计算机科学2002Vol. 29№. 9

信息系统风险的组合评估方法*)

The Combination Evaluation Method of Information System Risk

钱 钢

(南京师范大学计算机系 南京210097)

Abstract Based on process control SSE-CMM model, by using risk analysis on character of information system, we give the method of applying combination analysis to the information system's risk. To a certain extent, this method overcomes the unilateral and randomicity of the traditional method and improves the accuracy of the risk analysis.

Keywords Information system, SSE-CMM model, Risk, Combination evaluation

1 引言

随着我国信息化的进程,信息安全问题也日渐突出。如何有效防止信息系统灾难性事件的发生,降低风险,已是我们所面临的重大课题。以往国外针对信息安全采取的是风险消除方法,传统的"可信计算机安全评价准则(TCSEC)"以及国际标准"信息技术安全评价公共准则(CC)"(ISO/IEC 15408 1998年通过)都是基于风险消除制定的[1]。国内对信息安全风险评估的研究和应用目前还处于初始阶段,尚未见到全面论述如何在信息系统建设过程中进行风险评估并大规模加以实践验证的文章和专著。也未形成这方面的规范或标准。我们认为在当今大规模的信息网络环境下,无论采取多么完善的信息安全手段,风险也总会存在。因而很难采取风险消除的方法实现安全性,适宜的方法是在整个信息系统生命周期中进行风险管理。风险管理承认在生命周期中成功的攻击将会存在,如非法访问、信息或服务受到损害甚至破坏等,但发生的可能性及产生后果的严重程度将被限制和控制在可承受的范围。由此可见风险管理体现了对信息系统安全性的动态管理。风险管理的核心是风险评估,因此建立适宜风险管理的、科学的风险评估体系就显得尤为重要。为此受国家有关部门的委托,我们引入国际上新公布的基于过程的、动态控制的系统安全工程能力成熟模型作为信息安全工程风险评估的理论依据,针对该模型只是一个指导性模型并未指出具体实施时要做的工作,根据以往我们在实际工作中的经验,我们构建了一个基于模型的、针对信息系统的、具体有效的风险评估方法,并将其在一个较大范围内加以应用。

2 基于过程的 SSE-CMM 模型

基于过程的系统安全工程能力成熟模型 SSE-CMM (Systems Security Engineering Capability Maturity Model)来源于能力成熟框架 CMM 模型。CMM 模型是建立在统计过程控制理论基础之上的。统计过程控制理论发现,所有成功的管理其共同特点都是具有一组定义严格、管理完善、可测可控而高度有效的工作过程[2]。因而这些工作过程具有连续性、可重复性和有效性,CMM 模型从中抽取"关键的"工作过程并定义过程的"能力"。一个过程的能力是指通过执行这一过程所可能得到结果的质量的变化范围。其变化范围越小,过程的能力越"成熟";反之则越"不成熟"。SSE-CMM 模型运用了上述的概念,它力图通过对信息系统安全进行过程管理的途径将信息安全工程转变为一个完好的、成熟的、可测量的先进学科。信息安全工程的实施之所以难以直接测控,除安全的渗透性使安全系统建设成为一项复杂的系统工程外,另一原因是安全系统的评定不仅要求对系统安全功能加以评测,也要求对系统的安全可信度进行评测。为此模型将信息系统安全工程分为三个相互联系的部分:风险评估、工程实施和可信度评估。针对这三个部分 SSE-CMM 定义了11项关键过程(KPA),同时模型还定义了5个能力成熟度等级,每个等级的判定由一组共同特性(CF)反映,只有某一级别的所有共同特性都得到满足时,该过程的实施能力才达到对应的能力级别。

从整体上看,SSE-CMM 模型定义了一个"二维"架构[3](图1),横轴上是11个系统安全工程的过程域,纵轴上是5个能力成熟度等级,如果给每个过程域赋予一个能力成熟度等级的评定,所得到的"二维"图形便形象地反映了工程队伍实施信息系统安全工程的能力成熟性,也间接地反映了安全工程的质量以及系统在安全上的可信度,而且为实施队伍提高自身的能力指出了方向。由于 sse-cmm 模型的能力成熟度的定义与 CMM 模型的定义是一致的,下面仅对 sse-cmm 模型独有的11个安全工程的过程域加以描述。

