第29卷 第10期 计 算 机 工 程 2003年6月
Vol.29 № 10 Computer Engineering June 2003
· 安全技术 · 文章编号：1000—3428(2003)10 —0122—02 文献标识码：A 中图分类号： TN918

信息安全能力成熟度模型(IS-CMM)的建构

邓 冰
(上海交通大学管理学院及软件学院，上海 200052)

摘 要：在能力成熟度模型(CMM)的基础上提出“信息安全能力成熟度模型”(IS－CMM)这一构想，并着重探讨了IS－CMM各级中的核心流程域KPAs的构建。

关键词：信息安全能力成熟度模型(IS－CMM)；总体信息安全流程(TISP)；核心流程域(KPAs)；基本实践(BPs)

Construction of Information Security Capability Maturity Model (IS-CMM)

DENG Bing
(Management School & Software Engineering School, Shanghai Jiaotong University, Shanghai 200052)

【Abstract】Information security capability maturity model (IS-CMM) is a model for the maturity capability assessment/evaluation in information security processes of one or more organizations. It is based upon the Software Engineering Institutes (SEI) CMM and proposed by Dr.Deng Bing,at Shanghai Jiaotong University.This paper mainly discusses the construction of key process area (KPAs) for each level of IS-CMM.

【Key words】Information security capability maturity model (IS-CMM)；Total information security process (TISP)；Key process areas (KPAs)；Basic practices (BPs)

1 背景与定义

美国国防部下属软件工程研究所(SEI)制定的能力成熟度模型(Capability Maturity Model，简称CMM)可被用于信息安全流程的评估，将其称为“信息安全能力成熟度模型”(Information Security Capability Maturity Model，简称IS-CMM)。该模型在SEI的年度国际会议——The SEPG Conference on Tour in Asia Pac 2002——上公布(详见SEI、QAI和SoftwarePxiode网址中的相关会议部分)。

信息安全能力成熟度模型的开发目的是为包括企业在内的机构提供一种基于流程的安全评估和改进体系。对所开发模型的主要要求包括：安全过程行为可被定义、预测和控制，并可持续提高；体系分级合理；核心流程域(Key Process Areas，简称KPAs)及基本实践(Basic Practices，简称BPs)定义准确、可行；以定量化的测度作基准；利于评估和改进双重实践；符合SEI的规范；等等。

按照IS－CMM的观点，信息安全是一个持续的流程，而非单一的技术、产品或解决方案。在此，一个或数个机构的信息安全流程环境被定义为总体信息安全流程(Total Information Security Processes，简称TISP)，内容包括工程流程安全(项目，运作等)；系统流程安全(硬件，软件，数据等)；人力流程安全(培训，安全意识等)和组织流程安全(机构，文化等)4个部分。只有整个机构的总体信息安全流程得到保障，它的产品，技术和服务才有可持续确保安全的基础。IS－CMM为TISP的4个部分提供了定量化的评测和改进基础。

2 IS－CMM体系结构

可以把信息安全能力成熟度等级(Information Security Capability Maturity Level)理解为：机构的安全流程在由低到高的演进过程中所经历的集合了一定成熟度标志的平台。在IS-CMM中,不成熟(Immaturity)的标志体现在：机构没有明确的安全流程体系可以依据，无法对安全性进行预测；未严格定义并执行安全流程，无健全的流程控制及质量控制体系；安全结果依赖于团队或个人的主观因素及能力发挥，无定量基准；等等。成熟度(Maturity)的标志体现在：安全流程依据机构明确定义的准则实施；存在健全的流程控制并可对安全性做出预测；安全质量得到有效监控(借助定量化的数据)并较少依赖团队或个人的主观能力和自然因素；过去的安全经验得以积累并可系统地用于现行和未来的安全之中；等等。

