面向 21 世纪电子政务专业核心课程系列教材

全国高等院校电子政务联编教材

电子政务安全技术

Security Technology of E-Government

陈　兵　钱红燕　冯爱民
谢维杲　王立松　编著

北京大学出版社
PEKING UNIVERSITY PRESS

内 容 提 要

本书是“面向 21 世纪电子政务专业核心课程系列教材”中的一本，围绕电子政务安全技术进行展开，全书主要从电子政务的安全体系、各种常见的攻击技术和防范技术、信息加解密技术和鉴别认证等方面进行探讨，最后给出一个电子政务总体安全解决方案。

本书适合用作高等院校、党校、行政学院电子政务相关课程的专业教材，也可用作政府公务员的培训教材，对相关企业的管理和技术人员同样具有参考价值。

图书在版编目（CIP）数据

电子政务安全技术/陈兵等编著．—北京：北京大学出版社，2005.7
（面向 21 **世纪电子政务专业核心课程系列教材）**
ISBN 7-301-08993-7

I．**电**…　II．**陈**…　III．**电子政务－安全技术－高等学校－教材**　IV．D035.1-39

中国版本图书馆 CIP **数据核字（**2005**）第** 035799 **号**

书　　名：电子政务安全技术
著作责任者：陈兵　钱红燕　冯爱民　谢维杲　王立松
责 任 编 辑：黄庆生　汉明
标 准 书 号：ISBN 7-301-08993-7/F・0791
出　版　者：北京大学出版社
地　　址：北京市海淀区成府路 205 **号**　100871
电　　话：邮购部 62752015　**发行部** 62750672　**编辑部** 62765013
网　　址：http://cbs.pku.edu.cn
电 子 信 箱：xxjs@pup.pku.edu.cn
印　刷　者：
发　行　者：北京大学出版社
经　销　者：新华书店
787 **毫米×**1092 **毫米**　16 **开本**　12.75 **印张**　303 **千字**
2005 **年** 7 **月第** 1 **版**　2005 **年** 7 **月第** 1 **次印刷**
定　　价：24.00 **元**

前　言

随着全球政治经济一体化的日益明显，以电子政务为代表的政府管理服务职能的电子化、自动化、无纸化正在悄然兴起。电子政务在“信息高速公路”的应用领域中被列为首位，可以说，政府信息化是社会信息化的先导，电子政务是信息化社会发展的必然。

但是，电子政务作为一项新生事物，它的发展道路并不是一帆风顺的。世界各国在实施电子政务过程中普遍存在的问题是重硬件、轻应用，重形式、轻内容，在应用开发和安全措施等方面还处于较为初级的阶段，尤其是电子政务的安全问题。这一方面是因为电子政务涉及对国家秘密信息和高敏感度的核心政务的保护、涉及到维护公共秩序和行政监管的准确实施、涉及到为社会提供公共服务的质量保证，由于关系到国家政府的形象，所以电子政务系统一旦被攻击成功，则影响十分巨大；另一方面，电子政务是搭建在基于 Internet 技术的网络平台上，而 Internet 是一个安全性先天不足的全球网络，自身缺少设防，安全隐患很多，使基于 Internet 开展的电子政务应用面临着严峻的挑战。

本书作为“面向 21 世纪电子政务专业核心课程系列教材”的一种，主要围绕电子政务安全技术进行展开，从电子政务的安全体系，各种常见的攻击技术和防范技术，信息加解密技术和鉴别认证等方面进行探讨，最后给出一个总体安全解决方案。

本书共分为 9 章，各章内容分布如下：第 1 章概括性地介绍了电子政务系统所涉及的相关安全问题；第 2 章介绍了现代加解密技术在电子政务中的应用；第 3 章介绍了电子政务中的鉴别和认证技术；第 4 章介绍了电子政务的常见攻击技术；第 5 章介绍了电子政务的安全防范技术；第 6 章介绍了移动政务的安全问题；第 7 章介绍了计算机病毒与电子政务的安全；第 8 章从技术方面给出了电子政务的整体安全解决方案；第 9 章介绍了电子政务的安全管理方案。

本书在编写过程中参考了大量的国内外优秀的文献，大部分已经列在参考文献中，部分参考文献或因出处不祥、或因作者疏忽等原因没有进行标注，敬请原作者谅解。在此，谨向各位为中国的电子政务发展作出贡献的理论研究者和实践探索者致以深深的敬意，没有你们坚持不懈的努力，中国的电子政务发展肯定无法取得今天令人鼓舞的进展，当然，本书的成稿也是不太可能的。

在本书的编写过程中，我们得到了众多师长、同事和学生的关心、支持和帮助，沈学馗、顾其威教授提出了很多有价值的建议，朱敏、蔡伟星、王文娟、薛亮等提供了大量的资料，张淼、董涛、胡莹、葛广超、蒋俊峰、彭星等进行了校对工作。在此一并向诸位表示最诚挚的谢意。

