信息安全保障人员认证培训教材

电子政务安全

DIAN ZI ZHENG WU AN QUAN

中国信息安全认证中心

◎主 编 张 剑 ◎副主编 汤志伟 张会平

★★★ CISAW ★★★

电子科技大学出版社

信息安全保障人员认证培训

电子政务安全

DIAN ZI ZHENG WU AN QUAN

中国信息安全认证中心

◎主 编 张 剑 ◎副主编 汤志伟 张会平

★★★ CISAW ★★★

电子科技大学出版社

图书在版编目（CIP）数据

电子政务安全 / 张剑主编. —成都：电子科技大学出版社，2015.2
ISBN 978-7-5647-2852-6

Ⅰ.①电… Ⅱ.①张… Ⅲ.①电子政务-安全技术
Ⅳ. ①D035.1-39

中国版本图书馆 CIP 数据核字（2015）第 037897 号

内 容 提 要

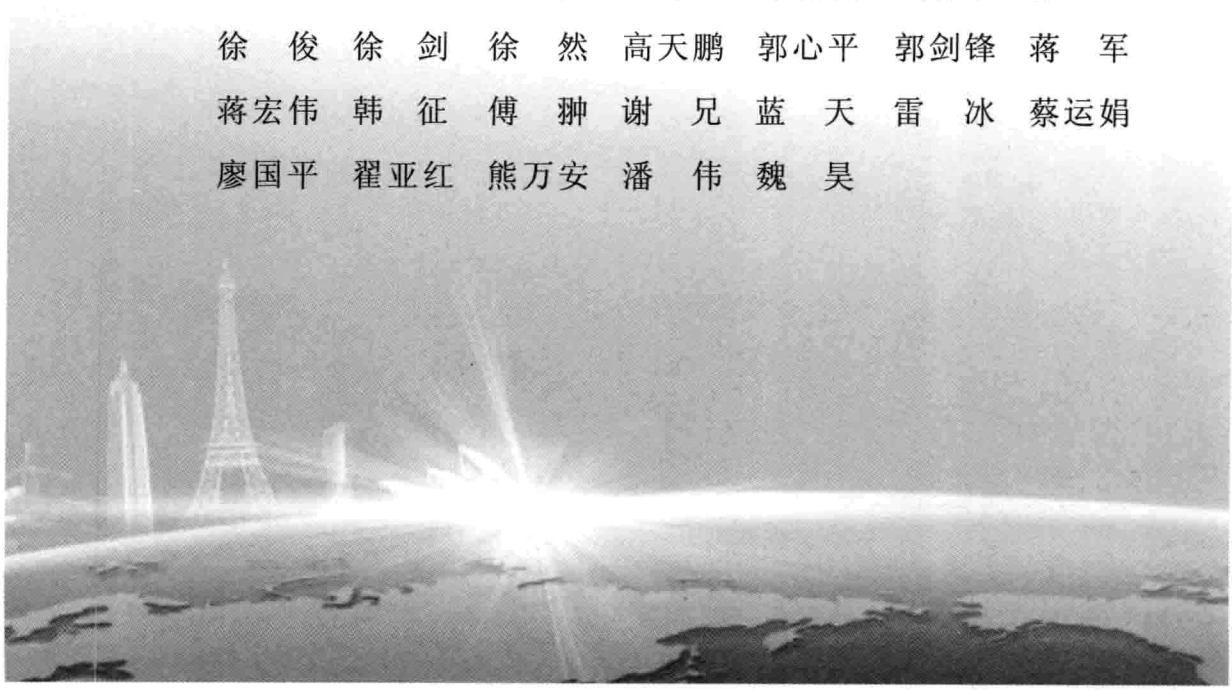
本书以信息安全保障人员认证(CISAW)培训的需求为总纲，结合 CISAW 电子政务安全保障模型，从电子政务领域的特点和电子政务安全保障的具体环节出发，详细介绍了电子政务安全保障中的合规性分析、安全策略制定、安全风险评估、安全保障措施、安全监测和安全提升等内容，并结合实际案例阐述了安全保障措施在电子政务工程中的具体应用。

