单元 1　网络安全的基本概念

计算机网络技术的快速发展为信息传递提供了便利条件，也为扩大计算机应用领域提供了基本保障，但是，在计算机网络应用层次不断提高、应用领域不断扩大的同时，网络安全管理也成为全球共同关注的话题。信息资源在网络环境传播、共享使用的过程中，一些重要的信息可能被网络黑客觊觎而出现被窃取、篡改，也可能因为攻击行为导致网络崩溃出现丢失，诸如此类问题影响了信息产业正常有序的发展，严重时甚至会造成人类社会的动荡。因此，保证网络安全、有序运行是发挥网络作用的基础。2010 年以来，世界各国相继制定和大幅调整网络安全战略，增设专门机构，加大人员和资金投入，最大限度维护自身网络空间的安全和利益。

任务 1　了解网络安全的基本含义

从社会学的角度看，网络安全是关系国家安全、社会稳定、民族文化继承和发扬的重要问题。从技术的角度看，它又是一门涉及计算机科学、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综合性学科，内容广泛且技术复杂，因此也造成了网络安全保障工作的复杂性。

任务描述

在人类社会信息化建设的进程中，网络安全问题是一项长期而复杂的社会系统工程，既需要网络管理者充分运用先进的管理手段和专门技术进行专项治理，也需要网络应用者提高安全防护意识和安全应用技术，以有效保护应用环节的安全。或许很多人都听说或知道“网络安全”这一热门词汇，但是“网络安全”究竟涵盖哪些内容？是哪些因素导致了网络应用的不安全？人类社会需要什么样的安全网络？等问题未必人人清楚。本任务将帮助学习者了解网络安全的基本概念，全面或重新认识网络安全。

任务分析

了解网络安全的基本含义，是深入学习网络安全防护技术的基础，究竟网络安全涵盖哪些内容，则可以通过对已经发生的各种危害案例的分析寻找答案。因此，学习任务可以被分解成以下三个活动。

活动 1　危害网络安全案例研讨。

活动 2　了解产生网络危害的原因。
活动 3　掌握网络安全的基本要求。

活动 1　危害网络安全案例研讨

了解危害网络安全事件既是揭示网络安全重要性的基础，也是提高网络用户对网络安全防护重要性认识的基础。本活动将通过集体研讨、有针对性的信息查询等多种手段，帮助学习者理解学习网络安全知识和提高安全防护技能的重要性。

1．危害网络安全案例展示

案例 1：罗伯特制作“蠕虫”事件

“蠕虫”病毒的始作俑者是美国康奈尔大学计算机科学系一年级研究生罗伯特·潘·莫里斯。罗伯特从小就表现出了超出常人的计算机天分，在康奈尔大学有“孤独的才华横溢的程序专家”的名声。

在 20 世纪 80 年代，苹果Ⅱ型 PC 首次出现病毒，当时人们对计算机病毒并不十分了解，而此时罗伯特心中的目标就是编写一个无害的能够传染尽可能多的计算机的病毒。1988 年 10 月，罗伯特开始了自己的计划，他一面集中精力编写病毒程序，另一方面寻找计算机系统中可以施放病毒程序的漏洞。1988 年 11 月 2 日美国东部标准时间晚上 7 点 30 分，罗伯特完成了病毒的编写工作，一个小时后，他在麻省理工学院人工智能实验室的计算机上以 RTM 名登录，并下达了病毒执行指令。在罗伯特按下“ENTER”键的瞬间，病毒开始扩散，几分钟之内已在网上肆虐，一台台计算机被感染病毒陷入瘫痪。罗伯特吃完晚饭去检查病毒的进展情况，发现计算机已经毫无反应，他意识到大事不妙，病毒已经失去了控制，这时才想起编写病毒时把复制参数设置错了。

这一事件使互联网上 10%的计算机受到感染，美国的直接经济损失将近 1 亿美元，罗伯特也因此受到控告，被判 3 年缓刑、1 万美元罚款和 400 小时的社区服务。

思考：病毒制作者的行为可能造成什么样的可怕后果？

案例 2：江西卫生厅考试中心数据库被非法操作事件

2008 年 6 月，江西省公安厅网监总队接到江西省卫生厅考试中心报案，称该厅网站的医师资格查询数据库被他人非法操作，有人修改了数据库内容并制作虚假“医师资格证书”牟利。6 月初，有人持假“医师资格证书”到浙江省相关部门办理“行医许可证”，虽经专门机构认定证书是假的，但查询江西省卫生厅网上数据库发现确有其人，于是向江西省卫生厅核实。江西省卫生厅在检查考试中心网站时发现，几个月前该网站曾遭到黑客侵入，数据库被大量篡改，遂向警方报案。

6 月 19 日，江西省公安厅网监总队立案侦查此案。通过对被攻击受控制服务器的现场勘验，民警发现黑客于 3 月 26 日起入侵江西省卫生厅网站，并上传网站后门程序对网站服务器进行控制。经查，黑客是利用境外新加坡的 IP 地址将篡改的数据上传至数据库，手

段非常隐蔽，有较高的反侦查意识。办案民警经过几天的艰苦侦查，终于将黑客在网上的其他虚拟身份锁定，并最终确定犯罪嫌疑人上网的地点。

6 月 24 日，民警展开抓捕行动，在某租住地将犯罪嫌疑人李某及其同伙 5 人当场抓获，缴获作案用笔记本电脑 4 台，打印机 1 台，各类银行卡 25 张，虚假身份证 13 张，虚假空白“医师资格证书”6 本，“医师执业证书”1 本，“建造师证书”2 本。随后，民警又在武汉将另一名主要犯罪嫌疑人王某抓获。

据警方介绍，2007 年，就读于南昌某高校计算机专业的李某因毕业论文没有通过，无法取得毕业证书，遂产生贩卖假证的念头，只是苦于网上数据库查不到这些假证。2008 年 3 月，李某发现网上要求办理“医师资格证书”及“毕业证书”的信息非常多，于是在网上找到王某，要求王某侵入一些网站，在取得使用权限后交给自己使用，然后通过入侵修改数据—办理假证—贩卖假证—用假证办理从业许可证等环节从中非法牟利。

经查，王某先后入侵江西省卫生厅考试中心网站、湖北省卫生厅网站、贵州人事考试网、四川人事考试网、湖北荆州人事局网站、江苏自考网、辽宁省建设厅网站等 10 余个网站，并以每个网站管理员权限 5000～8000 元的价格卖给李某。李某则对下线收取代理费，每添加一个客户收取 1000～2500 元不等。据李某交代，他共添加了包括江西省卫生厅网站在内的网站数据 700 余个，获利 200 余万元。据一名受害者反映，为了弄到一个上网可查的假证书，他就花了 8000 多元。

思考：此案暴露出了网络应用中的哪些不安全问题？危害性有哪些？

案例 3：以奥运为名的网络诈骗案

2008 年 1 月 4 日，南京公安局网络警察支队接到举报，称有人假冒 2008 年奥运会名义建立网站，实施诈骗活动。南京警方经过缜密调查，于 1 月 28 日在海南儋州抓获许某、陈某等 9 名犯罪嫌疑人。

据该团伙成员交代，2007 年 12 月底，许某和陈某等建立了网站，假冒“系统提示”信息，向众多网络游戏玩家发送中奖消息。当游戏玩家登录他们建立的网站后，中奖页面会显示用户中得 18800～38800 元不等的“惊喜奖金”及奥运会门票一张，但领奖的前提是向一个银行卡号汇款 998 元作为手续费。案发时，全国各地共有 100 多名受害者向涉案银行账户汇款共 30 余万元。

思考：为什么网络诈骗的危害性比传统形式的诈骗更严重？

案例 4：美国加州 5 名用户指控 Facebook 违反隐私法事件

据国外媒体报道，2009 年 8 月美国加利福尼亚州 5 名 Facebook 用户向奥兰治县法院提起民事诉讼，指控 Facebook 违反该州隐私法，并在如何使用个人信息方面误导用户。

原告要求 Facebook 支付赔偿金和诉讼费用，并要求陪审团参与审理。原告诉称，Facebook 将用户提交的个人信息提供给第三方，违反了加州隐私与网络隐私法。该网站还在未向用户披露的情况下进行数据挖掘等工作。5 名原告分别包括 1 名专业摄影师、2 名 13 岁以下的儿童、1 名原 Facebook 用户，以及 1 名洛杉矶女演员兼模特。

