电子政务信息安全体系结构研究

Research on e－Government Information Security Architecture

秦天保 （上海海事大学 交通运输学院 200135）

摘要：电子政务信息安全是电子政务正常运行的基本前提，信息安全的保障需要从电子政务安全体系结构的角度加以研究。电子政务信息安全体系结构是指能够保证电子政务安全运行的各种保障措施、技术和体制的有机综合体。本文提出了一个综合性的电子政务信息安全体系结构，研究了其组成。

关键词：电子政务 信息安全 安全体系结构

1 引言

电子政务信息安全的最终目的是确保信息的机密性、完整性、可用性、可审计性和抗抵赖性，以及信息系统主体（包括用户、团体、社会和国家）对信息资源的控制。任何通过单一手段保障信息安全的企图都是片面的，信息安全的保障需要从电子政务安全体系结构的角度加以研究，所谓电子政务信息安全体系结构是指能够保证电子政务安全运行的各种保障措施、技术和体制的有机综合体。在科学的安全体系结构指导下，从不同的方面采取综合性的保障措施保障电子政务的信息安全。本文提出一种综合性的电子政务信息安全体系结构，该体系结构由安全控制和安全管理流程保障体系、安全技术保障体系、安全组织保障体系、安全制度保障体系构成，其整体构造如图 1 所示。

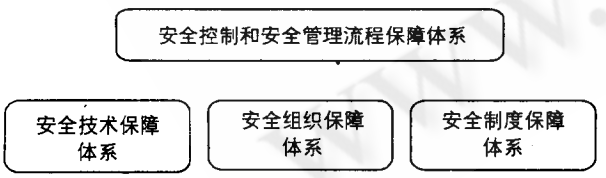

图 1　电子政务信息安全体系结构

2 安全技术保障体系

信息安全技术保障体系从技术角度提出保障信息安全所需的相关技术，技术体系可以按照协议层次、安全服务，安全机制和系统构成单元等组织成多维结构，如图 2 所示。面对一个实际的电子政务应用，应该根据这些维度实施、验证安全技术措施，以从技术上保障电子政务应用的安全性。

在该体系结构中，在不同的协议层次上，需要配置相应的安全服务，每一种安全服务可以由一种或多种安全机制实现。建立安全系统时，除了考虑协议层次、安全服务、安全机制外，还应该从系统构成单元的角度考察安全技术配置，其不同单元可能采取的安全技术措施如表 1 所示。

表 1　不同系统构成单元的安全措施

系统构成单元	安全技术举例
物理环境安全	警卫、锁、跟踪设备
网络外围安全	防火墙、VPN 、端口封堵、IP 地址转换、
内部网络安全	IPSec、网络分段、网络通讯加密、阻塞通讯端口、对网络数据包签名、身份认证
主机安全	身份认证、加强操作系统的安全设置、安装安全更新程序、实施审核、禁用或删除不必要的服务、安装和维护防病毒软件
应用程序安全	只启用必需的服务和功能、配置应用程序安全设置、安装应用程序的安全更新程序、安装和更新防病毒软件、以最低权限运行应用程序
数据安全	对文件进行加密、用访问控制列表限制数据访问、创建数据备份和恢复计划

