

对我国信息系统认证与认可过程的探讨

王贵骊 江常青 张利
中国信息安全产品测评认证中心

摘要 本文首先简要介绍了美国的信息系统认证与认可过程和我国现阶段的信息系统测评认证的现状。通过我国与美国的信息系统认证与认可过程的比较,分析了我国现阶段信息系统测评认证过程特点,并对今后信息系统测评认证的发展给出了相关建议。

关键词: 信息系统, 认证与认可, 建议

当前,我国政府正大力推进电子政务,越来越多的政府信息系统开始建设并投入运行,这样,创建满足政府法律法规和策略控制的信息安全管理体系面临着新的挑战,如何保证投入运行的信息系统的安全性也成为十分重要的问题。特别是一些跨部门和跨机构信息系统的建设通常需要采用一些新的安全管理方式,使这个问题更加复杂化。维护信息系统全生命周期的安全,需要严格的信息系统认证与认可(C&A)过程,完善的风险评估体系和先进的风险管理策略。

信息系统的认证与认可过程实质上是通过建立了一个标准的过程、一套标准的活动、普遍的任务以及一个管理体系来认证和认可信息系统,一旦获得认证与认可,这个信息系统将能够有效地维护和保障信息系统的基本安全要求。

严格来说,我国信息系统的认证与认可过程正处在发展的初期阶段。整个过程以及方法还需要进行深入的研究,该认证与认可过程的建立应当符合我国信息化建设的实际情况。中国信息安全产品测评认证中心已经建立了一套信息系统测评认证的流程,并完成了党政机关、网上银行和CA体系等几类信息系统的测评认证。本文首先介绍了国外信息系统测评与认证的发展情况,然后,根据我们的工作实践,针对我国信息系统测评认证的特点,分析了我国现阶段的信息系统测评认证过程,并探讨了信息系统认证与认可过程发展方向。

1 美国的信息系统认证与认可过程

美国是最早进行信息系统认证与认可的国家,当前,美国遵行的信息系统认证与认可过程主要有四种:NIACAP(国家信息保障认证与认可过程);DITSCAP

王贵骊,1970年生,中国信息安全产品测评认证中心副主任,高工,中国计算机学会理事

(国防部信息技术安全认证与认可过程); NSTISSI(国家安全通讯和信息系统安全导论); FIPS 102(计算机安全认证与认可指南)。其中, 2000 年制定的 NIACAP 参照了美国国防部的 DITSCAP。每一种认证与认可方法由一些通用的行为构成标准过程, 并且根据信息系统的敏感程度划分了不同严厉等级的评估准则。

这里, 我们着重介绍 FIPS 102 和 DITSCAP。FIPS 102 针对非涉密的, 民间机构信息系统的测评认证, 而 DITSCAP 则是 1997 年开发的, 针对美军方系统的认证与认可过程。

FIPS 102^[1]于 1983 年 9 月发布, 它不仅仅能够对建立 C&A 过程提供指导, 而且能够对 C&A 过程的实施提供指导。FIPS 102 中的认证与认可过程具有六个步骤: 计划; 数据收集; 基本评估; 详细评估; 认证报告; 认可。

DITSCAP^{[2][3]}由美国国防部 1997 年发布, 它由四个阶段组成: 定义 (definition) 阶段, 验证(Verification)阶段, 证实(Validation)阶段, 发布认可(Post Accreditation)阶段。定义阶段主要是由认证与认可各方对信息系统的安全需求, 边界, 规划, 认证与认可所需要的资源和认证等级等进行协商, 达成协议, 完成文档 SSAA(System Security Authorization Agreement), SSAA 就是将认证与认可参与各方对于信息系统的安全需求及其安全策略等所达成的一切协议以书面的形式记录下来。从我们的理解来看, 其作用相当于信息系统的保护轮廓 (PP)。验证阶段就是核查所建立的信息系统是否与 SSAA 中的定义相符。证实阶段则通过安全测试与评估, 渗透性测试等技术手段来验证所集成的信息系统与 SSAA 中规定的安全策略与安全需求一致, 该阶段为指定认可机构(DAA)发布认可提供足够的证据。发布认可阶段则是确保系统被可靠管理、运行和维护, 并保持可接受的残余风险等级。

FIPS 102 和 DITSCAP 这两种认证与认可过程对信息系统全生命周期内的安全评估和安全状态管理提供了标准的流程。它们均指定了相似的参与方, 参与方的职责也相似。DITSCAP 参与方有认可方 (Accreditor), 负责设备采购方, 认证方, 用户。整个 DITSCAP 依赖于这四方所达成的协议 SSAA。FIPS 102 参与方有认可方, 认证方, 设备采购方, 评估方。其最终的成果是评估报告, 内容包括信息系统评估结果以及对信息系统的安全建议, 评估报告包含进行认可所需要的一切证据。这两种认证与认可过程中认可方具有相同的职责。DITSCAP 过程