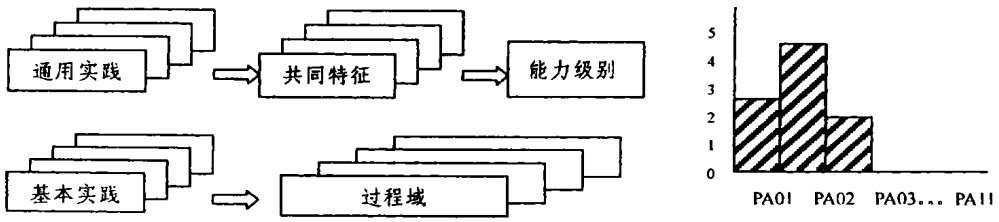

图1 系统安全工程能力成熟模型

针对风险的评估,模型认为足以成为风险的事件有三个组成部分:威胁,系统脆弱性,事件造成的影响。一般而言这三

*)国家863信息安全应急计划项目(863-301-7-8)。钱 钢 副教授。

种因素必须全部存在才足以构成风险。而安全机制在系统中存在的根本目的是将风险控制在可接受的程度内，由此模型定义了四种风险过程：评估威胁过程(KPA04)，评估系统脆弱性过程(KPA05)，评估风险事件影响过程(KPA02)以及在前三种过程基础上的评估系统安全风险过程(KPA03)。

值得注意的是，SSE-CMM 模型本身并不是安全技术模型，它虽然给出了信息系统风险分析需要考虑的关键过程以及为完成该过程所必需的基本活动，但并未给出具体的实施方法。这就需由实施单位提供适合所评估系统的具体方法。显然，若具体使用的评估方法本身存在片面性，则即使使用了 SSE-CMM 来进行过程管理，其效果也会受到影响。因此，探讨一种新的通用的评估方法，提高评估精度，就显得十分重要。

3 基于 SSE-CMM 模型的一种组合风险分析法

3.1 组合分析法的原理

当前已有多种风险评估方法可供我们使用，但由于单一的风险评估方法[5~7]其结果都具有一定的片面性，故我们设想用几种评估方法组合来取得更合理的评估结论。首先根据方法评价准则得到不同方法的权重，再按权重将不同方法的具体评估值组合起来，得到系统的最终评估结果，从而消除单一方法的片面性和随机性。这一思路通过实践证明是完全可行的。为此我们给出计算权重的示意图如图2所示。

图2这一层次模型中，目标层为对评估方法的综合评价；准则层为对评估方法的评价准则，如检验指标良好程度、方法的科学性和合理性等(注意：评价准则是可以进一步分解的)。最底层为采用的评估方法。

