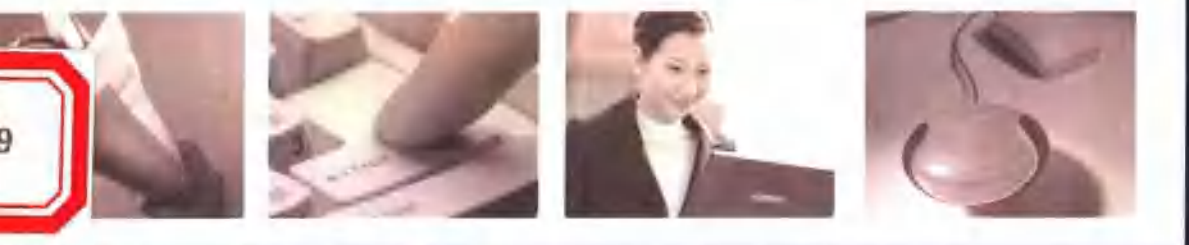
高等职业教育教材丛书

GAODENG ZHIYE
JIAOYU JIAOCAI CONGSHU

计算机安全概论

习题与指导

边奠英　主编
焦树海　李勤　编著



高等职业教育教材丛书

计算机安全概论
习题与指导

边奠英　主编

焦树海　李　勤　编著

南开大学出版社

天　津

内容提要

本书是与《计算机安全概论》一书配套的辅导教材。本书共分2编，每编7章，分别对计算机安全与评估的一般知识、物理防护、访问控制、加密技术（包括数据加密与压缩技术和软件加密技术）、防病毒技术、防火墙和计算机安全教育与立法的相关知识点、考点给予解答，并配有相应练习题和模拟试卷。

本书可作为高职、高专院校计算机专业学生的自学教材，也可供该课程的命题人员参考。

图书在版编目(CIP)数据

计算机安全概论习题与指导 / 焦树海，李勤编著.
天津：南开大学出版社，2003.8
（高等职业教育教材丛书 / 边奠英主编）
ISBN 7-310-01933-4

Ⅰ.计… Ⅱ.①焦…②李… Ⅲ.电子计算机－安全技术－高等学校：技术学校－教学参考资料
Ⅳ.TP309

中国版本图书馆CIP数据核字(2003)第041249号

出版发行 南开大学出版社
地址：天津市南开区卫津路94号 邮编：300071
营销部电话：(022)23508339 23500755
营销部传真：(022)23508542
邮购部电话：(022)23502200
出版人 肖占鹏
承 印 南开大学印刷厂印刷
经 销 全国各地新华书店
版 次 2003年8月第1版
印 次 2003年8月第1次印刷
开 本 787mm×1092mm 1/16
印 张 8.75
字 数 218千字
印 数 1—5000
定 价 13.00元

序

中国要振兴，归根到底，要靠我们中国人自己的努力奋斗、开拓进取，要靠我们的全体劳动者创造出数十倍于今天的劳动生产率。这是一个全体国民素质不断提高的过程，人们自然要寄希望于教育。

我国高等职业教育的目的是为生产、管理、服务第一线培养具有综合职业能力和全面素质的高级实用型人才。我们要努力造就一大批能将科学技术转化为生产力的高级技术应用型人才，能完成从方案设计到产品转化的高级专门人才，能把决策意图贯彻到实际工作中去的一线管理人才和具有特定专门业务知识的智能型操作人才。

要搞好高等职业教育，有很多事情要做，其中重要的一件就是教材建设。高等职业教育的教材建设，可分为两种体系：

一种是传授基础理论知识的教材体系。这种教材的内容，要从职业分析入手，根据特定的职业岗位群所需的知识结构并兼顾长远需要来确定，按照“必需、够用”的原则，构筑具有高职特色的理论知识体系。我们已经组织编写并由南开大学出版社出版的计算机技术与应用系列教材，就属于这一种体系的教材。

