黑客防线

系统防护与反入侵

王瑞洋　编著

机械工业出版社
CHINA MACHINE PRESS

黑客防线

系统防护与反入侵

王瑞洋　编著

机械工业出版社

本书由浅入深地介绍了网络安全的基础理论知识，详细阐述了计算机信息系统的安全组成和内容，路由器的安全防护，各种操作系统的安全问题和防护措施，计算机病毒的危害，安全策略制定的原则和实际策略建议，高级安全防护技术介绍和入侵检测系统以及入侵后的分析和应急反应措施等。通过阅读本书，可以了解中国计算机信息系统安全的现状、网络安全产生的隐患和风险来源，以及风险给计算机信息系统运行带来的危害和具体的安全防护措施和技术。

本书中的部分内容涉及到网络结构、网络协议等知识点，读者应具备基本的网络操作技能和对网络结构及协议的了解。

本书系统全面，阐述透彻，实用性强，对网络管理员和广大计算机爱好者是一本难得的学习和参考工具书。

图书在版编目（CIP）数据

系统防护与反入侵/王瑞洋编著．—北京：机械工业出版社，2003.8
（黑客防线）
ISBN 7-111-12573-8

Ⅰ．系… Ⅱ．王… Ⅲ．计算机网络—安全技术 Ⅳ．TP393.08

中国版本图书馆 CIP 数据核字（2003）第 056298 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
责任编辑：田 梅
责任印制：付方敏

三河市宏达印刷有限公司印刷·新华书店北京发行所发行

2003 年 8 月第 1 版·第 1 次印刷
787mm×1092mm 1/16 ·14.5 印张·359 千字
0 001—5 000 册
定价：22.00 元

出 版 说 明

近年来，计算机网络在国内得到了迅速的发展。在网络的大量应用中，安全正面临着前所未有的挑战。信息安全已经成为一个综合的工程，甚至将成为一门新兴的研究学科，需要我们在网络安全领域进行长期的研究和攻关。

网络的基础在于资源的共享，这一直是网络的基本准则。随着 Internet 的飞速发展，网络上的资源共享越来越强化。随之而来的，网络安全问题也越来越突出了。网络在带给人们诸多便利的同时，也成了许多犯罪分子攻击的目标。他们以计算机为工具，同时又以计算机为目标，在网上对计算机数据信息进行恶意的修改、删除，从而造成计算机系统难以正常运行甚至瘫痪。如果我们从另一方面去看问题，黑客也使我们发现自己网络的缺陷并改进它，从某种意义上说，日益完善的安全系统和逐渐完美的防火墙，是和黑客技术密不可分的。黑客的存在是网络发展的必然结果，尤其在我国，互联网络还处于雏形阶段，存在着不可忽视的缺陷与漏洞。如何改良网络结构，完善网络安全体系，是我们的当务之急。政府部门也对网络信息安全非常重视，并鼓励大力发展信息安全事业，以使我国在全球信息网络化的发展中占据主动地位。

目前，社会上对精通网络与信息安全知识的人才需求越来越强烈，广大技术人员和网络用户也十分希望能迅速提高自己应对安全问题的能力。由此，机械工业出版社联合北京地海森波网络技术有限公司《黑客防线》编辑部共同策划出版了“黑客防线”丛书，旨在为读者提供有关网络安全方面的知识和技术，从不同侧面阐述网络安全的相关技术。在丛书撰写过程中，切实考虑读者对知识的需求，内容做到通俗易懂，其中涉及的很多技术都是工作在网络安全第一线作者的心血结晶。对从事网络安全事业的技术人员来说，本套丛书是一个很好的帮手，从中可学到很多实用技术和宝贵经验，从而得心应手地应对各种网络安全问题。对于那些想学习网络安全知识和技术的读者而言，本套丛书也不失为好的学习工具书，通过学习不仅能迅速掌握网络安全知识，提高自身防范能力，而且为走上网络安全事业的道路奠定了基础。

我们始终坚持以普及网络安全知识，加强全民安全意识，提高我国信息技术和网络安全水平为己任，希望这套丛书的出版能满足读者的需求，并请广大读者批评指正，提出宝贵意见。

机械工业出版社

前　言

Internet 已遍及世界 240 个国家和地区，每时每刻都在为用户提供各种类型的信息服务。随着计算机科学技术的飞速发展，Interent 的服务已经日益呈现出多样化的特征。除了最初的电子邮件、WWW 外，越来越多的集视频、声音、网络于一体的服务在 Internet 上出现了，如视频会议、网络电话等。