本书适合于政府公务员、电子政务系统开发与管理人员、党校与行政学院学员、高等院校相关专业师生以及其他对电子政务技术与安全感兴趣的读者使用。

由于电子政务应用涉及的范围广、内容多、发展更新快，加之编委学识、资料和编写时间所限，书中肯定有不少疏漏和不妥之处，敬请广大读者和专家批评指正。

编　者

2005 年 1 月

目　　录

第 1 章　电子政务安全概述 1
1.1　电子政务的安全问题概述 1
1.1.1　电子政务安全问题的提出 1
1.1.2　对电子政务的安全威胁及其产生 2
1.2　电子政务的网络安全与信息安全 3
1.2.1　电子政务网络安全 4
1.2.2　电子政务信息安全 5
1.3　电子政务安全体系 7
1.3.1　构建电子政务系统安全体系的基本原则 8
1.3.2　电子政务安全体系结构 8
1.4　电子政务安全评估 11
1.4.1　安全评估内容 11
1.4.2　安全评估标准发展概况 14
1.4.3　国际安全标准 15
1.4.4　国内安全标准 17
1.5　本章小结 18
第 2 章　现代加密技术在电子政务中的应用 19
2.1　引论 19
2.2　加密与解密的基本概念 20
2.3　对称加密系统 22
2.3.1　对称加密系统的工作原理 22
2.3.2　对称加密系统的密钥管理 24
2.3.3　DES 算法 26
2.4　非对称加密系统 27
2.4.1　非对称加密系统概述 27
2.4.2　RSA 算法 29
2.4.3　非对称加密系统的应用 30
2.5　对称加密系统和非对称加密系统的混合使用 32
2.6　本章小结 33
第 3 章　电子政务鉴别和认证技术 34
3.1　引论 34
3.2　报文鉴别 35
3.2.1　报文鉴别码与单向 Hash 函数 35
3.2.2　散列函数 36

3.2.3 MD5 37
3.2.4 SHA-1 37
3.3 数字签名及算法 38
3.3.1 数字签名的概念 38
3.3.2 直接数字签名 39
3.3.3 需仲裁的数字签名 40
3.3.4 专用数字签名方案 43
3.4 数字证书 45
3.4.1 什么是数字证书 46
3.4.2 数字证书的作用 46
3.4.3 数字证书的类型 47
3.4.4 数字证书使用举例 49
3.5 认证中心 49
3.6 本章小结 53
第 4 章 电子政务的常见攻击技术 54
4.1 黑客与电子政务 54
4.1.1 黑客——电子政务网站的潜在威胁 54
4.1.2 对黑客问题的进一步思考 56
4.2 IP 欺骗与防范 57
4.2.1 IP 欺骗原理 57
4.2.2 IP 欺骗的防范 62
4.3 Sniffer 探测与防范 63
4.3.1 Sniffer 原理 63
4.3.2 发现 Sniffer 65
4.3.3 防止 Sniffer 65
4.4 端口扫描技术 66
4.4.1 什么是端口扫描 66
4.4.2 网络测试的常用命令 66
4.4.3 扫描器 70
4.5 特洛伊木马 71
4.5.1 什么是特洛伊木马 71
4.5.2 木马的特点 72
4.5.3 发现和删除木马 74
4.6 拒绝服务式攻击 77
4.6.1 拒绝服务式攻击的原理 77
4.6.2 拒绝服务式攻击的防范措施 79
4.7 本章小结 79
第 5 章 电子政务的安全防范技术 80
5.1 防火墙技术 80
5.1.1 防火墙的定义 80

5.1.2 防火墙的优缺点 81
5.1.3 防火墙类型 83
5.1.4 分布式防火墙 89
5.1.5 防火墙最新发展趋势 91
5.2 虚拟专用网技术 92
5.2.1 VPN 的构成和功能 93
5.2.2 VPN 连接的类型 94
5.2.3 VPN 管理 99
5.2.4 VPN 采用的协议 99
5.2.5 VPN 和防火墙 103
5.3 入侵检测技术 105
5.3.1 入侵检测模型 106
5.3.2 入侵检测系统的分类 106
5.3.3 入侵检测系统的发展趋势 109
5.4 本章小结 111
第 6 章 移动电子政务安全 112
6.1 移动电子政务概述 112
6.2 移动电子政务系统的安全问题 114
6.3 移动电子政务系统的安全解决方案 116
6.3.1 移动电子政务服务方的安全策略 116
6.3.2 移动电子政务客户端的安全策略 118
6.4 本章小结 120
第 7 章 计算机病毒与电子政务安全 121
7.1 计算机病毒的产生及危害 121
7.1.1 病毒产生的背景 121
7.1.2 病毒产生的原因 122
7.1.3 病毒的发展概述 122
7.1.4 病毒的危害 124
7.2 计算机病毒基础知识 125
7.2.1 病毒的定义 125
7.2.2 病毒的特征 126
7.2.3 病毒的分类 127
7.2.4 病毒的组成 131
7.2.5 病毒的传播途径 132
7.2.6 病毒的识别与防治 132
7.3 网络病毒 134
7.3.1 网络病毒的特点 134
7.3.2 网络病毒的传播 134
7.3.3 网络病毒的防治 135
7.4 电子政务系统的病毒防治 137

