单元　8　计算机信息系统安全基础

以云计算、大数据、物联网、人工智能为代表的新兴技术的快速发展，计算机安全风险全面泛化，复杂程度也在不断加深。在加速企业数字化转型进程的同时，计算机安全风险开始出现在越来越多的场景之中。网络安全问题日趋严峻，各地发生多起重大网络安全事件，既有公民信息遭泄露，也有多起因为遭遇勒索软件攻击而被迫停工、停产的事件。计算机安全中非常重要的是存储数据的安全，其面临的主要威胁包括计算机病毒、非法访问、计算机电磁辐射、硬件损坏等。

针对表8-1中所列出的各项安全措施，你在日常生活、学习、工作中哪些已完全做到了，养成了良好习惯，请在“日常行为”列画“√”。对于暂时还没有做到的，今后应努力做到。

目录

表8-1　保证智能手机和网络通信安全的措施

场景类型	安全措施	日常行为
安全使用智能手机	① 手机设置自动锁屏功能，避免手机被其他人恶意使用	
	② 手机系统升级通过自带的版本检查功能联网更新，不通过第三方网站下载系统更新包进行更新	
	③ 尽可能通过手机自带的应用市场下载手机应用程序	
	④ 为手机安装杀毒软件	
	⑤ 经常为手机做数据同步备份	
	⑥ 手机中访问Web站点应提高警惕	
安全使用电子邮件	① 为电子邮箱设置高强度密码，并设置每次登录时必须进行用户名和密码验证	
	② 开启防病毒软件实时监控，检测收发的电子邮件是否带有病毒	
	③ 定期检查邮件自动转发功能是否关闭	
	④ 不转发来历不明的电子邮件及附件	
	⑤ 收到涉及敏感信息的邮件时，对邮件内容和发件人信息进行反复确认，尽量进行线下沟通	
	⑥ 不要随意单击不明邮件中的链接、图片、文件	
	⑦ 使用电子邮件地址作为网站注册的用户名时，应设置与原邮件密码不相同的网站密码	
	⑧ 适当设置找回密码的提示问题	
	⑨ 当收到与个人信息和金钱相关（如中奖、集资等）的邮件时要提高警惕	
安全使用QQ、微博等账号	**① 账号和密码尽量不要相同，定期修改密码，增加密码的复杂度，不要直接用生日、电话号码、证件号码等有关个人信息的数字作为密码**	
	② 密码尽量由大小写字母、数字和其他字符混合组成，适当增加密码的长度并经常更换	
	③ 不同用途的网络应用，应该设置不同的用户名和密码	
	④ 在网吧使用计算机前重启机器，警惕输入账号密码时被人偷看	
	⑤ 为防止账号被监听，可先输入部分账号、部分密码，然后输入剩下的账号、密码	
	⑥ 涉及网络交易时，要注意通过电话与交易本人确认	

8.1　计算机安全基础

随着计算机信息系统功能的日益完善和速度的不断提高，系统组成越来越复杂，系统规模越来越大，特别是互联网的迅速发展，存取控制、逻辑连接数量不断增加，软件规模空前膨胀，各种隐含的缺陷、失误都能造成巨大损失。必须不断提高计算机安全意识和安全保障能力。

8.1.1　基本概念界定

《中华人民共和国计算机信息系统安全保护条例》的第二条规定：本条例所称的计算机信息系统，是指由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统；第三条规定：计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、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。该条例所涉及的计算机信息系统适用于本单元。

1．计算机信息系统安全的基本范畴

本单元涉及的计算机信息系统安全、计算机安全、计算机网络安全和计算机信息安全的基本概念及基本范畴说明如下。

计算机信息系统安全工作的目的就是在法律、法规、政策的支持与指导下，通过采用合适的安全技术与安全管理措施，维护计算机信息系统安全。计算机信息系统安全主要涉及**计算机单机安全、计算机信息安全和计算机网络安全**3个方面。

① 计算机单机安全（以下简称为计算机安全）是计算机信息系统安全的重要环节，主要是指管理和保护计算机信息系统的硬件部分，包括计算机本身的硬件和各种接口、各种相应的外部设备、计算机网络通信设备、线路和信道等，以保证在计算机单机环境下，硬件系统和软件系统不受意外或恶意的破坏和损坏，得到物理上的保护。

