评价风险评估方法有效性的DEA模型

杨晓明[1,2]，罗衡峰[2]，王佳昊[1]，秦志光[1]

(1. 电子科技大学计算机科学与工程学院 成都 611731; 2. 工业和信息化部电子第五研究所 广州 510610)

【摘要】决定信息安全评估结果是否科学有效的前提和基础是选择正确的风险评估方法，因此如何选择就成为关键。该文将模糊综合评价方法和数据包络(DEA)方法相结合，提出一种筛选评估方法的数学模型，用于评价风险评估方法的有效性。该方法充分考虑评价指标的客观性，从工程的角度综合计算进行风险评估活动的投入与产出，从定量的角度考察风险评估的评估效果，该方法具有良好的可操作性，为风险评估人员筛选更有效、科学、合理的评估方法提供一个具有实用价值的数学工具。

关 键 词 DEA模型; 模糊综合评价法; 风险评估; 方法有效性

中图分类号 TP309 文献标志码 A doi:10.3969/j.issn.1001-0548.2014.04.019

DEA Model for Effectiveness Evaluation of Risk Assessment Methods

YANG Xiao-ming[1,2], LUO Heng-feng[2], WANG Jia-hao[1] , and QIN Zhi-guang[1]

(1. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 611731; 2. The Fifth Electronics Research Institute of Ministry of Industry and Information Technology Guangzhou 510610)

Abstract The legitimacy method selection is the precondition and foundation of a scientific and effective assessment process in information security assessment. By considering the relevant criteria and the cost in the view of project risk assessment, this paper proposes an optimized method for effectiveness evaluation of risk assessment methods based on the fuzzy integrated assessment method and the DEA-model. By taking full consideration of the objectivity of evaluations, this method calculates the input and output of risk assessment activities and inspects the assessment effect of risk evaluation. This method has good maneuverability and thus it could be an option to select more efficient and scientific assessment methods when carrying out risk assessment.

Key words DEA-model; fuzzy integrated assessment; risk assessment; validity of method

随着信息化的发展，信息系统的大量出现，人们需要评估并解决越来越多的安全问题。目前国内外已有风险评估方法达百余种，各种方法的机理不同，对信息系统安全进行评价的效果差异很大。在风险评估过程中，选择不同评估方法，可能会得到不同的结果。国内外对单一风险评估方法的研究已经很深入，但对方法之间的比较研究相当缺乏，如何从众多方法中选出一种或几种最合适的评估方法变得非常必要。评价风险评估方法时，由于评价指标本身存在抽象、模糊和难以量化的问题，对风险评估方法的科学性和有效性评价就变得尤为复杂。

本文充分考虑了评价的定量和定性指标，将模糊综合评价方法和DEA方法结合引入信息安全风险评估领域，在使用模糊综合评价方法对评估结果的科学性和合理性进行评价的基础上，从工程的角度综合考虑进行风险评估活动的投入与产出，结合DEA方法，筛选科学评估更有效的方法。

1 模糊综合评判模型

对于风险评估方法的有效性评价，存在众多相关联的评价因素，若仅考虑主要因素而忽略次要因素，会导致重要信息的丢失，使得最终的评价结果不准确。为了保证准确性，必须考虑所有评价因素，四级模糊综合评价模型，建立过程如下[1-3]：

首先，建立一级指标集 $\boldsymbol{D}=(d_1,d_2,\cdots,d_n)$，划分为$t$个子集：

$$\boldsymbol{D}_i=(d_{i1},d_{i2},\cdots,d_{in}) \qquad i=1,2,\cdots,t \tag{1}$$

并满足条件：

$$\bigcup_{i=1}^{t}\boldsymbol{D}_i=\boldsymbol{D} \tag{2}$$

收稿日期：2013 – 05 – 02；修回日期：2014-01-19
基金项目：四川省科技支撑计划(2013GZ0022)；新疆教育厅教育科学研究项目(XJEDU2013128)
作者简介：杨晓明(1974–)，男，博士生，高级工程师，主要从事信息安全方面的研究.

$$\boldsymbol{D}_i \cap \boldsymbol{D}_j = \varnothing \tag{3}$$

其次，对每个评价指标 $\boldsymbol{D}_i$ 分别进行综合评价，$\boldsymbol{D}_i$ 中各项因素的权重分配为：

$$\boldsymbol{K}_i = (k_{i1}, k_{i2}, \cdots, k_{in_i}) \tag{4}$$

$$\sum_{i=1}^{t} n_i = n \tag{5}$$

式中，$\sum_{j=1}^{n_i} k_{ij} = 1$，评语集为：

$$\boldsymbol{V} = (v_1, v_2, \cdots, v_m) \tag{6}$$

假设 $\boldsymbol{R}_i$ 为 $\boldsymbol{D}_i$ 的评语矩阵，得第一级评价结果为：

$$\boldsymbol{B}_i = \boldsymbol{K}_i \circ \boldsymbol{R}_i = (b_{i1}, b_{i2}, \cdots, b_{im}) \qquad i = 1, 2, \cdots, t \tag{7}$$

$$\boldsymbol{V}_i^* = \boldsymbol{B}_i \circ \boldsymbol{V} = (b_{i1} \wedge v_1) \vee (b_{i2} \wedge v_2) \vee \cdots \vee (b_{im} \wedge v_m) \tag{8}$$