7.4.1 建立网关拦截机制 138
7.4.2 服务器防毒机制 138
7.4.3 客户端防毒机制 139
7.4.4 网络防病毒的整体模型 141
7.4.5 病毒防范管理策略 141
7.5 电子政务系统防病毒软件选用原则 142
7.6 电子政务系统典型病毒及其防治 144
7.6.1 宏病毒 144
7.6.2 网络蠕虫病毒 147
7.7 本章小结 150
第 8 章 电子政务的整体安全解决方案 151
8.1 整体安全解决方案概述 151
8.2 电子政务系统物理层面安全 152
8.3 电子政务系统网络平台安全 157
8.4 电子政务系统软件平台安全 159
8.4.1 操作系统平台的安全 159
8.4.2 数据库平台的安全 162
8.4.3 办公平台的安全 165
8.5 电子政务系统应用层面安全 168
8.5.1 DNS 的安全解决方案 169
8.5.2 政府网站的安全解决方案 169
8.5.3 电子邮件安全解决方案 170
8.5.4 网络化办公的安全解决方案 175
8.6 本章小结 179
第 9 章 电子政务安全管理方案 180
9.1 确定电子政务安全系统的实现目标 180
9.2 电子政务系统风险评估与安全策略 181
9.3 制定电子政务系统安全管理措施 183
9.3.1 网络实体的安全管理 183
9.3.2 保密设备与密钥的安全管理 184
9.3.3 安全行政管理 185
9.3.4 日常安全管理 187
9.4 强化安全标准 188
9.5 实施安全防御系统，进行监控与检测 188
9.6 电子政务系统安全实施建议 190
9.7 本章小结 191
参考文献 192

第 1 章　电子政务安全概述

电子政务系统是通过 Internet 等公网实现通信的网络，然而随着 Internet 的飞速发展，各种安全问题接踵而至：黑客入侵、病毒肆虐、网络瘫痪、主页篡改，各种案例不胜枚举，因此，如何保证电子政务的安全已成为迫在眉睫的问题。本章首先介绍了电子政务面临的威胁的来源和种类，然后给出有关电子政务网络安全和信息安全的概念，并分析了安全评估的重要性，最后介绍了国内外的安全评估标准。

本章主要内容：

★　电子政务的安全问题概述
★　电子政务的网络与信息安全
★　电子政务的安全体系结构
★　电子政务安全评估

1.1　电子政务的安全问题概述

随着全球政治经济一体化的日益明显，以电子政务为代表的政府管理服务职能的电子化、自动化、无纸化正在悄然兴起。电子政务在“信息高速公路”的应用领域中被列为首位，可以说，政府信息化是社会信息化的先导，电子政务是信息化社会发展的必然。

电子政务，目前有很多种说法，如：电子政府、网络政府、政府信息化管理等。但真正的电子政务绝不是简单的“政府上网工程”，更不仅仅是个网站系统。

严格地说，所谓电子政务就是政府机构运用现代计算机技术和网络技术，将其管理和服务的职能转移到网络上完成，同时实现政府组织结构和工作流程的重组优化，超越时间、空间和部门分隔的制约，向全社会提供高效、优质、规范、透明和全方位的管理与服务。

电子政务推动了整个社会的信息化，它不仅仅是“将服务放到网上”而已，其主要意义在于：在虚拟空间里，政府能跨越部门间的限制，进行再造，为公众提供完整而便利的服务，突破传统“一站式”的政府办公模式，促进观念的转变，强调政府的服务功能，通过建立适应网络时代的“一网式”和“一表式”政府工作新模式，逐步实现向服务型政府的转变。电子政务将实现政务“四化”：办公信息化、政务公开化、管理一体化、决策科学化，有利于政府转变职能，提高运作效率。

1.1.1　电子政务安全问题的提出

电子政务涉及对国家秘密信息和高敏感度的核心政务的保护、涉及到维护公共秩序和行政监管的准确实施、涉及到为社会提供公共服务的质量保证，由于关系到国家和政府的形象，

所以一旦被攻击成功，影响十分巨大（严重时甚至会影响民众对政府的信心，引起恐慌，导致社会动荡），因此电子政务系统容易成为不法之徒的攻击目标，必然会遇到各种破坏和攻击。电子政务是搭建在基于互联网技术的网络平台上，包括政务内网、政务外网和互联网，而互联网是一个安全性先天不足的全球网络，自身缺少设防，安全隐患很多，使基于互联网开展的电子政务应用面临着严峻的挑战。

电子政务能够提供科学决策、监管控制、大众服务等功能，是政府和公众之间联系的纽带之一，它本身的重要性和特殊性决定了网络安全和信息安全是成功实施电子政务的首要条件，具体体现在：

（1）电子政务系统中有众多的政府公文在流转，其中不乏重要情报，有的甚至涉及国家安全，这些信息通过网络传送时要求不能被窃听、泄密、篡改和伪造。因此，必须保证电子政务系统中信息传输过程的安全和信息内容本身的安全；