3 安全组织保障体系

电子政务信息安全的运作需要强有力的组织体系保障，以使得有关信息安全管理和实施的政令通畅。通常，电子政务安全组织保障体系包括三个层次，即决

策层、管理层、和执行层，一个典型的组织形式如图 3 所示。

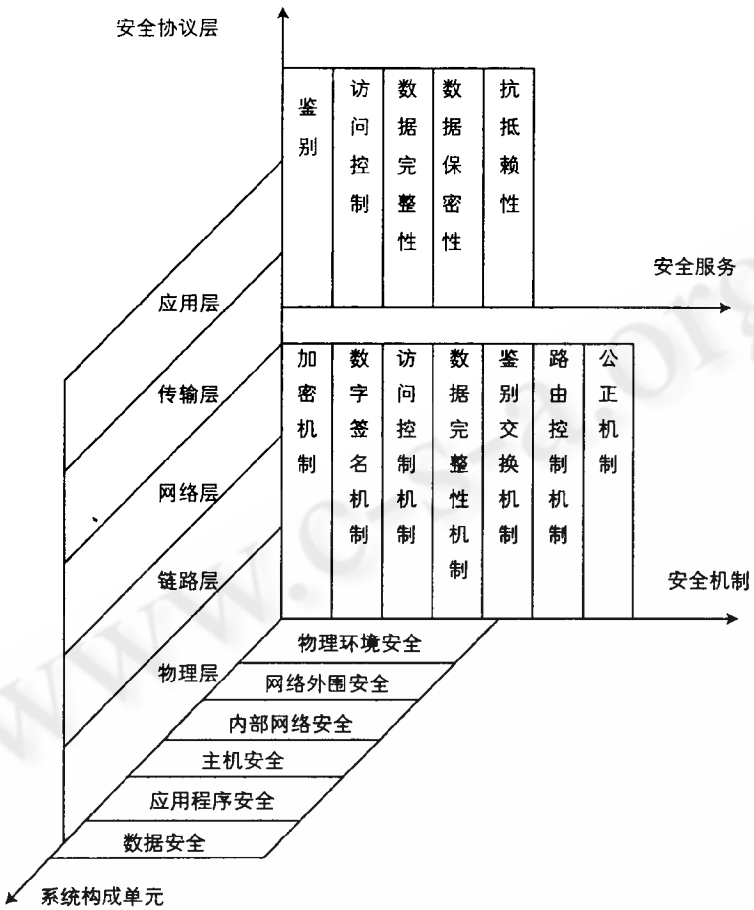

图 2　安全技术保障体系

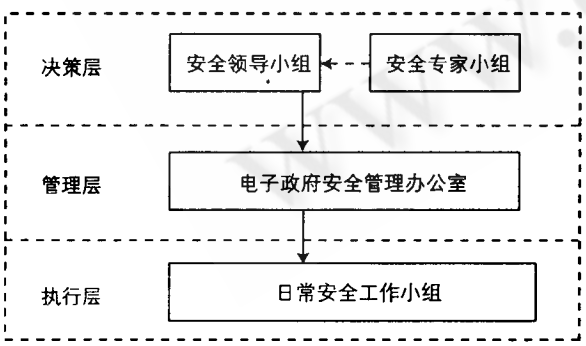

图 3　安全组织保障体系

3.1 决策层

决策层是决定信息系统安全重大事宜的领导机构，决策层主要包括安全领导小组和安全专家小组。安全领导小组是常设机构，是单位信息安全工作最高领导决策机构，不隶属任何部门，直接对单位最高领导层负责。

安全专家小组以单位信息安全领导小组成员为核心，邀请本单位或社会上与信息安全、法律政策、行政（企业）管理等有关的专家学者参加，组成智囊团，对单位信息安全领导小组负责。

3.2 管理层

管理层是日常管理机构，核心实体是电子政务安全管理办公室，其主要职能是在单位信息安全领导小组直接领导下进行工作的，负责处理本单位信息安全管理的日常工作，根据决策层的决定全面规划并协调各方面力量实施信息系统的安全方案，制定、修改安全策略，处理安全事故，设置安全相关的岗位。

3.3 执行层

执行层是在管理层协调下具体负责某一个或特定几个安全事务的逻辑群体，这些群体形成单位日常安全工作小组，分布在信息系统的各个操作层岗位上。小组成员包括信息安全员、系统安全员、网络安全员、设备安全员、数据库安全员、数据安全员、防病毒安全员、机房安全员、警卫人员和防火安全员等。对安全工作小组人员应严格审查、签订保密协议、分散权力。

4 安全制度保障体系

信息安全制度保障体系是指安全相关的标准、法律法规和日常制度等组成的制度体系，如图 4 所示。

4.1 安全标准保障体系

电子政务信息安全管理如果缺乏相应标准的支持，安全管理就会陷于混乱。信息安全标准体系由信息安全基础标准、物理安全标准、系统与网络安全标准、应用与工程安全标准、安全管理标准、安全产品标准、安全评估标准等组成，图 5 所示。