中,设备采购方负责设备购买以及系统开发,而 FIPS 102 中设备采购方则负责其机构内安全程序定义和管理。DITSCAP 中的认证者的责任是 FIPS 102 中认证方和评估方的总和, DITSCAP 中还包括了用户代表方。

DITSCAP 从 1997 年建立以来,已经进行了 400 多个信息系统的认证与认可。应该说已经进入了发展相对成熟的时期。对我国信息系统的认证与认可过程具有较大的借鉴意义。

2 我国现有的信息系统测评认证过程

信息系统测评认证在我国可以说是一项新兴业务。中国信息安全产品测评认证中心开展这项业务才两年多时间,但发展很快,已经建立了一套符合现阶段我国信息化发展的测评认证过程。该过程由五个阶段组成,见图 1。

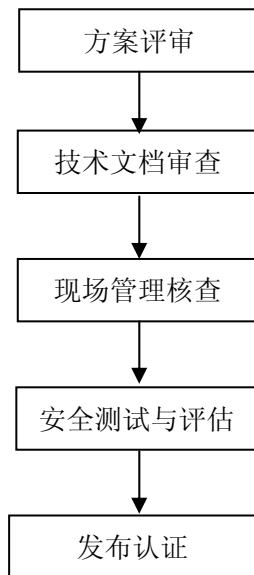


图 1 我国现阶段的信息系统测评认证过程

方案评审阶段由用户向中国信息安全产品测评认证中心提出申请,并提交他们的信息系统建设的安全需求和技术方案,又测评认证中心组织专家对其技术方案与其安全需求的符合性以及技术方案的技术完备性进行审查,并最终给出方案评审报告和技术方案审定书。

技术文档审查阶段则是用户对其信息系统申请认证后,应当按照测评认证中心的要求提交相应的技术文档^[4],见图 2。并由认证中心对技术文档的内容的合

理性进行审查，这部分的技术文档的作用相当于美国 DITSCAP 过程的 SSAA。现场管理核查阶段则是根据 ISO17799 及其安全策略，对信息系统的安全管理进行现场核查。ISO17799 源自英国标准 BS7799 的第一部分：信息技术—信息安全管理实施细则。该标准从以下十个方面对信息安全进行评价：信息安全政策；安全组织；资产分类与管理；个人信息安全守则；使用环境的信息安全管理；通讯和操作过程管理；存取管理；信息系统的开发和维护；业务持续性；合法性，共 10 大类，36 个目标，127 个措施。

安全测试与评估阶段则是通过脆弱性测试和渗透性测试等技术手段对信息系统的的状态进行评估。安全测试不同于黑客攻击行为，它要比黑客攻击行为复杂得多。安全测试的目标是尽可能地发现信息系统所存在的所有安全隐患。因此，安全测试需要标准和方法进行指导。中国信息安全产品测评认证中心将整个安全测试分为六大部分：Internet 安全；Information 安全；社会工程测试；无线安全；通讯安全；物理安全，共包括 33 个模块，每个模块又由若干任务组成。模块之间相互关联，构成了一个比较全面的安全测试通用方法。现场管理核查和安全测试与评估阶段为信息系统认证提供足够证据。