（2）电子政务系统一般通过政府网站对外界发布各种信息，包括政策、法规和条例，等等。这些信息是严肃的、权威的，不能被入侵者篡改、歪曲；同时，政府网站收集的各种公众反馈信息必须真实、完整，能够安全地反馈到相关的政府部门。因此，必须保证政务网站是安全的，不能够被入侵者攻击和破坏；

（3）电子政务系统一旦启用后，必须稳定可靠，从而保证各种业务的连续性和一致性。

综上所述，解决好电子政务系统中信息共享与保密性、完整性的关系，开放性与保护隐私的关系，互联性与局部隔离的关系，是实现“安全的”电子政务的前提。

1.1.2 对电子政务的安全威胁及其产生

1．对电子政务的安全威胁

无可否认，电子政务给我们打开了一个广博的天地，但人们在尽情享受电子政务所带来的便利的同时，却也存在着各种安全威胁。对电子政务系统而言，主要的安全威胁包括：

（1）网上黑客的入侵和犯罪；
（2）网络病毒的泛滥和蔓延；
（3）信息间谍的潜入和窃密；
（4）网络恐怖集团的攻击和破坏；
（5）内部人员的违规和违法操作；
（6）网络系统的脆弱和瘫痪；
（7）信息安全产品的失控等。

2．造成电子政务安全威胁的原因

而造成上述种种威胁的原因，无外乎归结为以下几条：

（1）来自内部和外部的各种攻击　电子政务极易受到来自外部或内部的各种攻击。攻击的手段包括被动攻击和主动攻击。所谓被动攻击是指侦听、截获、窃取、破译、业务流量分析、电磁信息提取等行为，被动攻击虽然不会对信息进行修改，但会造成信息内容的泄密。这对带有国家秘密信息的电子政务系统来说，是绝对不允许的。而主动攻击是指对网络传输的信息进行修改、伪造、破坏、冒充等操作，或者在电子政务网络上进行病毒扩散，这种攻

击将对电子政务的安全运行造成极大的危害。典型的例子如冒充领导审批、签发文件等，这种攻击的后果也将是极其严重的。从来源看，攻击有来自外部和内部两种。一些黑客试图穿过电子政务的边界防火墙进入到内部网络中，当然由于有防火墙，这种来自外部的攻击行为大部分会被阻断，只有少数真正的高手才能穿越防火墙进入到内部系统中。而绝大部分攻击（包括被动攻击和主动攻击）主要来自内部，且大多采用被动攻击方式，即进行网络窃听，了解一些自己感兴趣而又没有权限查看的内容，这也许是人天生的好奇心导致的。更有少数人为达到某种目的，对内部各种服务器进行主动攻击，由于他们身处防火墙内部，而防火墙无法防范内部的各种攻击行为，因此，内部的主动攻击已经成为电子政务系统面临的最大威胁之一；

(2) 软件漏洞　软件漏洞主要体现在操作系统的漏洞和各种应用软件的漏洞。这些漏洞可能是软件编制人员为了调试方便预留的，但在软件正式发行时忘记删除了，从而为一些软件高手或者不速之客留下了入侵的后门。当然，也有的漏洞可能是程序员故意预留的，这种情况尤其值得重视。由于电子政务系统的各种应用，如办公系统、审批系统、档案系统等，一般都由第三方开发，因此，在项目最终验收时，尤其要重视安全性方面的测试，防止出现后门；

(3) 关键技术失控　目前电子政务系统常用的操作系统和应用软件均采用的是国外产品，其中的许多关键技术并没有被我国掌握，更为糟糕的是这些被广泛使用的操作系统大多都有“后门”，尽管正常情况下，这些后门不会被使用。但一旦出现诸如国家之间的信息战等紧急情况时，黑客攻击可能上升为一种国家间的战争行为，为了各自国家的利益，这些所使用的进口操作系统的厂商可能会被本国政府强行要求公开后门，甚至要求公开源码，到那时，后果将不堪设想；

(4) 管理水平落后　网上新业务的开展、传统业务的开放式改造、不断变化的网络应用、网上攻击风险的日益增大，都对电子政务系统的安全管理提出了更高的要求。俗话说“三分技术，七分管理”，而恰恰是由于管理跟不上，制度不完善，加上采用的安全技术和产品是零散的，导致许多电子政务系统的网络即使在采用先进技术、经过安全配置、甚至在已经使用了一部分专门的安全产品之后，管理人员和技术人员依旧对自己网络的安全性没有很好的把握。如何有效地提高网络的安全性，保障网上业务顺利安全地进行，将网络的安全隐患降低到一个可以接受的程度，让安全管理人员做到心中有数，是电子政务安全亟待解决的重要问题。

1.2　电子政务的网络安全与信息安全

无论在计算机上存储、处理和应用，还是在通信网络上传输，信息都可能被非授权访问而导致泄密，被篡改破坏而导致不完整，被冒充替换而导致否认，也可能被阻塞拦截而导致无法存取。这些破坏可能是有意的，如黑客攻击、病毒感染，也可能是无意的，如误操作、程序错误等。

