基于ISM模型的电子政务信息系统风险分析

汤志伟，杜人杰，高天鹏

(电子科技大学人文社科学院 成都 610054)

【摘要】以系统安全工程能力成熟模型作为理论依据，构造出基于模型的风险因素，采用解释结构模型对电子政务信息系统的风险进行了科学的分析与评价，并结合具体实例，重点探讨了方法的应用与结果的分析，给出了预防电子政务信息系统风险的思路和方法。

关 键 词 电子政务信息系统； 系统安全工程能力成熟模型； 解释结构模型； 风险分析

中图分类号 TP315； TP391 文献标识码 A

Risk Analysis of E-Government Information System Based on ISM

TANG Zhi-wei，DU Ren-jie，GAO Tian-peng

(School of Humanities and Social Science, UEST of China Chengdu 610054)

Abstract This paper constructs risk factors base on SSE-CMM，and Presents a scientific exploration of the analysis and assessment of e-government information system’s risk by applying the methods of system engineering and ISM. It focuses on the application of the methods and the result analysis in the actual case. Some proposals and solutions for the risk are also raised in the paper.

Key words e-government information system; systems security engineering capability maturity model; interpretative structural modeling; risk analysis

电子政务信息系统直接涉及对国家秘密信息和高敏感度的核心政务的保护，涉及到维护公共秩序和行政监管的准确实施，涉及到为社会提供公共服务的质量保证[1]。周密的电子政务信息系统风险分析，是制定可靠、有效的安全防护措施的必要前提。本文以系统安全工程能力成熟模型(Systems Security Engineering Capability Maturity Model, SSE-CMM)作为信息安全工程风险分析的理论依据[2]，结合实际工作中的经验，构建了基于过程模型的风险因素集，并采用解释结构模型法对电子政务信息系统的风险进行分析。

1 电子政务信息系统风险因素识别

在本文中，风险因素识别主要是对风险的认识与鉴别，判明电子政务信息系统安全存在哪些风险因素，采用基于过程模型SSE-CMM的指导来保证信息系统的安全。系统安全工程能力成熟模型是通过过程管理的途径将信息安全转变为一个完好的、成熟的、可测量的先进体系。SSE-CMM模型框架是一个二维架构[3]，横轴维上有11个系统安全工程过程域(PA01-PA11)，分别描述风险过程、工程过程和信任度过程。纵轴维上有6个能力成熟级别，每个级别的判定反映为一组共同特征(Common Feature, CF)，而每个共同特征进而通过一组确定的通用实践(General Practice, GP)来描述。过程能力由GP来衡量。GP、CF和能力级别组成三级结构。

SSE-CMM风险过程包括对威胁、脆弱性、影响和相关风险的分析。借助于SSE-CMM风险过程，可以得到电子政务信息系统的主要风险因素，包括来源于社会环境(各种社会组织机构和人员)的威胁、技术环境

收稿日期：2004－06－03
作者简介：汤志伟(1969－)，男，博士，副教授，主要从事信息系统开发与管理方面的研究.

(信息系统的技术因素，也包括安全人员管理和技术安全管理)的脆弱和物理自然环境的恶化。其中社会环境威胁方的主体是个人、组织和国家三个层次，具体攻击手段主要有中断、删改、窃取、伪造；技术环境的脆弱性来源于信息系统技术上和管理上的缺陷，典型的缺陷和安全隐患有系统缺陷或漏洞、系统后门。

2 解释结构模型法及具体实施

解释结构模型法(Interpretative Structural Modeling，ISM)是结构模型化技术的一种[4]。ISM的工作程序如下：1) 组织实施小组；2) 设定关键问题，选择构成系统的影响关键问题的导致因素；3) 列举各导致因素的相关性；4) 根据各要素的相关性，建立邻接矩阵和可达矩阵；5) 对可达矩阵分解后,建立结构模型；6) 根据结构模型建立解释结构模型。

2.1 确定导致因素与各导致因素的相关性，建立邻接矩阵

针对关键问题电子政务信息系统风险(S_0)，ISM小组深入分析某政府部门的电子政务系统的实际情况,利用过程模型SSE-CMM获取它的10个风险因素，即不完善的信息安全管理制度(S_1)、缺乏信息安全教育(S_2)、黑客攻击风险(S_3)、网络病毒的蔓延与破坏风险(S_4)、信息间谍潜入与机要信息流失风险(S_5)、内部人员违规与违法风险(S_6)、技术的缺陷或漏洞(S_7)、系统技术的后门(S_8)、物理自然环境恶化(S_9)和信息安全法制不健全(S_{10})。ISM小组成员经多次分析讨论确定10个风险因素之间的关系，从而可得到邻接矩阵$\boldsymbol{A}$，邻接矩阵表达了不同风险的结构关系。

$$\boldsymbol{A}=\begin{array}{c} \\ S_0 \\ S_1 \\ S_2 \\ S_3 \\ S_4 \\ S_5 \\ S_6 \\ S_7 \\ S_8 \\ S_9 \\ S_{10} \end{array}\begin{array}{c} \begin{array}{ccccccccccc} S_0 & S_1 & S_2 & S_3 & S_4 & S_5 & S_6 & S_7 & S_8 & S_9 & S_{10} \end{array} \\ \begin{bmatrix} 1&0&0&0&0&0&0&0&0&0&0 \\ 1&1&1&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&1&0&1 \\ 1&0&0&1&0&0&0&0&0&0&0 \\ 1&0&0&0&1&0&0&0&0&0&0 \\ 1&0&0&0&0&1&0&0&0&0&0 \\ 1&0&0&0&0&0&1&0&0&0&0 \\ 1&0&0&1&1&1&1&1&0&0&0 \\ 1&0&0&1&1&1&1&0&1&0&0 \\ 1&0&0&1&1&1&0&0&0&1&0 \\ 1&1&1&1&1&1&1&1&1&0&1 \end{bmatrix} \end{array}$$

