e电子政府丛书

DIANZIZHENGFUCONGSHU

保证电子政府安全运行的基本方法

BAOZHENG DIANZI ZHENGFU ANQUAN YUNXING DE JIBEN FANGFA

◆ 丛书主编 罗元铮 焦宝文

中国财政经济出版社

——《电子政府丛书》

保证电子政府安全运行的基本方法

主　编　焦宝文　刘　岩

副主编　贺连英　张和龙

中国财政经济出版社

图书在版编目（CIP）数据

保证电子政府安全运行的基本方法/焦宝文等主编. —北京：中国财政经济出版社，2002.11

ISBN 7-5005-6190-3

Ⅰ.保… Ⅱ.焦… Ⅲ.电子政务—安全技术 Ⅳ.D035.1-39

中国版本图书馆 CIP 数据核字（2002）第 085885 号

中国财政经济出版社出版

URL：http://www.cfeph.com.cn

E-mail：cfeph@drc.gov.cn

社址：北京海淀区阜成路甲 28 号 邮政编码：100036

发行处电话：88190406 财经书店电话：64033436

北京市密云县印刷厂印刷 各地新华书店经销

787×960 毫米 16 开 15.5 印张 223 000 字

2003 年 1 月第 1 版 2003 年 1 月北京第 1 次印刷

印数：1—5000 册 定价：32.00 元

ISBN 7-5005-6190-3/F·5400

丛书编委会名单

前　言

保证电子政府安全运行的基本方法

信息技术的迅猛发展极大地推进了全球信息化和网络化的进程，把人类带入了一个崭新的信息时代。国际互联网的日益扩大，实现了信息跨国界快速而自由的流动。一方面，它使各国政府对信息扩散的控制能力明显减弱；另一方面，它又使一个国家可以不通过控制别国领土就可以获取所需资源。因此，信息安全已成为对主权国家的国家安全提出严峻挑战的突出问题。信息安全是指在一定范围内的社会环境下，由信息和网络技术与国家安全因素的相关性所构成的国家安全的一种态势，这种态势描述了国家免受国外信息威胁的能力和以信息手段维护国家综合安全的能力。可见，建立健全国家信息安全保障体系是加

强每一个主权国家的政治边界，保护本国的信息资源，强化主权国家安全能力的关键。

透视全球电子政府的发展概况，我们已经清楚地看到，电子政务的业务模型再造主要是围绕着与其相关的三个主体，即政府、企（事）业单位、居民三者之间的互动展开的。既然电子政务将这三方的互动置于一个数字的、网络的环境中，并要保证信息交流、服务传递以及在线支付安全可信，这就需要采用一种国际上普遍认可的有效方法。目前，数字签名和公钥基础设施（PKI）已经成为世界各国构建电子政府安全保障体系的基础。国际上已有20多个国家完成了与数字签名相关的立法，主要发达国家都在加快公钥基础设施建设。随着电子政府、电子商务和电子社区的发展，公钥基础设施的地位将像电信网是国家通信的基础设施一样，很快成为国家信息安全最核心的基础设施。

在《关于我国电子政务建设指导意见》中，明确指出要正确处理发展与安全的关系，综合平衡成本和效益，一手抓电子政务建设，一手抓网络与信息安全，制定并完善电子政务网络与信息安全保障体系。为了贯彻指导意见的精神，我国的电子政务试点示范工程开始采用具有自主知识产权的PKI信息安全技术进行政务内网和政务外网两个安全平台的建设。安全支撑平台主要由下述六部分组成：

（一）统一信任服务。主要解决分布式电子政务应用环境中实体身份的认证问题。数字证书的签发集中在CA中心进行，证书认证由分布式的证书认证服务系统完成。

（二）统一授权服务。将根据资源所有者的实际需要提供资源的访问授权管理服务。

（三）统一密码管理服务。将建设符合国家密码管理的有关政策的统一密码管理。

（四）网络安全防御。通过安全策略实施统一的管理和服务，每个独立的网络系统都要配备网络安全支撑系统，具体的子系统则根据需要选择。

（五）可信时间戳服务。为保证网上行为的不可抵赖性和可审计性，基于国家权威时间源和公钥基础设施提供可信时间戳服务。

（六）可信网络管理。针对不可信的IP网络，提供基于“一人一证，一机一证”电子政务网络系统的可信管理，其建设将覆盖整个政务网络。政务外网建设面向公众服务的安全支撑平台，原则上在国家公众根CA尚未建成之前，各部门之间的信任关系通过桥CA来实现，部门与地方的公众服务认证系统可通过桥CA实现交叉认证。

