教育部职业教育与成人教育司推荐教材
电子政务应用教学用书

电子政务系统安全

■ 戴凤弟 主 编

高等教育出版社

教育部职业教育与成人教育司推荐教材
电子政务应用教学用书

电子政务系统安全

戴凤弟　主编
王　强　郭占春　主审

高等教育出版社

内容提要

本书是教育部推荐教材，是电子政务应用专业教学用书。

本书系统地介绍电子政务系统安全的相关知识。全书共分为6章，包括电子政务系统安全概述、信息安全基础、电子政务的网络安全、电子政务的软件安全、电子政务系统安全与技术管理、电子政务系统安全与行政管理，并在每章的教学内容后面安排了一定数量的习题和实验。

本书可供职业学校电子政务专业的学生使用，也可供从事电子政务公务员和网络管理的人员参考。

图书在版编目(CIP)数据

电子政务系统安全/戴凤弟主编. —北京：高等教育出版社，2006.4

ISBN 7-04-018696-9

Ⅰ. 电… Ⅱ. 戴… Ⅲ. 电子政务-专业学校-教材 Ⅳ. D035.1-39

中国版本图书馆CIP数据核字（2006）第015234号

策划编辑 李 波 **责任编辑** 焦建虹 **封面设计** 张申申
版式设计 胡志萍 **责任校对** 俞声佳 **责任印制** 朱学忠

出版发行 高等教育出版社
社 址 北京市西城区德外大街4号
邮政编码 100011
总 机 010-58581000

经 销 蓝色畅想图书发行有限公司
印 刷 北京明月印务有限责任公司

开 本 787×1092 1/16
印 张 9.75
字 数 230 000

购书热线 010-58581118
免费咨询 800-810-0598
网 址 http://www.hep.edu.cn
http://www.hep.com.cn
网上订购 http://www.landraco.com
http://www.landraco.com.cn
畅想教育 http://www.widedu.com

版 次 2006年4月第1版
印 次 2006年4月第1次印刷
定 价 12.70元

物料号 18696-00

前　言

如今，互联网在我国已成为影响最广、增长最快、市场潜力最大的产业之一，它为发展我国的电子政务奠定了社会基础。电子政务在政府实际工作中的作用已越来越重要，电子政务中的信息会涉及国家秘密、国家安全，因此它需要绝对的安全。作为电子政务的发展方向，一是要为社会提供行政监管的渠道，二是要为社会提供公共服务，因此如何合理地划分安全域、在这两者之间寻求一个平衡点就显得非常重要。

电子政务安全属于国家安全范畴。政府机构从事的事业与国家紧密联系，电子政务平台上有相当多的重要政府公文在流转，其中不乏重要且保密的情报，它们关系到国家安全和社会稳定，一旦机密信息被泄露，或受到黑客的侵扰和计算机病毒等的破坏，影响的将不仅是电子政务应用系统的正常运行，还可能是整个国家的政治秩序。所以，信息安全问题在电子政务领域中显得尤其重要，它是电子政务建设过程中的头等大事。

电子政务安全直接影响着社会安全和经济安全。政治秩序的稳定决定了经济秩序和生活秩序的正常运转，电子政务是经济与社会信息化的先决条件，因此电子政务安全既是政治安全，也是经济安全和社会安全。保障电子政务安全不仅要保护电子政务系统的安全，也要保证国民经济和基础设施的信息安全，还要抵御有关国家、地区或集团可能对我国发动信息战的威胁和攻击，并防范国内外的高技术犯罪。保障国家的社会稳定和经济发展是发展电子政务过程中面临的重要且严峻的挑战。

电子政务系统安全主要涉及计算机安全、网络安全、信息安全和内部管理安全等领域。可以毫不夸张地说，只要在某一方面稍有疏忽，就可能影响到国家安全、社会稳定和经济秩序以及生活秩序的正常运转。

曾经有计算机安全专家做过长期调查，得出的结论是：无论是私人机构还是公共机构，大约65%的损失都是出于无意的错误或疏忽。例如，盲目地将一些信息公开化，导致了泄密事件的发生；管理制度混乱；计算机和网络管理人员的经验不足等。这些都会导致电子政务信息泄密或电子政务系统瘫痪。不幸的是，这些事实至今仍在延续。