对电子政务系统安全构成威胁的行为，最终都可归结为网络安全和信息安全问题。保证了网络的安全，就保证电子政务信息传输的安全；而保证了传输的安全，也就为电子政务的

信息安全提供了重要的保证。因此，电子政务的网络安全主要是采取各种措施，保证信息在传输过程中不会出错、丢失或者被窃听；而信息安全主要是采取各种措施，保证信息的机密性、完整性、一致性和不可否认性等。

1.2.1 电子政务网络安全

电子政务网络安全是指电子政务网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露。即通过各种计算机、网络、密码技术和信息安全技术，保护在公用通信网络中传输、交换和存储的信息的机密性、完整性和真实性，并对信息的传播及内容有控制能力。

电子政务的网络安全主要分为传输网络安全和业务网络安全两类。其中，传输网络安全主要保证参与电子政务系统各方主体之间的数据传输网络以及公共网络服务的安全可靠运行，从目前电子政务建设情况来看，传输网络安全需要由网络基础设施提供商或服务商保证。业务网络安全则主要包括控制拨号用户接入、设置防火墙、防范病毒、控制与公网互连、防范黑客入侵，以及对网络安全进行严格监控和规范管理等，以保护业务网络资源和电子政务应用。

考虑到上述两类网络安全所需的技术保证，这里简单阐述一下业务网络安全的内容，若需深入了解，读者可参阅本书后边的相关章节。

1．拨号用户接入问题

目前，我国电子政务系统网络建设并不完善，还存在部分网络环境较差的状况，在使用电子政务系统时通过拨号方式利用公用电话交换网在网络上传输数据。由于在公用电话交换网中搭线窃听的技术难度很低，所以传输的数据极易在传输过程中被窃听、篡改，因此不仅需要对拨号用户加强身份认证，必要时还需要对关键数据加密传输，防止数据泄漏和非法窃取；同时，严格限制拨号上网用户能访问的系统信息和系统资源，防止非法用户拨号进入电子政务系统所在网络。

2．防火墙设置问题

在电子政务系统运行的内网和外网之间、不同安全域之间根据需要可以设置防火墙，它在内部网络和外部网络之间提供了一个封锁工具。防火墙能增强机构内部网络的安全性，加强网络间的访问控制，防止外部用户非法使用内部网的资源，保护内部网络的设备不被破坏，保证内部网络的敏感数据不被窃取。防火墙系统决定了外界的哪些人可以访问内部的哪些可以访问的服务，哪些外部服务可以被内部人员访问，可以说，防火墙是保护电子政务网络安全的第一道屏障。防火墙设置需要综合考虑电子政务系统所要求的速度、性能、管理、便易性和性价比等各个方面，进行周密设计和总体规划；另外应注意加强安全管理，采取一些必要的措施保证较高的安全性。

3．防病毒问题

在电子政务系统中，需要基于业务需求建立多层次病毒防卫体系。无论是 B/S（Browser/Server:浏览器/服务器）还是 C/S（Client/Server:客户端/服务器）结构，均需要在电

子政务系统每一个运行点安装反病毒软件；在电子政务系统中的业务处理终端和服务器端，同时提供对应的防病毒保护措施。防病毒工作是一个长期的工作，应及时进行防病毒软件或系统的升级、换代工作。另外，除了采用各种防病毒产品以外，还应建立和实施完善的综合安全性操作程序，该操作程序应包括各种安全措施，如定期数据备份、关键信息加密保护等。

4．控制与公网互连的问题

为了将不同保密级别的电子政务网络隔离开，如密级较高的内部办公系统和密级稍低的政府网站系统，可以采用隔离技术将密级不同的网络在物理上进行隔离，采用网络分段将非法用户与敏感的网络资源相互隔离，从而防止可能的非法侦听，严格控制与公网互连，妥善解决公网与专网之间的数据传输问题。

5．防止黑客问题

随着网络规模的扩张和信息技术的飞速发展，黑客技术也不断发展，其攻击的范围和层次也不断扩张。电子政务系统作为我国政府信息化的重要项目，极易成为某些恶意黑客的攻击对象。因此在设计和实施电子政务系统安全体系时，应加强采用入侵检测技术防范黑客入侵和侵袭，并在必要的时候采取证据记录、跟踪恢复、强制断开等措施保证业务网络的安全。

6．网络安全管理和监测

网络安全管理和监测是电子政务系统安全设施和安全机制有效发挥作用的重要保证，主要包括安全规范的制定和实施、各类操作用户的安全管理、安全体系的运营监控、应急处理和安全控制等。

1.2.2　电子政务信息安全

电子政务系统为政府、公众服务，既要求相当的保密性，又要求一定的公开度，这就给电子政务的安全性提出了更高的要求，这个要求主要是信息安全，即保证数据传输完整性、保密性、真实性和不可抵赖性等，只有这些问题得到很好的解决，才能促进电子政务的不断发展。

1．完整性

完整性是网络信息未经授权不能进行改变的特性，即网络信息在存储或传输过程中保持不被偶然或蓄意地添加、删除、修改、伪造、乱序、重放等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和正确传输。

影响网络信息完整性的主要因素有：设备故障、误码（传输、处理和存储过程中产生的误码，定时的稳定度和精度降低造成的误码，各种干扰源造成的误码）、人为攻击、计算机病毒等。保障网络信息完整性的主要方法有：