本书除了介绍一些常用的计算机系统的保密策略、信息加密策略以及信息安全管理策略之外，重点介绍了公钥基础设施的组成和基本原理，同时对信息安全核心技术和关键信息安全产品做了有选择的介绍，希望读者能对电子政府整个安全保障体系有一个比较全面的了解。

焦宝文

2002年10月1日

目　录

保证电子政府安全运行的基本方法

第一章 信息安全对国家安全提出的新挑战

20世纪90年代后期，计算机网络特别是Internet的各种应用发展迅猛，已经涉及到了人们的日常生活、学习、工作及商业、媒体、军事等诸多领域。无可置疑，计算机网络，尤其是Internet已成为21世纪知识经济社会运行的必要条件。以Internet为主的计算机网络改变了传统的社会运行方式，大多数情况下，人们不需要面对面地进行交流或是实施商务活动。事物都有两面性，人们在享受网络所拥有的快速便捷和高度信息共享之时，也对网络安全的漏洞防不胜防。用户失误、服务攻击、非法访问、盗取信息、商业间谍、病毒破坏、黑客行为……都使得各色各样的社会信息每时每刻身处险地。“天有不测风云”不再是危言耸听，而令人心悸的莫过于瞬间发生的自然灾害和人为制造的灾难，例如世界各地的大地震和美国“9.11”事件。当灭顶之灾到来时，身处险境的计算机网络系统也面临着空前的考验。一旦计算机系统中存储的数据被毁，人们失去的将不仅仅是记忆。试想，如果中央银行的账号信息全部在

灾难中丢失，整个社会的金融体系就将面临崩溃的危险。人类正向信息化社会迈进，信息已成为最能代表综合国力的战略资源。如何利用和保护这一战略资源是目前急需解决的问题。信息安全是保护信息资源、保护信息化进程健康有序和可持续发展的基础，也是一个国家政治、军事、经济以及社会生活正常运行的基础，并且是一个国家综合实力的重要体现。信息安全问题已成为关系到国家、政府、企业甚至个人安全的重大战略问题。

第一节　互联网与信息安全

近年来，互联网正以惊人的速度在全球发展，信息技术和信息产业正在改变着传统的生产、经营和生活方式，信息已成为人类社会宝贵的资源。当人们充分享受信息的同时，由互联网的发展带来的网络系统的安全问题，也变得日益突出，并受到了越来越多的关注。

一、信息安全的定义

关于信息安全，国际标准化组织（ISO）定义为："为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和显露"。

二、信息安全的内涵与特征

信息安全在内涵上包含两层意思，一是信息系统的安全，二是信息的安全，而保护信息的安全则是最终的目的。

信息安全性通常有四个方面的特征：保密性、完整性、可用性和可控性。

所谓保密性，即利用密码技术对敏感信息进行加密处理，同时采取抑制、屏蔽措施，以防电磁泄漏，保证信息不泄漏给非授权的个人和实

体，只有合法用户才能利用。这是信息系统安全性最重要的要求。通常涉及如下内容：密码体制、密钥管理、传输加密保护、存储加密保护、防电磁信息泄漏。

所谓完整性，即防止信息在存储或传输过程中被非法复制、修改、丢失和破坏，以保证信息的正确性、有效性、一致性。保证信息完整性是信息安全性的又一基本要求。通常信息系统的完整性包括：软件完整性、数据完整性，存储媒体的完整性及信息交换过程中的数据完整性。

所谓可用性，一方面要防止未授权者进入系统访问、窃取或破坏信息资源，另一方面应保证合法用户能够访问和有权访问信息及信息系统。在网络环境下，破坏网络和有关系统的正常运行，就属于对可用性的攻击。通常对可用性的要求如下：身份识别的确认、访问控制、审计。