另一种是训练职业动手能力的实践技能教材体系。这种教材的内容，要根据教学计划的安排和专业课程内容的进程需要，作相应的确定。我们这次组织编写出版的实习指导教材就属于这一种教材。这种教材是以能力培养为中心，贯穿于整个教学活动的始终，依据专业的特色和课程的要求，给予具体化、定量化、规范化和系统化，成为能力训练的新型教材体系。

以上两种教材相互配合，互为表里。

我国高等职业教育的教材建设还刚刚起步，特别是以能力培养为中心的实训教材，在内容选择、层次安排以及广度、深度等方面，难免存在不足之处，敬请读者不吝指教。

主编谨识

2002.12

前 言

随着计算机及计算机网络在社会各个领域的广泛应用以及互联网上业务的增加，以计算机为核心的信息系统的安全运行和保密问题越来越突出。

科技是把双刃剑，它使人们在享受计算机系统带来的方便和迅捷的同时，也常常为计算机系统所固有的脆弱性付出惨痛的代价。1988 年 11 月爆发的“蠕虫”事件，直接经济损失近亿美元。2000 年 2 月 7 日发生的黑客攻击互联网著名网站事件，使网络的安全问题受到了空前的关注。

计算机安全的研究内容随着计算机系统价值的变化而变化，从实体安全向着信息安全发展，同时由于计算机系统的特殊性，又使得计算机安全的研究必须综合考虑各种安全措施，进行综合防护，因此本书是以信息安全为核心进行防护设计的。

目前计算机安全学正处于发展阶段，而对计算机安全的深入研究将涉及计算机很多方面的深层次知识，对于这些知识的普及有助于提高计算机系统的安全性，但同时也可能给计算机犯罪提供手段，所以大众化的计算机安全教育应着重于安全防护的一般常识和提高安全防护意识，并促使计算机使用者接受法律和道德的约束。

本书对教材中的一些问题作了进一步论述，对一些问题的解答应以本书为准。由于作者水平所限，本书存在的不当甚至错误之处，敬请读者批评指正。

本书共分 2 编，每编分 7 章，第 1~4 章及综合模拟试题由焦树海编写，第 5~7 章由李勤编写，全书统稿由焦树海完成。本书最后由边奠英教授审定。

编者

2002．12

目 录

第一编　课程基本要求

第一章　计算机安全概述

1.1　本章知识点

1．计算机安全方面的历史事件及其危害

有关事件发生的时间、地点和危害。

了解计算机犯罪所造成的经济损失。

2．计算机系统的脆弱性和面临的威胁

计算机犯罪、黑客、有害程序、后门、漏洞。

要求能够默写黑客、有害程序、后门等概念的定义以及计算机犯罪的一般行为。

黑客行为的利与弊，黑客行为与计算机犯罪的区别，后门与漏洞的区别。

要求能够对以上三个问题给以理解并能够结合实际给以简单论述。如“黑客行为与计算机犯罪的区别”，学生可以从两种行为的目的、方式及后果方面给以论述。

3．计算机系统的安全防范体系

计算机系统的分层保护体系。

要求能够默写计算机系统的分层保护体系各层的名称。

计算机安全防护体系中各层的作用。

要求能够对5个防护层的作用给以简单的论述，并能够对现有的一些防护措施进行归类。

4．计算机系统安全评估的有关标准

《可信计算机系统安全评估准则》的有关内容。

1.2　本章学习重点

1．历史上的计算机安全事件及其危害

（1）1988年11月2日，美国康乃尔大学的研究生罗特·莫里斯编制了一个被称为“蠕虫”(worm)的程序，使美国军方MIL网和APPA网中的6 000台计算机受到感染，甚至欧洲联网的计算机都受到影响，直接经济损失近亿美元。

（2）2000年2月7日，来历不明的黑客对雅虎、电子湾（eBay）、亚马逊、微软网络等多个美国大型互联网络实施连续大规模网络袭击行动，使网络服务无法进行，造成服务中断