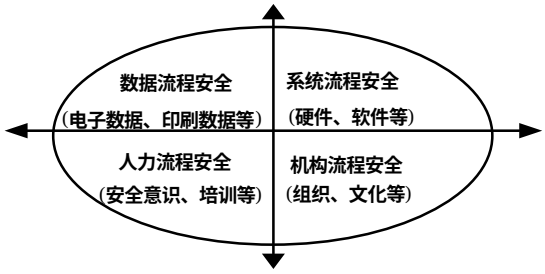

图1 总体信息安全流程结构图

IS-CMM可用的功能如下：

(1)由IS-CMM授权评估师对一个或数个机构实施信息安全流程评估；

(2)机构自身进行信息安全流程自测评定；

(3)风险分析与管理；

(4)脆弱性监测；

(5)信息保密性，完整性和可靠性改进；

(6)帮助一个或数个机构设计信息安全流程；

(7)帮助一个或数个机构规划信息采购方案。

基金项目：国家留学人员启动基金资助项目
作者简介：邓 冰(1967－)，男，留美博士，主研方向为流程管理、软件工程
收稿日期：2002-06-14

IS-CMM将信息安全流程实施的全部生命周期(不同于信息安全开发中的生命周期)分为4个相对独立的阶段：预防(Prevention)；监测(Monitoring)；修正(Amendment)；更新(Revision)。流程的第一阶段为预防，包括信息安全资产评估、安全需求细分、风险分析、安全计划与预防实施等。第二阶段为监测，着眼于安全脆弱性、安全灾难、操作失误等的监控跟踪。第三是修正阶段，针对第二阶段发现的问题进行更正，解决错误。最后是更新阶段，将涉及的部分或整体安全流程模块进行重新界定，重整和升级。

表1 信息安全流程实施生命周期

预防(P)	设 计
	实 施
	测 试
	维 护
监 测(M)	设 计
	实 施
	测 试
	维 护
修 正(A)	设 计
	实 施
	测 试
	维 护
更新(R)	设 计
	实 施
	测 试
	维 护

在IS-CMM中，机构的信息安全流程成熟度从低到高有5个能力等级：

第一级：无控制级(Uncontrolled Level)；

第二级：控制级(Controlled Level)；

第三级：定义级(Defined Level)；

第四级：定量级(Quantified Level)；

第五级：预防级(Preventive Level)。

将所有未参加以及未通过二级或二级以上评估的机构都归入无控制级。无控制级机构不一定不具备上述各等级的能力。例如，一个实力达到控制级的企业可能只是未参加任何评估，由于对它无法准确界定，便将其纳入无控制级。

从第二级(控制级)开始，IS-CMM定义了各级的核心流程域(KPAs)(见表2)。

表2 IS-CMM核心流程域

等级：	核心流程域
第二级 (控制级) (Controlled Level)	安全需求细分；
	安全流程计划；
	安全流程文档；
	安全执行跟踪；
	安全配置管理；
	威胁与脆弱度监测。
第三级 (定义级) (Defined Level)	机构安全流程定义；
	组际安全合作；
	安全培训；
	风险管理；
	代码安全。
第四级 (定量级) (Quantified Level)	定量安全数据收集；
	定量安全流程标准化；
	机构安全文化；
	跨机构安全协作。
第五级 (预防级) (Preventive Level)	缺陷与攻击预防；
	安全流程持续改进。