2.2 建立风险因素的可达矩阵$\boldsymbol{M}$

采用布尔代数可以从$\boldsymbol{A}$计算出可达矩阵$\boldsymbol{M}$。可达矩阵表示了不同风险之间所有存在的直接和间接的结构关系，如果$(\boldsymbol{A}+\boldsymbol{I})^n=(\boldsymbol{A}+\boldsymbol{I})^{n+1}$，则$\boldsymbol{M}=(\boldsymbol{A}+\boldsymbol{I})^n$，式中$\boldsymbol{I}$为单位矩阵，$n$为幂。按照此计算方法得到可达矩阵$\boldsymbol{M}=(\boldsymbol{A}+\boldsymbol{I})^2=(\boldsymbol{A}+\boldsymbol{I})^3$。

2.3 对可达矩阵进行级间划分并建立解释结构模型

所谓级间划分就是将不同风险划分为不同层次，这样风险管理者管理风险时心中就有一个孰先孰后与孰轻孰重的框架。从可达矩阵开始，分别找到它的各级最高级要素集$L_1=\{S_0\}$，$L_2=\{S_3,S_4,S_5,S_6\}$，$L_3=\{S_7,S_8,S_9\}$，$L_4=\{S_1,S_2,S_{10}\}$，从而可建立解释结构模型。

3 电子政务信息系统风险的解释结构模型分析

对图1建立的解释结构模型进行分析，电子政务信息系统风险是一个具有4级(层)的多级递阶结构，电子政务信息系统风险最直接的表现就是第二级的导致因素，即黑客攻击风险、网络病毒的蔓延与破坏风险、信息间谍潜入与机要信息流失风险、内部人员违规与违法风险，这些风险因素发生的主要原因是由于技术的缺陷或漏洞、系统技术的后门，也包括由于物理自然环境恶化，导致系统更易被黑客攻击和网络病毒的

入侵。

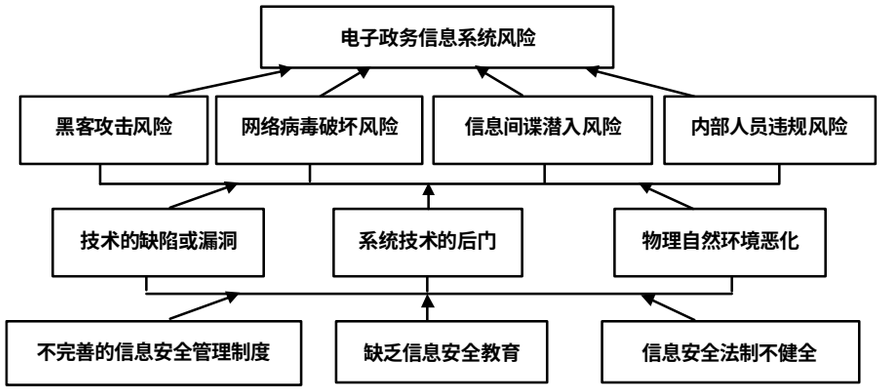

图1　解释结构模型

解释结构模型的最低一级的3个导致因素(即不完善的信息安全管理制度、缺乏信息安全教育和信息安全法制不健全)是影响电子政务信息系统全局的风险因素，它们可能出现的风险将大大增加技术的缺陷或漏洞风险、系统技术的后门风险、物理自然环境恶化风险发生的可能性，因而产生极大的危害。但是，要确保电子政务信息系统的安全，离不开管理，即使采用了最先进的安全技术，如果不对人员的权限进行有效合理的分配，相关人员照样可以越权操作；如果没有对异常事件处理的流程和规范，当遇到攻击时，电子政务信息系统仍然会不知所措；如果没有维护网络安全和信息安全的法律，网络和信息安全方面的不法行为会变得日益猖獗。

4　结束语

电子政务信息系统的风险实例分析符合当前电子政务系统的风险现状，政府在电子政务的建设过程中，应该对电子政务信息系统的风险管理从系统整体的角度进行分析，认真对待每一个环节，尤其是要重点解决影响安全的最基层因素产生的不利影响。各级政府只有把握住影响安全的最基层因素，不断地改进和提高，才能逐级改善和提升风险防范能力，保障电子政务系统的安全运行，促进电子政务建设健康发展。

本文研究工作得到电子科技大学青年科技基金(L08011201 YF021003)资助，在此表示感谢。

参　考　文　献

[1] 曲成义. 电子政务安全保障体系探索[J]. 信息安全与通信保密, 2003, 3(6): 22-26

[2] 钱　钢. 基于SSE-CMM的信息系统安全风险评估方法研究[J]. 计算机工程, 2002, 28(9): 98-100

[3] 宋如顺. 基于SSE-CMM的信息系统安全风险评估[J]. 计算机应用研究, 2000, 17(11): 12-14

[4] 汪应洛. 系统工程理论方法与应用[M]. 北京: 高等教育出版社, 1992

编　辑　熊思亮