从上述几个方面可以看出，电子政务系统安全已受到多方面的挑战，保障电子政务安全的重要性毋庸置疑，电子政务的安全问题已提到各级政府的议事日程。编写一本有关电子政务系统安全的教材已刻不容缓。培养掌握电子政务的理论知识、具有电子政务安全观念、能利用信息技术开展行政事务工作的人才已成为当务之急。

本书力求体现教育部技能型紧缺人才培养工程的精神，大部分章节都有较为丰富的实例，为案例教学和任务驱动教学提供了方便。书中在信息安全方面的实例可以直接在计算机上运行或进行修改。

本书可供职业学校电子政务专业的学生使用，也可供从事电子政务公务员和网络管理的人员参考。

本书由戴凤弟主编。其中第1、5、6章由招广文编写，第2章由戴凤弟编写，第3、4章

由钱立三编写。教育部聘请王强、郭占春两位老师审阅了全书，提出了许多宝贵意见，在此表示衷心的感谢。

在本书的编写过程中，得到了北京财贸职业学院孙万军教授、武汉市财政局高级工程师王静和武汉市财政学校的帮助，在此一并表示感谢。

由于编者水平有限，错误之处在所难免，敬请广大读者批评指正。

编者的 E-mail 是 wincetcn@yahoo.com.cn。

编　者

2005 年 6 月于武汉

郑重声明

目　录

第 1 章

电子政务系统安全概述

本章简介

本章主要介绍目前我国电子政务系统安全中存在的问题以及我国电子政务系统安全的目标。

知识目标

掌握电子政务系统安全的概念;
掌握电子政务系统安全所包含的内容;
了解我国电子政务系统安全的现状;
掌握电子政务系统安全支撑体系的结构。

能力目标

熟悉目前我国电子政务的应用状况，能正确说出政务安全所包含的内容。

1.1 电子政务系统安全受到的威胁

1.1.1 严峻的现实

电子政务是指政府机构运用现代信息与通信技术将管理与服务通过信息化集成，在网络上实现政府组织结构和工作流程的优化重组，超越时间、空间与部门分割的限制，全方位地向社会提供高效、优质、规范、透明的管理与服务。它作为当代信息化最重要的领域之一，已经成为全球关注的焦点，是我国现代化进程中不可缺少的一环，也是全面提升政府机构管理与服务水平的重要技术手段。但是，我们又不得不面对这样一个现实：在信息技术的发展进程中，由技术或非技术因素引发的安全威胁越来越多，其危险性也越来越大。

世界各国的政府信息系统都曾遭受过各种不同程度的入侵、攻击和破坏，并且大都造成了巨大的损失或带来了不良的影响。下面列举的是一些国家的政府或军方的信息网络系统遭受攻击和破坏的事件。

1988 年 11 月，美国康奈尔大学的学生莫里斯编制的名为“蠕虫”的计算机病毒通过互联网传播，致使网络中 6 000 多个系统被感染，几乎占当时互联网的 1/10，造成经济损失约 1 亿美元。

1995 年 7 月，黑客“闯入”法国海军参谋部的计算机系统，把包括几百艘盟军军舰的声音

识别密码及舰只航行图等军事机密窃走，引起了军事当局的高度恐慌。

1998 年，黑客向美国五角大楼网站发动了“有史以来最大规模、最具系统性的攻击行动”，打入了政府许多非保密性的敏感计算机网络，查询并修改了工资报表和人员数据。

1999 年 2 月，一些手段高明的黑客侵入英国军事卫星通信系统，并通过该系统操纵用于军事目的的 4 颗卫星中的一颗，修改了这颗卫星的正常工作内容。而且，黑客们还通过该系统发出勒索威胁，声称只有拿到钱才停止干扰这颗卫星。

1999 年 5 月，北约对中国驻南联盟大使馆的轰炸激起了中国网民的义愤。持续几个月，美国政府及北约的一些网站纷纷遭到中国黑客的攻击。黑客在美国能源部网站用几名死难中国记者的照片覆盖了其原有主页，并配有中国抗议群众举着写有“U.S.凶手”标语牌的照片以及“抗议美国的纳粹行径”的口号。除能源部网站外，美国驻中国大使馆网站、美国内政部网站、白宫网站和北约的邮件服务器等均遭到不同程度的攻击。