除无控制级(第一级)外，每一级成熟度都由若干KPAs构成，它们分别针对安全流程的某一方面阐述了某一等级能力应具备的成熟度标志。在第二级，IS-CMM注重基本安全层面的改进，它将信息安全流程中的需求、计划、文档、执行跟踪、配置管理和监测等基本环节确立为本级的KPAs。这一级的组织应该初步具备信息安全流程体系，并基于文档和以往的安全经验建立起了安全流程基准线。控制级既可以在整个机构范围内实施，也可以在机构所属的部门或团队中实施。如果是机构内部某一分支通过了控制级(第二级)评审，IS-CMM仍然承认其有效性。从定义级(第三级)开始，IS-CMM强调机构在信息安全流程上的整体参与，评估也主要基于全组织，而非单个部门或团队。第三级还特别强调了代码安全环节在安全流程的重要性，提出了“正确即安全”的安全流程管理理念。当机构达到前述两级的要求后，便进入定量级(第四级)阶段。在定量级，机构主要致力于两方面的改进：一是量化安全流程，为机构提供精确、全面的定量化数据和标准；二是员工安全文化的确立。IS－CMM的最高级是预防级(第五级)。机构能在前四级的基础上基本控制安全缺陷和攻击的发生及损害，并可针对自身特色制作有创造性的、持续的安全改进流程。

为了通过某一等级，组织必须具备这一等级所规定的所有成熟度标志(KPAs)。KPAs为机构指明了达到能力成熟度等级的目标组。此外，IS-CMM还设定了一系列基本实践(Basic Practices, 简称BPs)来实现这些目标组。机构达到某级标准意味着它不仅达到了本级所有的KPAs，而且包括所有下一级的KPAs。例如，第四级(定量级)的实现必须完成四级本身具备的4个KPAs，以及第三级中的5个KPAs和第二级中的6个KPAs，共15个KPAs。

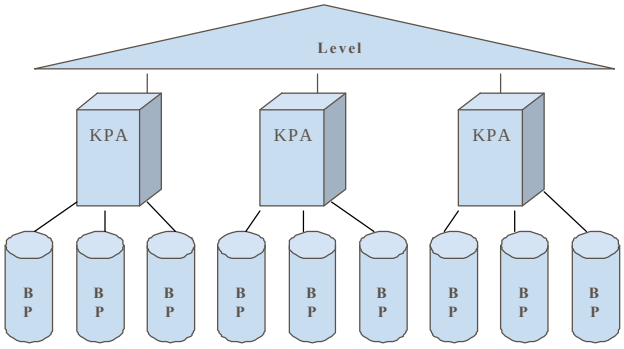

图2 IS-CMM结构图

按照TISP, 我们将全部KPAs作了以下划分(表3)。

表3 KPA分类说明

工程流程	系统流程	人力流程	组织流程
安全需求细分	安全配置管理	安全培训	机构安全流程定义
安全流程计划	代码安全	机构安全	组际安全合作
安全流程文档	定量安全数据收集		跨机构安全协作
安全执行跟踪			
威胁与脆弱度监测			
风险管理			
定量安全流程标准化			
缺陷与攻击预防			
安全流程持续改进			

限于篇幅，本文不深入探讨IS－CMM的定义细节。

(下转第126页)

全技术委员会以及相关信息安全服务单位为成员的安全组织体系，并规范了组织体系中主要部门的安全管理职能[4]。

3.3 建立制度体系

建立健全各项信息安全制度是进行安全管理的基础。路网目前有许多针对网络、系统、信息方面的安全制度，但是这些制度通常都是为某个方面的安全问题制定的，没有建立起一个系统的、分级分层的、能够对信息安全的各个方面都能有效约束的制度体系。建立联网收费系统信息安全的制度体系，就是要制定目前缺乏的管理制度，同时完善已经制定的各种管理制度，并由相应的安全组织部门监督执行，使其自上而下的对路网各级单位都具有相应约束力。

3.4 建立安全技术体系

在总体信息安全策略的指导下，把握安全技术本身的特点，解决联网收费系统信息安全中存在的技术问题是建立技术体系的目标。加强对信息安全管理技术的研究，对可采用的安全技术和产品进行研究和筛选，确定是否适合在联网收费系统中应用推广以及相关人员的技术培训是建立安全技术体系的两大工作。目前通过充分的研究论证，我们拟采取的主要安全技术措施有：

