首先建立了三级信息系统的测评指标体系结构，在此基础上对《信息系统安全等级保护基本要求》的 3 级系统各项测评指标进行了分解，使测

（下转 P65）