中国信息安全产品
政府采购指南

中国信息安全产品测评认证中心

2004年鉴

清华大学出版社
北京中电电子出版社

中国信息安全产品政府采购指南

（2004 年鉴）

中国信息安全产品测评认证中心

清华大学出版社
北京中电电子出版社

内 容 简 介

本指南涵盖了2003年度获得测评认证的信息安全产品(7类、60个)、安全服务提供商和信息安全专业人员(278人)名单。它是继2001年度和2002年度由中国信息安全产品测评认证中心推出的《信息安全产品政府采购指南》后出版的又一本新作。目的是为我国政府部门采购信息安全产品、保证信息系统有效运行以及制定信息安全决策提供及时、科学、权威、公正的技术依据和选用上述内容时的参考。

书　　名：中国信息安全产品政府采购指南（2004年鉴）
作　　者：中国信息安全产品测评认证中心
策　　划：高伟红　邵祖英
责任编辑：焦金生　邵祖英
装帧设计：冯小舟
广告代理：北京世纪浩天广告有限公司
许可证号：京密工商广字第0247号
联系电话：68026565　传真：68031515
出版发行：清华大学出版社、北京中电电子出版社
地　　址：清华大学出版社：北京海淀区双清路学研大厦A座
邮编：100084　电话：62776969
北京中电电子出版社：北京海淀区昆明湖南路九号云航大厦
邮编：100089　电话：88433856
印 装 者：北京华正印刷厂
开　　本：210×285　印张：16.5　字数：353千字
版　　次：2004年6月第1版　2004年6月第1次印刷
印　　数：1—2000
书　　号：ISBN 7-302-08558-7/TP·6138
光盘版号：ISBN 7-900057-82-X
定　　价：180.00元（含1CD）

前　言

自20世纪90年代以来，网络信息得到了惊人的发展。在网络给人们带来诸多好处的同时，也带来了不可避免的负面影响，比如遭受网络攻击、信息被盗等。为了有效地防范这些不良事件的发生，维护自己的权益不受侵犯，就需要我们开发、生产和使用各种工具和技术，及时保证我们的网络信息的安全性。这就使得网络与信息安全一直得到国家的重视，而各种网络信息安全产品的品质更是被政府及其他各级用户视为重中之重。

作为各级政府部门和信息安全厂商之间的纽带，中国信息安全产品测评认证中心自成立以来，一直秉承“科学、规范、客观、公正”的原则，严格按照国家信息安全测评认证标准及规范要求，为信息安全产品、信息系统、信息安全服务资质和信息安全人员资质的评测认证提供了保障。

2001年度和2002年度《信息安全产品政府采购指南》出版发行之后，受到了我国政府采购部门的一致好评。为了满足广大政府电子政务发展的需要，确保政府部门的信息安全，中国信息安全产品测评认证中心整理了2003年度获得认证证书的产品（共7类，60个产品）、安全服务提供商（共35家）和信息安全专业人员（共278人），汇编成今年《信息安全产品政府采购指南》，致力为我国政府部门采购信息安全产品、保证信息系统有效安全运行以及制定信息安全决策，提供科学公正的技术依据。并借此奉献给一直支持和关心我们的政府部门、产业界和广大社会读者。

最后，诚挚地感谢所有为本书的编写付出辛勤工作的认证中心同志以及各家获证的信息安全厂商。

中国信息安全产品测评认证中心

二〇〇四年五月

《中国信息安全产品政府采购指南》编委会

目　录

第1章　国家信息安全保障概述

1.1　信息化进程中的信息安全保障

国务院信息化工作办公室副主任　曲维枝

当今世界，国际局势正在发生深刻的变化，国家安全的内涵和外延发生了很大变化，除了国家主权、领土完整等传统安全外，大规模疾病流行、环境恶化、能源危机、跨国犯罪、恐怖主义等非传统安全正显现出来。特别是随着信息化的推进，国民经济和社会对信息和信息系统的依赖性越来越大，由此而产生的信息安全问题对国家安全的影响日益增加、日渐突出，国家安全面临着新的挑战。