1999 年夏天，李登辉抛出“两国论”，海峡两岸的黑客在计算机网络上展开了一场没有硝烟的战争。截至当年 8 月 20 日，台湾共有国民大会、行政院、监察院等十多个网站被黑客攻击。其中，国民大会的网站损失惨重，不仅被贴上五星红旗，且内部资料全部被清除，整个计算机主机瘫痪，这使台湾国安局等单位大为惊慌。此外，台湾调查局的网站也被贴上了五星红旗，5 个小时后才勉强恢复。而在大陆方面，证监会及多个党政机关网站同样遭到台湾黑客的入侵，损失也相当惨重。

2001 年，武汉一名年轻黑客为炫耀自己的技艺，通过境外代理服务器隐藏真实 IP，利用一种经自己改造过的黑客软件在网上大肆攻击国内一些软件有漏洞的网站。仅 3 天时间，就先后入侵武昌区政府网站、武汉电视台“科技之光”网站、楚天人才热线、大冶市政府网站、黄石热线网站、数字重庆网站以及福建的一个证券网站等多个国内网站，肆意修改其主页内容，粘贴色情淫秽图片，并对政府进行攻击。

2001 年 2 月到 2002 年 3 月，英国失业计算机工程师盖里·麦金农为了寻找美国政府掩盖 UFO 光临地球的“证据”，竟然在一年时间内“黑”遍了美国军方以及太空总署的 97 处计算机系统，使美国政府一度以为遭遇了“网络版 9·11”。

类似的安全事件不计其数，以上列举的只是其中的一小部分。这些安全事件的共同特征是：无论属于哪种类型的破坏，无论采用什么样的攻击手段，都会造成巨大损失（包括经济和政治上的损失等）。针对政府机构信息网络系统的破坏活动的危险性更大，因为它除了会造成直接的经济损失外，还会带来国家安全、社会稳定，甚至人类生存等重大问题。因此，发展电子政务的首要问题就是安全保障问题，然而实际情况却不容乐观，形势非常严峻。

1.1.2 威胁的来源

安全威胁是指信息系统中存在的对机构、组织或部门造成某种损害的潜在可能。电子政务系统很容易受到可造成不同程度损失的各种安全威胁，这些损失可能是由病毒造成的文件损坏和由火灾造成的整个计算机中心系统毁坏，也可能是由来自内部雇员的欺诈行为、无意过失或是来自外部黑客的非法入侵造成的损失。一般而言，电子政务系统不安全因素的产生和不断扩大的主要原因包括利益、技术、自然环境和心理等方面。有些是自然灾害造成的；有些是在国家利益、民族利益、经济利益的驱使下产生的；有些是随破坏技术的不断发展、保护技术的不

断进步而产生的；也有些是因猎奇心理、好胜心理、表现欲望强、破坏欲望强而产生的。

按照安全威胁是出于自然的还是人为的、是无意的还是有意的、是直接的还是间接的，可以将其进行分类。

1．自然威胁

自然威胁是指不以人的意志为转移的不可抗拒的自然事件，如地震、雷击、洪水和火灾等。自然威胁发生的概率比较低，而且与机构、组织或部门所处的自然环境密切相关。如有些地方是雷击易发区，则几乎每次有雷电产生时，都会损坏一些相关设施，包括通信器材、网络设备等。

2．人为威胁

一般来说，在现实中人为威胁造成的损失远远大于自然威胁造成的损失。

（1）意外的人为威胁

这类安全威胁是各种不确定因素（如不正确的操作、配置、设计或人员的疏忽大意等）综合在一起时偶然发生的，并不是有人故意造成的。意外的人为威胁在人为威胁中是经常发生的，其发生概率甚至比有意而为的安全威胁发生的概率还要大，产生的损失也可能是非常巨大的。曾经有计算机安全专家做过长期调查，得出的结论是：无论是私人机构还是公共机构，大约65%的损失都出自于无意的错误或疏忽。

错误和疏忽对于数据和信息系统完整性的威胁是很大的。用户、数据处理人员、系统管理员和程序员都会经常地、无意地犯一些错误，在某些情况下，这些错误就会成为一种威胁，如某一数据项的错误将导致系统的崩溃。