式中“∘”表示某种合成运算。最后，把每一个 $\boldsymbol{D}_i$ 看作一项因素，由此而构成一个新的因素集：

$$\boldsymbol{D} = (\boldsymbol{D}_1, \boldsymbol{D}_2, \cdots, \boldsymbol{D}_t) \tag{9}$$

对 $\boldsymbol{D}_i$ 进行权重分配，得到：

$$\boldsymbol{K} = (k_1, k_2, \cdots, k_t) \tag{10}$$

式中，$\sum_{i=1}^{t} k_i = 1$，设$\boldsymbol{D}$的评价矩阵为：

$$\boldsymbol{R} = \begin{bmatrix} \boldsymbol{B}_1 \\ \boldsymbol{B}_2 \\ \vdots \\ \boldsymbol{B}_t \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1m} \\ b_{21} & b_{22} & \cdots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{i1} & b_{i2} & \cdots & b_{tm} \end{bmatrix} \tag{11}$$

得到第二级评价结果：

$$\boldsymbol{B} = \boldsymbol{K} \circ \boldsymbol{R} = (b_1, b_2, \cdots, b_m) \tag{12}$$

$$\boldsymbol{V}^* = \boldsymbol{B} \circ \boldsymbol{V} = (b_1 \wedge v_1) \vee (b_2 \wedge v_2) \vee \cdots \vee (b_m \wedge v_m) \tag{13}$$

相应的，可以类推4个层次或更多层次的模糊综合评价。本文评价风险评估方法时，采用4个层次的模糊综合评价方法。

2 风险评估方法DEA评价模型

每一种评估方法均可类比为一个决策单元(decision making unit, DMU)，该决策单元接收特定的“输入(包括其所需人力物力)”，对信息系统做出科学、合理的风险评估“输出”结果，则可采用DEA方法进行评价[4-6]。

将DEA的输出指标赋值为评估方法的一级指标，DEA的指标值赋值为模糊综合评价二级评估结果，通过应用DEA方法评价不同评估方法的相对有效性，达到甄别出评估有效性较高的一种或者几种方法的目的。

由于可能需要使用组合评估法来进行风险评估，因此在评估方法库中会有N种方法备选，每种评估方法均有m种输入和s种输出。如下所示为第j种评估方法DMU_0的输入、输出向量：

$$\boldsymbol{X}_j = (\boldsymbol{X}_{1j}, \boldsymbol{X}_{2j}, \cdots, X_{mj})^{\mathrm{T}} > 0 \tag{14}$$

$$\boldsymbol{Y}_j = (Y_{1j}, Y_{2j}, \cdots, Y_{sj})^{\mathrm{T}} > 0 \qquad j = 1, 2, \cdots, n \tag{15}$$

式中，X_{ij}表示第j个评估方法的第i种输入的量；Y_{rj}表示第j个评估方法的第r个输出的量。评估方法DMU(x,y)基于输入的DEA模型为[7-8]：

$$\min \theta - \varepsilon(\boldsymbol{e}^{-\mathrm{T}} \boldsymbol{S}^- + \boldsymbol{e}^{+\mathrm{T}} \boldsymbol{S}^+) \tag{16}$$

$$\text{s.t.} \quad \sum_{j=1}^{n} \lambda_j \boldsymbol{X}_j + \boldsymbol{S}^- = \theta \boldsymbol{X}_0 \tag{17}$$

$$\sum_{j=1}^{n} \lambda_j \boldsymbol{Y}_j - \boldsymbol{S}^+ = \boldsymbol{Y}_0 \tag{18}$$

其中：

$$\boldsymbol{S}^- = (s_1^-, s_2^-, \cdots, s_m^-)^{\mathrm{T}} \qquad s_i^- \geqslant 0$$

$$\boldsymbol{S}^+ = (s_1^+, s_2^+, \cdots, s_m^+)^{\mathrm{T}} \qquad s_i^+ \geqslant 0$$

式中，s_i^- 和 $s_i^+ (i = 1, 2, \cdots, m)$ 为松驰变量；ε 为非阿基米德无穷小量，它小于任意正数而大于零；$\boldsymbol{e}^-$和$\boldsymbol{e}^+$是与$\boldsymbol{S}^-$和$\boldsymbol{S}^+$相对应的单位列向量。对于DEA有效，有如下定理[9-10]：