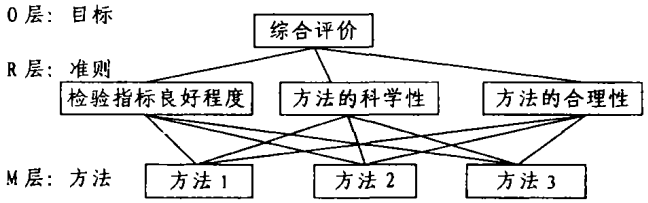

图2 组合 AHP 模型示意图

3.2 组合分析法的计算步骤

3.2.1 用 AHP 法得到权重

(1)建立层次结构模型。根据图2，求权重的关键是评价准则的细化(图3)。我们对评判标准的量化原则采用(1/9,9)EM 法进行评判。

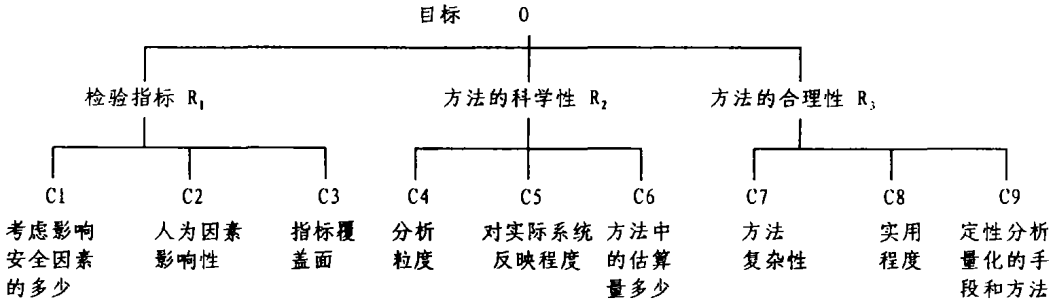

图3 对方法的综合评价层次目标树

(2)构造判断矩阵。根据图3，上下层次间的隶属关系已经确定。假定以上一层元素 R 为准则，支配的下一层元素为具体影响值 $C_1, C_2, \cdots, C_m$，则按照准则 R 的相对权重赋于 $C_1, C_2, \cdots, C_m$ 相应的权重。在指标体系中，由于 $C_1, C_2, \cdots, C_m$ 之间没有确定的定量关系，就需要针对准则 R 由专家、模型判断 C_i 与 C_j 哪个重要，并按1-9比例标度对其重要程度赋值。

第一层子目标 R 判断矩阵：$R=\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ & & & \\ r_{m1} & r_{m2} & \cdots & r_{mm} \end{bmatrix}$

R_i 权重向量计算：$W_i = W_i' / \sum_{i=1}^{m} W_i'$

而权重向量近似值：$W_i = \sqrt[m]{r_{i1} \cdot r_{i2} \cdot \Lambda \cdot r_{im}}$

可利用一致性指标(C. I.)检验权重有无逻辑错误。由算法模型 $\lambda_i = \Sigma r_{ij} w_j / w_i$，可得矩阵的特征根 λ，以及矩阵的最大特征根：$\lambda_{max} = \sum_{i=1}^{m} \lambda / m$，则一致性指标：

$C.I. = (\lambda_{max} - m)/(m-1)$

可表明判断矩阵具有满意的一致性，各项权重无逻辑错误。用同法对第二层子目标(C_i)比较打分，算出权重 W_{ij}。

(3)计算第二层子目标(C_i)各项的权重

各项的权重为各层对应权重乘积：$C_i = W_i * W_{ij}$

(4)求各方法对目标层 O 的权重

设 M 层有 j 种方法，用上述的 AHP 法可计算各方法的权重分别为 $\omega_1 = \sum_{i=1}^{9} W_{i1}$ (W_{i1} 为针对第一种方法，i 准则对 O 层的权重)，$\omega_2 = \sum_{i=1}^{9} W_{i2}, \cdots, \omega_j = \sum_{i=1}^{9} W_{ij}$。

3.2.2 用权重合成组合估算综合风险损失

定义 设 $f_1, f_2, \cdots, f_j$ 为 j 种不同方法所得的风险损失估算值，$\omega_i (i=1,2,\cdots,j)$ 为第 i 个方法的权重，则综合风险损失为：

$$f = \sum_{i=1}^{j} \omega_i f_i \text{ 且 } \sum_{i=1}^{j} \omega_i = 1$$

4 方法验证

在实际应用中为了验证新方法的效果，我们使用了当前三种流行的方法：AHP 法、类比法、Delphi 法对信息系统安全风险进行评估。并根据上述算式计算出三种方法的权重并加以组合成最终的风险评估结果。事实证明，使用新的权重组合方法的结果更接近于工程实际，而且简单、实用。

为了说明整个评估的过程，我们在此简要地介绍所用的三种方法的要点。

在用 AHP 法估算风险损失时，除对信息系统安全风险因素进行识别，从而估算灾难损失外，还必须考虑防灾投入和

灾难恢复费用[5]。可以建立如图4所示的层次模型。

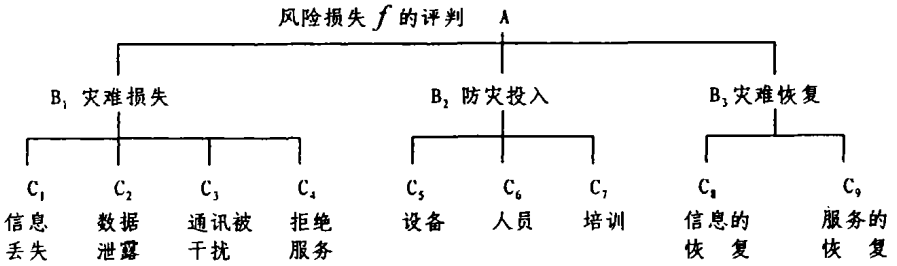

图4 风险损失评估层次模型

在用类比法估算风险损失时，必须注意算法的离散程度标准差，假定被评估的信息系统 i 类（设共有 M 种类型）第 j 等级的风险（设共分 N 个等级）发生周期为 N_{ij} 年，即每年的发生概率为 $1/N_{ij}$。选择若干性质相近的已有信息系统进行调查，设其平均损失为 S'，在一次灾害中的平均损失为 f'，则第 i 类风险每年对被评估的信息系统（设其成本为 S）造成的损失的预测值为：