Facebook 发言人巴里·斯彻内特拒绝对此做出评论，他表示：“我们认为该指控毫无

根据，并将积极应诉。”Facebook 目前的用户已增长至 2 亿多，隐私保护方面的问题日益突出。2009 年初，由于数万名用户抗议 Facebook 滥用在该网站上共享的个人信息，该网站宣布调整隐私控制方式，转而让用户选择多种不同的隐私政策。Facebook 于 2 月份表示，在采取新的隐私政策前，将允许用户对隐私、内容所有者，以及共享方面的调整进行评估、评价和投票。2007 年末，Facebook 推出了“Beacon”跟踪工具，该工具可以在用户毫不知情的情况下将其行为发布到其他网站，在自由主义 MoveOn 和会员的压力、抗议下，网站最终允许用户关闭该工具。

思考：网络隐私泄露会带来哪些严重危害？

2．危害网络安全案例收集

学生自主分组并充分利用网络资源进行案例收集，小组活动结束后应形成以下成果：

（1）收集到若干个危害网络安全的真实案例。

（2）一份简单的网络安全危害案例分析报告。

（3）简短的小组活动总结。

3．危害网络安全案例讨论

根据对教材展示案例和自己收集案例的讨论结果，分组发言表达各组对危害网络安全问题的看法，最终形成对危害性问题较为统一的认识。讨论可以围绕以下问题展开：

（1）目前的网络安全形势如何？

（2）对网络安全产生危害的形式有哪些？

（3）网络中的不法行为可能带来的危害是什么？

（4）如何看待提高网络安全的急迫性？

活动 2　了解产生网络危害的原因

只有充分了解发生网络危害的基本原因，才能更好地找出应对策略，从根本上解决网络安全危害问题。本活动将帮助学习者认识危害网络安全的各种因素，全面了解出现网络安全问题的原因，为深入学习网络安全技术做好铺垫。

1．危害计算机网络安全的形式

对于计算机网络应用领域的“危害”，可以从两个方面理解，一是各种外在或内在因素对计算机网络造成的危害，二是利用计算机网络对人类社会产生的危害。前者又分为人为与非人为两种，非人为危害主要指自然灾害对计算机网络造成的危害，如地震、水灾、火灾、战争等原因出现的网络中断、系统破坏、数据丢失等。人为危害是指对网络人为攻击，达到破坏、欺骗、窃取数据等目的。与其他危害相比，计算机应用领域的危害包含有较强的技术性，影响范围较大，由此造成的后果也更为严重。

危害计算机网络安全的表现形式多种多样，危害后果和抑制手段也不尽相同，这里归类列出常见的几种，旨在帮助大家认识出现危害事件的严重性，提高网络安全防护意识。

（1）自然灾害

自然灾害对计算机网络造成危害的事件在世界各国时有发生。如果建造机房、安装设备时没有考虑防水、防火、防静电、抗震、避雷等问题，计算机网络工作环境抵御自然灾害的能力会很差，发生灾害后有可能给网络系统造成灭顶之灾。例如，辽宁某铁路局控制机房因缺乏雷电防护设施曾 3 次遭受雷击，致使控制系统和一些终端设备损坏，严重影响了正常编组运输。日本东京电信局在电缆维护时，工人操作不慎造成火灾，由于缺乏有效的火灾控制手段，大火持续 16 小时，烧毁了大量的通信设备，导致数家银行和邮局的计算机通信网络中断，银行分布在各地的自动付款机被迫停机，邮局的一些业务只能暂停。

（2）系统漏洞

计算机网络系统本身存在的致命漏洞是威胁网络安全的重要因素。网络系统大型化使控制管理网络的复杂程度不断增加，隐藏其中的漏洞也越来越多，它们有可能引起网络系统崩溃，也有可能成为渗透网络系统的工具或通道。例如，微软公司曾在 IE 浏览器安全建议书中证实，IE 浏览器存在安全漏洞，由此可能引起零位指针失效或内存失效等错误。思科曾承认它的 Internetwork 操作系统存在处理 IPv6 包的漏洞，若向受影响的思科设备发送特制的 IPv6 包，有可能迫使设备重新启动，导致 DoS 攻击。

（3）操作失误

工作人员缺乏责任心或因专业知识滞后造成操作失误，也会导致意想不到的灾难事件。例如香港联合交易所工作人员在停电后按停警钟时，意外地按下后备电源的“紧急停止掣”，截断了大堂及自动对盘系统主机的电源，停电使系统停止工作 4 分 58 秒，结果导致收市延误，在延误收市的 4 分 58 秒期间，额外交易 1099 宗，成交额约 1 亿多元。延误时间内交易的合法性，引起了巨大争论。

（4）病毒侵袭

计算机病毒的产生和全球性蔓延对网络安全应用构成了严重威胁，且已经造成了巨大的损失，计算机病毒的危害之大，不亚于人类社会发生的瘟疫。台湾大学生陈盈豪制造的“CIH”病毒，首次发作就使全球约 6000 万台计算机受害。美国的罗伯特在互联网上传播“蠕虫”病毒，导致美国 6000 多个系统瘫痪，直接损失 9600 万美元。“爱虫”病毒发作，全球损失约 100 亿美元。某省财政厅财务管理系统感染病毒，破坏了 3 年的财务数据，造成无法挽回的巨大损失。

（5）人为恶意破坏

人为恶意的攻击、破坏是威胁网络安全的重要原因，也是最难控制和防范的危害因素。此种危害的表现形式很多，有对着计算机设备撒尿、浇油漆的物理破坏，有放置逻辑炸弹的应用系统破坏，有格式化磁盘的信息破坏，有篡改信息、盗窃程序数据的个人牟利行为，也有侵入重要、机密信息系统严重危害国家安全的重大事件。

（6）网络欺诈

网络欺诈已成为阻碍网络应用的重要顽疾，现在的网络不但是滋生欺诈性犯罪的新土壤，花样繁多、数量巨大的网络欺诈内容也严重影响了人们对网络信息的信任度。

（7）网络传黄

在互联网有害信息中，传播面最为广泛的就是网络色情信息。资料统计显示，互联网上的色情网站有 420 万之多，占全部网站的 12%，色情网页约有 3.72 亿个，每天色情主题

搜索约 6800 万次，占全部搜索问题的 25%。大量的不良信息对青少年网民的影响比例高于世界平均水平的中国，已经产生了严重的恶果，网络也成为引发一系列社会问题的根源。

（8）网络赌博

2009 年以来，全国破获了多起网络赌博案件，涉案金额之巨，危害之大，令人触目惊心。湖南省赌博案中的涉案金额高达百亿元以上，上海赌博案中的短期投注金额高达 66 亿元，这其中的大部分投注赌资通过网络流向境外，网络赌博已经成为一种严重的“灾害”，成为危害国家经济建设和社会治安稳定的重要因素。

2．发生危害网络安全事件的诱因

危害网络安全事件的发生数量居高不下，且逐年增加，说明危害网络安全有较为特殊的诱发原因，值得深究，认清引发危害网络安全事件的原因也有助于开展防范工作。

（1）网络系统本身存在脆弱性缺陷

计算机网络系统本身的脆弱性是诱发危害网络安全事件最根本的原因。计算机以高速度、高精度处理信息见长，它有许多其他设备不能比拟的优点，如信息存储密度高、易修改、能共享、网络传递方便等，正是这些优点使计算机倍受人们青睐。也正是这些特点使计算机具有先天的脆弱性，高存储密度使处理大量信息成为可能，而在大量信息中隐藏少量非法信息不易察觉，信息一旦丢失损失会很惨重；信息易修改的特性给正常工作带来很多方便，修改后不留痕迹又使犯罪分子有机可乘，使追查犯罪困难重重；网络传递、共享能使人们快速、充分地利用信息资源，但信息传递过程中的电磁泄露、搭线窃听、接收信息对象的甄别困难等问题，又使网络安全控制难以把握。

计算机网络系统的脆弱性和计算机技术的开放性，使针对网络系统的危害易于发生，而防护的薄弱又给了危害行为人可乘之机，所以计算机网络系统的脆弱性不可避免地导致了危害网络安全事件的发生。

（2）网络系统存在管理的复杂性问题

计算机网络系统的功能日益强大，计算机软、硬件的复杂程度随之成倍增长，计算机网络系统的管理也日趋复杂化。正是因为网络和计算机信息系统具有管理复杂性，工作中稍有不慎或管理策略不当，都会使网络系统出现安全隐患，这些不易察觉的安全漏洞，对拥有高技术、法制观念不强、时刻想捞取不法利益者是不小的诱惑，对刻意显示自己才能的人来说也是不可多得的机会。