数小时。

（3）1991年在海湾战争中，美国国家安全局研制出一种AF/91的计算机病毒，侵入到伊军的计算机网，使伊军的指挥系统失灵，削弱了伊军战斗力。

2．计算机系统的脆弱性或弱点

（1）易受环境影响。

（2）数据容易被偷窃。

（3）数据可以无痕迹地涂改。

（4）软、硬件设计上存在漏洞。

3．漏洞

漏洞是计算机系统硬件、软件或策略上的缺陷。

4．计算机系统面临的威胁

（1）计算机犯罪。

（2）黑客。

（3）有害程序。

（4）后门。

5．计算机犯罪的一般行为

（1）修改程序或数据。

（2）扩大授权。

（3）释放有害程序。

（4）释放有害数据。

6．有害程序

破坏计算机系统安全的程序或代码，如计算机病毒、特洛伊木马、蠕虫、逻辑炸弹等。

7．有害数据

含有色情、暴力的文字、图片及影视制品，非法言论、虚假广告和无意义的垃圾数据等。有害数据不仅可能诱导人们的不良行为，还可能使计算机系统瘫痪。

8．黑客

黑客是指那些对任何操作系统神秘而深奥的工作方式由衷地充满兴趣的人。黑客通常是些程序员，他们同时掌握有操作系统和编程语言方面的高级知识。他们善于发现那些被公众广泛使用的软件中的问题。

9．后门

后门是软、硬件制造者为了进行非授权访问而在程序中故意设置的万能访问口令。

10．黑客行为的利与弊

利：黑客善于发现那些被公众广泛使用的软件中的问题，这对改进软件十分有利。没有这些研究系统漏洞的黑客，就不会有今天相对安全的的网络。

弊：他们针对一些系统的漏洞制作了“简单易用”的黑客软件在因特网上发布，使得一些对系统没有深入研究的普通用户，也能轻松地使用他们制作的黑客软件进行妨碍网络安全的活动。

11．后门与漏洞的区别

漏洞是计算机系统硬件、软件或策略上的缺陷，是难以预知的或不可避免的（如在安全与方便上的一种权衡之策）。后门是软、硬件制造者为了进行非授权访问而在程序中故意设置的万能访问口令（或机制），是属于一种人为的故意行为，是可以避免的。

12. 计算机信息系统的安全防护体系

（1）法律、管理、伦理道德教育。

（2）物理防护。

（3）访问控制。

（4）加密技术。

（5）防病毒技术。

13. 法律、管理、伦理道德教育在计算机系统安全方面的作用

对计算机安全构成威胁的第一因素是人，对人的有效约束应该是计算机系统安全的第一策略。

对计算机犯罪定罪、量刑产生的威慑力可使有犯罪企图的人产生畏惧心理，从而减少犯罪的可能，相对地提高了计算机系统的安全性。

加强计算机安全管理，如制定人员管理制度，加强人员审查；在组织管理上，避免单独作业，操作与设计分离等。这些强制执行的制度限制了作案的可能性。

在法律和管理鞭长莫及的情况下，如目前互联网上的随意攻击和虚拟世界中的种种欺骗，有很多是不道德的行为。加强道德伦理教育，靠道德的约束来净化网络世界，对计算机系统的安全也是很重要的。

14. 物理防护在计算机系统安全方面的作用

物理防护主要是针对计算机硬件上的弱点进行防护，防止人为的或自然的因素造成计算机系统的损坏和丢失，防护措施包括：

（1）防止计算机设备丢失。

（2）阻止非授权人员和破坏者进入计算机的工作环境。

（3）规划对外通信的出口，阻止非法接线。

（4）防止设备或数据损坏。

（5）防止电磁辐射。

15. 访问控制在计算机系统安全方面的作用

访问控制可以防止未授权的用户非法使用系统资源，这种服务不仅可以提供给单个用户，也可以提供给用户组的所有用户。访问控制是通过对访问者的有关信息进行检查来限制或禁止访问者使用资源的技术，分为低层访问控制和高层访问控制。高层访问控制包括身份检查和权限确认，是通过对用户口令、用户权限、资源属性的检查和对比来实现的，很多大型软件都具有这样的资源管理系统，如 UNIX、Windows NT 的访问控制机制。低层访问控制是通过对通信协议中的某些特征信息的识别、判断，来禁止或允许用户访问的措施。如在路由器上设置过滤规则进行数据包过滤，就属于低层访问控制。