系统在配置及维护过程中也可能发生错误及疏忽。如不少的网站系统采用默认配置，身份验证不严格，未能及时为系统安装补丁升级程序，路由器、防火墙的配置错误，从而形成各种漏洞或薄弱环节。这些都为黑客的非法入侵或病毒的传播打开了方便之门。

要解决这类问题，减少这类错误及疏忽发生的概率，就必须对工作人员及软件编写人员进行培训，尤其是加强安全意识的培训，同时，也要加强安全管理。

（2）有意的人为威胁

有意的人为威胁包括欺诈或偷窃、内部人员的有意破坏、怀有恶意的黑客行为、侵犯他人隐私、恶意代码以及间谍行为等。

① 欺诈或偷窃。如某些人可能会利用金融系统中的金融结算系统不检查微小账目的一致性这一漏洞，设计一个把一些零头划入自己账号的程序，从而达到偷窃的目的；恶意网站的经营者可能会利用用户上网购物的机会获得他们的信用卡机密，从而达到偷窃的目的。

② 内部人员的有意破坏。计算机欺诈及偷窃行为既可能发生在机构外部，也可能发生在机构内部，且大部分的欺诈行为都应由机构内部的授权用户来负责。内部人员能够很方便地进入内部的计算机系统，而且他们熟悉这些计算机系统和应用程序，与外部人员相比，他们有更多的机会。

③ 怀有恶意的黑客行为。怀有恶意的黑客行为是指没有被授权的人非法入侵一个机构的计算机系统以进行破坏的行为。由于政府连接互联网的计算机系统的数量在迅速增加，因此大部分黑客有机会入侵这些系统。

④ 间谍行为。间谍行为是指为了某种目的而收集政府的敏感资料、数据的行为，其最终目的是要在竞争、对抗中处于有利地位。

⑤ 恶意代码。它是指病毒、蠕虫、木马、逻辑炸弹和其他一些意想不到的软件问题。

⑥ 侵犯他人隐私。在信息时代，个人隐私受到的威胁越来越严重。大量的个人信息被政府、信用机构以及私人企业所掌握，并被存放于计算机系统中，这就对个人隐私构成了一种威胁。如相关部门的职员就有可能随意查看其关心的所有个人信息，对他人的隐私造成非法侵犯。因此在这些系统中必须采取必要的保护措施以防止这种情况的发生。

通常，可以把电子政务系统或其所属的政府机关划分为内、外两个区域。内部区域是指电子政务系统及其所属政府机关，外部区域是指政府机关以外的社会环境。无论是内部还是外部，都存在对电子政务系统构成威胁的不安全因素。

如图 1-1 所示，围绕着电子政务的各种重要资源，存在着各种威胁因素。来自外部的威胁有病毒破坏、黑客攻击、信息间谍、信息恐怖活动、信息战争等；来自内部的威胁有内部人员的恶意破坏，内部人员与外部勾结，管理人员滥用职权，执行人员操作不当，安全意识不强，内部管理疏漏，软、硬件缺陷及自然灾害等。上述威胁往往都有各种具体的表现形式，如表 1-1 所示。