计算机网络系统管理的复杂性，使管理难度增大，同时，保证网络安全的难度也增大。这必然导致网络的安全性相对下降，使非法渗透网络系统更为容易，更多的人有机会，有可能使用计算机网络或针对计算机网络从事非法活动。危害网络安全事件的数量居高不下和网络系统管理复杂性有直接关系。

（3）网络信息的重要性使之成为攻击目标

计算机应用环境逐渐增多，使存储其中的信息量和信息重要程度相应增加，许多信息和财富直接关联，有些计算机中存储的数据和信息的价值远远超过计算机系统本身，因此，大量危害网络安全事件的指向是计算机网络系统中的信息。通过渗透网络系统能够窃取机密信息、能够获取钱财，这对于掌握计算机网络技术又想一夜暴富的人来说是不小的

诱惑，也促使一些人甘冒风险以身试法，信息、机密、财富密不可分是导致危害网络安全事件发生的主要原因。

（4）低风险的诱惑

从犯罪心理的角度看，犯罪行为人在实施犯罪前，关心该行为刑罚的轻重，更关心受到刑罚的可能性。刑罚很重，但受到刑罚的可能性微乎其微，会降低刑罚的威慑作用，犯罪人在趋利避害的侥幸投机心理支配下实施犯罪。危害网络安全的活动需要技术支持，隐蔽性较强，被发现和查获的可能性小，这一特征对有机会从事危害活动的人有极强的诱惑力。高回报低风险的利益驱动，是许多人甘愿冒险从事危害网络安全活动的主要原因。

（5）道德理念的差异

人类长期形成的道德观念与计算机技术不协调，也是诱发危害网络安全的一个原因。在计算机网络应用普及过程中，高技术人才一直是人们崇拜的对象，他们的越轨行为往往被当成“天才”杰作，即使有触犯法律的行为，也会放宽限制条件、降低处罚尺度，高技术和犯罪权衡，人们更看重技术姑息犯罪。

计算机网络应用环境固有的思维定式，也淡化了犯罪概念。私拆别人信件的人一定会有罪恶感，因为大多数人知道这是违法行为，但是不经允许点击、浏览别人的 E-mail 是什么性质，多数人认为不能与私拆信件相提并论。私人文件加密是计算机使用者在使用计算机过程中达成的默契，未加密文件是共享的，然而，这一惯例不能为法律所容。

3．网络危害问题讨论

根据教师对网络危害知识的讲解和自己对网络危害的认识，分组讨论遏制网络危害的必要性，强化提高网络安全防范的意识。讨论可以围绕以下问题展开：

（1）危害网络安全形式的演变趋势如何？

（2）网络黑色利益产业链的形成对网络安全有什么影响？

（3）如何解决管理复杂性带来的安全问题？

（4）网络行为的低风险表现在哪些方面？

活动 3　掌握网络安全的基本要求

本活动将帮助学习者了解什么样的计算机网络是安全的网络这一基本问题，为今后构建安全、可靠的网络应用环境做好基础准备。

1．什么是安全的计算机网络

从计算机网络应用的角度看，计算机网络是处理信息的具体工具，而信息则是以某种目的组织起来，经过加工处理使之形成一定结构的数据，因此，谈及计算机网络的安全问题，一定要涉及信息处理的全过程。

不同人站在不同的角度对计算机网络的安全要求有不同的理解，通常会出现以下几种情况。

（1）网络用户需要的安全

网络应用者在借助计算机网络处理信息时，不能出现非授权访问和破坏，即便是在信

息交换、传输过程中也不能出现任何意外事件。

（2）计算机网络系统管理者认为的安全

对自己管理的对象完全可控，任何时候都不能因黑客攻击、系统故障等问题出现管理失控，管理者能够按约定给用户提供井然有序的网络服务。

（3）公共信息受众理解的网络安全

过滤一切有害信息，享受信息给工作和生活带来的便利和快乐。

（4）机密信息拥有者要保证的网络安全

自己拥有的敏感信息不会以任何形式泄露出去。

（5）网络安全的综合性定义

综合不同网络应用者对网络安全的要求，可以提出网络安全的综合性定义，即计算机网络安全是指网络中的信息不会被故意的或偶然的非法授权泄露、更改、破坏，不会被非法系统辨识、控制，网络设备安全可靠，人们能有益、有序地使用计算机网络，安全、可靠地获取网络信息。

2．网络安全的基本内容

网络安全不仅涉及技术问题、管理问题，还涉及法学、犯罪学、心理学等问题，是一门由多学科综合形成的新学科。

（1）网络安全涉及的方面

计算机网络系统是由计算机实体、信息、人组成的人机系统，安全问题也应包括实体安全、信息安全、运行安全和安全管理等几个方面。内容涉及安全技术、安全管理、安全评价、安全产品、安全法律、安全监察等。

网络安全主要涉及信息存储安全、信息传输安全、网络应用安全 3 个方面，包括操作系统安全、数据库安全、访问控制、病毒防护、加密、鉴别等多类技术问题，可以通过保密性、完整性、真实性、可用性、可控性 5 种特性进行表述。

保密性：网络信息不会泄露给非授权对象的特性。

完整性：网络信息本身完整，且不会在未授权时发生变化的特性。

真实性：保证网络处理过程和内容真实可靠的特性。

可用性：合法对象能有效使用网络资源的特性。

可控性：对网络资源能进行有效控制的特性。

（2）网络安全控制层次

网络安全控制是复杂的系统工程，需要安全技术、科学管理和法律规范等多方面协调，并构成层次合理的保护体系，只有这样最终才能达到保证网络安全的目的。安全防护技术是保证实体、软件、数据安全的基础，有效管理是保障安全技术发挥作用的前提，法律规范是制约和打击危害网络安全的武器，所以，网络安全控制应在以下 4 个层次上考虑。

实体安全防护：对计算机网络实体进行安全防护是保证网络安全的重要环节，如果计算机硬件和工作环境出现安全问题，存储其中的信息和正常的网络应用很难幸免，所以，设置必要的实体安全防护设施是保证网络安全的基础。

软件安全防护：在实体安全的基础上增加软件安全防护措施是保证网络安全的进一步

要求，软件系统故障同样会导致网络安全问题，所以，软件和软件运行安全也是保证网络安全的基础。

安全管理：设置硬件、软件安全防护设施固然重要，让安全设施充分发挥作用更重要，而它主要依赖于对安全设施的科学管理。统计结果表明，70%以上的安全问题是管理不善造成的，真正由于技术原因出现的安全问题很少。由此可见，安全管理在保证网络安全中的作用极其重要。

法律规范：安全法律是安全防护技术以外的网络安全保障因素。在发生安全问题以前，安全法律起规范网络应用行为、威慑破坏行为的作用，是网络安全的法律保障。在发生安全问题以后，安全法律是处理安全问题的法律依据。

3．网络安全概念讨论

根据教师对网络安全概念知识的讲解和自己对网络安全的理解，分组讨论网络安全所涵盖的全部内容，深入理解网络安全的内涵和安全控制内容。讨论可以围绕以下问题展开：

（1）为什么不同的人会对网络安全有不同的理解？

（2）网络安全问题为什么会涉及众多学科或领域？

（3）分层控制网络安全的目的何在？

（4）本课程重点可以解决哪些方面的问题？

任务小结

学习任务贯穿在 3 个学习活动中，主要目的是帮助学习者理解什么才是安全的网络。

网络安全是一门由多学科综合形成的新学科，涉及安全技术、安全管理、法学、犯罪学、心理学等诸多问题，内容广泛且技术复杂。

不同的计算机网络应用者对网络安全的要求不同，综合来看，计算机网络安全是指网络中的信息不会被故意地或偶然地非法授权泄露、更改、破坏，不会被非法系统辨识、控制，网络设备安全可靠，人们能有益、有序地使用计算机网络，安全、可靠地获取网络信息。

网络安全主要涉及信息存储安全、信息传输安全、网络应用安全 3 个方面，主要依靠实体安全防护、软件安全防护、安全管理、法律规范制约 4 个层次上的控制，可以通过保密性、完整性、真实性、可用性、可控性 5 种特性进行表述。

任务 2　了解网络安全现状及安全防护技术发展趋势

随着计算机网络安全问题日益增多，人们对网络安全的防护意识不断增强，安装网络安全防护产品的环境也越来越多，网络安全防护产品的种类和相应技术也在不断进步，这在某种程度上降低了安全问题发生和产生危害的可能性，但网络安全形势依然严峻。