16. 加密技术在计算机系统安全方面的作用

加密技术包括数据加密和软件加密，它可以防止数据在被窃取或截获之后，不会暴露其中的信息或被非授权者使用。

数据加密是实现数据通信的必要条件。数据加密不仅能够保护信息不暴露，而且具有信息认证的功能，使收到信息的人能够确认信息没有被篡改，使发出信息的人无法抵赖，这一点在电子商务活动中尤为重要。此外，数据加密使信息的传播限定在掌握密钥的群体中，即便是在互联网上，不知密钥的人也会被排斥在这一加密信息网之外，对于某一特定的信息，Internet 只对掌握密钥的人透明，这就好像一个局域网或专用网。

软件加密可以对程序的运行实行加密保护，可以防止软件被非法复制，防止软件的安全机制被破坏。

17. 防病毒技术在计算机系统安全方面的作用

防病毒技术的作用是阻止有害程序或代码侵入计算机系统，防止计算机病毒对计算机系统的数据安全和运行安全构成威胁。

防病毒技术的作用主要包括：

（1）阻断病毒侵入途径。

（2）病毒检查和清除。

（3）监视程序行为，对有害程序行为给予报警或提示。

18. 计算机安全的含义

计算机安全是指计算机资源的安全，即计算机硬件资源、软件资源、数据与信息资源不受自然和人为的有害因素的威胁和破坏，系统安全可靠地运行并且提供不间断的服务。

19. 计算机安全研究的内容

实体安全——研究计算机设备和通信线路及设施、建筑物、构筑物的安全，预防自然和人为的破坏，研究供电、温度、湿度、清洁度、电磁辐射等对设备安全的影响，探索安全防护和灾害报警措施。

软件安全——研究软件生产、测试和发行的安全机制。包括防盗版、反跟踪技术，安全标准和产权立法等方面的内容。

数据安全——研究数据的完整性、有效性和保密性。包括访问控制技术、存储与备份技术、数据变换技术（加密、解密技术）和防病毒技术。通过口令、权限系统、数字签名、数据备份、病毒监控等保证计算机数据信息免遭破坏、修改、泄漏和窃取。

运行安全——研究各种应急措施，保证系统不间断地、可靠地运行。预防各种突发事件造成系统运行的中断，健全各种应急措施并能够自动地与系统对接，做好断点保护和事件审计，以利于快遭恢复和原因查找，建立防火墙屏蔽各种攻击。

20. 计算机安全评估的意义

计算机系统的安全是相对的、动态的。一个安全的系统是从安全评估到实施安全技术措施，到安全管理，再返回到安全评估，再实施安全技术措施和安全管理的循环往复过程。没有一劳永逸的安全措施，只有在不断评估、改进的动态过程中，才能保持一个安全的系统运行。对计算机系统的安全性进行评估，必要时对系统的安全活动进行检查、审计来确定它的可靠程度，以发现系统存在的薄弱环节，杜绝不安全的因素，是每个重要的计算机系统必须要进行的安全防护工作。