② 计算机信息安全（以下简称为信息安全）是指信息在传输、处理和存储的过程中，没有被非法或恶意地窃取、篡改和破坏。

③ 计算机网络安全（以下简称为网络安全）是指在计算机网络系统环境下的安全，主要涵盖两个方面，一是信息系统自身即内部网络的安全，二是信息系统与外部网络连接情况下的安全。网络安全的概念比较宽泛，是指网络系统的硬件、软件及系统中的数据受到保护，不因偶然或恶意的原因遭受到破坏、更改或泄露，系统连续、可靠、正常地运行，保障网络服务不中断。网络安全是我国国家安全的一项基本内容。

2．计算机安全概念

ISO将计算机安全定义为“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、更改和泄露”。此概念偏重静态信息保护，因此通常将其视为“信息保护”的概念范畴。也有人将计算机安全定义为“计算机的硬件、软件和数据受到保护，不因偶然和恶意的原因而遭到破坏、更改和泄露，系统连续、正常运行”。该定义着重于动态信息描述，而且提出了用户访问系统时系统的可用性要求，因此也将其视为“信息保障”的概念范畴。

由于网络技术的发展和进步，当今世界上很少有人使用未接入网络、不与其他计算机相连接的计算机了。如何对连接在同一网络中的多台计算机以及它们之间的连接设备进行保护，属于“网络安全”的定义范围。

3．信息安全的概念

从历史角度来看，信息安全早于网络安全。随着信息化的深入，信息安全和网络安全的内涵不断丰富，对网络的发展提出了新的信息安全目标和要求，网络安全技术在此过程中也得到不断创新和发展。

随着个人计算机和互联网的普及，越来越多的公司依赖于使用互联网经营其业务，行政机构和政府借助计算机存储重要的信息和数据，个人利用计算机与各式各样的终端设备享受互联网带来的快捷和便利。但是，大量敏感的信息（大到维系公共安全的重要行政信息和军事信息，小到个人隐私）不可避免地在互联网上传递和存储；大量的资金通过网络进行流通，通过网上银行进行支付。对怀有恶意的计算机攻击者来说，这些都是他们垂涎的目标。如果对其没有进行适当的保护以满足其安全性的要求，那么个人、公司或各种组织将会面临巨大的经济风险和信任风险。

从技术角度看，信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的边缘性综合学科。

狭义上讲，信息安全就是网络系统上的信息安全，是指网络系统的硬件、软件和系统中的数据受到保护，不因偶然的或者恶意的攻击而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。

广义上讲，信息安全是指信息在生产、传输、处理和存储过程中不被泄露或破坏，防止信息资源被故意地或偶然地非授权泄露、更改、破坏或使信息被非法阅读；确保信息的完整性、保密性、真实性、可用性和不可否认性，并保证信息系统的可靠性和可控性；避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。

4．网络安全的概念

网络安全（Network Security）不仅包括网络信息的存储安全，还涉及信息的产生、传输和使用过程中的安全。网络安全的目的是确保经过网络厂商和交换的数据不会发生增加、修改、丢失和泄露等。

网络安全从其本质上来讲就是网络上的信息安全。广义上讲，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。所以广义的网络安全还包括信息设备的物理安全，如场地环境保护、防火措施、静电防护、防水/防潮措施、电源保护、空调设备、计算机辐射等。

网络安全与信息安全有很多相似之处，两者都对信息（数据）的生产、传输、存储和使用等过程有相同的基本要求，如可用性、保密性、完整性和不可否认性等。但两者又有区别，不论是狭义的网络安全，还是广义的网络安全，都是信息安全的子集。

5．计算机安全、网络安全和信息安全三者的关系

信息安全是计算机信息系统安全的核心问题，计算机安全和网络安全的实现都是为了确保数据在传输、处理和存储全过程的安全、可靠。

计算机安全和网络安全是确保信息安全的重要条件和保证，信息安全贯穿于计算机安全和网络安全的所有环节。计算机安全、网络安全和信息安全三者之间是紧密联系、不能割裂的。只有计算机安全、网络安全和信息安全都得到切实的保障，才能保证计算机信息系统功能的发挥和目标的实现，真正起到为管理决策者提供信息和支持的作用。