任务描述

保证网络安全就是要解决网络中存在的不安全问题，不同的安全问题有相应的解决之道，安全问题不断变化，解决方案也将随之改变，所以，全面认识网络安全形势，了解网络安全防护产品及技术发展趋势，是学习网络安全技术保证网络安全的重要基础。计算机网络用户只有充分了解网络安全现状，了解网络安全防护产品，才能有效地选择安全防护措施保障网络安全。本任务将帮助学习者了解网络安全形势，认识网络安全防护产品和安全防护技术发展趋势。

任务分析

了解网络安全形式是认识网络安全问题的前提，更是强化网络安全防护意识的基础，只有了解网络中存在的安全问题和相应的防护技术，才能有效保证网络安全。因此，本任务可以分解成以下活动:

活动 1　网络安全形势研讨。

活动 2　了解网络安全防护产品应用现状。

活动 3　了解网络安全产品和技术的发展趋势。

活动 1　网络安全形势研讨

摸清网络应用中出现的安全问题是实施安全防护的基础，也是预测网络安全防护技术发展的风向标。本活动将通过教师对现有安全问题的提示和学生集体研讨、有针对性的信息查询等学习环节，帮助学习者了解网络安全问题的现状。

1．因特网的主要安全问题

从发生的因特网安全事件看，近两年中国虽然没有发生大规模的病毒威胁，也没有发生影响恶劣、损失严重的网络攻击事件，但网络安全威胁形势依然严峻，危害变化的发展趋势仍然令人担忧。

（1）网页仿冒依然活跃

网页仿冒问题一直居高不下，仿冒者充分利用更有效的技巧和自动操作技术，借助热点、敏感问题强化仿冒网页的可信度，使网页仿冒问题依然成为网络应用中的顽疾。

（2）垃圾邮件猖獗

随着垃圾邮件组织团伙 McMolo 曝光和反垃圾邮件过滤技术提高，全球垃圾邮件的比例显著下降，但问题没有根除，电子邮箱的使用者依然会收到干扰用户的垃圾邮件。有公司预测，在平静一段时间以后，未来垃圾邮件数量会大幅回升。

（3）数据泄露十分严重

数据泄露事件持续增长是由社会经济大环境种种因素造成的，现在网上有大量的数据信息被非法叫卖，某些数据包含有单位或个人的重要信息，泄露出去可能造成无法估量的损失，因此，强化技术防护、管理防护措施，防止数据丢失对于数据拥有者十分重要。

（4）系统漏洞不容忽视

新发现的漏洞数量不断增加，能够产生危害的严重程度也相当高，由此对网络应用安全构成了重大威胁。2011 年 4 月，国家信息安全漏洞共享平台收集整理系统安全漏洞 404 个，其中高危漏洞 130 个，可被用于远程攻击的漏洞有 353 个。受影响的软、硬件系统厂商包括 Cisco、Google、IBM、Microsoft、Linux、Novell、Oracle 等。国家信息安全漏洞共享平台的代码验证结果显示，4 月共出现了 72 个 0day 漏洞，影响较为严重的是“Graugon Forum SQL 注入漏洞”、“Winamp ′ .m3u8 文件远程缓冲区溢出漏洞”和“SimplyPly′ .pls′ 文件远程缓冲区溢出漏洞”，因特网上已经出现了针对上述漏洞的攻击代码。

（5）网站被篡改事件屡禁不止

2011 年 4 月中国大陆地区共有 3201 个网站被篡改，被篡改较多的类型分别是.com 和.com.cn 为 2291 个（占 71.57%），.gov.cn 为 228 个（占 7.12%），.net 和.net.cn 为 219 个（占 6.84%），其中代号为“soojoy”、“haaie”和“s4r4d0”的攻击者对中国大陆网站进行了大量篡改。中国大陆被篡改网站数量最多的地区分别是广东省 628 个，北京市 616 个和江苏省 308 个。

（6）僵尸网络遍布全球

CNCERT/CC 在 2011 年 4 月，对 177 种木马家族和 65 种僵尸程序家族进行了抽样监测，发现境内 1639144 个 IP 地址对应的主机被木马或僵尸程序控制，境外 952966 个 IP 地址对应的主机被木马或僵尸程序控制，境内受控主机数量较多的地区分别是广东省 187837 个、江苏省 153387 个和浙江省 101793 个，境外受控主机数量较多的国家分别是印度 181932 个、埃及 89365 个。因感染木马或僵尸程序而形成的僵尸网络中，规模大于 5000 的僵尸网络有 42 个，规模在 1000 至 5000 的僵尸网络有 170 个，规模在 100～1000 的僵尸网络有 951 个，占总数量的 81%以上。

2．网络病毒整体形势

病毒制造、传播者在巨大利益的驱使下，利用病毒、木马技术进行各种网络盗窃、诈骗活动，严重干扰网络的正常应用，应予以高度关注。

（1）恶意代码的主流是木马程序

木马在中国的恶意代码数量中占有绝对多数，2011 年 5 月公布的 10 大流行病毒中，仍以木马程序、后门程序为主。排在前三位的是“木马下载器”、“U 盘杀手”、“代理木马”，用于盗取网络游戏账号的木马程序“网游大盗”紧跟其后。木马程序制作者的牟利目的十分明确，均以盗取因特网上有价值信息资料转卖后获利。

（2）“挂马”成为病毒传播的主要手段

网站“挂马”成为病毒传播的主要手段，无论是主动或被动的“挂马”都为病毒滋生和传播提供了优越的环境，当前相当数量的病毒变种来自于这类网站。中国国家计算机病

毒应急处理中心检测发现，被挂马的网站覆盖政府、新闻、软件下载、娱乐等各种网站。当用户使用有安全漏洞的浏览器访问这些网站时，病毒利用脚本下载木马程序并激活。

（3）病毒的自我保护能力增强

一些新技术如主动防御技术、磁盘过滤驱动技术、影像劫持技术、穿透还原卡或还原软件技术被应用到恶意代码的编写中，使病毒从修改样本特征值躲避查杀逐渐过渡到直接与安全软件对抗。如“AV 终结者”可以通过释放并加载驱动程序，在获得系统权限后试图结束安全软件进程，让用户的计算机处于无防护状态。“机器狗”利用突破系统还原卡技术，让感染病毒的计算机在重启后，病毒样本仍存活在系统中。

（4）下载者病毒加剧了病毒传播

下载者病毒具备从指定地址下载大量其他病毒、木马程序的功能，使其成为病毒的快速输送者。网络用户的计算机一旦受到下载者病毒入侵，系统将会陆续下载安装几种，甚至几十种病毒、木马，种类几乎涉及所有流行的在线游戏盗号木马，危害十分严重。

（5）应用软件漏洞扩大了病毒传播途径

随着操作系统安全性的逐渐提高，病毒利用系统漏洞施法的空间越来越小，病毒制造者开始关注应用软件的漏洞。近年，病毒除了利用 Windows 系统漏洞传播外，开始综合利用各类应用软件的漏洞以扩大病毒传播，多数病毒利用两个及两个以上的漏洞传播病毒。其中微软 MS06-014 漏洞、百度搜霸漏洞、RealPlayer Import 缓冲溢出漏洞，都是常被利用的漏洞。

（6）病毒黑色产业链逐步形成

制造木马、传播木马、盗窃账户信息、第三方平台销赃、洗钱一整套完整病毒黑色产业链已经形成，且正朝着技术分工明细、销赃洗钱方式多元化的方向发展。

（7）利用社会工程学传播病毒

病毒制造者利用人们关注热点事件的心理或好友信任的关系设套，加速病毒传播，可以说近年出现的热点事件已经成为病毒的“帮凶”。将病毒伪装成热门电影、网络视频、照片等，借助高点击率可以诱骗用户点击下载，进而扩大传播范围。