对此必须予以高度重视，必须有充分的对策。要坚持积极防御、综合防范的方针，从国家安全、社会稳定、经济发展的高度去认识信息安全问题的极端重要性。在信息化规划和建设中，同步考虑信息安全问题，始终坚持一手抓信息化发展，一手抓信息安全保障工作。必须认识到，没有安全保障的信息化，会严重威胁国家安全和社会稳定，会置党和国家于一个非常危险的境地。同时，信息安全问题解决不好，有价值的信息不能上网，可以利用网络处理的业务不能用网络来处理，会严重影响和制约信息化的发展。必须辩证地看待信息安全问题，认识到没有绝对的安全，不存在没有风险的安全，安全风险和安全事件是不可能完全避免的。在具体信息化建设中，不能忽视信息安全威胁，也不能简单片面地夸大信息安全问题，必须综合平衡安全建设成本与安全风险，从实际安全需求出发进行安全建设和管理。

信息安全是信息化推进中出现的新问题，只能在发展的过程中加以解决。要坚持保障和促进信息化发展这一根本原则，以安全保发展，在发展中求安全。目前有些单位和地方简单地通过不上网、不共享、不互联互通来保安全，或者片面强调建专网。这样做的结果只能是造成不必要的重复建设，大量网络资源得不到充分利用，增加了信息化的成本，降低了信息化效益，失去了发展机遇。要立足安全防护，科学分析信息安全风险和威胁，采取多种技术和管理措施，加强预警和应急处置。要从安全保护、检测发现、应急处置、打击犯罪等各个环节，从法律、管理、技术、人才、意识等各个方面，从国家、企业、个人各个层面，采取综合的管理和技术措施，提高信息安全保障水平。

信息安全保障工作包括技术与管理两个方面，两个方面都很重要。但从目前我国实

际发生的安全事件看，较为薄弱的还是信息安全管理，有很多信息安全事件都是由于管理不到位，责任不落实造成的。要建立和完善信息安全管理责任制，加强管理，落实责任。信息安全是高技术的对抗，从根本上讲，解决信息安全问题还是要通过发展信息安全高技术。要坚持管理与技术并重，积极发展和采用先进技术来解决信息安全问题，同时也要注重通过加强管理弥补技术上的不足。

信息安全保障工作涉及到信息化建设的各个环节，包括法律、管理、技术、人才、意识等各个方面，与各部门、各地方都密切相关，是一个复杂的系统工程。网络中一个环节、一个局部、一台计算机出问题，都有可能迅速地扩展到各个系统和网络，影响全局。这就要求我们十分注重统筹规划、全面防护，从各个层面，各个环节上加强综合性的信息安全保障工作。与此同时，还要突出重点，有所为有所不为，将有限的资源用于基础部分、关键地方、要害部位。要重点防止那些关系到国计民生的重要基础设施和信息系统在遭到攻击、破坏和发生事故时，导致能源、金融、交通、通信、社会服务保障等的大面积瘫痪，给经济和社会造成的巨大损失。

安全单靠花钱是买不来的。发展信息和信息安全高技术、发展国家信息产业和信息安全产业、摆脱关键技术和设备受制于人的被动局面是掌握信息安全主动权的根本出路。要注重自主创新、自主可控。要大力推广应用国产软件、设备。虽然从总体上我们技不如人，但对于国家信息化建设中的很多方面，如电子政务中的机关办公、事务处理、对公服务等，国产软件、设备和服务是能够满足需求的。我们必须从保障国家信息安全、支持国家产业发展的高度，优先使用国产软件、设备和服务。另一方面，也要处理好自主研发与引进、采用国外先进技术和产品的关系，不能简单地认为只有自己的技术才是安全的，凡是国产设备就是可控的。要积极开展国际合作，认真学习国外信息和信息安全新技术，合理引进和利用信息安全产品。同时，要加强对引进技术和产品的安全可控研究，努力做到趋利避害，为我所用。