所谓可控性，是指合法机构能对信息及信息系统进行合法监控，防止不良分子利用安全保密设备来从事反对政府或破坏社会安定等犯罪活动。通过特殊设计的密码体制与密钥管理运行机制相结合，使政府及管理监控机关可以依法侦探犯罪分子的犯罪行为，同时保护合法用户的个人隐私。

三、信息安全的内容

从总体上来说，信息安全包括四个方面的内容。

（一）实体安全

实体安全是指保护计算机设备、设施（含网络）以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）的破坏。

（二）运行安全

运行安全是指为保障系统功能的安全实现，提供一套安全措施（如风险分析、审计跟踪、备份与恢复、应急措施）来保护信息处理过程的安全。

（三）信息安全

信息安全是指防止信息资源被故意的或偶然的非授权泄露、更改、破坏或使信息被非法系统辨识、控制和否认。即确保信息的完整性、保密性、可用性和可控性。

（四）管理安全

管理安全是指有关的法律法令和规章制度以及安全管理手段，确保系统安全生存和运营。

四、信息安全工作的特点

计算机网络的根本特点在于实现了网络资源的共享，极大地提高了系统资源的利用率，最大限度地实现所处理信息的价值。信息安全工作就是保护网络系统资源不受偶然的或者恶意的原因而遭到破坏、更改、泄漏，使之连续可靠正常地运行。与其他安全工作相比，信息安全工作有诸多独特之处。

（一）信息安全涉及面非常广

计算机网络系统庞大而构成复杂，无论从社会领域、技术层面、信息资源，还是从地理分布、使用人员等方面来看，其涉及面都很广，因而管理和控制非常困难，解决信息安全的技术也更加复杂和多样化。反黑客与防病毒是我们经常听到的两个概念，但它们只是保护网络中的主机或服务器不受外来侵害的两个方面。在网络运行期间，网上信息在处理、传输和存储过程中还有诸多安全问题，如操作系统本身的安全、防止计算机辐射造成的信息泄漏和控制不良信息的传播等。此外，所需要的保护措施比一般信息管理系统和数据库应用系统所涉及的技术层面更深、更广。

（二）信息安全是一个系统的概念

信息安全不仅是技术问题，更重要的还要有相关的法律法规和安全管理。此外还与社会道德、行业管理以及人们的行为模式都有紧密的联系。因此，信息安全是涉及社会方方面面的系统工程。

（三）信息安全是发展的、动态的

因为网络攻防是此消彼长的事情，尤其是安全技术，它的敏感性、

竞争性和对抗性都是很强的，这就需要不断地检查、评估和调整相应的安全策略。计算机网络没有一劳永逸的安全，也没有一蹴而就的安全。

（四）信息安全是相对的

信息安全一定是相对的，而不是绝对的，也不要去追求一个永远也攻不破的安全技术。在信息安全这个技术对抗的领域里，到处都存在着失败的可能性。这也是信息安全技术必然与相应的法律法规以及安全管理紧密联系的原因之一，网络工作者必须常抓不懈。

五、互联网时代信息安全的重要性

互联网的迅速发展使信息的传输与加工可以在瞬间跨越地理位置的障碍而遍布世界各地，信息处理深入到各个部门和领域并已经进入了家庭，这一切使得人类开始进入信息化社会。无疑，信息的重要性与战略地位使得信息安全与数据保护至关重要，并受到国际社会的普遍关注。当前由于信息保护措施的不利或失误，世界各国所遭受的损失是巨大的。在商业、金融、交通、通信、国防、外交等部门的大量事例已充分说明了这一点。下面介绍几种网络遭受攻击的常见形式：

（一）黑客的入侵

2001 年，从 2 月 8 日起黑客接连 3 天攻击了美国的至少 7 家大网站，迫使声称从来没有出现过问题的 YAHOO 网站关闭数小时；2 月 12 日欧洲最受欢迎的欧洲卫星电视台网站遭受黑客攻击，网站瘫痪 3 个多小时，在南美洲从哥伦比亚的新闻网站到秘鲁的政府竞选网站无一幸免；2 月 18 日黑客甚至闯入了美国一家生物技术公司的网站，在网页上宣布假合并的消息，股民纷纷买进有关两家公司的股票，结果大蚀血本。一名俄罗斯黑客通过安装在地下室的简单设备入侵层层防设的美国花旗银行，使其损失 1600 万美金；黑客入侵美国中央情报局主页，将中央情报局更名为中央笨蛋局；黑客入侵美国司法部主页增加纳粹标记，等等。以上事件均造成重大影响。

