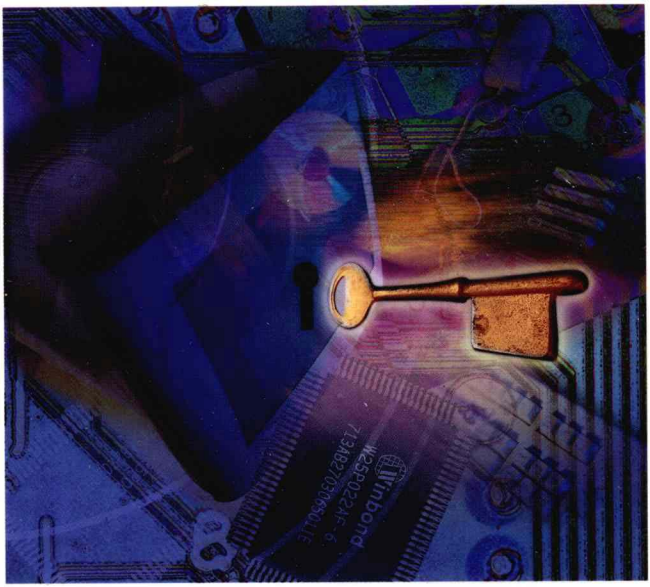
江苏省网络与信息安全协调小组办公室　编

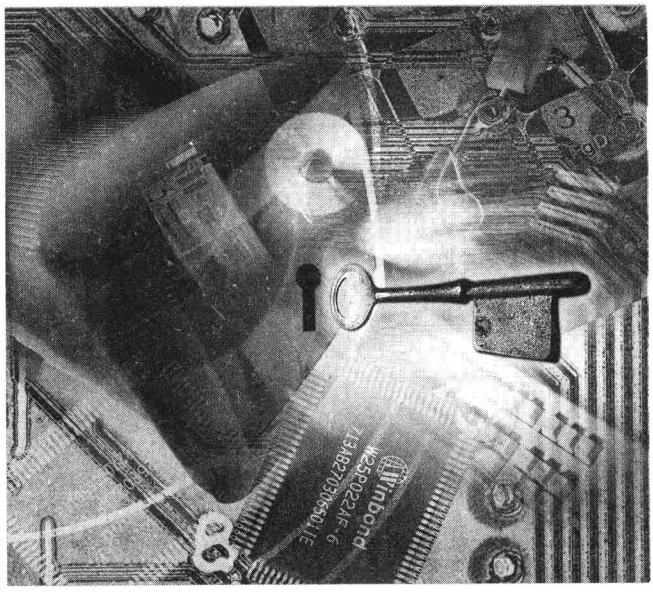
公务人员
信息安全知识读本



凤凰出版传媒集团
江苏科学技术出版社

江苏省网络与信息安全协调小组办公室　编

公务人员信息安全知识读本



凤凰出版传媒集团
江苏科学技术出版社

图书在版编目(CIP)数据

公务人员信息安全知识读本 / 江苏省网络与信息安全协调小组办公室编. —南京：江苏科学技术出版社，2009.1

ISBN 978-7-5345-6363-8

Ⅰ.公… Ⅱ.江… Ⅲ.信息系统—安全技术—基本知识 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2008)第 191532 号

公务人员信息安全知识读本

编　　著	江苏省网络与信息安全协调小组办公室
责任编辑	仲　敏
责任校对	郝慧华
责任监制	张瑞云
出版发行	江苏科学技术出版社(南京市湖南路 47 号，邮编：210009)
网　　址	http://www.pspress.cn
集团地址	凤凰出版传媒集团(南京市中央路 165 号，邮编：210009)
集团网址	凤凰出版传媒网 http://www.ppm.cn
经　　销	江苏省新华发行集团有限公司
照　　排	南京展望文化发展有限公司
印　　刷	南京大众新科技印刷有限公司
开　　本	850 mm×1168 mm 1/32
印　　张	4.875
字　　数	100 000
版　　次	2009 年 1 月第 1 版
印　　次	2009 年 1 月第 1 次印刷
标准书号	ISBN 978-7-5345-6363-8
定　　价	15.00 元

图书如有印装质量问题，可随时向我社出版科调换。

序 PREFACE

信息化是人类由工业社会向信息社会转型的必然进程。随着信息技术的迅猛发展和网络化应用的快速普及，信息化已渗透到国民经济和社会发展的方方面面，并深刻影响着人们的生产、生活和思维方式。与此同时，信息安全问题也日渐突出，形形色色的恶意程序、层出不穷的系统漏洞、日益猖獗的网络攻击等，对信息化的持续推进提出了严峻考验，成为事关一个国家军事、政治、经济、社会和文化安全的重大问题。近年来，按照中央要求，江苏在保障信息安全方面做了大量工作，但也存在不少问题，全社会信息安全意识有待提高，信息安全管理亟需加强。