定理1：设本文规划问题式(16)的最优解为 $\lambda^*, \boldsymbol{S}^{-*}, \boldsymbol{S}^{+*}, \theta^*$，于是：

1) 若 $\theta^* = 1$，则 DMU_0 为弱 DEA 有效($\mathrm{C}^2\mathrm{R}$)；

2) 若 $\theta^* = 1$，$\boldsymbol{S}^{-*} = \boldsymbol{S}^{+*} = 0$，则 DMU_0 为 DEA 有效($\mathrm{C}^2\mathrm{R}$)。

3 风险评估方法的DEA评价过程

风险评估专家主要关心评估效果的科学性与合理性。判断风险评估效果的指标很多，本文采用模糊综合评价法。首先对评估效果的科学性与合理性进行评价，然后应用DEA方法对评估结果进行筛选。

3.1 评价风险评估方法评估效果的指标体系

在某次风险评估活动中，有N种方法可供选择，主要关注风险评估方法的科学性、合理性，在深入研究中通过逐层分解，建立风险评估方法评估效果的评价指标集，如表1所示，表中权重的确定采用德尔菲法。

3.2 确定等级评估集

在风险评估活动中，假设有5种风险评估方法供选择。在不影响评价结果的前提下，采用评语集：

$$V=(V_1,V_2,V_3,V_4,V_5)=(\text{劣, 差, 中, 良, 优}) \tag{19}$$

采用专家结合风险评估标准对风险评估效果的各项性能指标按百分制进行评分，再将各项得分U

转换为模糊数学上的隶属度。得分根据评价集V的等级区间判定其归属。

将各项指标得分U转换为对评估集V的隶属度，并将其进行归一化处理：

$$r_{jk}^{i}=\frac{c_{jk}^{i}}{\sum_{i=1}^{n_i}c_{jk}^{i}}\qquad k=1,2,\cdots,5 \tag{20}$$

得到d_{ij}的评估向量：

$$\boldsymbol{r}_{j}^{i}=(r_{j1}^{i},r_{j2}^{i},\cdots,r_{js}^{i}) \tag{21}$$

表1　评价风险评估方法评估效果的指标体系

目标	一级指标	权重	二级指标	权重	三级指标	权重	分值
评估效果	科学性d_1	0.52	分析粒度d_{11}	0.2	对信息系统的分析d_{111}	0.6	u_{111}
					对信息安全管理制度的分析d_{112}	0.4	u_{112}
			对信息系统的反映程度d_{12}	0.5	面临的威胁d_{121}	0.4	u_{121}
					信息系统的脆弱性d_{122}	0.3	u_{122}
					信息系统的资产情况d_{123}	0.3	u_{123}
			数据的估算程度d_{13}	0.3	威胁发生可能性的估算程度d_{131}	0.5	u_{131}
					风险损失值的估算程度d_{132}	0.5	u_{132}
	合理性d_2	0.48	方法的复杂性d_{21}	0.1	评估过程d_{211}	0.6	u_{211}
					计算过程d_{212}	0.4	u_{212}
			实用程度d_{22}	0.4	周期d_{221}	0.4	u_{221}
					可操作性d_{222}	0.6	u_{222}
			定性分析量化的手段和方法d_{23}	0.3	采用数学模型d_{231}	0.3	u_{231}
					主观专家评判d_{232}	0.4	u_{232}
					概率统计d_{233}	0.3	u_{233}
			人为因素的影响性d_{24}	0.2	对信息系统的调查d_{241}	0.6	u_{241}
					数据量化的影响d_{242}	0.4	u_{242}

3.3　逐级进行模糊综合评价

利用式(1)～(13)逐级进行模糊综合评价，最后求得每种风险评估方法的科学性和合理性的指标值，如表2所示：

表2　风险评估方法有效性评价等分表

评估方法	输入指标		输出指标		评价得分
	人力投入	物力投入	科学性	合理性	
1	44	42	78	72	1.000
2	70	84	84	84	0.712
3	46	66	56	90	1.000
4	50	46	88	80	1.000
5	70	50	90	70	0.941

依据DEA评价原理，需要建立输入、输出指标体系。其中输入指标包含人力指标和物力指标。输出指标则为科学性与合理性指标。将指标值代入式(16)中进行求解[11]。在5种风险评估方法中，方法1、3、4具有相同的有效性，可以在这3种方法中选择1种、2种或3种，方法2最差，如果想用到更多方法来进行风险评估活动，也可以选择方法5。