可能从广义上来说它们都可以用来表示安全这样一个笼统的概念。但如果从狭义上理解，它们应该是有区别的，区别在哪呢？

计算机安全主要指单机（非网络环境下）的安全，网络安全主要考虑在网络环境下的安全问题，信息安全一般专指密码学，主要考虑信息的完整性、机密性、真实性等。

6．信息安全与网络安全的联系与区别

信息安全、网络安全一直存在争议，它们通常被认为是一回事，导致它们在安全领域容易被混淆。不过每天都有如此多的术语涌现和新技术出现，信息安全和网络安全的争论也就不足为奇了。

有人说，网络安全是信息安全的一部分，因为信息安全不仅包括网络安全，还包括电话、电报、传真、卫星、纸质媒体的传播等其他通信手段的安全。也有人说，从纯技术的角度看，信息安全专业的主要研究内容为密码学，如各种加密算法、公共基础设施、数字签名、数字证书等，而这些只是保障网络安全的手段之一。这些说法是否准确，可以从以下几个方面来分析。

（1）信息安全与网络安全的关系

广义上，信息安全是一个包括信息本身安全（信息内容安全）、信息载体安全（包括网络安全）、信息程序安全，以及影响和危害信息安全的因素和信息安全保障、维护等在内的内容广泛的安全问题，信息安全包括网络安全、操作系统安全、数据库安全、硬件设备和设施安全、物理安全、人员安全、软件开发、应用安全等。

网络安全只是一种信息载体安全，是信息安全的一种，也是信息安全的一个方面。当然，在信息存储和流动越来越依赖网络的今天，网络安全不仅是信息安全的一个方面，而且是信息安全的一个非常重要的方面，同时也是信息本身安全的重要保障和条件。

（2）信息安全与网络安全的概念区分

广义的信息安全是指信息在生产、传输、处理和存储过程中不被泄露或破坏。可以这样说，信息不一定存在于网络空间中，因此一切都有可能造成信息被泄露、被篡改等，除了常见的网络入侵窃密，还包括网络之外的场景，如利用人性的弱点、间谍等造成的信息安全事件。

网络安全是指利用网络管理控制和技术措施，保证在一个网络环境里，数据的保密性、完整性及可用性等受到保护。

（3）信息安全与网络安全的性质区分

信息安全关注数据相关的安全，监督未经授权的访问、修改、删除，保护数据免受任何威胁；网络安全深入了解恶意软件，预防数据丢失，做好恢复计划，侧重于计算机数据和信息的安全。

网络安全关注网络环境下的计算机安全，更注重在网络层面，例如，通过部署防火墙、入侵检测等硬件设备来实现链路层面的安全防护。而信息安全的覆盖面要比网络安全的覆盖面大得多，信息安全从数据的角度来看安全防护，通常采用的手段包括部署防火墙、入侵检测、审计、渗透测试、风险评估等，安全防护不仅是在网络层面，而且更加关注的是应用层面，可以说信息安全更贴近于用户的实际需求及想法。

网络安全主要涉及网络安全域、防火墙、网络访问控制、抗分布式拒绝服务（Distributed Denial of Service，DDoS）等场景，更多指向整个网络空间的环境。网络信息和数据都可以存在于网络空间之内，也可以在网络空间之外。“数据”可以看作“信息”的主要载体，信息则是对数据进行有意义分析后得到的价值资产，常见的信息安全事件有网络入侵窃密、信息泄露和信息被篡改等。

8.1.2　计算机信息系统安全涉及的内容

计算机信息系统安全包括**实体安全（硬件安全）、软件安全、数据安全、运行安全和管理安全**等几个部分。

1．实体安全

在计算机信息系统中，计算机及其相关的设备、设施（含网络）统称为计算机信息系统的“实体”。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、火灾、水灾、雷电、噪声、外界电磁干扰、电磁信息泄露、有害气体和其他环境事故（如电磁污染等）破坏的措施。实体安全保证计算机信息系统硬件安全、可靠地运行，确保它们在对信息进行采集、处理、传送和存储的过程中，不会受到人为或者其他因素造成的危害。特别是避免由于电磁泄漏产生信息泄露，从而干扰他人或受他人干扰。实体安全包括环境安全、设备安全和媒体安全3个方面。