电子政务是江苏信息化发展最快的领域之一，也是信息安全保障的重点领域。电子政务建设，电子是手段、政务是核心、应用是关键、安全是保障。根据发达国家和地区经验，信息安全保障，管理重于技术、平时重于战时、内部重于外部。广大公务人员既是电子政务的实践者，又是信息安全的维护者，在充分利用信息化手段开展公共管理、公共服务的同时，也对维护

和保障信息安全负有重要责任。

为加强全省公务人员信息安全基本知识和技能普及，省人事厅、信息产业厅（省信息安全办）组织编写了《公务人员信息安全知识读本》，这是贯彻“积极预防、综合防范”方针，切实增强全省公务人员信息安全意识的一项基础性工作，非常及时，也很有意义。各地、各部门要高度重视信息安全知识的宣传普及，推动广大公务人员认真学习基本知识、掌握基本技能，增强安全防范意识，共同维护信息安全，促进江苏信息化健康发展。

衷心希望这一读本的出版，能在全省信息安全保障体系建设中发挥积极作用。

2009 年 1 月

前言 FOREWORD

根据江苏省委、省政府“大力普及信息安全基础知识和基本技能”的工作要求，在江苏省人事厅、江苏省信息产业厅的支持和指导下，江苏省网络与信息安全协调小组办公室以公务人员宣传普及为重点，组织编写了《公务人员信息安全知识读本》。

全书共分九章，围绕公务人员日常工作中涉及的信息安全基础知识、基本技能组织有关资料。为突出重点、注重实效，读本采用了问答形式编写。在语言表达上，努力适应公务人员知识结构和阅读习惯，力求概念表述通俗易懂、原理论述简明扼要、操作步骤具体明晰，尽可能做到技术性与管理性、知识性与实用性、政策性与业务性相统一。

本书的编写凝聚了很多领导、专家和同仁的心血。江苏省人事厅赵永贤厅长，江苏省信息产业厅谢正义厅长、张坊副厅长等编委会的各位领导和专家非常重视本书的出版和宣传工作，对书稿的内容进行了认真审定，提出了重要的指导性意见。南京邮电大学王汝传教授、吴蒙教授受江苏省网络与信息安全

协调小组办公室委托，开展了专题研究，形成了较完整的读本文稿。江苏省网络与信息安全协调小组办公室王丹中、陈宇青同志根据工作需要和公务人员知识读本的特点，对书稿进行了较系统的修改、调整和补充。为确保内容的科学性，江苏省网络与信息安全协调小组办公室分别约请南京大学曾庆凯教授对第3章和第6章、黄皓教授对第8章、东南大学胡爱群教授对第7章、罗军舟教授对第4章、南京航空航天大学秦小麟教授对第2章、江苏省信息安全测评中心黄申高级工程师对第9章、苏州天创公司张瑞钦工程师对第5章进行了专业审定。王丹中同志负责全书的统稿工作。

本书的顺利出版，江苏科学技术出版社给予了大力的支持和帮助，江苏省信息安全测评中心的吴兰工程师也为书稿的修改、补充付出了辛勤的劳动，在此一并表示衷心感谢。

编写《公务人员信息安全知识读本》，是江苏省宣传普及信息安全知识、技能的首次尝试。由于水平有限、经验不足，加之信息安全新知识、新技术层出不穷，读本一定存在许多疏漏和不足之处，敬请广大读者提出宝贵意见。

江苏省网络与信息安全协调小组办公室

2009年1月

目录 CONTENTS

第1章 信息安全概述

1. 为什么信息安全形势日趋严峻?

