高等院校密码信息安全类专业系列教材
中国密码学会教育工作委员会推荐教材

网络信息安全与对抗

罗森林　王　越　潘丽敏　编著

WANGLUO XINXI
ANQUAN YU DUIKANG

国防工业出版社
National Defense Industry Press

高等院校密码信息安全类专业系列教材
中国密码学会教育工作委员会推荐教材

网络信息安全与对抗

罗森林　王　越　潘丽敏　编著

国防工业出版社
·北京·

内 容 简 介

本书共分6章，主要内容包括信息系统、信息网络的基本概念，工程系统理论，信息安全与对抗的基础理论，网络信息攻击基础技术，网络信息对抗基础技术，信息安全评估与立法，网络对抗系统工程实践等。

本书可作为信息安全、信息对抗技术、计算机应用等相关专业的正式教材，也可供实验选修课程、开放实验课程、专业课程设计以及信息安全对抗相关技术竞赛培训直接使用，同时该教材还可供科研人员参考和有兴趣者自学使用。

图书在版编目(CIP)数据

网络信息安全与对抗 / 罗森林，王越，潘丽敏编著.
—北京：国防工业出版社，2011.10
（高等院校密码信息安全类专业系列教材）
ISBN 978-7-118-07623-3

Ⅰ.①网… Ⅱ.①罗… ②王… ③潘… Ⅲ.①计算机网络-安全技术-高等学校-教材 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 198368 号

※

国防工业出版社出版发行
（北京市海淀区紫竹院南路 23 号 邮政编码 100048）
北京奥鑫印刷厂印刷
新华书店经售
*
开本 787×1092 1/16 印张 18¾ 字数 428 千字
2011 年 10 月第 1 版第 1 次印刷 印数 1—3000 册 定价 38.00 元

（本书如有印装错误，我社负责调换）

国防书店：(010)68428422 发行邮购：(010)68414474
发行传真：(010)68411535 发行业务：(010)68472764

总　序

信息系统所面临的各种安全威胁日益突出，信息安全问题已成为涉及国家政治、军事、经济和文教等诸多领域的战略安全问题。我国政府对网络与信息安全问题高度重视，国办印发的文件《关于网络信任体系建设的若干意见》明确指出了要特别重视网络安全的6方面内容；中办、国办印发的《国家2006年至2020年长期科学发展规划》中也突出了对各种网络安全问题的关注，将建设国家信息安全保障体系列为我国信息化发展的战略重点；国家“十一五”计划中也包含了提升国家信息安全保障服务能力的战略要求。西方发达国家纷纷制订了本国的网络与信息安全战略。比如，美国奥巴马政府正在采取措施加强美国网络战的备战能力，其中一项措施是创建网络战司令部，这表明美国的网络与信息安全战略已经由克林顿时代的“全面防御”、布什时代的“攻防结合”，转到奥巴马时代的“攻击为主，网络威慑”。

当前，制约我国网络与信息安全事业发展的瓶颈之一就是人才极度匮乏，为此，教育部从2001年起，陆续批准了包括北京邮电大学在内的近百所各类高校开设信息安全本科专业。但是，毕竟与其他经典的本科专业相比，信息安全本科专业的建设问题还面临许多挑战，需要全国同行共同努力，早日探索出一条办好信息安全专业的捷径。可喜的是，现在国内若干高校的教授团队都纷纷行动起来，各尽所能在信息安全本科专业建设方面取得了不少业绩。比如，灵创团队（http://www.cleader.net）就是众多热心于信息安全本科专业建设的创新团队，该团队中的“信息安全教学团队”被教育部和财政部批准为“2009年度国家级教学团队”；其完成的成果“信息安全专业规范研究与专业体系建设”获得了国家级教学成果奖二等奖；其带头人也被评为“国家级教学名师”并受到了胡锦涛等党和国家领导人的接见。希望国内能够有更多的类似教学团队投身于信息安全本科专业建设。