信息安全保障是国家的大事，是各级党委和政府的一项重要工作。政府要着重从政策引导、监督管理、人才培养、增强意识及基础技术研究开发等方面加强信息安全保障工作，同时也要做好政府本身信息系统的安全建设和管理工作，为社会做出榜样。但是，信息安全保障不仅是政府的事，仅靠政府部门是做不好信息安全工作的。在更大层面上，信息安全保障是广大企业、公民个人的责任和义务，需要全社会的共同努力。国家要鼓励社会力量参与信息安全建设。广大企业、科研机构应该成为信息安全技术研发、产业发展的主体，并为政府和社会提供安全服务。

国家信息安全战略是国家安全战略的重要组成部分，是国家信息化、信息安全保障的基本纲领，是党中央、国务院高层决策的基本依据。要根据国际国内的安全形势和国家的安全利益，全面分析评估面临的信息安全风险和威胁，形成信息安全的理论体系，重点是信息安全战略和关于信息安全重大问题的基本原则，确立战略目标、战略重点、战略步骤和总体思路，制定信息安全的中长期发展规划，指导信息安全建设和管理。

1.2 电子政务安全体系的建设与规划

中国工程院副院长 院士 邬贺铨

以信息化带动工业化,加快国民经济结构的战略性调整,实现社会生产力的跨越式发展,是党的十六大报告提出的重要任务。国家信息化领导小组决定,将推进电子政务建设作为今后一个时期我国信息化工作的重点。《我国电子政务建设指导意见》提出当前要以"两网一站四库十二系统"为目标的电子政务建设要求,目的是加强政府监管、提高政府效率、推进政府高效服务。

电子政务平台和安全体系

两网指政务内网和政务外网这两个平台,一站即政府门户网站,四库指人口信息数据库、法人单位信息数据库、自然资源和空间地理信息数据库以及宏观经济信息数据库。12个系统大体分为三个层次:办公业务资源系统和宏观经济管理系统,将在决策、稳定经济环境方面起主要作用;金税、金关(海关)、金财、金融监管(银行、证监与保监)、金审(审计)等五个业务系统服务于政府收支的监管;金盾(治安)、金社(社会保障)、金农、金水(水利资源)和金质(市场监管)等五个业务系统,重点是保障社会稳定和国民经济发展的持续。从技术上看电子政务平台的建设在物理层面上的核心网和城域网,将采用基于光纤的SDH和DWDM系统,保证足够的带宽和故障自愈恢复能力,接入网将以光纤为主多种接入手段并存。关于链路层技术,ATM能够提供业务质量保证(QoS),适于作为专线使用,以太网的帧简单,在企业网或机关内部网将有较多的应用。IP虽然并非理想但已无处不在,成为目前网络层的首选协议。当然在核心网上并不一定需要网络层操作,即ATM的信元交换可以代替路由器的选路,同样使用路由器在网络层实现对IP包选路后,链路层的ATM也并不一定是必须的,不过IP over ATM或IP与ATM混合使用的情况也不少。在电子政务平台的接入层面上IP是不可少的协议。从互联网发展起来的IP协议,存在着可扩展性、QoS和安全性的隐患,而电子政务对安全性尤为关注。因此电子政务平台的建设首先需要在安全体系上有很好的总体规划。信息安全是分布式计算环境中对信息的传输、存储、访问提供安全保护,以防止信息被窃取、篡改和非法操作。信息安全的三个基本要素是保密性、完整性和可用性服务。在分布式网络环境下还应提供鉴别、访问控制和抗否认等安全服务。完整的信息安全保障体系应包括保护、检测、响应和恢复等四个方面。网络的功能是分层的,因此网络安全与信息辈全也可分为五个层次,即安全的密码算法、安全协议、网络安全、操作系统安全(Windows、Linux等)和应用安全(Web安全、E-mail安全、病毒等)。图1-1表示了这五个层次。

