国家信息安全培训丛书

信息安全普及读本

（公务版）

中国信息安全测评中心　编著

航空工业出版社

信息安全普及读本

（公务版）

中国信息安全测评中心

二〇〇八年十一月

序

信息化是当今世界发展的大趋势，是推动经济社会发展和变革的重要力量。随着我国信息化的不断推进，国民经济和社会发展对网络和信息系统的依赖性越来越强，信息安全对国家经济、政治、文化和军事安全等方面的潜在影响力在逐步增大。近年来国内国际的一系列安全事件表明，在信息安全问题和信息安全保障工作中，人是最关键和最活跃的因素，信息安全是同信息化生活中每个人都息息相关的事情，信息安全保障工作需要每个人积极主动参与，需要每个人提高自己的信息安全意识和能力，需要每个人积极主动地保护自己和国家的信息安全空间。

信息安全宣传、教育和培训是国家信息安全保障工作的重要组成部分，国家也高度重视信息安全人才培养和全民信息安全意识的教育工作。2003 年《国家信息化领导小组关于加强信息安全保障工作的意见》明确提出了“加快信息安全人才培养，增强全民信息安全意识”的要求。为落实国家“加快信息安全人才培养，增强全民信息安全意识”的要求，适应加快信息安全人才培养、大力开展信息安全教育工作的迫切需求，国务院信息办委托中国信息安全测评中心承担信息安全培训教材的编写工作。

信息安全意识培训教材包括面向政府、企事业单位的公务版——《信息安全普及读物（公务版）》和面向公众的普及版——《信息安全普及读本（公众版）》。《信息安全普及读本》是中国信息安全测评中心组织有关专家编写的面向信息化工作中普通用户的一本普及信息安全意识和实践的教材。《信息安全普及读物（公务版）》从增强全民信息安全意识出发，比较系统地向广大政府、企事业单位的信息化用户介绍了信息安全基本原则、信息安全法律法规等信息安全基本概念，并从计算机安全、应用安全、数据安全、了解黑客等方面介绍了具体的信息安全操作实践。该教材浅显易懂、可操作可实践性较强，对普及和增强信息安全意识工作将提供有益的帮助。

信息安全意识培训教材的出版，是加快信息安全人才培养、大力开展信息安全教育工作的具体举措，是全面信息安全意识宣传和教育方面走出的第一步。希望该书的出版及在实践中不断取得进步和完善，有利于促进我国信息安全宣传、教育与培训工作的科学发展，为提高我国信息安全保障能力和水平做出贡献。

前言

信息技术的飞速发展与广泛应用，深刻地改变了人们生活、生产与管理的方式，加快了国家现代化和社会文明的发展。但由于信息技术本身的特性，特别是信息和网络无国界性的特点，整个信息化进程中存在着巨大的信息安全风险。

网络给人们提供一个发表个人观点和进行交流的渠道，同时它也成为一些恐怖组织宣传虚假消息的工具；网上大量的政治、经济、军事乃至生活信息在提供便利的同时，又成为犯罪分子和恐怖分子丰富的资料源。特别是信息系统在国家各级政府部门、金融部门、公共服务相关部门等的网络应用，使得信息系统安全保护不仅仅关系到计算机信息系统本身的安全，而且关系到国家安全、社会安定和经济的发展。因此，信息安全已经成为一个战略性问题。

作为一种全新的交流传播工具，网络的出现和普及在很大程度上改变了原有的人与人之间的联系方式、学习工作环境乃至整个社会结构。人既是网上资源的提供者和使用者，又是网络的建设者，是系统的主体，处于主导地位，系统的资源（包括硬软件、通讯网、数据、信息等）都要服务于“人”。因此，信息安全的主体就是“人”，信息安全是要保障主体对信息资源的控制。

在全体公众尤其是公务人员当中建立信息安全意识是网络信息应用的基础。它可以提高政府的公众服务效率，并通过服务加强全民的安全意识，推动信息安全的建设和发展。

最有效的防范措施应该是主动防止非授权访问操作，从客户端操作平台实施高等级防范，使不安全因素在终端源头得到控制。我们所关注的是同我们个人计算机、同我们个人使用互联网相关的安全问题。因此，在本书中，我们所讨论的信息安全主要是指个人计算机安全、以及家庭工作中访问互联网相关的安全问题。

本书目的

本书希望对各种计算机水平的使用者提供信息安全方面的知识：

- 理解信息时代的网络环境和威胁，了解信息安全风险评估的概念和意义；
- 理解和实践如何保护计算机和如何安全访问互联网；
- 理解恶意代码、黑客攻击的知识，并了解如何应对这些威胁。