电子政务安全

主　编　张　剑
副主编　汤志伟　张会平

出　　版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦　邮编：610051）
策划编辑：徐守铭
责任编辑：郭蜀燕　徐守铭
责任校对：刘　愚
主　　页：www.uestcp.com.cn
电子邮箱：uestcp@uestcp.com.cn
发　　行：新华书店经销
印　　刷：成都市川侨印务有限公司
成品尺寸：185 mm × 260 mm　　**印张** 16.75　　**字数** 337 千字
版　　次：2015 年 2 月第一版
印　　次：2015 年 2 月第一次印刷
书　　号：ISBN 978-7-5647-2852-6
定　　价：50.00 元

丛书编委会



编 写 组

主　编　张　剑

副主编　汤志伟　张会平

编　委　钟　毅　高天鹏　林　利　王　莉　蔡运娟　朱　强　成林芳

汤　亮　蒋　军

序

2014年，我国提出了建设网络强国战略与目标。实现网络强国，培养和造就网络与信息安全人才队伍是关键。据调查，截至2014年年底，国内网络与信息安全人才缺口高达50万人，并呈现持续增长的趋势。加快人才培养是我国经济社会发展和信息安全体系建设中的一项长期性、全局性和战略性的任务。

作为我国专业信息安全认证机构和培训机构，中国信息安全认证中心以保障国家网络与信息安全为己任，于2011年推出了信息安全保障人员认证（CISAW）。CISAW认证是面向IT从业人员、在校学生，特别是与网络与信息安全密切相关的高级管理人员、专业技术人员推出的人员资格认证和专业水平认证。CISAW认证的推出和实施，为培养和造就我国网络与信息安全人才探索了一条有效途径，得到了业内专家和社会各界的好评。

推行CISAW认证，编写高质量的教材尤为重要。鉴于此，中国信息安全认证中心组织国内信息安全保障的专业技术和应用领域的专家，依据《信息安全保障人员认证考试大纲》要求，结合信息安全保障工作的各岗位知识和应用能力要求，共同编著了信息安全保障人员认证系列教材。本系列教材包括《信息安全技术》《信息安全技术应用》和《信息安全实验》3种基础教材；《软件安全开发》《信息系统安全集成》《信息安全管理》《信息安全咨询手册》《信息系统安全运维》《信息系统安全审计》《信息安全风险管理》《网络攻防技术》《业务连续性管理》《云计算安全》《物联网安全》和《工业控制安全》12种专业技术应用教材；《电子政务安全》《电子商务安全》《交通服务信息安全》《能源服务信息安全》《医疗卫生信息安

全》《教育服务信息安全》《金融服务信息安全》《通信服务信息安全》《宾馆服务信息安全》和《物流服务信息安全》10 种应用领域教材。

本系列教材以实用为首要原则，从统一的信息安全保障模型出发，构建了包括信息安全技术基础知识、信息安全专业技术知识和应用领域安全保障管理知识的完整信息安全保障知识体系。既是广大 CISAW 认证申请者的考试指导用书，同时也是广大信息安全保障工作者的工作指南和参考用书。

希望本系列教材的出版，能为广大信息安全保障从业者学习、工作和申请认证提供指导和帮助。

是为序。

中国信息安全认证中心主任　魏　昊

2014 年 12 月 28 日

前　言

本书力求针对电子政务安全保障的实际要求，对 CISAW 框架下电子政务安全的必备重要知识进行了全面、简洁的介绍。本书共分 8 章，具体包括：第 1 章概述，详细介绍了电子政务安全的概念及电子政务安全保障模型，之后的各章以此电子政务安全保障模型为基础，分别阐述了电子政务安全的主要知识；第 2 章探讨了电子政务安全的合规要求和相关监管机构；第 3 章介绍了电子政务安全策略，它是指导电子政务安全实施的正式纲领性文件；第 4 章介绍了如何对电子政务安全实施评估；第 5 章介绍了电子政务安全的技术、资源、管理三大保障措施；第 6 章对电子政务安全中的监测和评价问题进行了介绍；第 7 章介绍了电子政务安全的一些典型工程；第 8 章给出了电子政务安全的典型案例和案例分析。