现在的社会是信息化的社会，计算机已经被应用到政治、军事、金融、商业、交通、电信、教育等各个行业。人们在日常的生活中，对计算机的依赖程度大大提高了。尤其是近年来国家实施的信息系统工程和信息基础建设，已经使计算机信息系统成为当今社会的一个重要组成部分。越来越多的各类信息管理系统，收集和储存了大量的机密资料和信息。而这些信息的处理和交换都无一例外地要通过计算机网络来完成。毫不夸张地说，网络已经成为人们获取信息的一个重要途径，正日益改变着人的生活方式。随着网络的不断发展，网络资源的共享性、开放性、交换性日益增强，各种原来无法实现的业务都能在网络上实现了。电子货币、数字签名、电子商务、政务上网、网络银行，使得人们可以在家中完成一切交易。各类银行网络的建设，更是使资金的异地流通变得快捷方便了。但是，这一切也随之带来了巨大的安全隐患和风险。

计算机犯罪已经成为一种新的高智能犯罪，它具有高度的隐蔽性。给社会带来巨大的危害，也给侦破带来了一定的困难。同时由于计算机网络的广泛互联和无地域性特征，使得罪犯可以轻松地实现异地甚至是跨国的犯罪和资金转移。

多年来，黑客对计算机信息系统的攻击一直没有停止过，其手段也越来越高明。从最初的猜测用户口令、利用计算机软件缺陷发展到现在的通过操作系统源代码分析操作系统漏洞。同时我们还发现网络的普及使得攻击工具和代码更容易被一般用户获得，这无疑给网络安全带来了更大的风险。

本书由浅入深地阐述了网络安全的基础理论知识，网络安全的重要性和网络固有的脆弱性和风险来源。我国对计算机安全保护的政策和计算机监察制度。国内国际的安全标准体系和法律法规。安全模型 P2DR 的定义、内容和 4 个要素。计算机信息系统安全的组成部分和内容，常用网络安全防护产品的介绍，路由器的安全防护，各种操作系统的安全问题和防护措施，计算机病毒的危害，安全策略制定的原则和实际策略建议，高级安全防护技术介绍和入侵检测系统以及入侵后的分析和应急反应措施。

本书系统性强，知识结构合理。通过本书的学习，可以全面了解网络安全及其防护技术。在内容上涉及安全定义、安全等级、网络安全、访问控制、操作系统安全、计算机病毒、密码技术等。

本书按知识体系分为三个部分。

第一部分内容在第 1～4 章中讲述，概要介绍了与网络安全有关的各类基础知识理论。包括安全的重要性和安全的原由，安全标准介绍，安全法律法规以及计算机信息系统安全的基本概要。

第二部分内容在第 5～8 章讲述，详细介绍网络安全的基础知识，常用的网络防护产品，

各种操作系统的安全防护技术，路由器的安全防护技术以及计算机病毒的防范。

第三部分是提高部分，在第9～11章中讲述。该部分主要阐述了有关计算机信息系统安全的高级知识和技术，供有一定技术和经验的专业人员参考。这一部分的内容主要包括各种环境和任务目标下的安全策略的制定和原则，书中其他部分涉及到或未涉及到的高级安全防护技术，如密码学、身份验证、数据安全服务、访问控制等，还有入侵检测系统的工作原理和实际应用以及在入侵发生后的应急方案和应急恢复技术和措施。最后介绍了系统安全评估的原则和手段。

阅读本书可以了解中国计算机信息系统的安全现状、网络安全产生的隐患和风险来源，风险给计算机信息系统运行带来的危害以及具体的安全防护措施和技术。

本书的部分内容涉及网络结构、网络协议等知识点，读者应具备基本的网络操作技能和对网络结构及协议的基本了解。

本书中的实验代码、病毒分析及安全漏洞资料，仅供技术研究用，不得利用其进行违法犯罪活动，否则后果自负，与本书作者无关。特此声明！

编　者

目　录

第1章 概 览

随着信息化的发展，信息已经成为一种特殊的生产力。尤其是信息战的出现，使得信息的争夺已经变得非常激烈。通过对信息的破坏和获取，可以实现以前用军事、文化、经济等方式侵略所不能达到的目的。同时，由于网络的快速普及，处理信息的多样性也使得计算机成为人类社会中一个不可或缺的工具。其提供的多种信息服务，给人类带来了便捷的生活方式。尤其是金融业的信息化进程，使资金流动加快，清算资料的速度大大提高，异地的资金划转也变得十分快捷了。可以这么说，信息化和计算机网络把人和人、国和国的距离缩小了。

