

NTCo.ORG.CN

工业和信息化部全国网络与信息技术培训考试项目(NTC)指定教材

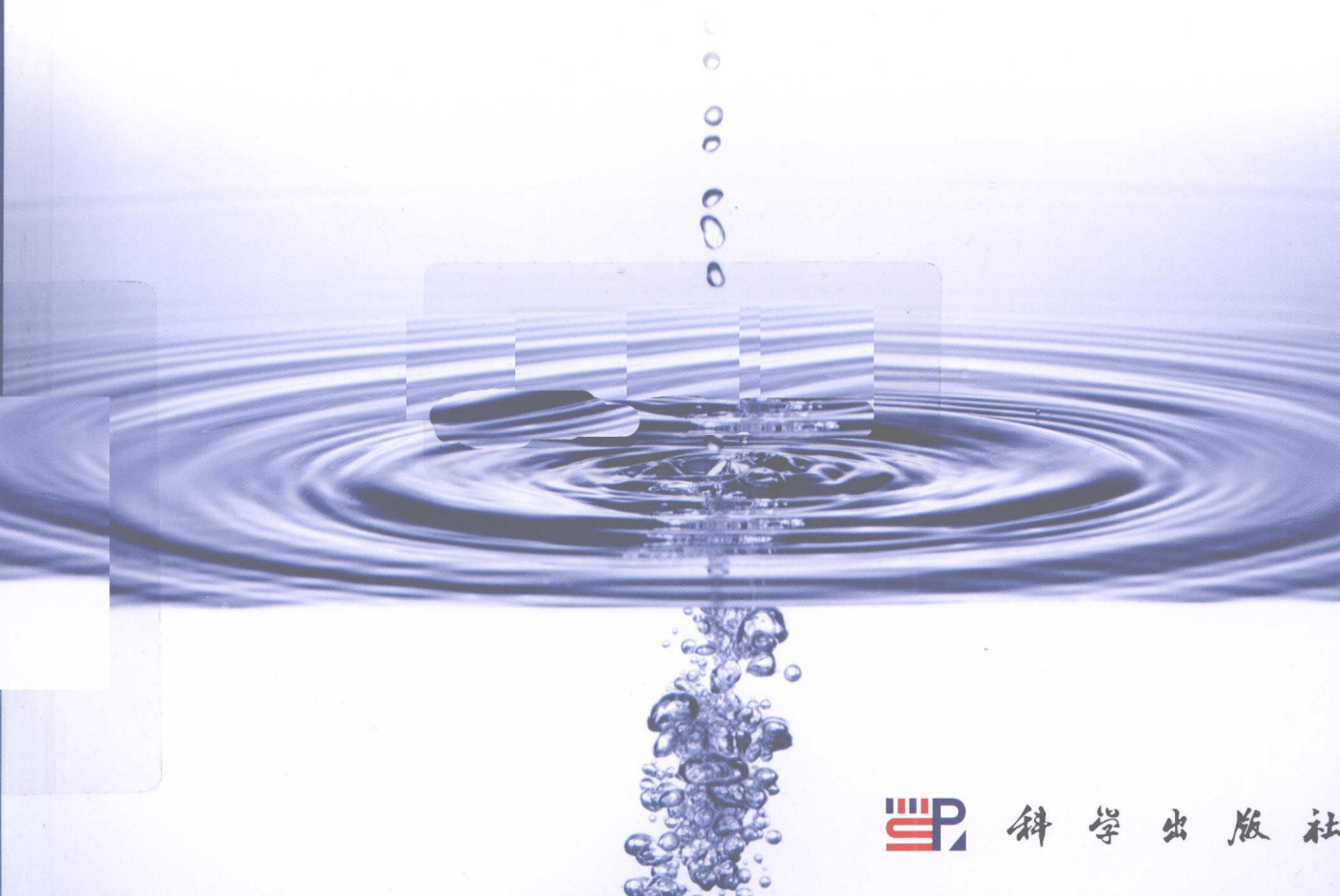
网络与信息安全专业指定教材

Network
and
information
security



网络与信息安全

胡铮 主编



科学出版社

工业和信息化部全国网络与信息技术培训考试项目（NTC）
网络与信息安全专业指定教材

网络与信息安全

胡 铮 主编

科学出版社

北 京

内 容 简 介

本书是工业和信息化部全国网络与信息技术培训考试项目(NTC)网络与信息安全专业指定教材。网络与信息安全是一门涉及计算机科学、网络技术、网络安全技术、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科学。网络与信息安全问题在许多国家已经引起了普遍关注,成为当今信息技术的一个重要研究课题。本书利用通俗易懂的语言阐述了网络所涉及的安全问题,主要内容包括第1篇(事前预防)、第2篇(事中监测与治理)和第3篇(事后恢复)三个部分。第1篇内容包括网络安全概述、操作系统安全常识、病毒知识介绍、数据安全技术和网络安全法律法规;第2篇内容包括防火墙技术、黑客攻击与入侵检测、虚拟专用网、网络通信安全和Web的安全;第3篇内容包括数据备份技术和安全恢复技术。

本书不仅适合各类院校及培训机构学生使用,同时也适合于任何对网络与信息安全感兴趣的读者。

图书在版编目(CIP)数据

网络与信息安全/胡铮主编. —北京:科学出版社, 2011

(工业和信息化部全国网络与信息技术培训考试项目(NTC)·网络与信息安全专业指定教材)

ISBN 978-7-03-030626-5

I. ①网… II. ①胡… III. ①计算机网络-计算机安全-教材
IV. ①TP 393.08

中国版本图书馆CIP数据核字(2011)第049125号

责任编辑:赵丽欣 陈晓萍 / 责任校对:刘玉靖
责任印制:吕春珉 / 封面设计:东方人华平面设计部

科学出版社出版

北京东黄城根北街16号

邮政编码 100717

<http://www.sciencep.com>