3．网络安全形势资料收集

学生自主分组并充分利用网络资源进行网络安全形势有关资料的收集活动，小组活动结束后应形成以下成果：

（1）收集到近两年中国互联网信息中心和国家互联网应急中心联合发布的《××年中国网民网络信息安全状况调查系列报告》。

（2）收集到年度《中国计算机病毒疫情调查技术分析报告》。

（3）收集到若干份近期由网络安全技术公司发布的《互联网安全威胁报告》。

（4）收集到公安部有关计算机安全专用产品检测情况报告。

（5）一份简单的网络安全形势分析报告。

（6）简短的小组活动总结。

4．网络安全形势讨论

根据教师的讲解提示和自己收集资料的分析讨论结果，分组讨论并发言表达各组对网络

安全形势的看法，最终形成对网络安全形势较为统一的认识。讨论可以围绕以下问题展开：

（1）当前网络安全形势的突出特点是什么？

（2）近期严重危害网络安全的病毒有哪些？

（3）专家预测的网络安全问题变化趋势是什么？

（4）对网络安全产品有哪些基本认识？

活动 2　了解网络安全防护产品应用现状

近几年网络安全防护产品的研发势头迅猛，应用普及迅速，但是网络安全形势依然严峻，原因何在，本活动将从了解网络安全防护产品应用现状开始，帮助学习者寻找其中答案。

1．网络安全产品的应用现状

网络安全产品应用现状是网络安全管理部门和网络安全产品生产企业共同关注的问题，它既能反映网络用户对网络安全的认知和需求，也能为安全产品厂商指明产品研发的基本方向。

（1）网络安全管理部门的调查结果

2004 年，公安部公共信息网络安全监察局与中国计算机学会计算机安全专业委员会共同对政府、金融证券、教育科研、电信、广电、能源交通、国防和商贸企业等重要信息网络、信息系统进行安全调查，结果显示，计算机病毒防治产品和防火墙是应用最为广泛的网络安全产品，分别占被调查用户的 81%和 82%，其他网络安全产品使用率普遍较低，均在 30%以下。这一结果说明大多数的计算机网络使用最基本的防护设施，认为设置防火墙，安装防病毒软件就能解决网络安全问题。2005 年的调查结果显示，这一现状并未改变，表 1-1 为公安部连续两年对中国计算机网络安全产品应用情况的调查结果。

表 1-1　网络安全产品应用情况一览表

产品 / 年份	防火墙	病毒防治产品	入侵检测	访问控制	网络隔离产品	身份鉴别	信息过滤	安全审计	虚拟专用网络	文件系统保护	网络漏洞扫描	防雷保安器
2004	82%	81%	22%	27%	18%	12%	11%	12%	11%	18%	17%	18%
2005	80%	80%	21%	25%	17%	10%～12%				17%	17%	16%

2004 年的调查对象是 7072 个，2005 年的调查对象增至 12019 个，但网络安全产品的应用比率几乎没有变化，这充分说明网络安全产品仍处于低水平应用状态，远远不能满足网络安全的需要。

（2）企业安全产品应用调查

某公司在 2008 年曾对企业网络安全产品应用状况进行专门调查，认为企业网络安全防护已经步入从网络安全向应用安全、数据安全和系统安全全方位、多层次推进的阶段，从重视网络设备安全、查杀病毒的被动防御向关注风险评估、数据库安全、数据备份的主动防护转变，内网安全、身份认证、安全监控也将成为成为新一轮采购热点。

调查结果显示，企业最重视的安全问题是病毒查杀，病毒为企业带来的种种困扰已经使杀毒措施深入人心。排在第 2 位的是信息资产，数据也成为了企业重点保护的对象，关注数据库安全、数据备份与恢复的企业已经超过半数。关注网络设备安全的占 46.0%，应用软件管理的占 32.6%，补丁升级管理的占 32.3%，系统加固的占 28.3%，网站运维安全的占 22.0%，安全风险评估的占 11.1%。多数企业将安全类设备作为 IT 建设的必需品，只有 2.6%的企业还没有购买网络安全产品。表 1-2 是 2008 年被调查企业已安装安全产品的比例和准备在 2009 年安装网络安全产品的比例，结果仍然显示病毒防治产品和防火墙是应用最为广泛的网络安全产品。

表 1-2　企业网络安全产品应用状况一览表

产品 / 年份	防火墙	计算机病毒防治产品	入侵检测	内网安全管理	网络隔离产品	身份鉴别	UTM 安全一体化网关	虚拟专用网络	安防监控	存储安全系统
2008	71.4%	78.3%	18.3%	23.7%	12%	28%	9.4%	44.9%	20.6%	18.3%
2009	42.1%	69.3%	%	28.1%	%		10.2	31.1%	17.3%	3.2%

2．网络安全产品开发现状

前几年中国网络安全产品研发呈现出较快的发展势头，2004 年升级或新开发的网络安全产品多达 394 项，比 2003 年多 71 项，2009 年 10 月公安部计算机信息系统安全产品质量监督检验中心检测并出具了 537 份网络安全产品检测报告。近十几年的网络安全产品数量统计如表 1-3 所示，从表中可见，2005 年以前是快速发展期，2006、2007、2008 年的产品数量趋于稳定，基本上保持在 450 个左右，说明网络安全产品研发正处于稳定发展的阶段。根据送检厂商提交的网络安全产品生产开发调查表统计，声明具有自主知识产权的产品占到了 84.2%～85.51%，说明有越来越多的企业严格遵守开放源代码许可协议，与软件的创始者达成商业许可，合法地在开放源代码的基础上推出新的网络安全产品，2008 年、2009 年送检的网络安全产品知识产权情况如表 1-4 所示。

表 1-3　网络安全产品数量统计

年份	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
数量	15	103	219	264	350	323	394	369	427	457	497	537

表 1-4　网络安全产品知识产权情况

知识产权种类	自主（包括由 FreeCode 改进）	进口	国外独资在国内生产	国内 OEM
2008	85.51%	8.45%	5%	1%
2009	84.2%	6.5%	6.9%	0.4%

目前用于保护网络安全的产品主要有：防毒杀毒产品、防火墙、入侵检测、网络隔离产品、信息内容过滤产品、访问控制产品、网络漏洞扫描器、防雷保安器、虚拟专用网络等。2009 年送检的网络安全产品分类如表 1-5 所示。公安部检验中心对主要安全产品进行技术分析发现，2009 年度送检的安全产品在技术、功能优化、性能稳定性等方面都有长足

进步。其中，本地数据备份与恢复、安全管理平台、身份鉴别、不可否认性鉴别、远程主机监测、IPS、小型防火墙等产品技术成熟，性能稳定；安全审计、物理隔离、网页恢复等产品在技术上有了较大改进和提升；防火墙等产品呈现出向更高性能发展的趋势，产品竞争力增强。此外，VPN、公钥基础设施（CA）、安全终端计算机系统、文件加密、不可否认性、完整性鉴别等产品应用日趋广泛，数量不断增多。但是，还有部分国内产品在功能和性能上，仍与国外产品存在一定差距，如 IDS、反垃圾邮件等产品，在其策略库的完备性和可扩展性等方面有待进一步改进。

表 1-5　2009 年公安部检验中心检测的网络安全产品详细分类

产品类别	细分类型			检测数量	不合格数量	不合格比例
主机安全	身份鉴别	电子信息鉴别（主机）		10	4	40%
		生物信息鉴别（主机）		5	0	0%
	主机防护	可信计算				
		主机入侵检测（一级）		3	1	33.33%
		终端计算机系统（一级）		4	0	0%
		个人防火墙（基本级—单机）		6	0	0%
		个人防火墙（基本级—带集中管理）		1	0	0%
		个人防火墙（增强级—单机）		1	0	0%
		个人防火墙（增强级—带集中管理）				
	防恶意代码					
	操作系统安全			5	0	0%
网络安全	通信安全	可用性保障（抗 DoS）		5	0	0%
		通信鉴别				
		通信保密（VPN）		7	0	0%
	网络检测	网络入侵检测		20	0	0%
		网络活动监测				
边界安全	边界隔离	安全隔离卡	物理隔离（基本级）	4	0	0%
			物理隔离（增强级）	2	0	0%
		安全隔离与信息交换	协议隔离（一级）	3	0	0%
			网闸（一级）	10	1	10%
			网闸（二级）	3	0	0%
			网闸（三级）	3	1	33.33%
	入侵防范	入侵防御系统		15	1	6.67%
		网络恶意代码防范				
	边界访问控制	防火墙	一级	63	5	7.94%
			二级	1	0	0%
			三级	2	0	0%
			小型防火墙	9	0	0%
		安全路由器（2007—一级）		1	0	0%
		安全交换机				