（1）良好的协议　通过各种安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段；

（2）密码校验和方法　它是抗篡改和传输失败的重要手段；

（3）数字签名　保障信息的真实性，保证信息的不可否认性；

（4）公证　请求网络管理或中介机构证明信息来源者身份的真实性。

2．保密性

保密性是指网络信息不被泄露给非授权的用户、实体或过程，即信息只为授权用户使用。保密性是在可靠性和可用性基础之上，保障网络信息安全的重要属性。保密性与完整性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因的破坏。

常用的保密技术包括：

（1）物理保密　利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄露；

（2）防窃听　使对手侦收不到有用的信息；

（3）防辐射　防止有用信息以各种途径辐射出去；

（4）信息加密　在密钥的控制下，用加密算法对信息进行加密处理。即使对手得到了加密后的信息也会因为没有密钥而无法读懂有效信息。

3．真实性

真实性是指用户的身份是真实的。例如在一个大型的电子政务网络内，用户张三声明他是张三，但是网络能够相信他吗？会不会是李四冒充张三呢？因此，如何能对通讯实体身份的真实性进行鉴别？如何保证用户的身份不会被别人冒充？尤其在电子政务系统中，不能允许冒充、伪造，这是真实性所需要解决的问题。

4．不可抵赖性

不可抵赖性也称作不可否认性。例如在一个电子政务系统中，考虑以下几种情况：

（1）甲明明给乙发了一封文件，但甲否认给乙发过文件；

（2）乙明明收到了甲发送的文件，但乙否认收到；

（3）丙冒充甲给乙发了一份文件。

这些行为实际上是不允许的，如何防止这些情况的出现呢？即在电子政务网络的信息交互过程中，要确信参与者的真实同一性。所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。数字签名技术是解决不可否认性的手段之一。

另外，在信息安全中，常常还要考虑信息的可靠性，可用性和可控性，具体而言：

5．可靠性

可靠性是指系统能够在规定条件和规定的时间内完成规定的功能特性。可靠性是系统安全的基础要求之一，是所有电子政务系统的建设和运行的基本目标。

可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性、环境可靠性等方面。硬件可靠性最为直观和常见；软件可靠性是指在规定的时间内，程序成功运行的概率；人员可靠性是指人员成功地完成工作或任务的概率。人员可靠性在整个系统可靠性中扮演重要角色，因为系统失效的大部分原因是人为差错造成的。人的行为要受到生理和心理的影响，受到其技术熟练程度、责任心和品德等素质方面的影响。因此，人员的教育、培养、训练和管理以及合理的人机界面是提高可靠性的重要方面。环境可靠性是指在规定的环境内，保证网络成功运行的概率。

6．可用性

可用性是指当用户需要使用网络时，网络能够及时地提供服务。例如，当用户登录某个电子政务网站的时候，如果总是提示你“无法打开网页”或者“无法连接该地址”，用户对这个政务系统可用性的印象一定很差，并且不愿意去使用它。

可用性是网络信息可被授权实体访问并按需求使用的特性。即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。网络信息系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的、有时还有时间要求。可用性一般用系统正常使用时间和整个工作时间之比来度量。

可用性通过以下手段来保证：

（1）身份识别与确认　一般通过用户名和密码进行识别；

（2）访问控制　对用户的权限进行控制，只能访问相应权限的资源，防止或限制经隐蔽通道的非法访问；

（3）业务流控制　利用均分负荷方法，防止业务流量过度集中而引起网络阻塞。如大型的网络服务提供商 ISP（Internet Service Provider）提供的电子邮件服务，一般都有几个邮件服务器进行负载均衡；

（4）路由选择控制　选择那些稳定可靠的子网、中继线或链路等；

（5）审计跟踪　把系统中发生的所有安全事件情况存储在安全审计跟踪之中，以便能够根据日志分析原因，分清责任，并且及时采取相应的措施。当然，平时对日志的分析，也能够判断是否有非法用户在尝试入侵等情况，便于系统管理员及时采取防范措施。所以，良好的审计跟踪系统能够起到事前预防、事后跟踪的作用。

7．可控性

可控性是对网络信息的传播及内容具有控制能力的特性。不允许不良内容通过公共网络进行传输。对于电子政务系统而言，可控性是十分重要的特点，所有需要公开发布的信息必须通过审计后才能发布。

保证了如上诸多性能，也就保证了电子政务信息的安全。

1.3　电子政务安全体系

电子政务是一个由内网（包括核心数据层和办公业务层）、外网（公众服务层）和专网（数据交换层）三级网络域构成的庞大的信息系统。各个网络域执行着不同的服务内容：内网是一个完整的政府办公自动化环境，外网担负着与公众间信息沟通的任务，而专网则负责政府间，内、外网间的数据交换。

如此复杂的应用环境给系统带来了大量潜在的安全隐患：黑客利用外网或专网攻击内部网络、数据在传输过程中的泄漏、网页遭篡改、伪造身份进入系统、操作系统漏洞、病毒等等。这些安全隐患不可能依靠某种单一的安全技术得到解决，必须在综合分析电子政务整体安全需求的基础上构筑一个完整的安全服务体系。