4.2 安全法律法规保障体系

信息安全律法规是信息安全的重要保障，我国为

了适应信息化的发展，已经制定颁布了一系列信息安

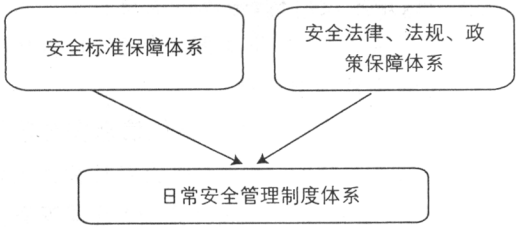

图 4　安全制度保障体系

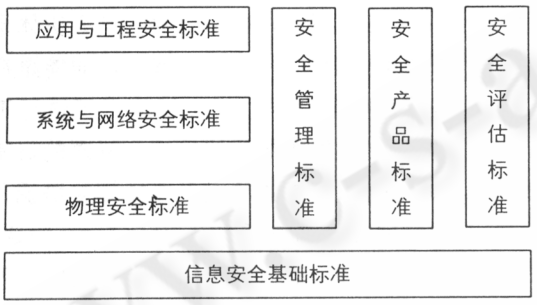

图 5　信息安全标准体系

全相关的法律法规，如《中华人民共和国计算机信息系统安全保护条例》、《商用密码管理条例》、《中华人民共和国电信条例》、《计算机信息系统国际联网保密管理规定》、《互联网信息服务管理办法》、《计算机信息系统安全专用产品检测和销售许可证管理办法》等，并对诸如《中华人民共和国刑法》等部分传统的法规进行了适应信息化发展的一些修订补充。

但是，信息化发展带来了许多新概念和管理上的新特点，不少问题还有待深入研究，在信息安全法律领域，尽管已做了大量工作，但目前我国有关信息化以及信息安全的法规体系尚未完全配套，尚未形成完善的法律法规体系，因此，未来信息安全法律法规体系的建设将是电子政务建设的一个重要任务。从大的方面来看，我国整个信息安全法律法规体系如图 6 所示。

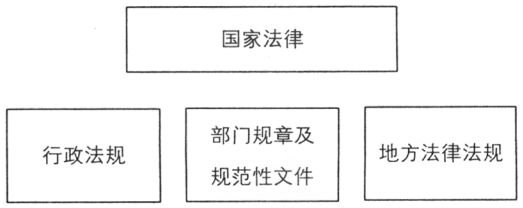

图 6　安全法律法规保障体系

5　安全控制与安全管理流程保障体系

信息系统安全需要通过一系列科学规范的安全管理流程组织实施，安全管理流程需要采用一系列控制措施实现其目标。因此在制定安全管理流程前，首先需要确定有哪些控制措施可供选择，即，首先要确定信息安全控制措施体系。

5.1　安全控制措施体系

组织的信息安全需要全面、科学的安全控制措施来保障，根据英国标准协会（BSI）制订的《信息安全管理标准》（BS7799），安全控制措施可以划分为如图 7 所示的 10 个领域。

（1）安全政策。制定信息安全方针政策，为信息安全提供管理指导和支持。

（2）组织安全。建立信息安全组织管理框架，管理组织范围内的信息安全；维护被第三方访问的组织的信息处理设施和信息资产的安全；以及当信息处理外包给其他组织时，维护信息的安全。