续表

产品类别	细分类型			检测数量	不合格数量	不合格比例
	网络终端安全	终端接入控制		74	10	13.51%
		终端使用安全				
	内容安全	信息内容过滤与控制	信息过滤（基本级）	18	1	5.56%
			信息过滤（增强级）			
			反垃圾邮件	10	0	0
		防信息泄露				
	其他	网关（一级）		2	1	50%
应用安全	应用服务安全	安全应用服务	电子签章	17	0	0
			Web 过滤与防护	7	0	0
		电子信息鉴别（应用）		20	3	15%
		生物信息鉴别（应用）		3	1	33.3%
	应用服务安全支持	应用数据分析				
数据安全	数据平台安全	安全数据库（国标—三级）		2	0	0
		数据库安全部件				
	备份与恢复	数据备份与恢复	网页恢复（基本级）	12	3	25%
			本地数据备份与恢复	10	1	10%
安全管理与支持	综合审计	安全审计	网络安全审计（国标—基本级）	8	3	37.5%
			网络安全审计（国标—增强级）			
			网络安全审计（行标—基本级）	9	2	22.22%
			网络安全审计（行标—增强级）	1	0	0
			数据库安全审计	13	1	7.69%
			日志分析	14	2	14.29%
			主机文件监测	4	1	25%
	应急响应支持					
	密码支持	密钥管理（一级）		2	0	0
		密钥管理（二级）		1	0	0
		密钥管理（三级）		1	0	0
	风险评估	系统风险评估				
		安全性检测分析	网络漏洞扫描（基本级）	6	0	0
			网络漏洞扫描（增强级）	1	0	0
			主机漏洞扫描	1	0	0
			数据库漏洞扫描	3	0	0
	安全管理	安全产品管理平台		8	1	12.5%
		安全监控	远程主机监测	50	10	20%
			非授权外联监测	5	1	20%
其他	文件加密			15	4	26.7%
	公共上网服务场所			12	0	0
	上网服务营业场所			13	0	0
	企业标准			12	0	0
	总计：			537	61	11.36%

3．网络安全产品应用问题讨论

根据教师对网络安全产品知识的讲解和自己对网络安全产品的理解，分组讨论网络安全产品的种类和功能，深入理解网络安全产品在网络安全控制中的作用。讨论可以围绕以下问题展开：

（1）从网络安全产品分类表找出网络安全产品发展变化的趋势。

（2）网络安全产品数量逐年变化说明什么问题？

（3）什么原因使防病毒产品、防火墙设备成为网络安全的首选产品？

（4）选用网络安全产品的标准是什么？

活动 3　了解网络安全产品和技术的发展趋势

随着网络安全问题不断增多，危害网络安全的手段、方法不断变化，网络安全产品和技术也将顺应网络安全需求进行改进，本活动将帮助学习者了解网络安全技术的发展方向。

1．网络安全产品和技术的发展趋势

未来网络安全产品和技术的变化主要集中表现在以下几个方面。

（1）技术整合势在必行

复杂的应用项目越来越多，各种攻击手段也趋于复杂化，混合性攻击已经成为一种新趋势。新的攻击方式催生新的安全产品，面对未知的危害手法，需要集多功能于一体的集成安全产品，现在已经出现了集防火墙、入侵检测、病毒防护于一体或在核心交换机上嵌入防病毒功能模块的安全防护产品。有人预测，未来网络安全产品的主流将是多功能整合式安全产品。

（2）产品标准化程度逐渐提高

网络安全产品标准化是必然趋势，标准化不但是规范安全产品市场的一种手段，也是提高安全产品的网络安全保障能力，有效保护网络安全的一种措施。随着国家颁布实施的网络安全产品技术标准增多，安全产品的标准化程度将逐渐提高。

（3）小型或个人网络安全产品越来越多

在经历 CIH 病毒、熊猫烧香病毒、网络诈骗、网络盗窃等一系列重大安全事件后，更多的人开始关注网络安全问题，小企业和个人也会逐渐考虑自己使用网络的风险。这一巨大的产品市场，将诱惑更多的网络安全产品厂商开发小型或个人网络安全产品，这种转变有利于信息社会的有序发展。

（4）新型网络安全产品种类逐渐增多

网络应用中的新问题，如垃圾邮件、蠕虫病毒、网络仿冒、手机病毒等，都需要有相应的安全产品与之对抗，层出不穷的安全问题，促使网络安全产品的种类增多。

（5）网络安全产品的升级换代越来越方便

危害网络安全手段的变化周期缩短，促使安全产品更新换代的速度加快，传统的产品升级方法将不能适应安全应用的需求，远程升级、自动升级是快速技术跟进的有效方法，

也是未来网络安全产品升级换代的主要手段。

（6）安全产品等级明晰化

随着安全保护等级制度的推广，安全产品等级化将成为必然趋势。2009 年度检测机构出具的分级检测报告近 300 份，约占检测报告总数的 40%。

（7）云计算在安全领域中的应用越来越广泛

云安全是云计算领域的重要应用，它是网络时代信息安全的最新体现。云安全融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户终端，对网络中软件进行异常监测，快速获取互联网中木马、恶意软件、攻击行为的最新信息，推送到云中进行自动分析和处理，再把解决方案分发到每一个客户端。云计算强大的数据运算能力和同步协调能力，可以极大地提升安全产品厂商对新威胁的响应速度，同时在第一时间将安全策略分发到各个分支节点。

2．网络安全技术发展趋势的讨论

根据教师对网络安全产品和技术发展趋势的讲解，有针对性地收集相关资料，讨论网络安全技术发展对网络安全的影响。讨论可以围绕以下问题展开：

（1）为什么说产品标准化程度提高有利于安全产品的开发？

（2）以杀毒软件为例阐述方便产品升级的必要性。

（3）安全技术整合的利与弊。

（4）“云计算”在安全领域的正面作用和负面效果。

任务小结

本任务是后续学习的基础，虽然提及安全产品种类和名称，但不涉及具体的安全产品包含的技术知识，某些安全产品的具体应用方法会在以后的学习和工作中逐步了解。认清网络安全形势是提高安全防范意识的基础，更是实施安全防范的动力，但是，只有全面了解安全产品才能进行有针对性的选择，进而构建满足应用要求的安全环境。安全技术的发展趋势预示着安全防范的未来，同时也能反映危害变化的方向，因此，网络用户需要时刻关注。

任务 3　理解网络安全防护整体框架

合理、可行、安全、可靠的网络安全保障体系，是包含安全标准、安全技术等多种内容的综合系统。安全标准体系描述了安全标准的整体组成，是整个网络安全标准化的工作指南，安全技术标准描述了网络安全实现的具体内容，是保证网络安全运行的技术指南。

任务描述

网络安全防护整体框架是科学制定网络解决方案的基础，也是规范网络安全各种措施的重要依据，所以学习网络安全技术必须从宏观上了解解决安全问题的整体框架。本任务

既要帮助学习者了解安全保护的基本模型，为后续学习做好知识铺垫，也要让学习者认识安全保障体系的基本组成，为学会制订安全整体解决方案做准备。

任务分析

网络安全防护整体框架是涉及面较广、理论性较强的内容，全面了解有一定难度，但是网络安全防护整体框架是后续学习的重要基础，更是制订网络安全解决方案的重要依据。为了降低学习难度，可考虑在了解网络安全保护基本模型，形成安全保护的整体概念后，学习安全保护体系的基本组成，认识实际的安全保护体系。因此，本任务可以被分解成以下活动:

活动 1　了解网络安全保护的基本模型。

活动 2　了解网络安全保障体系的基本组成。

活动 1　了解网络安全保护的基本模型

随着网络安全技术的不断发展，网络安全行业出现了多种安全体系模型，本活动将帮助学习者全面认识网络安全体系模型，为制订有效安全解决方案和进行网络安全建设奠定基础。

1. OSI 安全体系结构

国际标准化组织（ISO）在对开放系统互联环境的安全性深入研究后，提出了 OSI 安全体系结构，即《信息处理系统——开放系统互连——基本参考模型——第二部分：安全体系结构》，OSI 的标准体系被包括中国在内的许多国家采用，形成了针对通信网络的安全体系架构模型，即 GB/T9387.2—1995。该模型提出了安全服务、安全机制、安全管理和安全层次的概念。安全服务共 5 类，分别是鉴别服务、访问控制、数据保密性、数据完整性和抗抵赖性；支持安全服务的有 8 种安全机制，分别是加密机制、数字签名、访问控制、数据完整性、数据交换、业务流填充、路由控制和公证；安全管理则被分为系统安全管理、安全服务管理和安全机制管理；实现安全服务和安全管理的层面包括了 OSI 的 7 层，即物理层、链路层、网络层、传输层、会话层、表示层和应用层。

2. PDR 安全防护体系

为了解决网络安全问题，人们首先想到的是采取主动的防护手段，如对数据信息进行加密防止被窃取，安装防火墙防止系统被入侵等，但是主动防护存在防护设施失效危害已然发生的致命缺陷，因此人们又提出了新的防护思想。最具代表性的是 ISS 公司提出的 PDR 模型，该模型认为安全体系应包括防护（P）、检测（D）、响应（R）3 个方面。