1.3.1 构建电子政务系统安全体系的基本原则

构建电子政务系统安全体系应当遵循以下原则：

（1）全面设计、整体部署　电子政务系统安全体系设计要全面，应充分考虑到电子政务系统环境各个方面的风险，从物理、网络、数据、应用系统等多个方面进行综合考虑和设计，并作整体部署，同时加强安全制度建设和教育培训。只有做到不忽视或遗漏任何一个安全环节，才能够保证整个电子政务系统的安全；

（2）统一标准，加强管理　电子政务系统安全体系设计应遵循统一的技术标准和管理标准，除了采用国际标准和我国自主研究的算法之外（包括数据加密解密算法、数据摘要算法、数字签名算法、密钥管理算法等），还要考虑到安全体系将来的扩展性和系统接口要求，采用通用的数字证书标准、统一的接口规范、统一的数据包格式等；

（3）需求主导，重点突出　安全体系设计应该以需求为主导，切合电子政务系统对安全的要求，突出安全体系的重点，比如网络安全方面的防火墙设置、入侵监测等，统一的安全管理平台、安全认证平台，统一的日志管理、安全审计等，同时根据数据的安全级别、业务系统的安全层次等采取有区别的安全措施以兼顾系统的性能和效率；

（4）灵活配置、动态部署　安全相关的技术发展迅速，电子政务系统的安全需求也在不断变化，因此电子政务系统安全体系设计也需要能够根据变化易于调整和改变。安全体系设计应该提供多种安全策略和方法，并支持灵活的配置方式方便用户进行选择和动态部署。

1.3.2 电子政务安全体系结构

根据安全的“木桶原理”（一个木桶的容积决定于组成它的最短的一块木板），一个系统的安全强度等于它最薄弱环节的安全强度。因此，电子政务必须建立在一个完整的多层次的安全体系之上，任何的薄弱环节都将导致整个安全体系的崩溃。因此，借鉴网络的分层结构，可以采取这样一个安全体系结构模型，如图 1-1 所示。

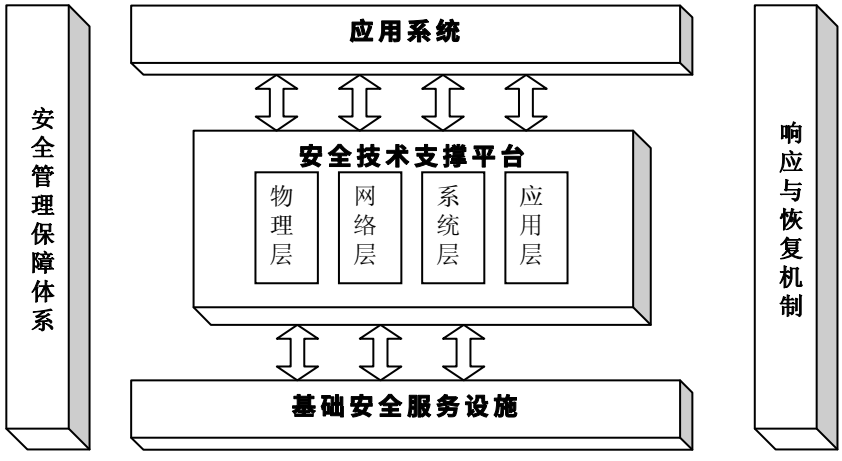

图 1-1　电子政务系统的安全体系结构模型

该模型由四部分组成：基础安全服务设施、安全管理保障体系、安全技术支撑平台和响应与恢复机制，它们共同联合起来，支撑电子政务的应用系统，保证电子邮件、政府网站等的安全。

1．基础安全服务设施

网络安全必须构筑在一个坚实的安全服务基础之上，就像大厦的地基支撑整栋大楼的稳定一样，支撑整个电子政务安全稳定的基础是“信任”。

基础安全服务设施的作用就是为电子政务系统建立一个可相互信任的网络环境，为其他安全技术的实施提供正确决策的基础。这其中必须解决的信任问题包括：

（1）可信的身份　即“你是谁”的问题。系统中的安全策略经常会根据用户的身份决定是否执行其提出的访问要求，这里用户身份是否可信就成为了该安全策略的核心问题。可信的身份服务就是为验证提供准确的用户身份确认信息。没有可信的身份验证服务，防火墙就可能根据伪造的合法用户身份做出错误的判断；

（2）网络信任域　即“你来自哪里”的问题。网络设备的可管理性对于网络安全来说同样十分重要。网络信任域就是通过赋予网络设备可信的识别码建立起一个可管理的网络，从而准确了解和控制访问设备的访问位置及访问权限；

（3）可信的数据　即数据是否完整、机密。用户从系统中获得的数据应该被相信是完整未被篡改的，同时数据在传输过程中应该是安全机密的；

（4）可信的时间服务　对于电子政务这类涉及大政方针执行、审批的应用来说，系统中的文件都应该具有可信的时间戳，因为，时间是政府工作中一个重要的工作和责任认定依据。

电子政务基础安全设施中应包括：个人 CA（Certificate Authority，即证书授权中心）实现可信的身份、设备 CA 实现网络信任域、安全 API 实现可信的数据和标准时间源实现可信的时间服务。