本书主要内容

本书围绕信息安全保护工作所关注的主要问题和所需了解的基础知识和实践展开，包括了非传统安全中的信息安全问题和安全防护的全面知识。希望本书能够成为一本适用于政务人员加强信息化建设和安全防护的实用、全面的参考资料。

本书共包括五个部分：

- **第 1 部分：信息安全概述**。在第 1 部分中，首先我们将向大家描述网络环境下的信息安全，并进一步深入地分析和描述讨论今天我们在互联网上所碰到的各种威胁的。特别针对中国面临的信息安全形式和威胁，让大家了解现在信息安全真实的威胁实例和热点。看完这些实例后，我们将通过孙子兵法的“知己知彼，百战不殆”的原则来生动地诠释信息安全风险的概念和信息安全风险管理的步骤。最后结合我国实际情况，介绍了我国的信息安全法律法规体系。
- **第 2 部分：主机安全。**在第 2 部分里，接下来我们从主机操作系统——包括 Windows XP SP2 操作系统的安全实践。这样从安全解决方案的思路上，根据“由外及内、由下及上”（由下及上—从操作系统安全基础，到 Web 浏览和邮件等应用的安全基础）的方式来诠释和组织完整的信息安全方案，更结构化地建立用户安全保护的整体方案。
- **第 3 部分：应用安全。**在第 3 部分介绍了主机操作系统上的电子邮件、Web 浏览器等常见的应用程序的基础安全知识，并以微软 Office Outlook、Outlook Express 邮件客户端、Firefox Web 浏览器为例讲解这些软件的最佳安全知识。然后，讨论了互联网安全保护的各种措施和考虑。
- **第 4 部分：数据安全。**第 4 部分，介绍了如何保护个人信息，免受信息恐怖主义的威胁的相关操作。为了防止你的信息遭到盗窃和破坏，保护你的珍贵数据，可以开启 Windows 的隐私属性，并为 Windows 账户设置口令，采取数据加密，数据备份等一系列措施。
- **第 5 部分：初识黑客。**在第 5 部分中，我们将换一个视角，从信息安全的另一个方面，从攻击的角度来讨论我们现在最主要面临的各种恶

意软件和黑客攻击，也就是从知彼的方面来讨论信息安全问题。这样，通过第 2、3 和 4 部分的学习，我们才能实现在第 1 部分中我们所提出的“知己知彼，百战不殆”的信息安全战争艺术。并从具体应用角度加以实践，使我们能更加安全地在互联网上访问、交流和共享信息。

本书作用

信息化正在全球范围内改变着政治对话和意识形态宣传的状况与格局。它提供了一种新平台，从而更为方便地收集和发布信息，更为快速地组织和协调全球范围的行动，更为有效地为决策者提供决策依据。但是，在利用信息化技术的同时，我们的政务人员必须提高安全意识，掌握操作系统、电子邮件、Web 浏览等信息活动中的安全知识和安全防护技术，对病毒、黑客有足够多的了解。本书循序渐近地介绍了各种最新的、最关键的信息安全方面的知识，帮助读者逐步了解自己所需的操作系统、互联网、个人隐私保护、信息共享等方面的安全知识与技术。每个读者可以根据自己的需求来有的放矢地阅读本书。

目录

第一部分
信息安全概述

本部分包含以下章节：

第 1 章　信息时代的网络环境和威胁

第 2 章　“知己知彼，百战不殆”—信息安全的风险管理概念

第 3 章　做个知法守法的公务员

在本部分中：

随着计算机的大范围应用，越来越多的机构不得不重新布局以与技术的发展保持一致。在这个过程中，社会作为整体，变得越来越依赖于大型的、微妙结合起来的技术系统。网络作为国家控制经济和安全的不可缺少的基础设施，它的安全、持续运转成为维系社会持续发展的先决条件。只有了解了这些系统本身的脆弱点以及可能受到的威胁，我们才可以更好地保护这些基础设施。

引入“知已知彼，百战不殆”的风险评估概念，防范和对抗对关键信息基础设施的信息攻击和破坏。

强化法律法规概念，使信息的使用者们能够有效地进行防范和反击，保障公民基本权利。

第 1 章 信息时代的网络环境和威胁

1.1 网络环境

信息时代的科技扩展了全球性知识，形成了全球性的政府、商业、军队和其他国际性组织。许多学者和政客将我们互相连通的世界亲切地称为“地球村”。在国内，信息时代的科技帮助创建和提高了国家的国内政治、经济和军事能力。这些科技同样帮助定义社会、文化和相关环境。在国家层面上，这些都是国家安全综合体中的重要组成部分，因为一个国家如果想要生存和发展，它必须将安全政策的基石建立在国内能力和环境之上。