计算机信息系统的实体安全是整个计算机信息系统安全的前提，因此，保证实体安全是十分重要的。对计算机信息系统实体的威胁和攻击，不仅会造成国家财产的重大损失，而且会使信息系统的机密信息被严重泄露和破坏。因此，对计算机信息系统实体的保护是防止对信息进行威胁和攻击的首要一步，也是防止遭受威胁和攻击的屏障。

实体安全是组织能够较好实现计算机信息系统整体安全的基础，但是较高的实体安全基础不能取代运行安全和管理安全。例如，一台昂贵的、具有良好安全性的服务器并不能防止因组织人员缺少责任心而导致的盗窃。

2．软件安全

软件安全首先是指使用的软件（包括操作系统和应用软件）本身是正确、可靠的，即不但要确保它们在正常的情况下运行结果是正确的，而且也不会因某些偶然的失误或特殊的条件而得到错误的结果。软件安全还指对软件的保护，即软件应当具有防御非法使用、非法修改和非法复制的能力，例如，操作系统本身的用户账号、口令、文件、目录存取权限的安全措施。

3．数据安全

数据安全是指防止数据资产被故意地或偶然地非法授权泄露、更改、破坏或信息被非法辨识、控制，确保数据的完整性、保密性、可靠性、可用性、可控性等，防止信息被非法修改、删除、使用和窃取，保证信息使用完整、有效、合法。

4．运行安全

运行安全是计算机信息系统安全的重要环节，因为只有计算机信息系统运行过程中的安全得到保证，才能完成对信息和数据的正确处理，达到发挥系统各项功能的目的。

运行安全指对运行中的计算机信息系统的实体和数据进行保护，其目标是保证系统能连续、正常地运行，保护范围包括计算机的软件系统和硬件系统。为保障系统功能的安全实现，运行安全提供一套安全措施（如风险分析、审计跟踪、备份与恢复、应急等）来保护信息处理过程的安全。它侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失。

运行安全与实体安全和管理安全密不可分。运行安全可以弥补实体安全的不足引起的缺陷。例如，一台不具有安全密码控制的主机，可以借助制订并实施密码轮换计划来提升其安全性，也可以根据已制定的管理条例向相关机构申请更换或附加安全密码控制功能。不过，运行安全的保障严重依赖于良好的管理安全。例如，若已经制订和实施了密码轮换计划（30天更新一次密码，密码必须是不低于8位的混合大写字母、小写字母和数字的字符串），但是相关操作人员未在规定更改期间按照要求进行密码修改操作，则这种密码轮换计划并不能提升安全性。

5．管理安全

管理安全和安全政策为整个组织的安全提供了最高级别的指导、规则和程序实施的安全环境。信息安全方面的专业人员可以向管理层提供有效的政策或相关建议，并需要得到管理层充分的支持。一个得不到管理层支持的安全人员不可能有效地实施任何安全措施。安全政策应用于整个组织而非组织内某一个或特定的层级。组织管理层应将管理安全定位在组织文化或组织人力资源战略相同的重要地位。

管理安全是组织安全中最高级也是最重要的一环。现实情况是大多数公司成员能够说出他们有多少假期或收入情况，但是不能说出公司哪些信息能够公开，哪些必须保证不被泄露。管理安全需要持续不断、自上而下地加强，包括所有组织成员的教育和培训。

所有计算机管理和操作人员必须经过专业技术培训，熟练掌握计算机安全操作技能，熟知计算机安全相关的法律知识，不断增强计算机使用人员的安全意识、法律意识、安全技能，以确保计算机信息系统的正常运行，增强信息系统的技术防范能力，保障信息系统安全。