铭浩彩色印装有限公司印刷

科学出版社发行 各地新华书店经销

*

2011年6月第一版 开本:787×1092 1/16

2011年6月第一次印刷 印张:18

印数:1—3 000 字数:429 000

定价:32.00元

(如有印装质量问题,我社负责调换<骏杰>)

销售部电话 010-62142126 编辑部电话 010-62135517-8003

版权所有,侵权必究

举报电话:010-64030229; 010-64034315; 13501151303

编 委 会

- 编委会主任：**洪京一 工业和信息化部中国电子信息产业发展研究院党委书记
- 主 编：**胡 铮 全国网络与信息技术培训考试管理中心（NTC-MC）主任
全国网游动漫学院项目管理办公室（GCC-MO）主任
工业和信息化部中国电子信息产业发展研究院培训中心副主任
- 副 主 编：**林 鹏 国家计算机网络应急技术处理协调中心科技委副主任、教授级高工
孙蔚敏 工业和信息化部信息中心 副主任
- 编 委：**刘占山 滕 伟 马 亮 童晓民 陈 耿 王连宝 温安顺 苏 红
谢赞福 高俊文 顾巧论 甘 宏 张慧丽 彭英慧 申莉莉 蔡振山

前 言

互联网的迅猛发展已经深刻地影响到国家的政治、经济、军事、文化等各个领域，与此同时，互联网的开放性和安全漏洞所带来的安全风险也给互联网的健康发展带来了不可忽视的影响。网络与信息安全问题不仅给相关单位及网民带来不便，而且已经威胁到国家的信息安全和经济发展。

随着信息化在我国不断深入和发展，信息技术和网络给社会的经济、科教、文化和管理等各个方面注入了新的活力，对信息化人才的培养与评估不断提出新的要求。建立一个技术领先、既广泛涉及多厂商产品又保持内容中立的政府认证品牌成为我国信息化发展的当务之急。

为深入贯彻落实科学发展观，坚持走中国特色新型工业化道路，加快通信技术产业的发展和应用，同时为贯彻落实国家关于网络与信息技术发展及加强职业教育工作的指示精神，促进我国此类技术领域人才建设，工业和信息化部有关部门推出了全国网络与信息技术培训考试项目（NTC），网络与信息安全项目是 NTC 的子项目及组成部分。