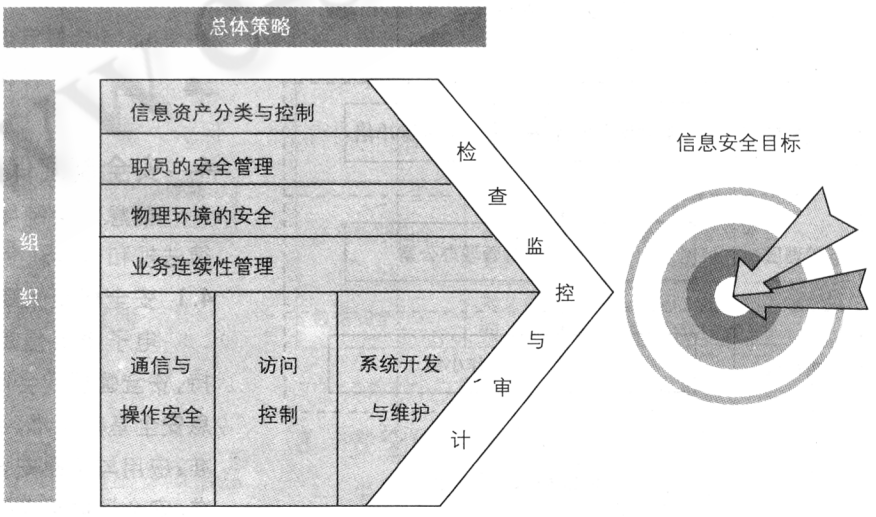

图 7　安全控制措施领域分类

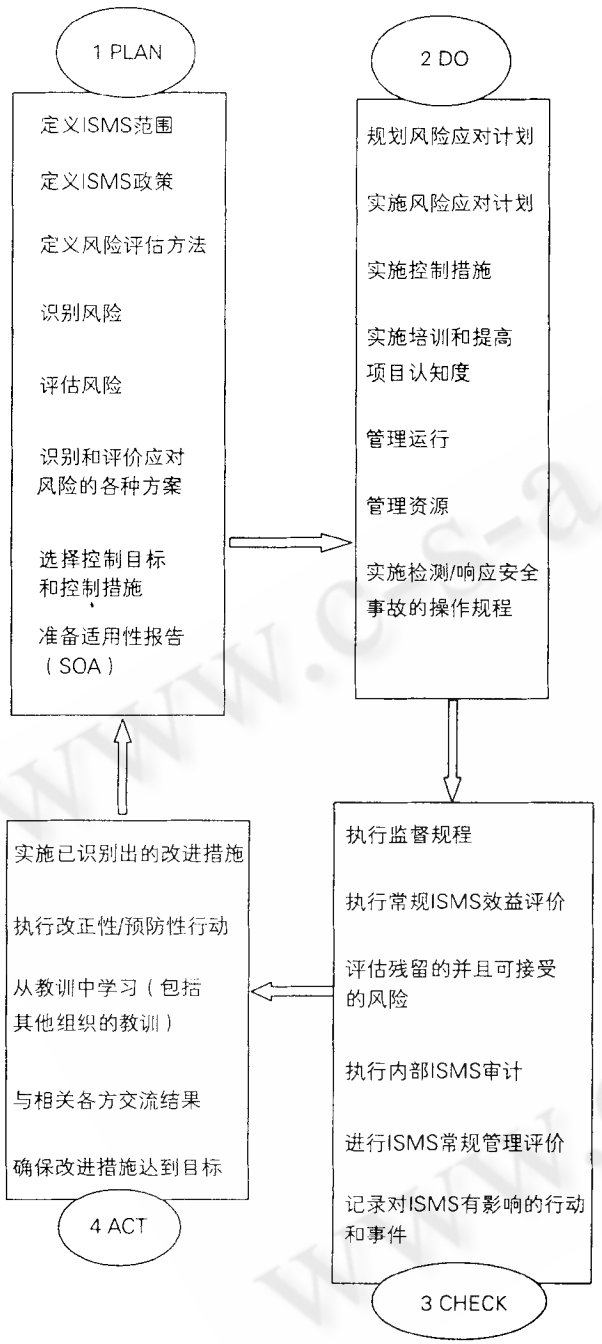

图 8　信息安全管理流程和活动

（3）资产的分类与控制。检查、清点、分类所有信息资产，确保各类信息资产受到适当程度的保护。

（4）人员安全。注意人员工作职责定义，减少人为差错、盗窃、欺诈或误用设施的风险。

（5）物理和环境的安全。定义安全区域，以避免对企业办公场所和信息的未授权访问、损坏和干扰；保护设备的安全，防止信息资产的丢失、损坏、泄露和业务活动的中断。

（6）通信和操作管理。制定操作规程和职责，确保信息处理设施的正确和安全操作；建立系统规划和验收准则，将系统故障的风险减到最小。

（7）访问控制。制定访问控制的业务要求，以控制对信息的访问；建立全面的用户访问管理，避免信息系统的未授权访问；让用户了解他对维护有效访问控制的职责，防止未授权用户的访问。

（8）系统开发和维护。明确系统的安全要求，确保安全机制被内建于信息系统内；控制应用系统的安全，防止应用系统中用户数据的丢失、被修改或误用。

（9）业务持续性管理。目的为了减少业务活动的中断，使关键业务流程免受主要故障或灾害的影响。

（10）符合性。信息系统的设计、操作、使用和管理要符合法律、法规及相关标准、文件的要求；定期审查安全政策和技术符合性。

5.2　安全管理流程保障体系

前述各种安全控制措施要通过安全管理流程来系统化实施，组织在建立自己的信息安全体系时，其安全管理流程应遵循著名的 Plan – Do – Check – Act 循环周期，在此周期中每个阶段的活动（步骤）如图 8 所示。

6　结语

电子政务安全保护涉及到多种因素、多个方面，非某一因素、某一方面所能独立完成，必须建立融合各种保护力量为一体的电子政务安全体系结构，从多个方面，多个层次采取安全措施，才能确保电子政务安全水平达到可接受的程度。

参考文献

1　李会欣，电子政务安全运行引论，中国经济出版社，北京，2003。
2　中国信息安全产品测评认证中心，信息安全工程与管理，人民邮电出版社，北京，2004。
3　秦天保、方芳，基于 BS7799 构筑企业信息安全管理体系，情报杂志，2004.2。