PDR 构建的完整安全防护体系，不仅需要防护机制（安装防火墙、信息加密等），也需要危害检测机制（入侵检测、漏洞扫描等），还需要在出现问题时做出响应（报警、断网等）。PDR 模型建立在基于时间的理论基础之上，认为网络安全相关的所有活动，无论是攻击行为、防护行为、检测行为，还是响应行为都要消耗时间，因此，可以用时间尺

度衡量 PDR 体系的能力。假定系统被攻破保护的时间为 Pt，检测到发生攻击的时间为 Dt，响应并反攻击的时间为 Rt，被暴露的时间为 Et，则系统安全状态的表达式为 Et=Dt+Rt-Pt。当 Et>0 时，说明系统处于安全状态；当 Et<0 时，说明系统已受到危害，处于不安全状态；当 Et=0 时，说明系统安全处于临界状态。

PDR 模型考虑的防护、检测和响应 3 个要素都局限于技术，明显与实际安全应用环境有出入，除了技术因素外，制约网络安全的还有人员、管理、制度和法律等方面的要素。为此，有专家对 PDR 模型进行了补充和完善，先后提出 PPDR、PDRR、PPDRM、WPDRRC 等改进模型。

3．IATF 信息保障技术框架

IATF 是和 PDR 一样被人们重视的安全保护模型，它是由美国国家安全局组织专家编写的全面描述信息安全保障体系的框架，它关注技术、管理、策略、工程和运行维护等各个环节，使安全保障贯穿整个系统。

IATF 首次提出了信息安全保障需要通过人、技术和操作来共同实现组织职能和业务运作的思想，同时针对信息系统的构成特点，从外到内定义了 4 个主要的技术关注层次，包括网络基础设施、网络边界、计算环境和支撑基础设施，完整的信息保障体系在技术层面上应实现保护网络基础设施、保护网络边界、保护计算环境和保护支撑基础设施，形成“深度防护战略”。

4．WPDRRC 信息安全模型

该模型是我国专家提出的适合中国情况的信息系统安全保障体系建设模型，它吸取了 IATF 关于安全需要通过人、技术和操作共同实现组织职能和业务运作的思想，在 PDR 模型的前后增加了预警和反击功能。WPDRRC 模型有 6 个环节和 3 大要素。预警（W）、保护（P）、检测（D）、响应（R）、恢复（R）和反击（C）6 个环节具有较强的时序性和动态性，能够较好地反映出信息系统安全保障体系的预警能力、保护能力、检测能力、响应能力、恢复能力和反击能力。人员、策略和技术 3 大要素的核心是人员，桥梁是策略，必要的技术则是最终的保证，只有将 3 种要素全面落实在 6 各环节中，才能将安全策略变为安全现实。

5．网络安全保护模型讨论

根据教师对网络安全保护模型的讲解，有针对性地收集与安全保护模型有关的资料，讨论网络安全保护模型的内涵，深入理解网络安全保护模型对网络安全实施的影响。讨论可以围绕以下问题展开：

（1）网络安全模型与实施网络安全保护的关系。

（2）为什么多数人重视对网络的保护，忽视检测和响应等环节？

（3）预警、恢复、反击的实例有哪些？

（4）人在安全管理中的作用有哪些？

活动 2　了解网络安全保障体系的基本组成

网络安全保障体系是涉及多种安全技术的复合体，只有各种技术共同发挥作用，才可能保障网络处于安全状态。本活动将帮助学习者全面了解网络安全保障体系的基本组成。

1．网络安全标准体系

网络安全标准体系是网络安全保障体系中重要的技术体系，主要作用体现在两个方面：一是确保网络安全产品、设施的技术先进、可靠，二是提供网络安全产品评测依据。网络安全标准体系框架描述了网络安全标准整体组成，是整个网络安全标准化工作的指南。

在借鉴和吸收国际先进的网络安全技术、方法和标准化成果的基础上，中国初步形成了以网络安全基础标准和网络安全管理标准为支柱，以物理安全标准、系统与网络标准、应用与工程标准为支撑的网络安全标准体系框架，示意如图 1-1 所示。

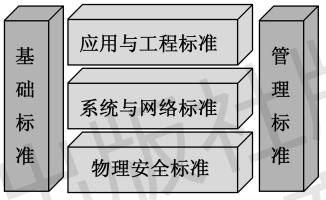

图 1-1　网络安全标准体系框架

尽管中国已初步形成了网络安全标准体系框架，一些应用部门也在网络安全标准体系框架指导下结合具体应用，初步形成了网络安全标准体系结构，如图 1-2 所示，但是这些标准体系结构还不成熟、不完善。网络安全标准体系研究是一项长期工作，也是今后信息化建设的重中之重。

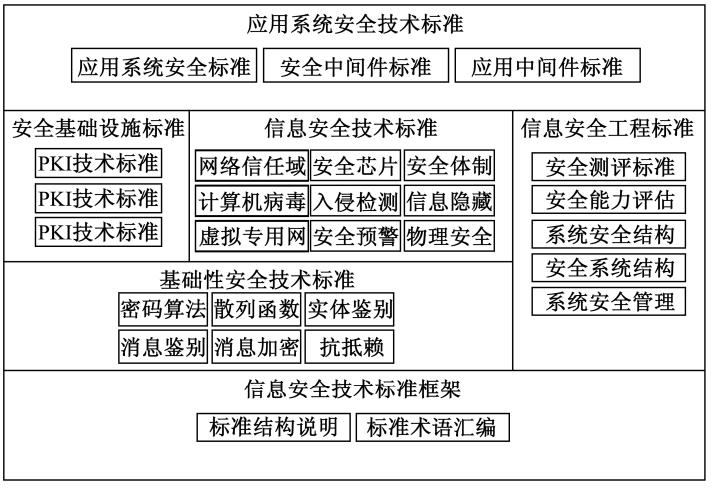

图 1-2　网络安全标准体系结构

2．网络安全保障体系

不同分析方法可以得到不同表述方式的安全保障体系，最常用的有以下两种。

（1）根据网络层次构筑安全保障体系

根据网络层次考虑设置安全保护体系，也需要将网络安全保障体系分成物理、网络、系统、应用和数据几个层面，不同的网络安全技术与控制层面存在一定的对应关系。某些安全技术只适用于特定的安全层面，如防雷、防火是针对物理层面的安全，边界防护、区域划分是针对网络层面的安全，而某些安全技术可以在多个层面实现，如身份鉴别、访问控制等可以分别针对网络层面、主机层面和应用层面的安全，因此，分层后的安全保障体系如图 1-3 所示。

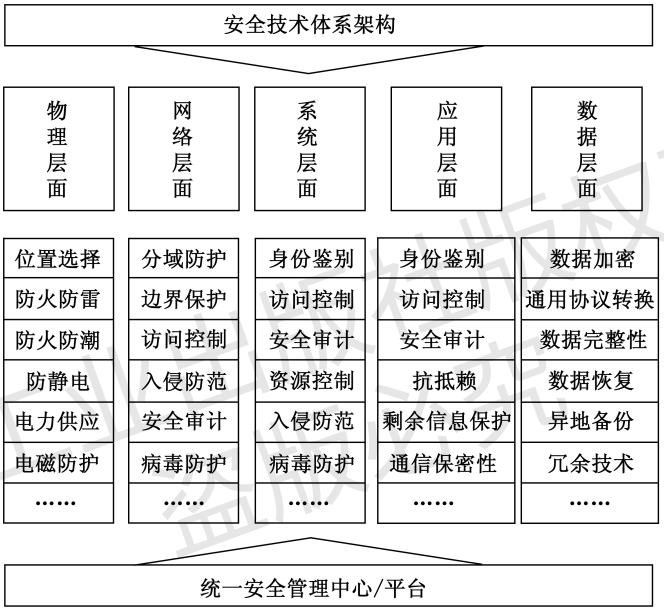

图 1-3　分层安全保障体系

（2）根据风险分析构筑安全保障体系

根据对网络安全威胁和系统脆弱性分析，找出安全风险进而有针对性地进行防护，是更容易实现的方法。系统风险分析通常包括物理安全风险分析、系统安全风险分析、信息安全风险分析和管理安全风险分析，在系统风险评估后提出安全管理策略和安全技术防护策略更具有针对性。根据风险分析提出的网络安全保障体系示例如图 1-4 所示。

3．网络安全保障体系讨论

根据教师对网络安全保护体系的讲解，收集网络安全标准、有关系统的安全保障框图，讨论网络安全保障体系对实施安全保护的作用，为以后制订网络安全解决方案奠定基础。讨论可以围绕以下问题展开：