网络安全是一个涉及到计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学等多种学科的边缘学科。随着全球信息化的发展，国家之间的距离越来越小。网络在带来了众多快捷、便利的服务的同时也带来了新的危害。如何解决网络安全问题？如何制止计算机犯罪？如何建立安全的网络体系？这些问题已经成为全球关注的焦点。解决网络安全问题，已经是迫在眉睫的事情了。

1.1 什么是网络安全

网络安全就其本质来说，就是网络上的信息安全，它所涉及的领域是相当广泛的。简单地说，网络中的安全是指一种能够识别和消除不安全因素的能力。

网络安全的定义随着应用环境的改变也有不同的诠释。在用户来看，个人隐私和机密数据的传输受到机密性、完整性和安全性的保护，避免他人窃取资料是他们的安全要求。而对安全保密部门来说，过滤非法、有害或涉及国家机密的信息，成为其安全的重点。在下面的章节中，我们将对网络安全的具体表现做进一步的说明。

1.2 网络安全和黑客

黑客是具有传奇色彩的崇尚自由的一群人，然而黑客行为的代价却是高昂的。据 CERT（计算机紧急事件响应小组）的调查显示，约 20%的网站都遭受过安全侵害，每年在美国由安全导致的损失可达 100 亿美元。从过去的 12 个月来看，大部分的入侵和安全事件的威胁并非来源于外部，而是来源于网络内部的破坏。虽然网络安全已经被全球重视，各大公司、机构也都纷纷建立了自己的安全策略，设置并使用了防火墙、入侵检测系统（IDS）以及跟踪和记录网络活动的程序，但仍然不足以阻止攻击的产生。为什么会这样呢？原因在于，黑客的攻击比起前几年来，越来越复杂，技术上越来越先进；超负荷的 IT 技术人员和由于侥幸心理所导致的资金投入的缺口，使得专业安全技术人员不能获得更多的资源；最重要的一点是没有严密安全保护的系统，正在全球被大量并快速地部署和投入使用。

1.3 网络安全和威胁、风险

网络所提供的资源共享性、用户使用的方便性、分布处理提高效率的特性以及可扩充性，在一定程度上大大增加了网络受攻击的可能性。网络的威胁来自众多方面，或者说，计算机信息系统本身的脆弱性，成为了被攻击的目标。网络威胁可导致信息的保密性、完整性、可用性降低，从而造成经济损失。当前主要的网络威胁主要有如下方面：

① 自然灾害、意外事故：由于自然灾害和人为的事故造成的威胁。如天灾、硬件故障、工作人员误操作等。

② 计算机犯罪：利用暴力或非暴力，故意破坏计算机中的机密信息，以及危害计算机实体和信息安全的不法行为。如数据欺骗、特洛伊木马等。

③ 黑客行为：由于黑客的入侵或干扰，比如非法访问、拒绝服务等。

④ 内部破坏：内部人员对计算机系统的破坏或泄密。

⑤ 电子情报：通过信息窃取、流量分析、监听等手段获取信息资源。

⑥ 信息战：为了军事目的，获取或干扰他国的信息和信息系统。

⑦ 计算机病毒：制造、传播和利用计算机病毒进行破坏计算机信息系统的行为。如常见的蠕虫病毒（求职信、红色代码等）。需要特别注意的是，现在的很多病毒都已经具备部分黑客软件的特征。

1.4 安全的相对性

由于网络的连通性存在，网络不可能达到 100%的安全。在制定安全策略限制非法用户访问的同时，你也必须保证合法用户对数据的访问权。一般的原则是给用户能足以完成其合法工作的最小权限。那么如何制定安全策略呢？制定安全策略的原则是什么呢？一个关键的安全原则应该是实用有效的，同时不会给合法用户在获取合法信息时增加负担的方案。寻找一个合适安全原则的过程实际上是一个寻求动态平衡点的行为。使用过于复杂的安全技术会使得合法用户的活动大大受限，从而厌烦和规避你的安全协议。而黑客则随时准备利用这样一个看上去无害的行为，因此拥有一个过分复杂的安全策略将导致安全有效性的降低。在制定安全策略的时候，你总是要考虑安全策略给合法用户带来的影响。在多数情况下，如果用户所感受到的不方便大于所产生的安全感，则该策略实际上是降低了网络的安全有效性。