(1)数据安全

1)从保护数据库的安全出发，对目前采用的SQL数据库，设置其自身的安全控制策略。

2)防止敏感数据泄露。由于高速公路收费网络是内部的专网，内部用户容易接触到一些内部数据且可能会出于一些个人目的对数据进行修改、删除等，因此应对内部用户进行行为监测，控制和管理内部用户对系统敏感资源的存取，从技术角度确保安全管理制度的执行。

3)采用防火墙对各安全域进行隔离，控制数据的流向。同级安全域之间不允许互访；下级安全域不允许访问上级安全域；上级安全域对下级安全域的访问应有相应的控制措施。

4)对用户基于角色配置相应的权限，使收费系统的使用者与收费系统安全配置的维护者分开，从而避免因安全配置而引起的安全问题。

(2)数据传输安全技术措施

对关键数据的传输和存储(如口令)进行加密处理。对传输重要数据(如收费记录或拆账记录)，在其表结构中增加校验字段(校验字段的值可以是日期、时间、收费员或业主代码、金额的函数)，解决重要数据被违规操作的监测问题。

(3)全面审计控制

记录和跟踪各种系统状态的变化，有效地对安全域内的用户操作行为(登录时间、地点、执行的操作、退出的时间等)进行审计和加以详细记录。在事后可以通过查询日志的方式，找到有关的线索和证据。

(4)应急措施

采取强化数据备份和数据恢复、启用备用设备或系统、制订应急收费方案等措施。如：汇总数据异地备份；出现车道计算机与收费站之间无法通信时，可暂停使用数据自动传输，将收费数据暂时保存在车道计算机，待通信恢复后再上传数据。此外还需要考虑相应的应急法律措施，该方面主要包括：外购设备或软件存在问题造成损失，应提出法律诉讼；系统存在问题使客户造成损失，客户提出法律诉讼时的应讼；对人为原因造成网络无法正常运行的，情形恶劣的，可对当事人提出法律诉讼。

通过这些措施，达到江苏省高速公路联网收费系统安全域的安全管理目标，进而实现江苏省高速公路联网收费系统的泛安全性。

4 结语

江苏省的高速公路建设已进入全国的先进行列，全省高速公路联网收费的建设正在有序推进，通过对目前江苏省高速公路联网收费系统安全的分析论证，我们得出必须从泛安全的角度出发，对已有联网收费系统规划作安全管理方面的补充和完善，整个安全体系结构的设计与安全解决方案的提出必须基于信息系统安全工程理论，从过程和可控的角度构造适合江苏省高速公路联网收费系统安全体系的方法。本研究初步成果已成为江苏省高速公路联网收费系统建设的安全技术规范，下一步的工作是随着江苏省高速公路联网收费系统建设的进行而加以具体实施。

参考文献

1 钱 钢．基于SSE-CMM的信息系统安全工程管理东南大学学报 2002,(1)：32-36

2 钱 钢．基于安全能力成熟模型的信息系统风险评估.管理工程学报，2001,15(4)：58-60

3 徐杰锋．大型企业网络安全如何规划．信息网络安全,2001,(4)：36-40

4 江苏省交通厅编.江苏省苏北高速公路联网收费暂行技术要求.2001

☆☆

(上接第123页)

参考文献

1 Jalote P.CMM in Practice.The U.S.A.:Assison-Wesley, 2000:145-174

2 Paulk M C.Capability Maturity Model for Software, Version 1.1. The U. S. A.: SEI, 1993:5-80

3 Andress M.Surviving Security: How to Integrate People, Process and Technology. The U. S. A.: Sams/Macmillan Computer Publishing, 2001:15-50

4 Parker D B.Fighting Computer Crime. The U. S. A.: John Wiley & Sons, Inc., 1998: 112-215

5 ISO/IEC 17799, First Version. 2000-12-01: 2-65

6 Alberts C J,Dorofee A J.OCTAVESM Criteria, Version 2.0. The U. S. A.: SEI, 2001:13-111