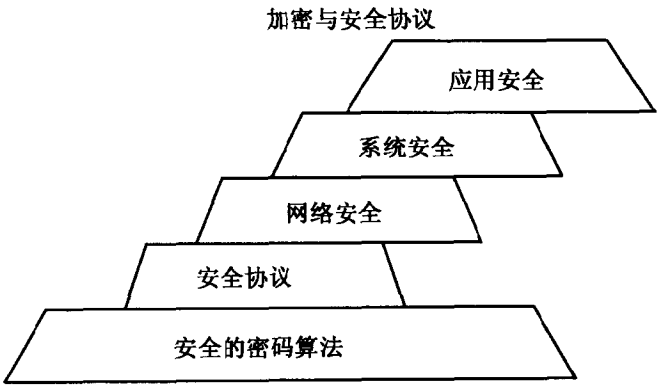

图 1-1 电子政务安全体系

密码技术是电子政务安全体系的基础，非对称密钥以及在此基础上发展的数字签名将在认证和访问控制等方面大量使用。在加密体制中通常涉及到 PKI，它是提供公钥加密和数字签名服务管理的综合系统。一个完整的 PKI 应该包括：认证机构(CA)、证书库、证书注销、密钥备份和恢复、自动密钥更新、密钥历史档案、交叉认证、支持不可否认、时间戳和客户端软件等。PKI 提供身份认证、消息完整性确认、保密和不可否认性的服务。将加密方法用到 IP 层是 IPsec 安全协议，它在 IP 包这一级为 IP 通讯业务提供保护，用于弥补 IPv4 协议在设计时安全性考虑的不足。它对于应用层是透明的，可针对链路，也可以针对最终用户，可以实现在防火墙或者路由器上。它的最常见的应用是构造虚拟专用网 VPN。将加密方法用到 TCP 层之上的例子是 SSL(安全套接层)和 TLS(传送层安全)访问控制协议，可按照身份、规则和角色来授权接入。单纯的加密方法突出了重要信息，容易引起攻击者的好奇成为破解或破坏的目标。信息隐藏(伪装)就是将需加密的信息秘密隐藏于另一非机密的文件内容之中，其形式可为任何一种数字媒体，如图象、声音、视频或一般的文档等。密码仅仅隐藏了信息的内容，而信息伪装不但隐藏了信息的内容而且隐藏了信息的存在。另外，对多媒体信息利用传统的加解密系统并不能很好地解决版权保护问题，原创作者没有办法追踪作品的复制。数字水印是携带所有者版权信息的一组记号，水印与源数据(如图象、音频、视频数据)紧密结合并隐藏其中，成为源数据不可分离的一部分，并可经历一些不破坏源数据使用价值或商用价值的操作而存活下来。被嵌入的记号通常是不可见或不可察的，但是通过一些计算操作可以被检测或者被提取。信息隐藏包括水印技术在电子政务的保密公文传递和审批中也很有使用价值。密码芯片相对软件加密具有较好的应用实时性和可靠性，加密设备应尽量使用基于自主研制的算法的密码芯片，嵌入密码芯片的密码卡辅以口令管理可在非加密终端上获得加密效果，卡内大容量存储器可存储用户证书、属性等多种信息，具有快速的签名运算能力，方便移动办公。