21. 可信计算机系统评估准则(TCSEC)包括的安全等级

准则将计算机系统确定为可信任的 D、C、B、A 四类和 D、C1、C2、B1、B2、B3、A1 七

个等级。其中 D 级安全级别最低，A1 级安全级别最高。

22. 可信计算机系统评估准则(TCSEC)的评估内容

从低到高（D→A1）每一级都包含四个方面的评估内容：安全策略、责任、保障和文档。

23. DOS,Windows 9x,Windows NT,UNIX,NetWare 的安全级别

DOS 的安全级别为 D 级。

Windows 9x 的安全级别介于 D 级和 C1 级。

Windows NT,UNIX,NetWare 的安全级别为 C1 级和 C1 级以上。

1.3 本章主要难点

1. 计算机犯罪与黑客行为的区别

计算机犯罪与黑客行为经常被一些媒体混为一谈，实际上两者有着本质区别。

从行为目的上看，计算机犯罪是利用计算机系统获取非法利益或故意破坏计算机系统安全，黑客的目的主要是查找系统上的漏洞，或向系统的安全体系提出挑战，以显示他们的才华或能力。从行为方式上看，黑客主要是通过网络“软进入”侵入系统，不会突破物理防护体系，即不会割破电线或跳窗而入，而计算机犯罪则会不择手段。从行为后最看，黑客行为有有利的一面，而计算机犯罪则百害而无一利。

2. 真假黑客的区别

由于一些媒体的报道或传言，人们常常将使用黑客工具进行攻击的人误认为是黑客，因此对黑客的理解要紧紧把握书中的定义。真黑客具有编程语言和操作系统方面的精深知识，其行为目的是寻找计算机系统漏洞。假黑客主要是利用黑客工具进行捣乱，没有太高的技术手段。

3. 可信计算机系统评估准则

此部分内容参考资料较少，较难理解，在大纲中属于一般考核内容，学员掌握以下内容即可。

（1）安全策略

指主体（人或程序）对客体（文档或设备）的访问形式。对数据的完整性、机密性和可用性做出规划和要求。

（2）责任

责任是一种能够对安全事故进行审计的机制。一个可信系统应将与安全有关的事件记录在一个审计日志中。审计信息必须妥善地保存，以防未经授机修改和损坏。

（3）保障

保障是实现安全策略和责任的安全机制。这些机制可嵌入操作系统之内，并用秘密的方法执行指定的任务。对这些安全机制必须能连续地提供保护，以对抗未授权的篡改。这部分要求不会出现绕过安全特性以及脱离安全策略和责任控制的操作。

（4）文档

为操作者、用户、维修人员和系统管理员等提供用户指南、可信设备手册、测试文件、设计文件等相应的文档。

(5) D→A1 级的主要特点

D 级(最小保护)

D 类操作系统是最不安全的。它没有识别键盘操作人员的功能。D 类系统对访问文件只有很少的或完全没有控制功能。安全测量失败的操作系统均划入 D 类系统。典型的例子是 MS-DOS 操作系统。由于在安装时许多安全特性未起作用，许多未通过测试的网络操作系统版本也列入了 D 类。

C1 级(自主安全保护)

符合 C1 级要求的操作系统可提供自主的安全防护功能，包括用户鉴别、访问控制、系统完整性、安全测试和完整的系统文件等。该级要求用户注册时必须向操作系统申请并经鉴别、确认后方可进入系统，对文件进行访问。“自主的”访问控制允许文件编写者本人修改，而对其他用户，只允许文件打开、使用和删除。由于提供了用户和数据分离的功能，用户可避免数据被另一用户读、改或破坏。这是通过文件正确性、属性和允许设置来实现的。总之，这一级中，要求访问是在需要知道用户名和密码的基础上进行的。满足这一级要求的操作系统有著名的 UNIX 和 NetWare 等。

C 2 级(访问受控的保护)

C2 级要求提供访问受控的安全防护。符合该级要求的操作系统不仅具有 C1 级操作系统的全部防护功能，而且可通过注册过程、资源隔离（对不同的用户分配不同的资源）等措施，来限制执行一些命令。此外，还要求审查与安全有关的事件，即具有审计功能。审计主要是保存所有安全事件的记录，如系统管理员进行的各种活动等，审计要求附加鉴别。访问受控的保护主要增加了审计和附加鉴别功能。