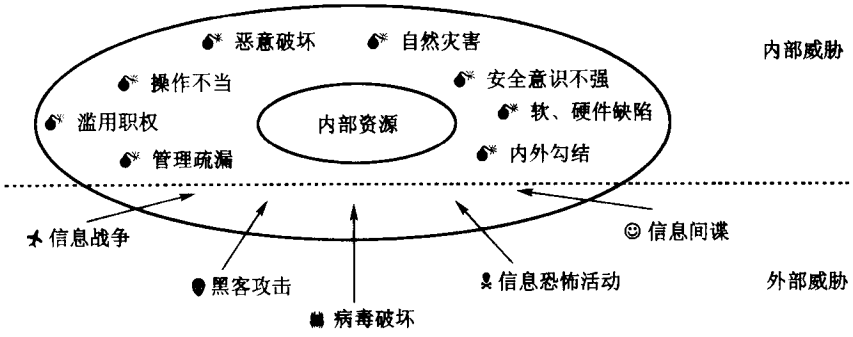

图 1-1　威胁的来源

表 1-1　电子政务安全威胁分析表

种　类		主要表现形式
内部威胁	恶意破坏	破坏数据、转移资产、设置故障及损毁设备等
	内外勾结	出卖情报、透露口令、入侵系统、破坏数据、设置故障及损毁设备等
	滥用职权	非职责查看内部信息、非职责使用系统等
	操作不当	数据损坏或丢失、硬件损坏及垃圾处理不当等
	安全意识不强	思想麻痹、经验不足及后果估计不足等
	管理疏漏	制度不完善、人员组织不合理、缺乏监控措施及权责不清等
	软、硬件缺陷	电磁泄露、剩磁效应、预置陷阱、操作系统漏洞、数据库缺陷、逻辑炸弹、协议漏洞、网络结构隐患及设备老化等
	自然灾害	因温度、湿度、灰尘、雷击、静电、水灾、火灾、地震及空气污染等因素使软、硬件设备被破坏或不能正常工作
外部威胁	病毒破坏	破坏文件、占耗内存、干扰系统运行、妨碍磁盘操作及扰乱屏幕显示等
	黑客攻击	系统入侵、网络窃听、密文破译、拒绝服务及传输通道损坏等
	信息间谍	信息窃取、网络窃听、密文破译、密钥破译、电磁探测及流量分析等
	信息恐怖活动	摧毁国家信息基础设施、制造并散布恐怖信息等
	信息战争	发布虚假信息、窃取军事情报、攻击指挥系统及破坏社会经济系统等

1.2 电子政务系统安全简介

1.2.1 电子政务系统安全的实质

电子政务系统安全主要是一种信息系统的安全，是指围绕信息系统安全的计算机安全、网络安全和管理制度等方面。电子政务安全也可称为政务信息安全，是信息安全在政务信息化领域的具体表现。

信息安全是指保障信息的机密性、完整性、可用性、可控性和不可否认性等几个方面。机密性指保证信息不泄露给未经授权的人；完整性指防止信息被篡改，保证信息的真实性；可用性指保证信息和信息系统确实被授权使用者所用；可控性指对信息及信息系统实施安全监控管理；不可否认性指保证信息行为人不能否认自己的行为。

1.2.2 电子政务系统安全的重要性

电子政务系统容易受到外部或内部的各种攻击，因此，要发展电子政务就必须保障其安全，将各种不安全因素对电子政务发展的威胁和制约降到最低。

一方面，电子政务安全属于国家安全范畴。政府机构所属的行业性质跟国家紧密联系，电子政务平台上有相当多的重要政府公文在流转，其中不乏重要且保密的情报，关系到国家安全和社会稳定，一旦机密信息被泄露或受到黑客的侵扰和计算机病毒等的破坏，那么影响的将不仅是电子政务应用系统的正常运行，而且可能是整个国家的政治秩序。所以，信息安全问题在电子政务领域尤其重要，是电子政务建设过程中的头等大事。

另一方面，电子政务安全直接影响社会安全和经济安全。政治秩序的稳定决定了经济秩序和生活秩序的正常，电子政务是经济与社会信息化的先决条件，因此电子政务安全既是政治安全，也是经济安全和社会安全。保障电子政务安全不仅要保护电子政务系统的安全，也要保证国民经济和基础设施的安全，还要抵御有关国家、地区或集团可能对我国实施信息战的威胁和攻击，并防范国内外的高技术犯罪。保障国家的社会稳定和经济发展是发展电子政务过程中面临的重要且严峻的挑战。

不过，电子政务的安全问题还有其特殊的一面。电子政务不仅要求政府完善行政管理职能，还要求政府加大公众服务的力度。在这样的要求下，政务信息既包括保密甚至是核心机密的部分，也包括面向公众、具有一定公开性的部分，这就对电子政务的安全性提出了更高的要求。电子政务的公众服务职能要求与公众信息网互连，但其核心业务层因有许多涉及国家机密的信息而需要与外界隔离，因此，在电子政务的不同安全域上，对安全的要求是不完全相同的。电子政务系统的建设不仅要考虑政府内部网络的安全，同时也要考虑面向公众服务的网络安全。

1.2.3 电子政务系统安全的内容

电子政务的主要应用可以用图 1-2 表示。社会公众和企业主要通过政务信息查询以及公共政务办公系统与电子政务平台建立联系，相关事务处理请求通过政府办公自动化系统转给政府