8.1.3　计算机信息系统安全面临的主要潜在威胁

随着科学技术的迅猛发展，威胁计算机信息系统安全的因素层出不穷。目前发现的主要风险如下。

（1）数据传输中的链路风险

数据在传输过程中很难保证不被非法窃取、篡改。入侵者在传输线路上安装窃听装置，监视网络数据流动，截取敏感信息造成泄密，或者通过篡改破坏数据的完整性。

（2）网络体系的安全风险

入侵者通过探测、扫描网络及操作系统存在的安全漏洞，利用相应攻击手段对网络发起攻击。

（3）系统的安全风险

当前操作系统与应用系统都存在许多安全漏洞，有巨大的安全隐患。

（4）应用的安全风险

网络系统的目的是实现资源的共享，在进行资源共享时可能会造成重要信息的泄露。

（5）管理的安全风险

系统管理是计算机信息系统中信息安全的重要组成部分，是防止网络攻击的重要部分。缺乏有效的管理措施如身份认证、权限认证等，势必引发安全风险。

对计算机信息系统安全的威胁大致可以分为以下类型。

1．自然灾害

计算机信息系统仅仅是一个智能的机器，易受火灾、水灾、风暴、地震等自然灾害的破坏以及环境（温度、湿度、振动、冲击、污染等）的影响。

2．恶意软件

恶意软件（Malware）由“恶意”（Malicious）和“软件”（Software）这两个词合并而来，是一个通用术语，是一种对计算机有害的程序或文件。常见的恶意软件类型有计算机病毒（Computer Virus）、计算机蠕虫（Computer Worms）、广告软件（Adware）、特洛伊木马（Trojan Horse）、间谍软件（Spyware）、勒索软件（Ransomware）等。恶意软件的目标是破坏设备的正常运行。这种破坏的范围很广，如未经许可在设备上显示广告，或者获得计算机root访问权限。恶意软件可能试图向用户进行自我掩饰，从而暗自收集用户敏感信息，或删除、修改文件，或者可能锁定系统和截留数据以进行勒索。在DDoS攻击中，Mirai等恶意软件会感染易受攻击的设备，在攻击者的控制下将其转变为机器人。遭到篡改后，这些设备便可作为“僵尸网络”的一部分用于进行DDoS攻击。

恶意软件在于它是故意为恶的，任何无意间造成损害的软件均不被视为恶意软件。

（1）计算机病毒

（2）计算机蠕虫

（3）广告软件

（4）特洛伊木马

（5）间谍软件

（6）勒索软件

3．系统漏洞

系统漏洞是指应用软件或操作系统在逻辑设计上的缺陷或错误。不同的软件、硬件设备和不同版本的系统都存在系统漏洞，容易被不法分子通过病毒进行控制，从而窃取用户的重要资料。不管是计算机操作系统、手机系统，还是应用软件，都容易因为漏洞问题遭受攻击，因此，建议用户使用最新版本的应用程序，并及时更新应用商提供的漏洞补丁。

4．非法侵入计算机信息系统

所谓“侵入”，是指非法用户利用技术手段或者其他手段突破或者绕过计算机信息系统的安全保卫机制“访问”计算机信息系统的行为。也就是指未经允许，采取各种手段，突破、穿越、绕过或解除特定计算机信息系统的安全防护体系，擅自进入该系统窥视、偷览信息资源的行为。这里，从用户的身份特征和访问权限来看，非法侵入行为可以分为两类：一是非法用户侵入计算机信息系统，即无权访问特定信息系统者非法侵入该信息系统；二是合法用户的越权访问，即行为人对特定信息系统有一定的访问权限和合法账号，但未经授权对无权访问的系统资源进行访问的行为。

非法侵入的行为方式多种多样，如非法用户、冒充合法用户，利用计算机技术进行技术攻击，通过“后门”“陷阱门”进行非法入侵，利用安全漏洞等。

非法侵入计算机信息系统罪是针对入侵者违反国家关于计算机信息系统管理的各项法律、法规，不具有合法身份或者条件而未经授权地擅自侵入计算机信息系统的行为的罪名。目前我国关于计算机信息系统管理方面的法律、法规主要有《中华人民共和国计算机信息系统安全保护条例》《中华人民共和国计算机信息网络国际联网管理暂行规定》《中国公用计算机互联网国际联网管理办法》《计算机信息网络国际联网安全保护管理办法》等，违反上述条例、规定、办法均可视为违反国家规定。