信息空间是一个没有边界的新的地理学空间，它的特征是技术和变化，并且也是具有全球性的地理空间。经济全球化与信息网络化的结合，形成了以全球金融网络为主体、以电子商务为主要形式的网络经济。这种网络形式是一个面向任何国家任何人开放的独立自主的网络。用户将其计算机连接到一个 Web 站点，就表明已经与互联网连接，可以非常轻松地跨越“国界”。从事网上活动的人，法律关系的主体处于不同国家的控制之下；任何团体和个人，不管其肤色、性别和政治、宗教信仰，也不管身处何方，都可以自由出入境。网络王国已经成为一个不需要任何护照，无边界检查站、出入畅通的“数字化王国”。

1.2 安全威胁

传统的威胁包括疾病、各种抢劫、偷窃等恶意和犯罪的威胁。在信息世界里，随着我们开始越来越多使用计算机连接到网络和互联网上，世界通过鼠标触手可及，同时各种信息安全的威胁也如魔魇一般不请自来。这就是信息社会最为显著的特点，起决定作用的不是资本而是信息，信息成为比物资或能源更重要的战略资源。所以争夺、获取、控制和破坏信息资源也就成为国家、团体、组织和个人在利益和权力竞争中的主要方式。

互联网访问中的种种威胁与现实生活中的威胁相类似，它们可能是各种计算机病毒、黑客攻击和破坏，甚至是各种计算机犯罪。居心叵测的不法分子可以利用信息空间进行反政府、反社会的政治动员和破坏；利用互联网内部反对力量，进行颠覆性宣传；挑起网络外交冲突和摩擦等。

互联网可以用来协调活动，发挥组织机构的职能。通过互联网，可以发布请愿书和行动警告，筹集资金，向民众和媒体进行宣传。在政治泛滥和公民意识强化的条件下，广泛性抵抗活动将会产生怎样的社会后果？当政治动员从孤立的事件转化为一种集中化的联合力量时，又将会怎样？这种势力或运动会不会有朝一日成为信息空间和现实世界中反政府的主导力量？

所有迹象表明，政府正面临着网络政治动员向网络政治行动转变的现实威胁和挑战。

为了进一步深入了解这些威胁所采取的形式和手段，我们将威胁分为：偶然威胁、恶意威胁、授权威胁、应用威胁、隐私威胁和访问控制威胁。了解了这些威胁，我们才能更进一步来学习如何防御这些威胁，确保我们自己的信息环境的安全。

1.2.1 偶然威胁

偶然威胁是指无计划的和无意识的威胁。这些威胁通常都是人为错误导致的，如弱口令、事故或错误的交易处理、信息的偶然暴露、应用软件的误用。偶然威胁通常是由于缺少在线安全意识，不正确的配置导致的。

1.2.2 恶意威胁

恶意威胁是有目的的针对组织机构的人，系统和网络所进行的攻击。恶意攻击可以进一步划分为以下两类：

- 恶意软件。我们传统意义上所讲的病毒（Virus）现在已经发展成为包括病毒、蠕虫、特洛伊木马、后门、广告软件、间谍软件等一系列概念的恶意软件（Malware）大家族。恶意软件及与黑客攻击相结合是我们当前所面临的主要安全问题。
- 社会工程威胁。社会工程威胁是一种最古老、并且也是最有效的信息安全威胁方式。

1.2.3 授权威胁

授权威胁是指黑客佯装成授权用户进行操作带来的威胁。常见的一个授权攻击是一个入侵者攻破用户的网络，获取用户口令并在系统上注册。入侵者使用各种方式攻破口令（如字典攻击或破解口令的设备）。

1.2.4 应用威胁

应用威胁是指计算机应用程序所可能带来的威胁。在因特网的早期，Web 网站通常呈现的是静态的网页，可以看见大多数网页代码，改变这些 Web 网站的代码是很容易的。

1.2.5 隐私威胁

隐私威胁包括各种各样的窃听攻击。

1.2.6 访问控制威胁

如名字所说的，访问控制威胁包括攻击进入网络系统。最常采用的方式是口令破解。其它的攻击包括攻击存取口令文件和通信点如调制解调器或使用软件挖掘网络上的漏洞并安装可见或不可见的后门进入内部或外部系统。