工作人员，由政府工作人员通过办公自动化系统进行处理，或对政务信息查询系统进行更新。通过对这一典型业务模型的分析，可以看出电子政务系统中主要存在3种信息流：政府机构内部办公过程中的政务办公信息流、政府机构对外办公过程中的公共事务信息流、社会公众和企业查询相关信息过程中的政务咨询信息流。

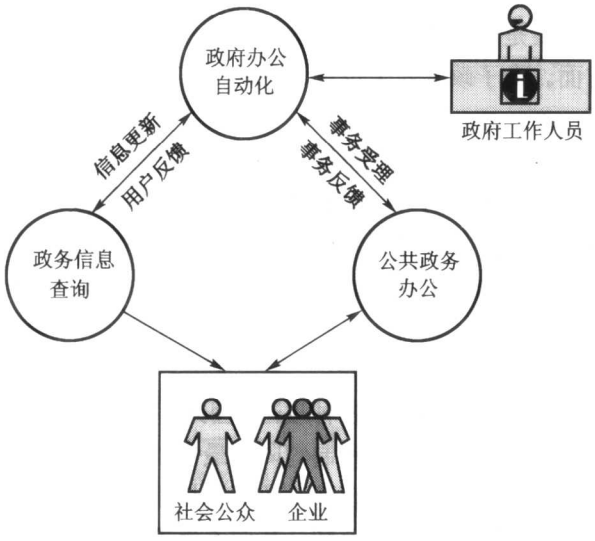

图1-2　电子政务应用示意图

根据电子政务的这一典型模型，我们需要考虑以下的安全问题：

1．办公环境的安全问题

为了保障电子政务系统安全，首先需要考虑办公环境的安全问题，即电子化的办公系统在运行过程中的安全问题。其中包括办公人员的身份和权限控制问题、办公系统中的数据安全使用和存储问题、日常的病毒防范问题、对付网络攻击的问题以及物理环境安全的问题等。

2．内部网络的安全问题

电子政务应用系统是在网络环境下运行的，因此，网络安全是安全保障的重要内容之一，它具体包括不同政府部门或不同级别的机构之间广域网数据传输的机密性和完整性问题、上下级之间网络互访的可控性问题及广域网有效带宽的可用性问题等。此外，还包括政府移动办公的安全问题。

3．对外服务的安全问题

电子政务不仅涉及内部办公的问题，还涉及许多对外服务的内容，包括对企业和个人的服务。这其中也存在很多安全问题，例如公众访问权限可约束的问题，信息服务防篡改问题，网络服务平台的可用性问题，网络访问的可控性问题，信息交互的机密性、完整性及不可否认性问题等。

4．电子政务的安全管理问题

电子政务的安全管理问题涉及安全策略的有效性和一致性问题、安全措施的互补和联动性问题、安全状态的可监控和可追溯问题、安全管理的集中化和异构化问题、安全服务的专业化

和一站式问题，以及安全管理人员的可审计性问题等。

1.2.4 电子政务系统安全的目标

电子政务系统安全的宗旨是在运行信息系统时充分考虑信息风险，从而确保政府部门能够有效地完成法律所赋予的政府职能。为此，电子政务系统必须实现如下的信息安全目标：

1．可用性目标

可用性目标是指确保电子政务系统有效运转并使授权用户得到所需的信息服务。通常，可用性目标是电子政务系统的首要信息安全目标。

2．完整性目标

完整性目标包括两个方面：数据完整性和系统完整性。通常，完整性目标是电子政务系统除了可用性之外最重要的信息安全目标。

3．保密性目标

保密性目标是指不向非授权个人和部门暴露私有或者保密信息。通常，对于大多数电子政务系统而言，保密性目标在信息安全重要程度中的排序仅次于可用性目标和完整性目标，然而，对于某些特定的电子政务应用系统和数据来说，保密性目标可能是最重要的信息安全目标。

4．可记账性目标

可记账性目标是指电子政务系统能够如实地记录一个实体的全部行为。通常，可记账性目标是政府部门的一种策略需求，可以为拒绝否认、威慑违规、隔离故障、检测和防止入侵、事后恢复以及法律诉讼等提供支持。