本书作为信息安全保障人员认证考试用书，是按照考试大纲的要求进行编著的，适合广大申请认证考试的人员使用；同时，也适合所有从事与电子政务安全相关的工作人员、期望了解电子政务安全相关知识的人员使用。与本书配套的基础教程《信息安全技术应用》详细介绍了相关的安全技术基础知识和应用原理，可供相关人员参考。

本书由张剑、汤志伟、张会平、钟毅、高天鹏、林利、王莉、蔡运娟、朱强、成林芳、汤亮、蒋军等共同编写，在此，对各位的辛勤付出表示衷心感谢。

本书在成书过程中得到了《信息安全保障人员认证考试用书》编委会的指导，得到了中国信息安全认证中心、四川省中认信安技术服务有限公司、四川亚和企业咨询服务有限公司、电子科技大学政治与公共管理学院、

湖南省网络与信息安全测评中心和湖南浩基信息技术有限公司的大力支持，在此表示衷心感谢。

本书在编写过程参考或引用了国内外同行的大量文献资料，在此向这些文献资料的作者表示衷心感谢。

我们力图通过较小的篇幅比较完整地、正确地介绍电子政务安全相关的知识，但由于水平有限、时间紧迫，书中仍难免存在疏漏和错误，在此，恳请广大读者和同行批评指正，以便我们再版修订时加以改正和完善。

张　剑

2014 年 12 月 20 日

目　录

第 1 章　电子政务安全概述

电子政务已成为政府履职的重要手段和国家竞争力水平的重要标志。由于政府的各项管理和决策活动是围绕对重要信息的处理，直接涉及到各级政府的核心政务，关系到国家安全和社会稳定，因此，国家对电子政务安全性有极高的要求，保障电子政务安全刻不容缓。习近平总书记在中央网络安全和信息化领导小组第一次会议上指出，“没有网络安全，就没有国家安全”，将网络安全的重要性提升到了国家安全的层面。电子政务安全保障是国家信息安全保障体系的核心部分，是电子政务能否健康发展的关键因素。

电子政务安全是一项复杂的系统工程，要保障电子政务安全，不能仅有安全基础设施和安全保障技术，必须站在国家安全的高度上，从国家安全的范围来统一规划，从政府业务安全的角度统一设计，涉及标准、技术、管理、业务、资源等多个方面。作为本书的开篇，本章从电子政务框架体系与电子政务安全的发展两个主要方面来阐述电子政务的安全保障问题，基于电子政务安全需求分析，提出了多层次、多环节、系统化的电子政务安全保障模型，为保障电子政务安全的建设与实施提供有力指导。

1.1　电子政务概述

对电子政务的理解涉及电子政务的定义和内涵、电子政务的应用模式、电子政务的基本发展情况以及电子政务总体框架等内容。

1.1.1　电子政务的定义与内涵

由于电子政务是一项复杂的系统工作，涉及政策、制度、组织和技术等多方面的因素，因此，不同的组织强调了电子政务不同的方面，对其定义也各有侧重。

世界经济合作与发展组织（Organization for Economic Co - operation and Development，OECD）对电子政务的定义为：“电子政务是将新的信息和通信技术运用到政府的各项职能中，特别是利用因特网及相关技术的网络潜能来改革政府的结构和运行。”

世界银行（World Bank Group，WBG）对电子政务的定义是："政府机构利用信息技术，改造政府与公众、企业与其他政府机构的关系。这些技术更好地向公众提供公共服务、改进政府与产业界的互动关系、使公众更方便地获得信息来增加公民权力、实现更有效的政府管理。通过电子政务的构建，政府可以实现减少政府腐败、提高政府透明度、增加政府收入和节约成本等目标。"