$$f_i=\sum_j(1/N_{ij})(f'/S')S$$

其离散程度标准差 δ 和变异系数 V 表示：

$$\delta^2=\Sigma(f_i-f_{ai})^2/N_i \quad V=S/f_{ai}$$

其中 f_{ai} 为 f_i 的均值。对同样的平均损失，δ 和 V 越大，风险也越大。

设共有 M 种风险因素影响信息系统，则信息系统的风险损失估算值为：$f=\sum_{i=1}^{m} f_i$。

在用 Delphi 法估算风险损失时，专家评估表要清晰明了，这里给出我们根据 SSE-CMM 模型编制的专家估算表。表3和表5则是我们为统一量化专家的主观评判而定义的，这些表被归一化处理后，加以综合。

表1 资产评估表

资产	权重
资产 A	
资产 B	
资产 C	
……	

表2 风险因素对资产影响程度表

资产 \ 风险	拒绝服务	信息丢失	……	数据泄露
资产 A				
资产 B				
资产 C				
……				

表3 影响程度性等级及定量度量表

等级	等级权数	说明
高危害	1.0	造成系统死机或失去系统控制权
中危害	0.7	后果严重，但未造成系统死机或失去系统控制权
低危害	0.3	一般不会引起系统使用者的注意，但一些漏洞集合的后果通常可能造成严重后果。

表4 风险因素发生可能性表

风险	拒绝服务	信息丢失	……	数据泄露
发生率				

表5 可能性等级及定量度量表

等级	等级权数	说明
A(频繁)	1.0	频繁发生
B(很可能)	0.7	在生命期内会出现若干次
C(有时)	0.5	在生命期内可能有时发生
D(极少)	0.3	在生命期内不易发生，但有可能
E(不可能)	0.1	很不容易发生以致可认为不会发生

由上表很容易得出，资产的风险损失 $f=\sum_i$ 资产 i 成本 * 资产 i 权重 * 影响因子。

其中，影响因子 $=\sum_j$ 风险因素 j 对资产 i 的影响程度 * 风险因素 j 发生率。

结语 当前，信息系统风险评估方法的研究越来越得到各界的重视，但在我国信息系统风险评估才刚刚起步，定量评估模型尚处于探索阶段。本文论述的权重组合风险评估分析方法是一种框架性的通用方法，具体采用哪几种评估方法，可在实施 SSE-CMM 工程时具体选定。因此，这一方法可为具体实施评估工作提供技术基础。此外，这种方法的框架结构还可以用在信息系统的效益分析、系统可靠性分析等方面，所以具有较大的推广价值。

通过我们的大量实践工作，我们深深感到信息系统风险评估需要简单、实用同时具有较高精度的方法，我们将上述方法投入实用后，收到良好效果。为了交流，我们将该方法总结出来供大家探讨，出于篇幅和课题的特殊性，未对方法的指标体系作过多叙述。

参考文献

1 Parker D B. Fighting Computer Crime. 北京：电子工业出版社，1999. 30～89

2 http://www.sei.cmu.edu. Capability Maturity Model Integration，1999.8

3 http://www.sei.cmu.edu.SSE-CMM Description Document V2.0，1999.4

4 宋如顺，钱钢. 基于 SSE-CMM 的信息安全管理与控制. 计算机工程与应用，2000(12)：37～48

5 秦效启，杨修竹. 重大工程灾害风险评估研究. 自然灾害学报，1997，6(2)：7～10

6 李新运，常勇，李望. 重大工程项目灾害风险评估方法研究. 自然灾害学报，1998，7(4)：24～28

7 钱钢，达庆利. 基于系统安全工程能力成熟模型的信息系统风险评估. 管理工程学报，2001(4)：58～60