NTC 项目是由工业和信息化部中国电子信息产业发展研究院与工业和信息化部通信行业职业技能鉴定指导中心联合共建。NTC 项目由全国网络与信息技术培训考试管理中心（NTC-MC）负责管理及运营，同时由国信高新技术培训中心（工业和信息化部有关部门批准设立的信息技术及游戏动漫培训考试机构）负责具体的运营工作，项目面向社会、各类院校、相关行业等，培养应用型、管理型信息技术复合型人才。学员考核通过后颁发工业和信息化部职业技能水平证书，作为职业技能水平的凭证及从事相关岗位的任职依据。

由于信息技术发展迅速，网络安全的相关技术在不断推陈出新，本书将从网络安全的事前预防（第 1 篇）、事中监测与治理（第 2 篇）和事后恢复（第 3 篇）三个层面，采用通俗易懂的语言，对网络与网络安全的各个方面进行阐述。

第 1 篇内容主要是对网络安全相关知识的介绍，包括网络安全概述、操作系统安全常识、病毒知识介绍、数据安全技术和网络安全法律法规；第 2 篇内容主要是关于网络运行过程中的相关安全技术，包括防火墙技术、黑客攻击与入侵检测、虚拟专用网、网络通信安全和 Web 的安全；第 3 篇内容主要是关于在网络安全事故发生后如何恢复的技术，包括数据备份技术和安全恢复技术。具体内容如下：

第 1 章是网络安全概述，包括网络安全简介、网络安全面临的威胁、网络出现安全威胁的原因、网络安全机制。

第 2 章是操作系统安全常识，包括安全等级标准、漏洞、Windows Server 2003 系统安全、UNIX 系统安全、Linux 系统安全、Windows XP 系统安全及 Windows 7 系统安全。

第 3 章是病毒知识介绍，包括计算机病毒简介、网络病毒及其防治、典型病毒介绍及常用杀毒软件介绍。

第 4 章是数据安全技术介绍，包括数据加密及数据压缩。

第 5 章是网络安全法律法规，包括与网络有关的法律法规、网络安全管理的有关法

律和其他法律规范。

第 6 章是防火墙技术，包括防火墙简介、防火墙的类型、防火墙配置、防火墙系统、防火墙的选购和使用及防火墙产品介绍。

第 7 章是黑客攻击与入侵检测，包括黑客常用的攻击方法和防范措施、入侵检测响应与追踪。

第 8 章是虚拟专用网，包括 VPN 概述和 VPN 的配置实现。

第 9 章是网络通信安全，包括网络通信的安全性、网络通信存在的安全威胁、调制解调器的安全及 IP 安全。

第 10 章是 Web 的安全，包括 Web 技术简介、Web 的安全需求、Web 服务器安全策略、Web 浏览器安全策略及 Web 站点安全八要素。

第 11 章是数据备份技术，包括数据完整性、容错与网络冗余及网络备份系统。

第 12 章是安全恢复技术，包括网络灾难、安全恢复的条件、安全恢复的实现及安全恢复案例。

本书由胡铮任主编，参与编写人员有林鹏、孙蔚敏、刘占山、滕伟、马亮、童晓民、陈耿、王连宝、温安顺、苏红、谢赞福、高俊文、顾巧论、甘宏、张慧丽、彭英慧、申莉莉、蔡振山等。

在编著本书过程中，我们得到了工业和信息化部中国电子信息产业发展研究院、工业和信息化部通信行业职业技能鉴定指导中心、全国网络与信息技术培训考试管理中心（NTC-MC）、全国网游动漫学院项目管理办公室（GCC-MO）的大力支持，在此一并表示感谢。

在编写本书过程中，我们参考了大量书籍，在此对这些书的编著者表示感谢。

由于编者水平有限，书中错误和疏漏之处在所难免，希望读者和各位专家批评指正。

目 录

第 1 篇 事前预防

第 1 章 网络安全概述	3
1.1 网络安全简介	4
1.1.1 物理安全	4
1.1.2 逻辑安全	5
1.1.3 操作系统安全	5
1.1.4 联网安全	5
1.2 网络安全面临的威胁	6
1.2.1 物理威胁	7
1.2.2 系统漏洞造成的威胁	7
1.2.3 身份鉴别威胁	8
1.2.4 线缆连接威胁	8
1.2.5 有害程序	9
1.3 网络出现安全威胁的原因	9
1.3.1 薄弱的认证环节	9
1.3.2 系统的易被监视性	9
1.3.3 易欺骗性	10
1.3.4 有缺陷的局域网服务和相互信任的主机	10
1.3.5 复杂的设置和控制	11
1.3.6 无法估计主机的安全性	11
1.4 网络安全机制	11
1.4.1 加密机制	11
1.4.2 访问控制机制	11
1.4.3 数据完整性机制	12
1.4.4 数字签名机制	12
1.4.5 交换鉴别机制	12
1.4.6 公证机制	12
1.4.7 流量填充机制	13
1.4.8 路由控制机制	13
小结	13

