<<计算机网络安全>>

图书基本信息

书名：<<计算机网络安全>>

13位ISBN编号：9787030296818

10位ISBN编号：7030296818

出版时间：2011-1

出版时间：科学出版社

作者：梅挺

页数：312

<<计算机网络安全>>

内容概要

梅挺编写的《计算机网络安全》是在广泛调研和充分论证的基础上，结合当前应用最为广泛的操作平台和网络安全规范写作而成，强调理论与实践相结合，具有科学、严谨的体系结构。
全书内容丰富、构思新颖，全面阐述了网络安全理论与实践技术。

《计算机网络安全》可作为网络安全领域的科技人员与信息系统安全管理人员的参考用书，也可作为高等院校研究生的教学用书。

<<计算机网络安全>>

书籍目录

章节摘录

插图：1　绪论1.1　研究背景及意义2000年7月，八国集团在日本冲绳发表的《全球信息社会冲绳宪章枠中认为：“ 信息通信技术是21世纪社会发展最强有力的动力之一，并将迅速成为世界经济增长的重要动力。
”随着社会信息化浪潮的不断冲击，建立在信息通信技术基础上的信息通信产业已经成为国民经济中的重要产业，也是信息产业中发展最快、规模最大的产业之一。
信息通信产业的技术和资金密集性特点，决定了其发展需要从国家整体的高度来确定目标和引导。
发达国家的经验也表明，政府对信息通信产业的大力支持主要体现为制定国家信息通信政策和各种法规来保障其发展。
制定高质量的信息通信政策是推动信息通信产业发展的前提和基础，信息通信政策不仅影响到信息通信产业的发展规模和增长速度，而且影响到国家整体的经济和发展潜力。
从全世界信息通信产业的发展历程来看，虽然各国的信息通信产业改革之间存在着或多或少的政治制度和经济基础方面的差异，但是世界性的大趋势是在信息通信产业领域内都经历了从垄断到竞争的改革历程，打破垄断、放松管制、自由化和民营化已成为信息通信产业改革的大趋势。
而在这个过程中政府发挥着重要作用，没有政策的扶持和政府的推动，信息通信产业的改革是不可能实现的。
因此，信息通信政策的制定和选择成为政府决策者在制定总体发展战略和信息通信产业发展过程中关注的最重要内容，因此有必要对促进信息通信产业的政策措施进行深入研究。
1963年京都大学比较文明学教授梅棹忠夫就发表了《信息产业论枠一文，在世界上首次提出了“ 信息产业 ”的概念，并精确预言工业社会发展到一定的阶段后，人们将进入以“ 信息产业为中心 ”的信息化社会。
梅棹忠夫在《信息产业论枠之后连续发表了一系列论述信息社会的文章，其对信息产业和信息化的精辟论述，引发了日本人对信息社会、信息化的关注和探讨，对当时日本政府和企业界的信息政策研究、制定产生较大的影响。
20世纪60~70年代，日本学术界对信息化和信息社会进行了大量的研究工作，其中许多研究成果受到政府和企业界的高度重视，并成为日后日本信息通信政策的主要内容。
通过多年的建设，如今日本已成为世界上最先进的信息化国家之一。
究其原因，除了其特定的内外政治、经济环境和其自身独特的文化背景之外，主要还是由于日本政府重视信息通信产业发展，信息通信政策同整个国家经济发展目标相适应、相协调的结果。
正是日本政府在财政、信贷、税收等方面制定了很多发展信息通信产业的战略和倾斜性政策，才使日本信息通信产业的发展有了雄厚的经济基础和极大的推动力。
从20世纪90年代开始，我国也深受全球信息化浪潮的影响，信息通信产业迅速成长且不断壮大，目前已经成为国民经济的重要支柱产业。
但我国还只是一个发展中国家，与发达国家相比差距依然很大，目前我国信息通信产业还存在经济效益不高、关键技术相对落后、结构性矛盾较为突出等很多问题。
长远来看，我国基础产业发展迅速、市场广大、已建成了较好的工业基础，在发展信息通信产业上具备一定的后发优势，只要有效地吸收发达国家信息通信政策制定和实施的经验和教训，就有可能实现信息通信产业的跳跃式发展。
为更好地研究制定国家信息通信政策，一方面必须研究各国信息通信政策的历史经验，另一方面必须跟踪研究国际信息通信技术的发展趋势。
作为一衣带水的邻邦，日本与我国有着悠久的文化交流历史，日本的经验和教训从国情上便于我国借鉴。
日本的信息通信产业及政策为亚洲之标杆，认真研究日本信息通信政策的目标内涵、形成过程、模式机制等可以为我国信息通信政策的制定提供参考，对我国信息通信发展战略政策的制定和实施具有重要的指导意义和现实意义，对于以信息化带动工业化进程中的我国来说无疑有着极其重要的参考价值。

（2）人为因素的威胁虽然人为因素和非人为因素都对计算机及网络系统构成威胁，但精心设计的人为攻击（因素）威胁最大。
人为因素的威胁是指人为造成的威胁，包括偶发性和故意性威胁。
具体来说主要包括网络攻击、蓄意入侵和计算机病毒等。
一般来说，人为因素威胁可以分为人为失误和恶意攻击。
①人为失误。
一是配置和使用中的失误，比如系统操作人员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不恰当，用户将自己的帐号随意转借给他人或信息共享等都会对网络安全带来威胁。
二是管理中的失误，比如用户安全意识薄弱，对网络安全不重视，安全措施不落实，导致安全事故发生。
据调查表明，在发生安全事件的原因中，居前两位的分别是“ 未修补软件安全漏洞 ”和“ 登录密码过于简单或未修改 ”，这表明了大多数用户缺乏基本的安全防范意识和防范常识。
②恶意攻击。
恶意攻击是当前计算机及网络面临的最大威胁，主要分为两大类：一是主动攻击，它使用各种攻击方式有选择地破坏信息的完整性、有效性和可用性等；二是被动攻击，它是在不影响计算机及网络系统正常工作的情况下，进行信息的窃取、截获、破译等，以获取重要的机密信息。
这两类攻击均能对计算机及网络系统造成极大的破坏，并导致机密信息泄露。
3.网络所面临的主要安全隐患隐患不等于威胁，但隐患来源于各种安全威胁。
隐患所涉及的面要比威胁本身广得多，因为同一种威胁可能在不同方面造成安全隐患。
一般来说，个人网络安全问题仅限于与因特网连接时的网络安全，因此它唯一的安全隐患就是因特网。
但对于企业网来说，其安全隐患不仅来自于因特网，内部网的安全隐患也非常值得重视，因为外网中的安全隐患同样也可以在内网中发生。
即是说企业网的安全隐患有内、外网之分。
正因为如此，企业网的安全策略设计中所考虑的不仅是病毒入侵、外网攻击那么简单了，而是要充分考虑内、外网的安全隐患，而且内、外网的安全隐患不是完全孤立的，在大多数情况下，对外网的安全问题最终来源于内网。

编辑推荐

《计算机网络安全》是由科学出版社出版的。

<<计算机网络安全>>

版权说明