4　结 束 语

从目前信息安全风险评估的研究现状看，关于风险评估方法具体实施的研究比较多，而对如何评价风险评估方法评估的研究很少，使得评估人员在开展风险评估工作时，对于如何选择合适的风险评估方法进行评估缺乏科学依据。本文从定量的角度对风险评估方法评估效果进行研究，引入模糊综合评价和DEA方法，提出一种筛选评估的数学方法，为风险评估人员在风险评估实施中提供更有效的风险评估方法。在以后的研究中将对提出的模型进行具体的系统实现，输入各指标得出的评分结果，系统能自动计算最后每个风险评估方法评价的得分并进行排序，方便人工进行风险评估方法的选择，减少工作量。

参 考 文 献

[1] 潘波, 姜同敏. 基于故障树的飞机结构腐蚀损伤模糊综合评判[J]. 北京航空航天大学学报, 2012, 38(1): 39-42.
PAN Bo, JIANG Tong-min. Fuzzy comprehensive evaluation of corrosion damage of aircraft structures based on fault tree[J]. Beijing University of Aeronautics and Asteonautics, 2012, 38(1) : 39-42.

[2] 唐炎钊. 区域科技创新能力的模糊综合评估模型及应用研究——2001年广东省科技创新能力的综合分析[J]. 系统工程理论与实践, 2004(2): 37-43.
TANG Yan-zhao. The fuzzy comprehensive evaluation

model for scientific and technical innovation ability of regions and its apply—the comprehensive analysis of guangdong's scientific and technical innovation ability in 2001[J]. Systems Engineering-Theory & Practice, 2004(2): 37-43.

[3] SHI M, WANG S Y, XU S Y. Amendatory sharpe index and its application in funds' performance evaluation[J]. Systems Engineering-Theory & Practice, 2006(7): 1-10.

[4] CHARNES A, COOPER W W, RHODES E. Measuring efficiency of decision making units[J]. European Journal of Operational Research, 1978, 2(6): 429-444.

[5] 王恩茂, 刘晓君. 层次分析与模糊综合评判法在节能住宅设计方案优选中的应用[J]. 四川建筑科技大学, 2007(33): 146-149.
WANG En-mao, LIU Xiao-jun. Application of analytic hierarchy process and means of fuzzy comprehensive evaluating in choosing optimal plan of design about energy efficient residential buildings[J]. Sichuan Building Science, 2007(33): 146-149.

[6] 郑雷雷. 故障树分析法在信息安全风险评估中的应用[J]. 计算机科学, 2011, 38(10) : 107-108.
ZHENG Lei-lei. Application of FTA in information security risk assessment[J]. Computer Science, 2011, 38(10): 107-108.

[7] 宁淑婷. 基于二级模糊综合评判的建筑物和桥梁打击效果评估研究[M]. 西安: 西安电子科技大学, 2012: 1-59.
NING Shu-ting. Battle damage assessment of buildings and bridges based on two-level fuzzy comprehensive evaluation[M]. Xi'an: Xi'an University of Electronic Science and Technology, 2012: 1-59.

[8] CHARNES A, COOPER W W, WEI Q L, et al. Cone ratio data envelopment analysis and multi-objective programming [J]. International Journal of Systems Science, 1989, 7(20): 1099-1118.

[9] SINUANY-STERN Z, ABRAHAM M, YOSSI H. An AHP/DEA methodology for ranking decision making units[J]. International Transactions in Operational Research, 2000, 7(2): 109-124.

[10] 魏权龄, 王日爽, 徐兵. 数学规划引论[M]. 北京: 北京航空航天大学出版社, 1991, 1-568.
WEI Quan-ling, WANG Ri-Shuang, XU Bing. Introduction to mathematical programming[M]. Beijing: Beijing University Press, 1991, 1-568.

[11] 杨武俊. 多层次模糊综合评判法在信息安全风险评估中的应用[J]. 网络安全技术与应用, 2013(11): 32-34.
YANG Wu-jun. Applying multi-level fuzzy comprehensive evaluation in informaion security risk assessment[J]. Network Security Technology & Application, 2013(11): 32-34.

[12] 李海滨. 基于模糊综合评价的沥青路面施工质量过程控制模型[J]. 西安科技大学学报, 2012, 32 (4): 459-463.
LI Hai-bin. Asphalt pavement construction quality process control model based on the fuzzy synthetic evaluation[J]. Journal of Xi'an University of Science and Technology, 2012, 32(4) : 459-463.

[13] 褚冬莉, 李静, 范君, 等. 模糊故障在通风系统可靠性研究中的应用[J]. 西安科技大学学报, 2011, 31(6): 750-754.
CHU Dong-li, LI Jing, FAN Jun, et al. Application of fuzzy fault tree to reliability of dynamic ventilation system[J]. Journal of Xi′ an University of Science and Technology, 2011, 31(6): 750-754.

编 辑 叶 芳