如果行为人访问计算机信息系统没有违反国家有关规定，即访问是合法的，不构成本罪。

5．网络攻击

网络攻击（Cyber Attack）是指利用计算机信息系统存在的漏洞和安全缺陷，针对计算机信息系统、基础设施、计算机网络的任何类型的进攻动作。对计算机和计算机网络来说，破坏、揭露、修改、使软件或服务失去功能、在没有得到授权的情况下窃取或访问任何一台计算机的数据，都被视为对计算机和计算机网络的攻击。

网络的复杂性会导致出现很多难以想象的漏洞，其复杂性表现在主机系统配置、信任网络关系、网络进出难以控制等。由于TCP/IP是公开发布的，数据包在网络上通常采用明码传送，容易被窃听和欺骗；网络协议本身存在的安全缺陷；网络结构存在的安全缺陷，如以太网的窃听；攻破广域网上的路由器来窃听；网络服务的漏洞，如Web服务、电子邮件服务等的漏洞。网络攻击者正是利用这些不安全因素来攻击网络的。

网络攻击的出现，并非黑客制造了入侵的机会，而是他们善于发现漏洞。即信息网络本身的不完善性和缺陷，成为被攻击的目标或被用作攻击的途径，并构成自然或人为的破坏。就目前网络技术的发展趋势来看，网络攻击的方式越来越多样化，对没有网络安全防护设备（防火墙）的网站和系统具有强大的破坏力，这给信息安全防护带来了严峻的挑战。

6．网络犯罪

网络犯罪多表现为诈取钱财和信息破坏，犯罪内容主要包括金融欺诈、网络赌博、网络贩黄、非法资本操作和电子商务领域的侵权欺诈等。随着信息社会的发展，目前的网络犯罪主体更多地由松散的个人转化为信息化、网络化的高智商集团和组织，其跨国性也不断增强。日趋猖獗的网络犯罪已对国家的信息安全以及基于信息安全的经济安全、文化安全、政治安全等构成了严重威胁。

8.1.4　影响计算机信息安全的主要因素

影响计算机信息安全的主要因素如下。

1．个人操作因素

计算机的使用由人完成，因此在使用的过程中信息安全受到多种人为因素的影响，在实际生活中影响信息数据安全的人为因素具有多种形式，常见的就是黑客、计算机病毒入侵等。黑客通过一定手段进入个人或者企业计算机的内部，进而窃取个人或者企业的信息数据，对个人或者企业往往造成较大影响。由于对黑客的入侵难以准确掌握其规律，因此在实际应用中对这种因素的防范具有一定的困难。

2．非人为因素

计算机本身在使用过程中会出现各种故障或者受到一定的感染，常见的就是计算机硬件损坏、操作系统失效或者相关器材的更换等，这也会造成计算机信息的外泄。例如，在维修计算机的过程中维修人员可以检查计算机硬盘内的信息资料；当计算机的正常运转受到影响如电磁波干扰时，会导致计算机运行不利，也会造成信息的泄露。

8.1.5　计算机网络攻击的常用手段及方式

网络攻击是某种安全威胁的具体实现，当信息从信源向信宿流动时，可能受到各种类型的攻击。网络攻击可以分为主动攻击、被动攻击、物理临近攻击、内部人员攻击、分发攻击等几类。

1．主动攻击

（1）篡改消息

（2）伪造消息

（3）拒绝服务

2．被动攻击

（1）窃听

（2）流量分析

3．物理临近攻击

未授权者可在物理上接近网络、系统或设备，其目的是修改、收集或拒绝访问信息。

4．内部人员攻击

5．分发攻击

8.1.6　常用的安全防御技术

信息技术的不断普及和应用，虽然为人们的生活带来了便利，但网络环境中信息资源的开放性和共享性等特点，也为信息的管理带来了一些安全性问题，从而使信息安全面临着巨大的威胁，因此有必要采取一定的信息安全防御技术来维护信息安全。