习题	13
第 2 章 操作系统安全常识	17
2.1 安全等级标准	17
2.1.1 美国的“可信计算机系统评估准则”	18
2.1.2 中国国家标准《计算机信息安全保护等级划分准则》	19
2.2 漏洞	21
2.2.1 漏洞的概念	21
2.2.2 漏洞的类型	21
2.2.3 漏洞对网络安全的影响	22
2.2.4 漏洞与后门的区别	23
2.3 Windows Server 2003 系统安全	23
2.3.1 Windows Server 2003 的安全等级	23
2.3.2 Windows Server 2003 的安全性	24
2.3.3 Windows Server 2003 的安全设置	24
2.4 UNIX 系统的安全	26
2.4.1 UNIX 安全等级	26
2.4.2 UNIX 的安全性	26
2.4.3 UNIX 系统的安全漏洞	27
2.5 Linux 系统安全	28
2.5.1 Linux 安全机制	28
2.5.2 Linux 安全设置	30
2.6 Windows XP 系统安全	30
2.6.1 Windows XP 安全性	30
2.6.2 Windows XP 安全策略	32
2.7 Windows 7 系统安全	36
2.7.1 Windows 7 安全性	36
2.7.2 Windows 7 安全策略	37
小结	40
习题	40
第 3 章 病毒知识介绍	44
3.1 计算机病毒简介	45
3.1.1 病毒的概念	45
3.1.2 病毒的发展史	45
3.1.3 病毒的特点	46
3.1.4 病毒的分类	46
3.1.5 病毒的结构	47

3.1.6 病毒的识别与防治	49
3.2 网络病毒及其防治	52
3.2.1 网络病毒的特点	52
3.2.2 网络病毒的传播	54
3.2.3 网络病毒的防治	54
3.2.4 网络反病毒技术的特点	57
3.2.5 病毒防火墙反病毒的特点	58
3.3 典型病毒介绍	59
3.3.1 宏病毒	59
3.3.2 电子邮件病毒	60
3.3.3 几个病毒实例	62
3.4 常用杀毒软件介绍	65
3.4.1 360 安全卫士	65
3.4.2 瑞星杀毒软件	68
3.4.3 金山毒霸杀毒软件	70
小结	71
习题	71
第 4 章 数据安全技术介绍	74
4.1 数据加密	75
4.1.1 数据加密基本概念	75
4.1.2 数据加密技术	76
4.1.3 典型的对称密码技术——替代密码和换位密码	78
4.1.4 数据加密标准 DES	80
4.1.5 公开密钥密码体制——RSA 算法	86
4.1.6 RSA 算法的应用	87
4.2 数据压缩	88
4.2.1 数据压缩基本概念	88
4.2.2 WinZip 压缩工具的使用	88
4.2.3 WinRAR 简介	92
小结	93
习题	93
第 5 章 网络安全法律法规	96
5.1 与网络有关的法律法规	97
5.1.1 Internet 的不安全形势	97
5.1.2 国际法律法规	97
5.1.3 中国法律法规	104

5.2 网络安全管理的有关法律	105
5.2.1 网络服务业的法律规范	105
5.2.2 网络用户的法律规范	107
5.2.3 互联网信息传播安全管理制度	108
5.3 其他法律规范	109
5.3.1 有关网络有害信息的法律规范	109
5.3.2 电子公告服务的法律管制	110
5.3.3 网上交易的相关法律法规	110
小结	110
习题	111