网络安全

网络安全包括防护、评估和应急服务等方面。图1-2表示了网络安全体系包括的内容。

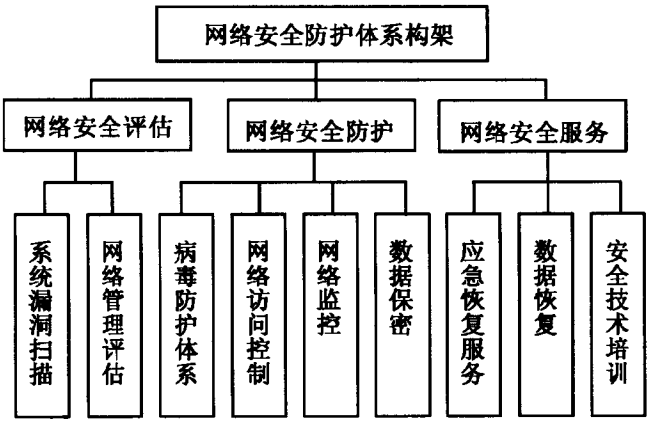

图1-2 网络安全体系

网络安全最基本的方法是使用防火墙,它设在需保护的网络或某一部分的入口,根据源和目的地地址、端口号和所用的IP协议以及高层协议等一些预置的规则,判断对IP包采取转发或丢弃措施,挡住未经授权的访问流量,避免各种IP地址和E-mail地址的欺骗和路由攻击。防火墙提供了一个监视各种安全事件的位置,防火墙可以作为IPsec的实现平台,还可以在防火墙上实现地址转换、Internet日志、审计、报警甚至计费功能。防火墙按照设置的位置(在IP层、应用层、应用层与传送层之间嵌入的套接层)而分为包过滤路由器、应用层网关(代理服务器)和电路层网关(代理服务器)。包过滤型防火墙成本低、对网络性能影响小,但无用户认证和通信状态记录,仅识别有限的通信状态消息,定义过滤规则复杂。应用代理型防火墙基于对用户的认证,可以监视包的内容,有较高的安全性能,但开销大,对网络时延等性能有影响,且可扩展性差,每增加一种网络服务必须增加相应的代理。另外,无论哪一种防火墙都不能防止内部的攻击,不能防止被病毒感染的程序或者文件、邮件等进入。因此内网与外网的物理隔离、外网与互联网的逻辑隔离是需要的。

虚拟专网(VPN)也是保护网络向特定对象开放的办法,VPN有虚拟专用远端连网(即VPRN隧道)、虚拟路由器和虚拟专用中继几种,前者需要使用IPsec保证安全性,但性价比、灵活性都较后两者好。VPN从技术上可分为IP VPN、ATM VPN和MPLS VPN,IP VPN具有可扩展性、建立和维护方便的长处,ATM VPN具有安全性和业务质量保证,MPLS VPN综合两者的优点,有发展潜力。