安全防御技术主要用于防止系统漏洞、防止外部黑客入侵、防御病毒破坏和对可疑访问进行有效控制等，同时还应该包含数据灾难与数据恢复技术，即在计算机发生意外或灾难时，可以使用备份还原及数据恢复技术将丢失的数据找回。

学习一些常用的信息系统安全防御技术，有助于我们更好地保护信息安全。典型的安全防御技术有以下几大类。

1．数据加解密技术

（1）对称加解密技术

（2）非对称加解密技术

2．认证技术

（1）身份认证技术

（2）数字摘要

（3）数字信封

（4）数字签名

（5）数字时间戳

3．防火墙技术

4．入侵检测技术

5．访问控制技术

6．系统容灾技术

（1）数据容灾

（2）应用容灾

7．防治病毒技术

8．VPN技术

9．安全审计技术

8.2　计算机病毒及其防治

随着计算机在社会生活各个领域的广泛运用，计算机病毒攻击与防范技术也在不断发展。据报道，世界各国遭受计算机病毒感染和攻击的事件数以亿计，严重干扰了正常的人类社会生活，给计算机系统和网络带来了巨大的潜在威胁和破坏。可以预见，随着计算机、网络运用的不断普及、深入，防范计算机病毒将越来越受到各国的高度重视。

8.2.1　计算机病毒的概念

计算机病毒因带神秘感且类似生物病毒而受关注，普通人为计算机也会“染毒”“接种疫苗”感到好奇与恐惧。按我国相关条例，计算机病毒是插入程序中破坏计算机功能、毁坏数据、影响使用且能自我复制的指令或代码。它如生物病毒般有自我繁殖等特征，复制能力独特，蔓延迅速且难根除，会干扰破坏计算机正常运行，致其无法使用甚至损坏系统或硬盘。病毒程序不独立，附于文件上随文件传播，影响运行速度或致系统瘫痪，给用户带来巨大损失。互联网普及为计算机病毒传播开辟新径，使其更易成灾，传播更快，反病毒任务更难。互联网带来文件下载和电子邮件两种安全威胁，被浏览或下载文件可能带毒，带毒文档或文件可通过网关和邮件服务器涌入局域网，网络便捷与开放使威胁加剧。

8.2.2　计算机病毒的特征

计算机病毒一般具有如下特征。

（1）传染性

（2）破坏性

（3）潜伏性

（4）可触发性

（5）衍生性

除了以上特征外，计算机病毒还有其他的一些特征，如攻击的主动性、执行的非授权性、欺骗性、持久性、检测的不可预见性、对不同操作系统的针对性等。

8.2.3　计算机病毒的传播途径

计算机病毒的传播主要通过文件复制、文件传送、文件执行等方式进行。计算机病毒的主要传播途径有以下几种。

① 通过移动存储设备进行传播。例如，U盘、移动硬盘、光盘等都可以是传播计算机病毒的途径，用户在互相复制文件的同时也就造成了病毒的扩散。因为移动存储设备经常被移动和使用，所以它们更容易得到计算机病毒的“青睐”，成为计算机病毒的携带者。

② 通过计算机网络进行传播。网页、电子邮件、聊天工具、BBS、下载软件等都可以是计算机病毒的传播途径，例如，下载了携带病毒的软件，打开了不安全的链接和电子邮件等。勒索病毒WannaCry就是通过网络传播的，“熊猫烧香”病毒通过被绑定病毒的软件进行传播，也可以通过移动存储设备进行传播，这充分说明了计算机病毒的传播途径不唯一。计算机病毒附着在正常文件中，然后通过网络进入一个又一个系统，是目前计算机病毒传播的首要途径之一，其传播速度呈几何级数增长。

③ 通过点对点通信系统和无线通道传播。计算机病毒可以从正常、无毒的文件中进入系统中，目前，这种方式并不是计算机病毒传播的主流途径，但是在未来可能会被黑客大肆利用。

④ 利用计算机信息系统和应用软件的弱点传播。近年来，越来越多的计算机病毒利用计算机信息系统和应用软件的弱点进行传播，因此这种途径也被划分在计算机病毒基本传播途径中。