第 2 篇 事中监测与治理

第 6 章 防火墙技术	115
6.1 防火墙简介	116
6.1.1 防火墙的概念	116
6.1.2 防火墙的功能特点	116
6.1.3 防火墙的安全性设计	117
6.2 防火墙的类型	118
6.2.1 包过滤防火墙	118
6.2.2 代理服务防火墙	119
6.2.3 状态检测防火墙	120
6.3 防火墙配置	121
6.3.1 服务器置于防火墙之内	121
6.3.2 服务器置于防火墙之外	123
6.3.3 服务器置于防火墙之上	123
6.4 防火墙系统	125
6.4.1 屏蔽主机防火墙	125
6.4.2 屏蔽子网防火墙	127
6.5 防火墙的选购和使用	127
6.5.1 防火墙的选购策略	127
6.5.2 防火墙的安装	128
6.5.3 防火墙的维护	129
6.6 防火墙产品介绍	130
6.6.1 Check Point FireWall-1	130
6.6.2 AXENT Raptor	132
6.6.3 CyberGuard FireWall	133

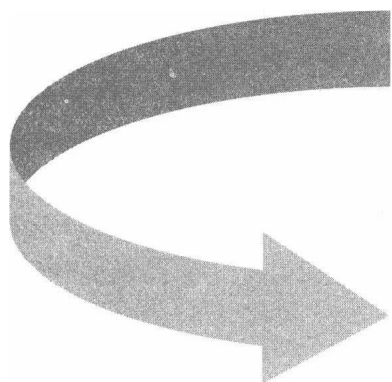
6.6.4 Cisco PIX FireWall 520	133
小结	133
习题	134
第 7 章 黑客攻击与入侵检测	137
7.1 黑客攻击	137
7.1.1 什么是黑客	137
7.1.2 黑客常用的攻击方法和防范措施	140
7.2 入侵检测	146
7.2.1 入侵检测的定义	146
7.2.2 入侵响应	148
7.2.3 入侵追踪	150
7.2.4 入侵检测工具介绍	151
小结	152
习题	152
第 8 章 虚拟专用网	155
8.1 VPN 概述	156
8.1.1 VPN 基本概念	156
8.1.2 VPN 的应用领域	157
8.1.3 VPN 的优缺点	159
8.2 VPN 的配置实现	160
小结	163
习题	163
第 9 章 网络通信安全	165
9.1 网络通信的安全性	166
9.1.1 线路安全	166
9.1.2 不同层的安全	166
9.2 网络通信存在的安全威胁	168
9.2.1 传输过程中的威胁	168
9.2.2 TCP/IP 协议的脆弱性	169
9.3 调制解调器的安全	172
9.3.1 拨号调制解调器访问安全	172
9.3.2 RAS 的安全性概述	173
9.4 IP 安全	173
9.4.1 IPSec 概述	173
9.4.2 IP 和 IPv6	174
9.4.3 IPSec: AH 和 ESP	177
9.4.4 IPSec: IKE	180

小结	182
习题	182
第 10 章 Web 的安全	186
10.1 Web 技术简介	187
10.1.1 Web 服务器	187
10.1.2 Web 浏览器	188
10.1.3 HTTP 协议	188
10.1.4 HTML 语言	188
10.1.5 CGI 公共网关接口	189
10.2 Web 的安全需求	189
10.2.1 Web 的优点与缺点	189
10.2.2 Web 安全风险与体系结构	190
10.2.3 Web 的安全需求	191
10.3 Web 服务器安全策略	192
10.3.1 Web 服务器上的漏洞	192
10.3.2 定制 Web 服务器的安全策略和安全机制	192
10.3.3 认真组织 Web 服务器	193
10.3.4 配置 Web 服务器的安全特性	194
10.3.5 安全管理 Web 服务器	195
10.3.6 Web 服务器的安全措施	195
10.4 Web 浏览器安全策略	197
10.4.1 浏览器自动引发的应用	198
10.4.2 Web 页面或者下载文件中内嵌的恶意代码	198
10.4.3 浏览器本身的漏洞及泄露的敏感信息	199
10.4.4 Web 欺骗	200
10.4.5 Web 浏览器的安全使用	200
10.5 Web 站点安全八要素	201
小结	202
习题	202

第 3 篇 事后恢复

第 11 章 数据备份技术	207
11.1 数据完整性	208
11.1.1 数据完整性概述	208
11.1.2 提高数据完整性的办法	210
11.2 容错与网络冗余	211
11.2.1 容错	211