访问控制：细化到可在单个主体(或客体)之间进行。

审计功能：可以跟踪记录所选的事件。

监督功能：发现可疑事件及时通知系统管理员。

加密功能：可依用户的要求进行加密处理。

附加功能：可以采用软件包附加到系统中（打补丁），提高安全性。

经改进，VMS V4.3 版本的安全性已达到 C 2 级的要求。此外，NetWare 3.37 版本的安全性也已达到 C 2 级的要求。

B 类(强制性保护)

B 类操作系统开始丢掉了与用户友好的界面特性。它必须具备 C 类全部的安全特性，同时还应对所有命名的主体和命名的客体实施强制性的访问控制。用户文件和程序必须被确认并分配相应的安全级，这个过程称为标号。所有输入、输出数据必须有标号。标号的完整性和用标号来执行强制性访问控制是这类保护的主要要求。此外，要求开发者提供安全策略模型，根据此模型对系统提出一系列安全要求，同时还应提供安全技术规范说明等。

该类保护对审计有更高的要求，审计必须记录：

- 所有删除记录；
- 操作人员的全部活动；
- 系统管理员的全部活动；
- 失败的注册；

• 辅助设备的使用；

• 所有打开的文件。

UNIX 作为早期的操作系统，虽然有安全性设计，但安全缺陷很多。经多年改进，特别是通过重写的 UNIX 内核，提供了 B 级安全机制，许多安全功能已达到 B2 级要求。

B 类分为 B1、B2、B3 三个等级，其中 B1 级为有标号的保护，B2 级为结构化保护，B3 级为安全域保护。每级除要求具有上一级所要求的全部特征外，还要满足本级的额外要求。

A1 级(验证设计保护)

A1 级在功能上与 B3 级相同，没有增加任何有关策略或结构特征的要求。本等级的显著特点是用形式化顶层规范说明(FTLS)和验证技术来进行分析，以确保系统安全要求的实现。

1.4 本章主要考点

1. 填空、选择、判断

识记：(下划线部分)

(1) 1988 年 11 月 2 日，美国康乃尔大学的研究生罗特·莫里斯编制了一个被称为“蠕虫”(worm)的程序，使美国军方 MIL 网和 APPA 网中的 6 000 台计算机受到感染，甚至欧洲联网的计算机都受到影响，直接经济损失近亿美元。