联合国经济和社会理事会（Economic and Social Council，ECOSOC）将电子政务定义为："政府通过信息通信技术手段的密集性和战略性，应用组织公共管理的方式，旨在提供效率、增强政府的透明度、改善财政约束、改进公共政策的质量和决策的科学性，建立良好的政府之间、政府与社会、社区以及政府与公民之间的关系，提高公共服务的质量，赢得广泛的社会参与度。"

除了上面三个组织的定义以外，各国政府和一些国际性组织、研究电子政务的学者及参与电子政务的企业等对电子政务的认识和理解还有很多，其中较系统、全面且又代表性的观点有广义、中义、狭义三个层次的定义。

广义的电子政务定义认为电子政务本质上是把工业化背景下的大政府管理体系转变为新型的管理体系，以适应虚拟的、全球性的、以知识为基础的数字经济。

中义的电子政务定义认为电子政务最重要的内涵，是运用信息技术以及通信技术打破行政机关的组织界限，构建一个电子化的虚拟机关，使得公众摆脱传统的层层关卡的限制以及书面的审核方式。而政府机关之间以及政府与社会各界之间也是经由各种电子化渠道进行相互沟通，并依据人们的要求、人们可以获取的形式、要求的时间及地点等，向人们提供各种不同的用户选择，从应用、服务及网络通道三个层面进行电子化政府基本框架的规划。

狭义的电子政务定义认为电子政务就是各级政府机构的政务处理电子化，主要包括政务电子化和公众服务电子化等在计算机网络上进行的政府管理活动。

结合以上几种观点，本书认为电子政务是指公共管理部门应用计算机技术、网络通信技术、数据库技术和人工智能技术等，以服务型政府为核心，将管理和服务的一项项具体业务集成，实现组织结构和工作流程的优化，提高内部协调与管理效率，以及公共服务的质量与效率。最终实现政务"四化"：行政自动化、政务公开化、管理一体化和决策科学化。

关于电子政务的内涵可以从以下三个方面把握：

（1）电子政务以信息技术为基础

电子政务的实现依托于信息技术平台，没有这一平台，就没有电子政务，因此对于这一平台的规律要有全面的认识。信息技术与传统技术的最大不同在于其高度渗透性和广泛影响面，其运用带来了前所未有的工作效率，甚至改变着人们的工作方式，

在电子政务建设和应用中要深入地理解各种信息技术的潜在能力，充分挖掘它们的能力，做过去没有做过的事情，不断实现管理和服务的创新。要避免仅把信息技术视为政务的简单工具和附庸的误区，理论和实践都已证明用技术简单模拟和固化传统的政务流程对政务绩效的提升作用是非常有限的，这就需要电子政务的参与者充分理解信息技术的能动性。

（2）电子政务以政务为核心

尽管强调技术的重要性，但是电子政务毕竟有其自己的方向，一切技术的能动性都是为达成政务目标服务的，即电子政务的核心是政务。由技术所带来的政府效率的提升、公共服务的便捷和丰富最终将促进政府职能的转变及政府组织的重构，电子政务的落脚点是技术进步所带来的政务活动规律的革新，技术要在这一规律的指引下运用才不会偏离社会公共管理的方向。这里要避免唯技术论的误区，认为技术可以解决一切问题，把政务变革的任务交给软件公司，这种本末倒置的认识是根本错误的。

（3）电子政务是技术支撑下的政府管理方式的革命，要求信息化环境下政府治理方式的变革

电子政务经过几十年的发展，技术的进步与政务创新应用相互交融，电子政务已经从最初的新生事物成为被广泛接受的政府管理方式。电子政务的运用使其更深、更全面地触及到当前政府管理模式的深层次问题，电子政务的概念已经上升到电子治理的高度，融合发展、连接性治理等也成为当前各国电子政务建设的热门话题，电子政务将会真正融入政府行政和公共服务的全过程。电子政务已远不是技术和政务的简单加总，它将带来信息化环境下新的政府治理格局，需要对其新规律进行深入的研究。