1.5 黑客的分类

黑客的分类有很多标准，我们一般以黑客的行为态度和动机来划分，主要有以下三类：

① 偶然的破坏者：顾名思义，这类人喜欢进入你的系统，但不一定有明确目标，多数情况下是个恶作剧。大部分黑客属于这一类。

② 坚定的破坏者：这类黑客的入侵都带有明确的目标，并会给系统带来巨大的甚至是毁灭性的破坏。

③ 间谍：窃取商业资料，获得信息或摧毁服务，对资源不加限制的访问。

1.6 我国计算机信息系统安全保护

在《中华人民共和国计算机信息系统安全保护条例》中，规范了计算机信息系统安全保护的概念："计算机信息系统的安全保护，应当保障计算机及其相关的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。"

1．计算机信息系统安全保护的基本概念

计算机信息系统安全保护主要包括两个方面，一是国家实施的安全监督管理，二是计算机信息系统使用单位自身的保护措施。实施计算机信息系统保护的措施主要有安全法规、安全技术和安全管理三个方面的内容。

（1）安全法规

计算机信息系统安全保护的安全法规，有着多层次的具体内容。并且形成了从宏观的法律规范直到技术规范标准和管理制度的一整套制度化法规体系，是一个包括技术行为在内的计算机信息系统安全保护的行为规范层次。其中，有国家依据强制性规范的社会行为关系，建立的国家法律。有各级主管部门，围绕国家法律法规，根据实际情况制定的相应行政法规；有地方制定的实施细则；也有计算机信息系统使用单位以上述法律法规标准为依据，结合本单位的安全保护实际情况和需要，制定出的各种规章制度。这些法律法规形成了一个规范、标准的规章体系。在实际的计算机信息系统安全保护中，安全法规和安全技术、安全管理分属于不同的专业范畴；它们的目标是一致的，协同实现计算机信息系统的实体安全、运行安全、信息安全和人员安全。

（2）安全管理

在群体活动中，为了有效地完成一定的任务，达到既定的目标，针对特定的对象，遵循确定的原则，按照规定的程序，运用恰当的方法，所进行的计划、组织、指挥、协调和控制等活动，我们称之为管理。

在计算机信息系统安全方面，安全管理的目标是管理计算机系统资源和信息资源的安全。安全管理主要包括以下 5 个方面：实体安全管理、行政安全管理、信息流程安全管理、技术安全管理、安全稽核。

计算机信息系统安全管理有以下特点：

1）综合性

计算机信息系统本身具有综合性的特点，它决定了计算机信息系统安全管理是长期和复杂的工作，必须采取综合治理的方式。第一，安全治理的各个方面，是技术的、管理的和法制的。第二，安全管理是分工的组织形式。第三，安全管理是方式方法，主要有培训教育、规章制度、法纪法规。第四，安全所涉及的专业具有广泛性。第五，相关人员的专业类型和层次。以上内容都说明了安全管理的综合性特点。

2）系统性

使用计算机信息系统的单位，其内部组织结构都是有一定的系统性的，而计算机信息系统是单位的中枢系统，它具有其使用单位的性质，这决定了计算机信息系统的构架和运作也必定具有完全相同的系统效应。而信息本身的交互性和分布性特征，以及信息系统和信息网

络的构架，无论在形式还是内容、应用上，也是一个有序的整体。只有使用系统性的管理，才能有效地解决问题。

3）高科技性

信息时代的显著特征就是高科技。而计算机信息系统，正是信息时代高科技的结晶。与此相关的管理，无论从思想还是内容、方式方法上，都必须应具有同样的高科技性。否则是很难有效管理好计算机信息系统安全的。