网络安全防护比检测和恢复更重要，黑客是利用网络的漏洞而得逞的，通过安全评估

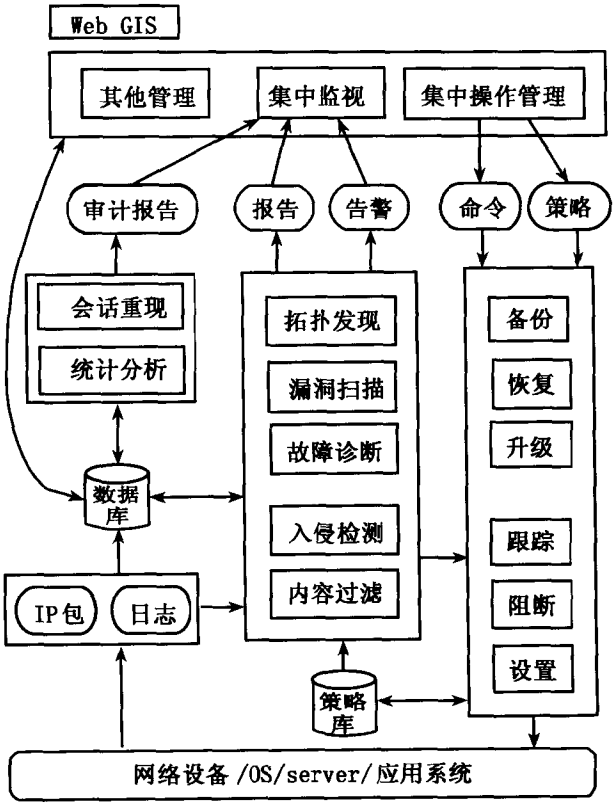

图 1－3　审计、检测与应急服务

和漏洞扫描可以及时发现网络隐患，防范于未然。设置入侵检测系统(IDS)跟踪未授权的接入，检测可基于主机、网络、内核和应用分别进行，对比基于行为和特征建立的知识库，根据流量和日志记录，找出目录、文件和程序运行中的异常，利用模式匹配技术、专家系统、状态转换分析技术、神经网络检测技术等来发现异常，一旦检测到人侵攻击必须尽快响应，启动防护系统和防火墙。另外还需要加强审计，记录所有的访问并作统计分析，堵塞内部的漏洞。一旦遭到攻击破坏，要及时评估影响，要启动备份系统实现灾难后的迅速恢复。系统的容灾解决方案包括基于数据块的远程复制(基于磁带或存储系统或主机的数据定期备份)和基于数据库的远程备份(包括异步备份和异构同步备份)。图 1－3 表示了检测、恢复与审计系统。需要指出，一个网络安全系统不应该是漏洞扫描系统、入侵检测系统、防火墙和容灾备份系统等松散的堆砌，需要从全网的体系构架出发，将所有这些功能有机的融入一个管理框架内，使其成为一个完整的互动的安全管理系统，提供从告警事件发生前到事后的全方位、全过程的集中处理。

操作系统的安全

在电子政务应用中PC机是用得很普遍的终端，Windows是常用的操作系统，不同的版本安全性能有差别，但都存在安全问题。如下的一些注意事项对于增加安全性是有益的。使用安全的密码，不要直接使用常见的单词、数字串以及可能暴露的主机信息（比如主机名、用户名等）等不安全的口令；需要了解缺省配置的不安全，在兼容性和安全性间求平衡；关闭不必要的服务和端口，因为各种服务打开的端口往往成为黑客攻击的入口，如果没有文件和打印机共享要求，最好禁止一些端口上（例如Windows 2000的139和445端口）的空会话；及时更新操作系统厂商发布的Service Pack补丁程序；打开跟安全有关的日志功能，且经常备份和检查；经常利用net session、netstat查看本机连接情况，并利用Task Manager查看本机运行的进程，及早发现异常情况；可以利用一些安全工具（如LockDown、BlackICE等）提供的本机程序安全管理功能，监控本机程序的异常状态（如主动连接外部陌生的地址），以增强主机对木马程序的监控能力。除了Windows外，Linux也存在漏洞，在使用上也需要注意。在电子政务的很多应用中可以使用NC代替PC，由于NC内装的软件相对简单，安全性防护的责任主要落在服务器上。

网站的安全

电子政务中网站的安全也是需要特别关心的。为了提供Web服务，必须要开放端口和一些目录，还要接受各种正常的连接请求，防火墙对Web服务器的保护是有限的，因此Web服务器往往是网络攻击的入口点。由于Web服务器在使用认证协议与授权机制方面要向下兼容访问者终端，在协商时要注意安全性最低的认证协议；在服务端的运行代码中，对于来自客户端的输入一定要进行验证；保护好口令的以及客户信息的安全存储；打开系统中对于Web服务的日志功能和日志记录。控制目录和文件的权限，只有指定范围的文件才可以被访问；检查每一个cgi文件，禁止通过Web读写，不要保留有漏洞的cgi文件，特别是系统预装的一些安全性考虑较欠缺的cgi示例文件；及时打上Web服务器软件厂商提供的补丁程序；Web应用的开发人员还要注意开发时防止缓冲区溢出。电子政务的安全除了上述技术措施（信息加密通信、身份认证、授权技术、防火墙技术、网络防毒等）和审计措施（实时监控企业安全状态、提供实时改变安全策略的能力、对现有的安全系统实施漏洞检查等）外，法律、规章制度和管理以及安全教育是必不可少的保证。安全总是相对的，魔高一尺，道高一丈，安全技术需要与时俱进。