1.1.2　电子政务的应用模式

电子政务在世界范围内的逐渐发展，形成了其自身的应用模式，目前，电子政务应用的主要模式有以下四类：

1.1.2.1　G2C 模式

G2C 的英文是 Government to Citizen，也可写作 GtoC，是政府与公民之间电子政务的简称。G2C 模式是指政府部门向公众提供的各种服务，公众在线获得政府信息和服务的电子政务模式。通过这种模式，提高了政务活动的透明性，有利于公众的民主参与和有效的监督，促使公务人员的廉洁自律，而且公民可以快捷、方便获得到各类信息和服务，大大地节约了公民的时间。目前这种模式主要有以下具体应用：电子身份认证、电子社会保障服务、电子民主管理、电子医疗服务、电子就业服务、电子教育培训服务等。

1.1.2.2　G2B 模式

G2B 的英文是 Government to Business，也可写作 GtoB，是电子政府与企业之间电子

政务的简称。G2B 模式是指政府通过电子化网络系统为企业提供公共服务的电子政务模式。通过该模式，打破了政府部门之间的界限，实现业务部门在资源共享的基础上为企业提供各种信息服务，精简工作流程、简化审批手续、提高办事效率、减轻企业负担、节约时间。目前这种模式主要有以下具体应用：政府电子化采购、电子税务、电子工商行政管理、电子外经贸管理、中小企业电子化服务、综合信息服务等。

1.1.2.3 G2G 模式

G2G 的英文是 Government to Government，也可写作 GtoG，是政府与政府之间电子政务活动的简称。G2G 模式是指政府内部、政府上下级之间、不同地区和不同部门之间实现的电子政务模式。通过该模式，打破机关组织部门的垄断和封锁，加速政府内信息的流转和处理，克服政府各部门相互推诿的现象，提高政府内部的行政效率。目前这种模式主要有以下具体应用：政府内部协同办公、政策法规、电子公文处理、电子司法档案管理、电子财务管理系统、电子资料库、电子培训系统等。

1.1.2.4 G2E 模式

G2E 的英文是 Government to Employee，也可写作 GtoE，是政府与政府公务员即政府雇员（Employee）之间的电子政务活动的简称。G2E 模式是利用 Intranet 建立起有效的行政办公和员工管理体系的电子政务模式，是政府机构通过网络技术实现内部电子化管理的重要形式。通过该模式，提高了政府工作效率和公务员管理水平。为 G2G、G2B 和 G2C 模式的实施奠定了基础。目前这种模式主要有以下具体应用：公务员日常管理、电子人事管理等。

1.1.3 电子政务的发展

本节从国外、国内两个方面介绍电子政务的发展概况。

1.1.3.1 国外电子政务发展历程

进入 20 世纪 90 年代，美国克林顿政府推动了新一轮政府改革。启动了所谓的“全国绩效评估”运动，探讨行政过程改革。在这一绩效评估运动中，政府主动引入了“依靠信息技术再造政府”的观念，提高了政府员工的工作活力与创造力，提升了公共服务水平。在此基础上，国家绩效评估委员会提出了一系列报告，其中《运用信息技术改造政府》报告中强调利用信息技术来“革新”政府，并明确提出了电子政务的概念。随着美国电子政务理念的提出，以及它在美国的成功应用，全世界许多国家日益重视电子政务的建设。实施电子政务成为各国政府改革的一个重要方向，也揭开了全球电子政务建设的序幕。

美国是电子政务的发源地，其电子政务发展已成为全球电子政务的“样本工程”。

1994 年美国的“政府信息技术服务小组”强调：利用信息技术协助政府与公众间的互动，建立以公众为导向的电子政府，为公众提供更多获取政府服务的机会与渠道。