4）发展性

计算机信息系统及其相应的技术，无时无刻不是在高速发展中的。这使得计算机信息系统的安全管理也必须保持主动进取、提高效率、创新发展的工作姿态。

5）实践性

计算机信息系统之所以可以高速发展，一个根本或者说关键的原因就是实践——计算机信息系统中的强大功能被广泛、大量被实践。在广泛的实践中，信息管理系统不断地被完善。然而，信息系统的安全防护措施却明显地滞后于应用，没有能和应用同步地发展。在计算机安全管理学科中，管理方法和思想的形成和发展，总是和安全隐患经历着复杂的对抗。在不断的攻防实践中，安全管理才能有所发展。

安全管理的核心是管理好业务人员的思想素质、职业道德教育和业务素质。计算机总是由人来操作和使用的，人员的素质是否合格是计算机安全管理的关键所在。试想，有了非常完美的管理措施，却没有合格的人员去执行和贯彻，这些管理措施就不能有效的实施。普及安全教育，提高安全意识，是改善计算机信息系统安全管理的关键。

（3）安全技术

计算机信息系统安全的对象，不仅是计算机信息系统本身，还有计算机及所处的环境，还有一个最重要的是人。由此可见，计算机安全技术是多个专题的有机结合，涉及的学科有电子工程、软件工程、保密学、管理学、心理学、法律等。安全技术还包括安全产品，网络安全产品在一定程度上提高了网络安全的刚性，避免了人治的弹性效果。从实践来看，安全技术的硬性制约和纪律法规的软性约束，在安全管理中都是不可缺少的，只有发挥相通互补性，才能使安全管理切实有效。

实体安全、信息安全、运行安全、人员安全，是计算机信息系统安全保护的主要目标。每一项目标的实现，都需要安全法规、安全技术和安全管理的综合性措施。或偏重一方，或多方并重。

2. 计算机信息系统安全保护的基本目标和任务

无论是计算机信息系统安全保护的政策法规，还是安全保护的技术产品，或者是安全保护的管理制度，其基本目标和任务都是一致的，所不同的是涉及的专业领域和具体内容。

（1）计算机信息系统安全保护的基本目标

国家的信息安全的目标是，保证国民经济基础设施的信息安全；抵御敌对势力的信息战威胁，保障国家的安全和社会的安定；对抗国内外的信息技术犯罪，保证国民经济协调、高速、持续、健康的发展。

各计算机信息系统的使用单位，应结合本单位情况，明确各自的具体信息安全的目标。基本内容应是，努力保证在有充分保护的安全环境中，由可靠的人员，按正确的规范，使用符合安全标准的计算机及其信息系统。确保信息系统的实体安全、运行安全和信息安全。

（2）计算机信息系统安全保护的基本任务

努力提高和强化社会的信息安全意识，确立信息安全管理的基本思想与政策，加速制定和完善法律体系，这是实现信息安全目标的基本前提。

建立、健全统一指挥、统一步调的强有力的各级信息安全管理机制，这是实现信息安全目标的基本组织保障。

积极创造条件，加快信息安全人才的大力培养，形成水平高、门类全、训练有素的信息安全人才队伍。这是搞好信息安全治理的关键因素。

认真借鉴国际先进经验，自主地进行信息安全关键技术和设备的研究、开发，有效地完成技术成果的转化，大力发展独立的民族信息安全产业，形成规模，在相应的范围内积极推广和应用。这是实现信息安全的强有力的手段。

积极推进信息安全技术和经验教训的国际交流；平等互利，求同存异，互通信息，结成最广泛的和平利用国际信息基础设施的统一战线，形成和平与发展的信息安全的国际氛围。

（3）计算机信息系统安全保护的基本策略

一切影响计算机信息系统安全的因素，以及保障计算机及其运行的安全措施，都属于计算机安全保护所涉及的内容。

任何危害，都有一个过程。在这个过程的任何环节，我们都可以采取相应的有力措施，予以制约或制止，避免或减轻所遭到的危害。也就是说，在计算机安全保护的各个层次上，都可以制止或制约危害的产生，以确保计算机信息系统的安全运行。

很显然，不管是安全法规的，还是安全技术的，要想其发挥有效的功能，都要依附于有效的社会公共安全管理和使用单位的内部管理制度。而针对不同的计算机信息系统，既要看到其作为信息系统的共性，又要根据不同的具体系统所面临的威胁，以及实际的安全需要来采取适度的安全措施。