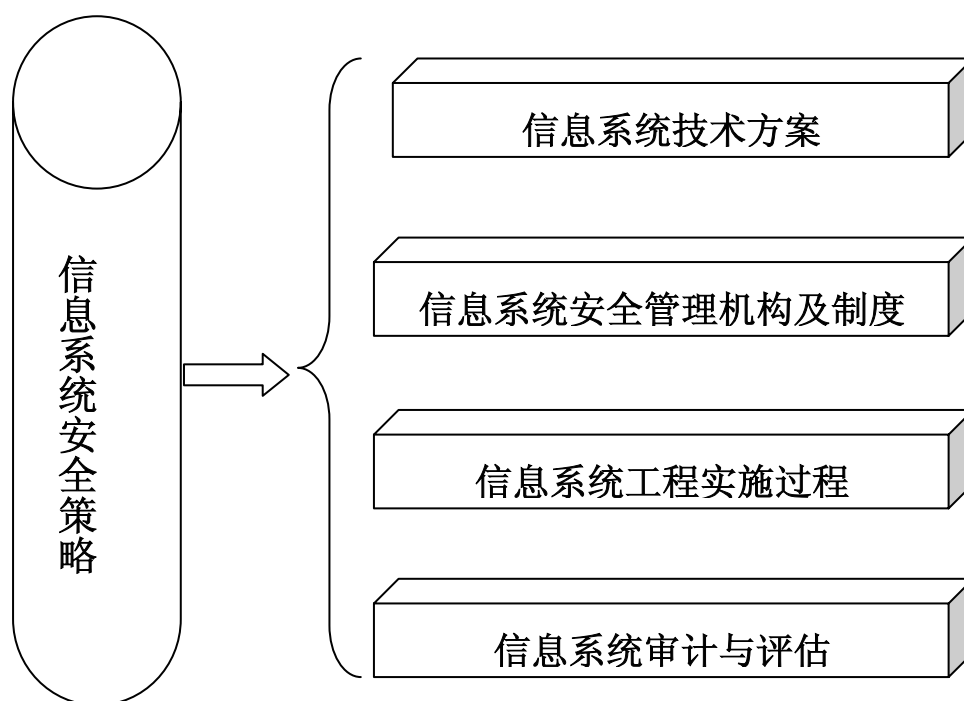


图 2 认证申请者的文档要求

4 对我国信息系统测评认证工作的展望

随着我国信息化进程的不断深入，对信息系统测评认证的要求会越来越迫切，对信息系统测评认证的技术需求同样会提高，这种状况进而会不断推动测评认证过程的日趋规范。

为了保证我国的信息系统测评认证过程跟上信息化发展步伐，同欧美等信息技术发达国家和地区相比，我们在法律法规、测评标准、测评技术、组织管理和人才培养等方面还有大量的工作要做，需要得到政府相关部门的进一步的指导与支持。

1、法律法规方面：信息系统测评认证需要国家相关的法律加以支持，正如上文中提到的美国，正是用国家法律法规的形式规定了政府机构信息系统安全性必须进行强制性的认证与认可，政府的采购也必须在产品测评认证的基础上进行。目前我国，只有北京和上海这两个信息化建设发展较快的城市已经发布了相关的地方性法律法规来对其电子政务信息化工程来进行管理，如：

《北京市政务与公共服务信息化工程建设管理方法》、《北京市人民政府关于加快政务信息化建设的意见》、《北京市党政机关网络与信息安全管理办法》、《关于加强上海市信息安全工作的若干意见》和一些金融、证券机构《网上证券委托暂行管理办法》等。这样地方性法规很容易造成各地政令不一，缺乏统一管理。国家应当通过立法，对不同信息系统是否进行强制性认证进行法律意义上的明确规定。

2、标准体系方面：标准是认证的基础，标准相对滞后于技术发展是全球普遍存在的规律。就信息安全测评认证标准而言，针对产品的信息技术安全性评估准则（GB/T 18336）及相关安全补充要求经过几年的研究开发，已逐步形成体系，但是对信息系统安全性进行评估的标准及相关配套的标准仍需要在实践中不断地完善和发展。具体到信息系统安全性测评认证，以下标准的制订至关重要：

- ✓ 信息系统安全评估通用准则；
- ✓ 党政机关信息系统安全评估细则；
- ✓ 网上银行安全评估细则；
- ✓ 网上证券委托系统安全评估细则等。

3、**测评技术方面：**对于信息系统安全性测评认证，标准是基础，技术是关键。只有在测评技术上一直保持领先，才能真正发现系统中可能存在的安全隐患，才能真正提出行之有效的整改措施，也才能达到为电子政务的发展保驾护航的目标。由于电子政务的发展对测评认证提出了相当艰巨和复杂的任务，认证中心应尽快提高对政府服务的能力和水平，加大测评技术研究开发方面的投入，建立相应的测评环境和人才队伍，满足日益增长的电子政务安全管理的需求。

信息系统测评与认证业务的发展需要相关各方的共同努力。我们热烈欢迎大家一起研究，推动我国的信息系统测评认证事业的发展。

参考文献：

- [1] Federal Information Processing Standards Publication, FIPS PUB 102, Sept. 1983
- [2] DoD Information Technology Security Certification and Accreditation Process(DITSCAP), No.5200.40, Dec. 30, 1997
- [3] DoD Information Technology Security Certification and Accreditation Process(DITSCAP) Application Manual, July, 2000
- [4] 国家信息安全测评认证系统认证申请书，中国信息安全产品测评认证中心，2001，12

Investigation to our country's Information System Security Certification and Accreditation Process

Wang guisi Jiang Changqin Zhang Li

China Information Technology Security Certification Center

Abstract In this paper, it first introduces nowadays information system security certification and accreditation (C&A) process of American and our country. Through the comparison to the two process, the characteristics of the C&A process in our country is analyzed, and some suggestions is presented to the development of our country's C&A process.

Key words: information system (IS); certification and accreditation; suggestion