信息安全的概念,有广义和狭义两种。广义的信息安全,指一个国家的信息化状态和信息技术体系不受威胁和侵害;狭义的信息安全,指信息资产(信息网络、信息系统及其运行软件、数据等)不因偶然或故意的原因被非授权泄露、更改、破坏,或被非法系统辨别、控制。

随着信息化的深入发展,信息安全的概念也将不断扩展和深化。信息安全的本质,就是通过一系列管理和技术措施,实现信息网络和信息系统的正常运行,确保信息在产生、传输、使用、存储等过程中的保密、完整、可用、真实和可控。

当前信息安全形势日趋严峻,从世界范围看,有下列政治、经济和社会因素:

① 各种敌对势力将互联网作为政治扩展、意识形态渗透和机密信息窃取的工具,严重威胁国家安全和政治、经济与社会稳定。

② 不法分子利用网络开展违法犯罪活动牟取利益。网络盗窃、网络诈骗、网络侵犯知识产权已成为新型多发违法犯罪,网络

淫秽色情案件、网络赌博团伙犯罪明显增加，以敲诈勒索为目的的黑客攻击频繁发生，社会危害性不断加大。

③ 网络信息系统本身的缺陷不断暴露。路由器、交换机等网络设备以及常用系统或软件的严重级别漏洞增多，客观上造成了重大网络安全隐患。

④ 病毒等恶意程序数量大幅度增长。不法分子出于牟利或恶意炫耀等目的，制造大量新恶意程序，致使逐年成倍增长。其中，“木马”最为严重，恶意程序传播的趋利性日益突出，反查杀能力不断增强。

⑤ 别有用心者传播谣言，通过制造色情、暴力、迷信等不良信息，发泄不满情绪，扰乱公众思维、破坏社会稳定。

⑥ 伴随互联网技术的迅速发展和网络应用的日益普及，网络公共安全管理基础设施建设和技术手段相对滞后，公众对信息安全的认识和防护能力不足等。

2. 信息系统面临哪些安全威胁？

威胁是指可能对信息系统和用户造成潜在破坏的事件。造成威胁的原因是多方面的，包括物理环境的影响、操作系统的不健全、应用软件的缺陷、网络协议的不完善、用户不正确的使用习惯、恶意程序等。

(1) 物理环境因素

物理环境因素包括自然事件因素，如地震、雷击、洪灾、火灾等导致的安全威胁；电磁辐射或人为操作过失，如错误地删除文件、格式化硬盘等导致的安全威胁等。

(2) 操作系统因素

操作系统本身存在漏洞可能导致的安全威胁。

(3) 应用软件因素

因程序设计时疏忽或考虑不周而留下的错误或漏洞可能导致的安全威胁。

(4) 网络协议因素

网络协议在安全方面存在的先天性缺陷导致的安全威胁，如最常用的 TCP/IP 协议就存在 TCP 序列号预计、IP 源路由选择等多方面的隐患，可被利用发起 IP 欺骗、分布式拒绝服务攻击等攻击行为。

(5) 用户的不安全使用

用户由于缺乏信息安全防护知识或安全意识淡薄，不能安全使用信息系统可能导致的安全威胁，如一些用户为了方便而采用很容易被破解的简单短小的密码。

(6) 恶意程序

恶意程序是有目的地编写出来的威胁信息安全的计算机程序，常见的有传统病毒、“木马”病毒和“蠕虫”病毒，它们会破坏系统硬件、威胁用户数据、阻塞网络通信。

3. 网络安全体系由哪几部分构成?

一个常见的网络安全体系包括防护、检测、响应、恢复四个部分，被称为 PDRR 体系。

防护包括对系统、网络和数据的安全防护，是主动地发现问题、完善防范措施的过程，是整个安全体系的基础。这一阶段可以

采取的措施是多样的，包括部署访问控制设备、安装防火墙、安装杀毒软件等。这一阶段应重视风险评估等安全测评工作，以便明确信息安全隐患，有针对性地制定安全措施。

检测是对防护措施的验证和补充，其目的是及时发现攻击行为，对攻击进行阻拦并记录。它依据入侵行为的特征来发现攻击行为。检测的结果应反馈至防护环节，作为完善防护措施的重要参考。

能否及时、有针对性地响应，会在很大程度上影响系统的安全状态和在突发信息安全事件下的损失。响应分为应急响应和一般事件处理，应急响应指当信息安全事件发生时紧急采取的对策；一般事件处理包括咨询、培训、技术支持等。

恢复是当信息系统遭到破坏后，还原系统状态、恢复数据的过程，包含恢复系统和恢复数据两个含义。对于大部分网站和网络应用来说，数据信息是最宝贵的财产，应当重点保护。

4. 信息系统安全防护体系设计应遵循哪些原则？

（1）建设与安全同步

信息安全防护应贯穿信息系统建设运行全过程，在信息系统设计、建设、运行维护、废弃的整个生命周期都要同步考虑信息安全问题。

（2）管理与技术并重

在重视加强技术防护能力建设的同时，要充分发挥人在信息安全防护中的作用，通过信息安全制度建设增强意识、明确责任、健全机制，主动有效地预防信息安全威胁。