1.7 我国计算机信息系统安全保护的基本政策

计算机信息系统的安全保护是国家信息化建设的重要组成部分。具有战略性、长期性、整体性的特点，且涉及国民经济和社会发展的各个领域。是一个宏大的社会系统工程，要从全局出发，发挥综合优势，把各地区、各部门的计算机信息系统安全保护工作当作一个有机的整体来安排。统一思想，统一认识，统一行动，使计算机信息系统安全保护沿着正确的方向健康发展。

计算机信息系统安全保护政策，是指一个国家或地区，在正确分析计算机信息系统的基本特点和造成计算机信息系统不安全因素的基础上，为了有效地实施计算机信息系统的安全保护，从维护国家主权、社会安定、经济发展的高度着眼，科学地、实事求是地从宏观到具体的业务范畴，为规范和制约有关计算机信息系统的信息活动的安全保护，所制定的一系列方针、原则、措施和方法。

1．我国信息化建设的总指导方针

（1）信息化建设的总指导方针

1997 年 4 月，在全国信息化工作会议上，确定了今后一段时期全国信息化工作的总体要求：坚持以邓小平建设有中国特色社会主义理论为指导，全面贯彻邓小平和江泽民同志关

于信息化的重要指示，认真贯彻信息化建设的“统筹规划，国家主导，统一标准，联合建设，互联互通，资源共享”的二十四字指导方针，进一步加快国家信息基础设施和信息产业的发展，积极推进“两个根本性转变”，提高对外合作水平，为促进国民经济持续、快速、健康发展和社会全面进步发挥更大的作用。

（2）信息系统安全保护的基本国策

围绕我国信息化建设的总任务的最终实现，遵循信息化建设的总指导方针，实施我国计算机信息系统安全保护的基本国策应当是，为建设有中国特色的社会主义，立足国情，坚持改革开放，搞好安全教育，强化安全意识，坚持兴利除弊，认真把握发展需要安全，安全促进发展的辨证关系。在促进发展的同时，在管理、立法、技术、产品各个方面采取配套的，切实有效的措施，做好信息化体系的安全工作。

2. 计算机信息系统安全保护的一般原则

根据我国信息化建设的总指导方针，我国计算机信息系统安全保护的方针是：统一领导，分工负责；合理应用与安全管理相结合；积极预防与应急处理相结合；把安全工作做在事件发生之前。这里包括三层含义：首先，计算机安全是个社会问题，涉及国家政治、军事、科学文化、社会活动等一系列的全局性利益，又是一个包括多学科的系统安全工程。安全必须是整体的安全，中间缺少任何一个环节都会影响安全，因此，需要综合的考虑问题，统一指挥和组织，不能大家都来做，结果是浪费了大量的人力和物力，而效果却不好。要注意在统一的领导下，各司其职，这样才能有效的实施安全保护。其次，既要发展应用，又要保证安全。一手抓应用，一手抓安全，二者不可偏废。第三，以预防事件发生为主，因为计算机安全事件一旦发生，其经济损失和社会影响都比较大，所以必须以预防为主，主动采取安全措施，对已经发生的事件要有应急的处理方法。

我国计算机信息系统安全保护的基本原则：

1）等价原则

用于保护的总开销，与计算机信息系统本身的价值相当。需要注意的是，这里的总价值不单指有价的费用，更包括不可用金钱衡量的重要性。这种重要性体现在由该计算机构成的计算机信息系统的安全等级。计算机及其构成计算机信息系统的安全等级，是评估其实际价值的一个关键权值，它反映了该信息系统中信息和用途的重要程度。

2）系统应用开发、安全设计同步原则

安全为了应用，应用必须安全，这对于关系国家安全、社会安定的计算机信息系统的重点用户来说，是非常关键的。应引起足够的关注。系统应用开发和安全设计的同步原则，正是强调了应用与安全的辨证统一思想。

3）综合治理原则

计算机信息系统在各个领域的广泛应用，使得计算机信息系统的安全保护成为涉及全社会的公共安全治理的系统工程，唯有领导重视，最大限度地动员和组织各种类型、各个层次的人员，在各个不同的领域，采取综合防治措施，才能收到良好的效果。

4）突出重点的原则

突出重点的本质，就是突出计算机信息系统安全保护的分工，使各自的目标和责任清楚，各司其职。《中华人民共和国计算机信息系统安全保护条例》明确规定：“计算机信息系统的安全保护工作，重点维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算