(2) 计算机系统的脆弱性或弱点

① 易受环境影响。

② 数据容易被偷窃。

③ 数据可以无痕迹地涂改。

④ 软、硬件设计上存在漏洞。

(3) 计算机犯罪的一般行为

① 修改程序或数据。

② 扩大授权。

③ 释放有害程序。

④ 释放有害数据。

(4) 计算机系统面临的威胁

① 计算机犯罪。

② 黑客。

③ 有害程序。

④ 后门。

⑤ 信息对抗战（此条暂不列入考核）。

(5) 有害程序

破坏计算机系统安全的程序或代码，如计算机病毒、特洛伊木马、蠕虫、逻辑炸弹等。

(6) 有害数据

含有色情、暴力的文字、图片及影视制品，非法言论、虚假广告和无意义的垃圾数据等。

(7) 计算机信息系统的安全防护体系包括的方面

① 法律、管理、伦理道德教育。

② 物理防护。

③ 访问控制。

④ 加密技术。

⑤ 防病毒技术。

（8）可信计算机系统评估准则(TCSEC)包括的安全等级

准则将计算机系统确定为可信任的D、C、B、A四类和D、C1、C2、B1、B2、B3、A1七个等级。其中D级安全级别最低，A1级安全级别最高。

（9）可信计算机系统评估准则(TCSEC)包括的评估内容

从低到高（D→A1）每一级都包含四个方面的评估内容：安全策略、责任、保障、文档。

（10）DOS,Windows 9x,Windows NT,UNIX,NetWare的安全级别

DOS的安全级别为D级。

Windows 9x的安全级别介于D级和C1级。

Windows NT,UNIX,NetWare的安全级别为C1级和C1级以上。

2. 概念与简答题

理解：

（1）漏洞。

（2）黑客。

（3）后门。

（4）黑客行为的利与弊。

（5）后门与漏洞的区别。

（6）法律、管理、伦理道德教育在计算机系统安全方面的作用。

（7）物理防护在计算机系统安全方面的作用。

（8）访问控制在计算机系统安全方面的作用。

（9）加密技术在计算机系统安全方面的作用。

（10）防病毒技术在计算机系统安全方面的作用。

（11）计算机安全的含义。

（12）计算机安全研究的内容。

（13）计算机安全评估的意义。

第二章　物理防护

2.1　本章知识点

1．物理环境的防护

物理环境安全的因素：

（1）计算机机房场地的安全要求。

（2）证章与钥匙的管理。

（3）机房禁带物品。

（4）防盗设备。

（5）空调系统的作用（温度、湿度、洁净度的影响）。

（6）防静电措施。

（7）计算机场地的防火（防火措施、灭火器的选择、管理措施）。

2．电源

掌握工作原理，性能指标，连接方法。电源对计算机系统安全的影响，理解超载，电源线干扰对计算机系统的影响，能够根据要求对电源系统进行设计。

电源线干扰：

（1）中断。

（2）异常状态。

（3）电压瞬变。

（4）冲击。

（5）噪声。

（6）突然失效事件。

电源保护装置：

（1）金属氧化物可变电阻(MOV)。

（2）硅雪崩二极管(SAZD)。

（3）气体放电管(GDT)。

（4）滤波器。

（5）电压调整变压器(VRT)。

（6）不间断电源(UPS)。

3．硬件保护

计算机设备的安全设置：

（1）计算机加锁。对控制线路加锁或开关，如键盘锁，软盘读写口等。

（2）专门的信息保护卡。设置保护电路，如加密狗和硬盘保护卡等。

（3）用界限寄存器对内存单元进行保护。

计算机外设的安全、数据备份：

（1）打印机。

（2）磁盘阵列。

（3）计算机终端。

（4）备份方式：静态备份（离线备份）和热备份（在线备份）。

（5）备份介质：纸带，磁带，磁盘，光盘等。

（6）保存方式：现场保存（on site），异地保存（off site）。

（7）电磁辐射对计算机系统安全的影响及防护措施（电磁泄漏，电磁干扰，电磁屏蔽）。

2.2 本章学习重点

1．机房进出人员的控制

机房进出人员的控制措施：警卫、锁、电子识别系统。

鉴别访问者的依据：

（1）访问者的特征——这个人是谁？

根据这个人的身份特征，通过观察、听、签字鉴别等进行识别，或与已保存的物理特征(如指纹等)相比较进行识别。

（2）访问者知道的事——这个人知道什么？

根据口令或密码授权访问。

（3）访问者持有的物品——这个人拥有什么？

根据拥有的钥匙、智能卡、证章或其他访问控制物品授权访问。

2．计算机机房场地的安全要求

（1）易于出入管理，以便对进出的人员和物品进行监控。

（2）远离公共场所，使攻击者不容易接近。

（3）选择适当的楼层，减少自然原因的影响和侵入的可能。

（4）在进出口设置接待室。

（5）电梯和楼梯应设计成不能直接进入机房。

（6）建筑物周围应有足够亮度的照明设施和防止非法进入的设施。

（7）外部容易接近的进出口，如风道口、排风口、窗户、应急门等应有栅栏或监视控制措施，而周边应有物理屏障(隔墙、带刺铁丝网等)和监视报警系统。窗口应采取防范措施，必要时加装自动报警设备。

（8）机房进出口须设置应急电话。

（9）机房供电系统应设计成动力照明用电与计算机系统供电线路分开，机房及疏散通道应配备应急照明装置。

3．证章与钥匙的管理

（1）定期更换，以防丢失或私配钥匙带来的安全隐患。

（2）关键部位的钥匙只能由专人管理，或使用多人共同打开的锁具。