11.2.2 网络冗余	212
11.3 网络备份系统	214
11.3.1 网络数据备份系统方案需求分析	214
11.3.2 数据库备份的评估	217
11.3.3 数据库备份的类型	219
11.3.4 数据库备份的性能	220
11.3.5 系统和网络完整性	220
11.3.6 数据库的恢复	221
小结	224
习题	224
第 12 章 安全恢复技术	227
12.1 网络灾难	228
12.1.1 灾难定义	228
12.1.2 计算机系统灾难	228
12.1.3 网络灾难	228
12.1.4 灾难预防	228
12.1.5 安全恢复	229
12.1.6 风险评估	229
12.2 安全恢复的条件	229
12.2.1 备份	230
12.2.2 网络备份	231
12.2.3 备份设备	232
12.2.4 备份方式	232
12.3 安全恢复的实现	233
12.3.1 安全恢复方法论	233
12.3.2 安全恢复计划	234
12.4 安全恢复案例	238
12.4.1 Ghost 硬盘还原工具	238
12.4.2 双机热备软件 LEGATO Octopus V4.0 for Windows 简介	242
小结	243
习题	243
附录	246
附录 1 全国网络与信息技术培训考试项目 (简称 NTC 项目) 介绍及实施办法	246
附录 2 全国网游动漫学院项目 (简称 GCC 项目) 介绍及实施办法	254
部分习题解答	261
主要参考文献	274



第 1 篇

事前预防

- 第 1 章 网络安全概述
- 第 2 章 操作系统安全常识
- 第 3 章 病毒知识介绍
- 第 4 章 数据安全技术介绍
- 第 5 章 网络安全法律法规

第 1 章

网络安全概述

知识点

- 网络安全的定义
- 网络面临的安全威胁
- 网络出现安全威胁的原因
- 网络的安全机制

难点

- 网络安全威胁产生的原因

要求

熟练掌握以下内容：

- 网络安全的定义
- 网络面临的各种安全威胁
- 网络的安全机制

了解以下内容：

- 产生网络安全威胁的原因

随着网络技术的不断发展，网络在人们的生活中已经占有一席之地，给人们的生活带来了方便。然而，网络也不是完美无缺的，给人们带来惊喜的同时，也带来了威胁。计算机犯罪、黑客、有害程序和后门等严重威胁着网络的安全。目前，网络安全问题在许多国家已经引起了普遍关注，成为当今网络技术的一个重要研究课题。

1.1 网络安全简介

网络安全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科学。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，确保系统能连续、可靠、正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说，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。

(1) 保密性：信息不泄露给非授权用户。

(2) 完整性：数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

(3) 可用性：可被授权实体访问并按需求使用的特性，即当需要时能否存取所需的信息。例如，网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

(4) 可控性：对信息的传播及内容具有控制能力。网络安全包括物理安全、逻辑安全、操作系统安全、联网安全。

1.1.1 物理安全

物理安全是指用来保护计算机硬件和存储介质的装置和工作程序。物理安全包括多方面的内容。

1. 防盗

像其他的物体一样，计算机也是偷窃者的目标，如盗走光驱、主板等。计算机偷窃行为所造成的损失可能远远超过计算机本身的价值，因此必须采取严格的防范措施，以确保计算机设备不会丢失。

2. 防火

计算机机房发生火灾一般是由于电气原因、人为事故或外部火灾蔓延引起的。电气设备和线路可能因为短路、过载、接触不良、绝缘层破坏或静电等原因引起电打火而导致火灾。人为事故是指由于操作人员不慎、吸烟、乱扔烟头等，使充满易燃物质（如纸片、磁带、胶片等）的机房起火，当然也不排除人为故意放火。外部火灾蔓延是因外部房间或其他建筑物起火而蔓延到机房而引起火灾。

3. 防静电

静电是由物体间的相互摩擦、接触而产生的，计算机显示器也会产生很强的静电。静电产生后，由于未能释放而保留在物体内，会有很高的电位（能量不大），从而产生静电，放电火花，造成火灾；还可能使大规模集成电路损坏，这种损坏可能是不知不觉造成的。