2．安全管理保障体系

常言道“三分技术、七分管理”，安全方案的实现离不开管理。即使采用了最先进的安全技术，如果不对人员的权限进行有效合理的分配，照样可以越权操作；如果没有对异常事件处理的流程和规范，当遇到攻击时仍然会不知所措；如果没有维护网络安全和信息安全的法律，不法行为将变得日益猖獗。

网络安全管理问题关键在于制度的完善和严格的管理，而不只是网络设备和软件的应用。如果有一系列的安全设备，而没有完善的实施计划和管理制度，电子政务网络安全仍然是一句空话。这包括制定和实施一系列规章制度如网络操作使用规程、机房管理制度、网络系统的维护制度和应急措施；加强员工安全培训并采用专业安全人员对网络进行管理、维护和升级；必要的话还可以选择安全顾问公司进行技术支持。所以，在必要的时候，应当以法律的形式来约束网络管理员。我们建议对现有的法令或规章作一些调整，加大执法的力度，没有强硬的法制保障是不可能顺利发展电子政务的。

3．安全技术支撑平台

解决了网络中的信任问题，我们就可以在这样一个可信任的环境下利用现有的安全产品和技术无偏差地实施既定的安全策略，包括：访问控制、通讯加密、防病毒、日志与审计、

漏洞扫描、入侵检测、物理安全等。这些策略的执行为整个网络构筑起了一个真实的安全环境——抵御网络攻击，防止信息泄密，预防信息破坏，控制用户访问范围和权限。安全技术支撑平台就是指利用各类安全产品和技术建立的执行安全策略的环境。

在电子政务安全技术支撑平台上应该实现的基本安全策略包括：

（1）基于安全岛实现电子政务内网与对外服务网、专网间安全的数据交换　电子政务应用中势必要在内网、专网和外网间进行信息交换，然而基于内网数据保密性的考虑，我们又不希望内网暴露在对外环境中遭到攻击，这种矛盾需要采用安全岛的策略来解决。安全岛是电子政务中为安全数据交换而设计的。隔离网闸是电子政务安全岛中采用的一种核心产品。它和其他安全设备组合，就可构成实现安全数据交换的信息安全岛。详细内容，读者可参见第 8.2 节物理安全的网络分段的内容；

（2）网络域访问控制　电子政务系统无论对系统内部设备还是对远程接入设备都需要控制其对网络的访问权限，限定其在合理的范围内使用网络。在网络边界利用防火墙的包过滤或代理技术，在网络内部采用 VLAN（Virtual Local Area Net：虚拟局域网）技术，合理地划分网络范围并制定过滤策略，就能有效地实现网络域的访问控制；

（3）内部网的 Internet 访问策略　电子政务内网原则上必须与公众网络(Internet)物理隔离，但内网中用户在办公过程中也有访问 Internet 的需求，解决的方法是采用物理隔离卡将单一网络划分成物理隔离的双网，这样在保证内部网网络安全的同时，又使内网用户具有了方便的 Internet 访问能力；

（4）身份识别/认证　利用安全基础平台提供的可信身份服务和安全 API（Application Program Interface：应用程序接口）接口，我们可以对电子政务中每一项应用如数据库访问、网页访问、文件转发等建立起安全统一的身份识别/认证。同时，针对应用的不同特点和等级要求，在 CA 认证的基础上，我们还可以附加其他具有互补性的认证机制作为补充。如外网上的政府电子办事窗口就可以使用相较 CA 认证更快捷，注册使用更方便，管理简易的硬件身份认证系统；

（5）通讯加密　政府中重要数据在网上转发过程中都应加密传输，在网络内部利用安全基础平台提供的数字证书和安全 API 接口或 IPSEC（Internet Protocol Security：Internet 协议安全）技术，能够实现机密数据的安全通讯。在网络的边界，VPN（Virtual Private Network：虚拟专用网）或硬件加密机等同样能为通讯提供可靠的数据加密服务；

（6）防病毒　电子政务系统的防病毒软件应具备以下几个安全要素：一是该软件应基于网络环境设计，能监控到网络的各个角落；二是应具有自主同步升级能力；三是兼容性强，电子政务环境中可能包含各类操作系统，防病毒软件应对它们提供全面的支持；

（7）系统漏洞防护　系统漏洞由两方面原因产生：一是产品本身的设计漏洞；二是配置不当造成的漏洞。因此，首先在电子政务系统中，尤其是核心的数据库系统应该运行在安全性较高、代码开放的操作系统之上，便于升级和管理；其次，应采用系统加固软件加固系统的安全性；第三是采用漏洞扫描工具发现问题，并修改系统配置，将运行的系统服务减少到最低限度；

（8）网页保护　对政府网站的网页防篡改涉及到政府形象的问题。网页保护目前有许多工具，如 WaveBreaker 等产品，可以通过系统进程实时监测保护方法防止未授权用户篡改网页。