5．保障性目标

保障性目标是电子政务系统信息安全的信任基础。保障性目标应提供并正确实现所需的电子政务功能，并在用户或者软件偶然或无意出现差错时，能够提供充分保护。

1.3 我国电子政务系统安全存在的问题

1．信息与网络的安全防护能力差

随着 1999 年“政府上网工程”的全面启动，我国各级政府已陆续设立自己的网站，电子商务也得到迅速发展，但许多应用系统却存在着极大的信息安全风险和隐患，在金融领域中尤其突出。在我国，高技术犯罪的案件数量直线上升，金融银行业计算机犯罪个案的金额已从数十万上升到上百万。银行计算机犯罪最具破坏性的类型是篡改数据，而各银行对计算机数据、操作密码、储户密码的保护都缺乏有力措施。如证券系统采用的 Novell 服务器是在 DOS 平台上的，证券系统每天的交易量达几百亿元，而交易的基础却建立在缺少安全性的系统之上，实在令人担忧。

2．引进技术和设备缺乏安全检测

由于国外的计算机硬件、软件中可能隐藏着“特洛伊木马”，因此一旦发生重大情况，则隐藏在计算机芯片和操作系统中的“特洛伊木马”就有可能在某种秘密命令下被激活，使计算机无法启动，导致政府、军事计算机网络、电信系统瘫痪，最终给我国的经济、社会和军事部门带来灾难性的后果。我国的政府部门全部处在信息化和网络化的进程中，却很少有人关注安

全，这样就等于敞开大门让人攻击。未来的战争绝对不会是单纯用武力攻击军事目标，而很可能是利用信息武器直接攻击国民经济的要害部门。

3．基础信息产业严重依赖国外

我国的信息化建设基本上是依靠国外的技术设备进行的，在国际财团涌向我国信息化建设的市场，大举推销电子信息设备的时候，我们却相对缺乏知识和经验，这就存在着国外势力预埋信息安全隐患的危险。我国计算机制造业的许多核心部件都是原始设备制造商提供的，我们对这些部件的研发、生产能力很弱，关键部分完全受制于人。例如，美国微软公司几乎垄断了我国计算机软件的基础和核心市场，离开了微软的操作系统，大多国产软件都将失去操作平台。

4．信息犯罪有快速蔓延之势

根据我国安全部门掌握的情况，外国情报机关的情报手段的现代化程度越来越高。他们可以在传真机、电话交换机中运用远程诊断、远程修复功能进行信息窃取。他们拥有的技术手段可以从泄露的电磁信号中提取信息。在这种情况下，我国极高层次、极小范围的核心机密也有被窃取的危险。另外，在国家级研究开发计划中，对信息安全的投入很少，和国外的差距越来越大。以上问题如果不能切实解决，那么我国的信息安全将面临严重威胁，在激烈的信息争夺和信息战中我国就会处于被动挨打的地位。因此，充分重视我国的信息安全问题已迫在眉睫。

1.4 安全支撑系统

1.4.1 安全支撑系统概述

安全支撑系统是整个政务网络系统安全运行的基础层系统，它实现了电子政务总体逻辑分层结构中信息安全支撑系统层的功能，为上层应用提供一致的信任服务基准，并进一步为政务系统提供统一信任服务、统一授权服务、统一密码管理、信息安全防御、可信时间戳服务、可信网络管理等功能。其层次结构如图 1-3 所示。

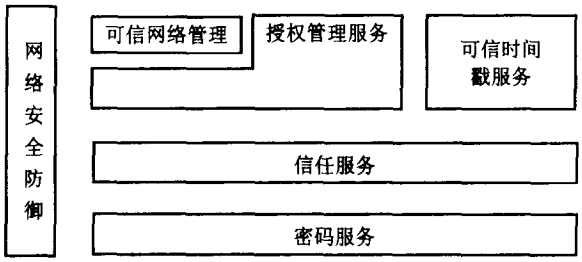

图 1-3　安全支撑系统示意图

根据服务范围的不同，可将安全支撑系统划分为公共安全支撑系统和应用安全支撑系统。公共安全支撑系统为整个电子政务系统提供基础安全服务，包括 PKI 体系中的证书认证（CA）中心、审核注册（RA）中心、密钥管理（KM）中心以及可信时间基准。在电子政务系统中，无论是政府计算机中心网络，还是各个机关、政务部门的计算机中心网络，所有的政务应用、用户管理、权限管理、信息交换都将基于这些公共安全支撑系统提供的证书以及时间基准，实