（1）为什么说目前的网络安全标准体系不够成熟？

（2）网络安全标准体系和安全模型的关系。

（3）网络安全标准体系和保障体系的关系。

（4）网络安全保障体系与后续学习内容的关系。

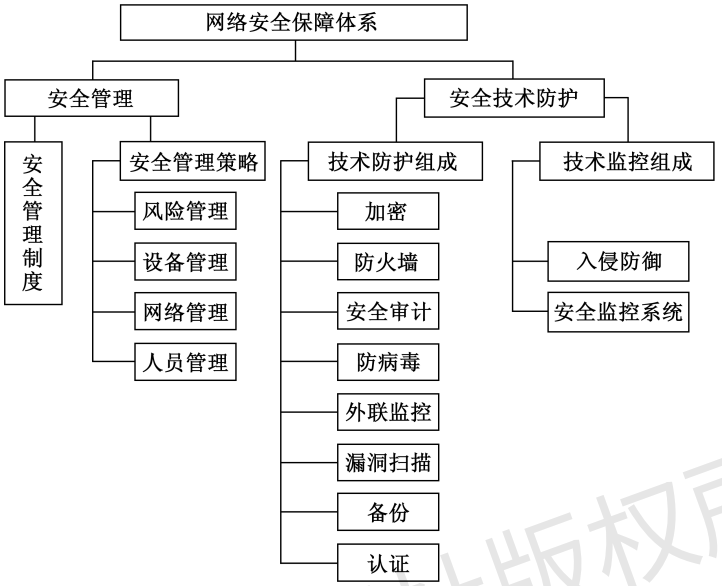

图 1-4　风险分析安全保障体系示例

任务小结

本任务介绍的网络安全保护模型和网络安全保护体系基本组成，是一般性的知识学习，更是未来设计、制订网络安全解决方案的基础。网络安全保护模型有多种形式，中国提出的 WPDRRC 模型有 6 个环节和 3 大要素，较为全面地反映了网络保护的全部内容。不同系统的安全保护体系存在差异，需要用户找出问题，有目的采取措施降低问题发生的风险。

只有充分理解安全模型的作用和安全保障体系的组成内容，才能学会表述自己应用系统需要的安全保障体系，也才可能制作出满足安全需要的解决方案。

单元小结

通过具体网络安全危害案例研讨和总结各种危害因素，可以初步了解出现在网络环境中的各种危害行为，在此基础之上确定网络安全所涵盖的内容，进而深入了解网络安全的基本概念。全面了解网络安全现状和技术发展趋势，需要完成 3 个学习活动，了解网络中出现的安全问题是实施安全防护的基础，了解网络安全产品应用状态可以寻找采取保护措施后仍然出现问题的根源，了解安全技术发展趋势是为了紧跟网络安全需要强化安全措

施。理解网络安全整体保护框架是为了更好地构筑安全防护体系，保障网络可靠、有序运行。了解网络安全保障体系能够全面认识网络安全涉及的内容，也是为安全解决方案学习奠定必要的基础。

单元 1 学习评价标准

学习任务完成后，可以根据任务活动评价标准进行自评、互评和教师点评，形成个人和学习小组任务完成情况总体评价。标准 1 是合作学习评价参考标准，标准 2 是知识、技能评价参考标准。

标准 1　合作学习评价参考标准

评价项目	评价内容及评价分值		
	优秀（15～11 分）	良好（10～6 分）	继续努力（6 分以下）
分工协作	成员分工明确，任务分配合理	成员分工较明确，任务分配较合理	成员分工不明确明确，任务分配不合理
信息获取	能使用多种搜索引擎多渠道获取网络信息，并能合理地选择及使用信息	能从网络获取信息，并能较合理地选择及使用信息	能从网络或其他渠道获取信息，但信息选择不正确、信息使用不恰当
分析讨论	讨论热烈、发言积极，问题分析思路清晰、逻辑性强	讨论较为积极，问题分析思路基本清晰	能够组织讨论，问题讨论不充分，思路不清晰
成果要求	提交成果完整，内容质量高	提交成果完整，内容质量一般	提交成果不完整，内容质量一般
成果展示	语言表述准确，问题说明清楚，结论正确	语言表述基本准确，问题说明基本清楚，结论基本正确	语言表述不准确，没有说清问题，结论不正确

标准 2　单元 1 知识、技能评价参考标准

评价项目	评价内容及评价分值		
	优秀（15～11 分）	良好（10～6 分）	继续努力（6 分以下）
危害网络安全因素	清楚了解危害网络安全的各种因素，并能举例说明危害后果	了解危害网络安全的因素，能够说明病毒、黑客攻击的危害性	对危害网络安全的因素不清楚
网络安全基本要求	准确说明网络安全内容的 3 个方面、5 种特性和安全控制的 4 个层次	简单或部分说明网络安全内容的 3 个方面、5 种特性和安全控制的 4 个层次	对网络安全的基本要求不清楚
网络安全定义	准确说明不同用户定义的网络安全	简单说明网络安全的定义	不清楚网络安全的基本定义
网络安全形势	清楚了解网络安全形势，能说明当前存在的网络安全问题	了解网络安全形势，能说明当前存在的主要安全问题	不能说明当前的网络安全问题
网络安全产品	了解安全产品分类，能说出常用的安全产品	能说出常用的安全产品	不知道有哪些常用安全产品
网络安全保障体系	了解网络安全保护模型，能够说明安全保护体系的基本组成	能够说明安全保护体系的基本组成	不清楚网络安全保护体系的内容

习题 1

1．单项选择题

（1）网络安全系统本身的缺陷是诱发危害网络安全事件的_____原因。

A．主要　　B．次要　　C．部分　　D．全部

（2）计算机网络系统的管理日趋_____。

A．简单化　　B．复杂化　　C．程序化　　D．规范化

（3）公共信息受众理解的网络安全是过滤一切_____，享受信息带来的便利和快乐。

A．垃圾信息　　B．无用信息　　C．有害信息　　D．错误信息

（4）网络安全产品研发正处于_____的阶段。

A．起步　　B．快速发展　　C．过渡　　D．稳定发展

（5）小型或个人网络安全产品会_____。

A．越来越多　　B．逐渐消失

C．逐步整合　　D．被大型产品取代

（6）IATF 定义的 4 个主要的技术关注层次，不包括_____。

A．网络基础设施　　B．管理策略

C．网络边界　　D．计算环境

2．多项选择题

（1）危害网络安全的表现形式有_____。

A．自然灾害　　B．人为破坏

C．工作失误　　D．病毒侵袭

（2）网络安全主要涉及以下哪些方面？_____

A．信息存储安全　　B．信息传输安全

C．信息应用安全　　D．信息管理安全

（3）网络安全涉及技术问题，也涉及_____问题。

A．管理问题　　B．法律学

C．犯罪学　　D．心理学

（4）网络用户需要的安全是指他们借助计算机网络处理信息时，不会出现_____和_____。

A．非授权访问　　B．干扰

C．信息丢失　　D．破坏

（5）目前用于保护网络安全的产品主要有_____。

A．防毒杀毒产品　　B．防火墙

C．入侵检测　　D．访问控制产品

（6）PDR 模型认为安全体系应包括_____3 个方面。

A．防护　　B．检测　　C．恢复　　D．响应

3．判断题

（1）计算机信息系统本身的脆弱性不是诱发危害网络安全事件的根本原因。（　）

（2）信息领域的危害仅指利用信息对社会产生危害。（　）

（3）信息安全是指信息不会被故意地或偶然地非法授权泄露、更改、破坏。（　）

（4）人类长期形成的道德观念与计算机技术不协调，也是诱发危害网络安全的一个原因。（　）

（5）根据网络层次考虑设置安全保护体系，也需要将网络安全保障体系分成几个层面。（　）

（6）网络安全标准体系是网络安全保障体系中重要的技术体系。（　）

4．简答题

（1）危害网络安全的形式有哪些？

（2）为什么说计算机信息系统本身的脆弱性是诱发危害网络安全的根本原因？

（3）怎么理解危害网络安全活动的低风险？

（4）建立网络安全标准体系的意义是什么？

（5）简述网络安全产品的发展方向。

（6）网络安全模型的作用是什么？

5．实训

（1）利用已掌握的网络安全知识，简单分析自己的网络行为可能出现的安全问题，提出需要防护的基本内容、必须采取的措施和使用的防护产品。

（2）根据房屋防盗经验，分析网络安全防护的特殊性。

（3）收集危害网络安全案例，反思出现问题的原因，写出学习心得。