（二）计算机病毒

随着互联网的发展，计算机病毒的种类急剧增加，扩散速度大大加

快，而且破坏性也加大，受感染的范围也越来越广，对各国信息系统造成了严重危害。计算机病毒可经电子邮件、互联网下载文件、浏览网页感染以及黑客恶意侵入等方式传播。主要的病毒种类有：1. 能够渗透到电话局、公共电视网及其管理系统并致使它们瘫痪的计算机病毒；2. 计算机逻辑炸弹；3. 能直接攻击和破坏计算机硬件系统造成主板损坏致使网络系统瘫痪。

（三）垃圾信息的侵入

网络信息的垃圾问题越来越严重，在跨国际数据流中存在大量有害信息，如虚假信息冗余、过时信息、黄色淫秽信息、政治反动信息、种族歧视信息等，这些垃圾信息在网上随意流动，相互渗透。由于全球系统的贯通，任何一个系统任何一个环节的污染都将给整个信息社会带来难以估计的破坏和损失，也会对国家安全、社会稳定造成极大的危害。由此可见，随着互联网的高速发展和应用的日益深入，网络环境下的信息安全问题已经浮出水面，如果忽视了这一问题，在信息系统网络化、国际化、公众化的今天必然会带来一系列的问题，甚至会危及到网络环境下国家的经济安全。随着信息高速公路的兴起，网络信息安全必须引起高度的重视，并探索和解决不断出现的新问题，以确保计算机信息系统真正造福于国家和人民。

六、信息安全的实现

要实现信息的整体安全，需要解决好以下诸多问题。

（一）环境安全

保护计算机信息系统免受水、火、有害气体、地震、雷击和静电的危害，实现受灾报警、受灾保护和受灾恢复；通过电子手段（如红外扫描等）或其他手段对特定区域或活动区域进行保护（如监测和控制等）。

（二）设备安全

使用一定的防盗手段（如移动报警器、数字探测报警和部件上锁）用于计算机信息系统设备和部件，以提高计算机信息系统设备和部件的安全性；使用一定的防毁措施保护计算机信息系统设备和部件，对抗自

然力或人为的破坏；防止计算机信息系统中的电磁信息的泄漏，提高系统内敏感信息的安全性；预防、探测、定位和对抗线路截获，防止对计算机信息系统通信线路的截获和外界对计算机信息系统的通信线路的干扰；对抗或消除外界对计算机信息系统的电磁干扰；为计算机信息系统设备的可靠运行提供能源保障，例如不间断电源、纹波抑制器、电源调节软件等。

（三）媒体安全

做好媒体的防盗、防毁（如防霉和防砸）工作；防止媒体数据被非法拷贝；在媒体数据的销毁环节上，要对媒体进行彻底的销毁（如媒体粉碎、消磁等），防止媒体数据删除或销毁后被他人恢复而泄露信息；防止意外或故意的破坏使媒体数据丢失。

（四）风险分析

对系统进行静态的分析（尤指系统设计前和系统运行前的风险分析），发现系统的潜在安全隐患；对系统进行动态的分析，即在系统运行过程中测试、跟踪并记录其活动，发现系统运行期的安全漏洞；对系统运行后进行分析，并提供相应的系统脆弱性分析报告。

（五）审计跟踪

记录和跟踪各种系统状态的变化，如对系统故意入侵行为的记录和对系统安全功能违反的记录；实现对各种安全事故的定位，如监控和捕捉各种安全事件；保存、维护和管理审计日志。

（六）备份与恢复

对系统设备和系统数据进行备份，以便在系统出现问题后能及时恢复。

（七）应急

对紧急事件或安全事故发生时的影响进行分析，制定完善的应急计划；当紧急事件或安全事故发生时，能够及时提供应急设施。

（八）操作系统安全

使用具备安全策略的操作系统；通过构建安全模块和安全外罩，增强操作系统的安全性。