由于教材建设是信息安全专业建设的重点和难点之一，中国密码学会教育工作委员会自成立以来就一直致力于推进密码学与信息安全方面的教学和教材建设，比如，与国防工业出版社联合主办了“密码学与信息安全教学研讨会”等一系列研讨活动，并成立“普通高等教育本科密码信息安全类系列教材”编审委员会来组织策划相关系列教材。编审委员会在充分研究信息安全本科专业规范的基础上，经过细致研究，多次反复讨论，规划了与信息安全本科专业规范相配套的本系列教材。

本系列教材参照荣获国家级教学成果奖的信息安全最新专业规范，确定教材题目，组织教材书稿内容。所有教材严格按照“规范”要求，结合信息安全专业的学制、培养规格、素质结构要求、知识结构要求撰写，使其所含知识点完全覆盖“规范”中的要求，确保能够达到“规范”中的学习目标。由于本系列教材涉及的内容比较多，在教材内容选择时，一

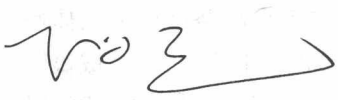
方面要考虑教材内容相互的衔接，另一方面要考虑许多课程相互之间有内容交叉的现象；同时，充分考虑了先进性和成熟性之间的和谐关系，确保教材既能够反映信息安全领域的前沿科研状态，又能使学生掌握基础的核心知识和较成熟稳定的技能；编审委员会多次召开会议，审定教材的大纲，落实教材的主要知识点，避免了内容的重复。

本系列教材的作者都是在我国信息安全领域具有丰富教学和实践经验的一流专家，部分教材已经被评为“普通高等教育‘十一五’国家级规划教材”。

为便于高校教师选用本套教材，我们将为高校教师提供完善的教学服务，免费为选用本套教材的教师提供所有教材的电子教案和部分教材的习题答案。同时我们还提供信息安全专业本科教学实验室建设方案与实验教学指导咨询和信息安全专业本科生实习、实训与技能认证咨询。

本系列教材尽管通过反复讨论修改，但限于作者水平和其他客观条件限制，难免存在不足和值得商榷之处，敬请批评指正。

教授　博士生导师　国家级教学名师
灾备技术国家工程实验室主任
网络与信息攻防教育部重点实验室主任
北京邮电大学信息安全中心主任



2009 年 9 月 30 日星期三

高等院校密码信息安全类专业系列教材
编委会名单

前　言

随着网络技术及其数字化的快速发展和应用，其信息安全问题越来越重要，信息安全意识的提升和基础知识的普及有着极其重要的作用。在技术、管理和人才三要素中人才是核心，信息安全与对抗的竞争归根结底是人才的竞争，信息安全人才的培养有着时代的迫切性、突出性和专业性。

网络是由具有无结构性质的节点与相互作用关系构成的体系，本书基于广义网络空间的安全与对抗问题展开讨论，根据信息对抗技术、信息安全等专业的特点，以及培养高素质专业人才需求而编写，是信息对抗技术、信息安全专业不可缺少且极为重要的教学内容之一。本书从基础理论到技术方法再到工程实践，从顶至下纵向上分为三个层次，第一层次是信息安全与对抗领域的基本原理和方法分析；第二层次是信息安全与对抗领域的基础技术讨论；第三层次是信息安全与对抗技术的工程实践与应用。此外，从横向上教材还融入了信息安全标准、信息安全评估、信息安全管理和信息安全立法等内容。通过本书，可以较为系统、全面地理解和学习信息安全与对抗领域的重要知识点，掌握信息安全对抗的核心概念、原理和方法，从更高层次上认识信息安全对抗的系统工程思想，同时还可以实践信息安全具体技术。

本书共分6章，各章的主要内容安排如下：

第1章是绪论。内容包括信息、信息技术、信息系统、信息网络的基本概念，工程系统理论等。

第2章是网络信息安全与对抗基础理论。内容包括信息安全与对抗的基本概念，信息安全与对抗的历史发展，信息安全问题产生的主要根源，针对信息安全问题的基本对策，信息安全与对抗的基础层原理，信息安全与对抗的系统层原理，信息安全与对抗的系统性方法，信息安全保障体系建设框架等。

第3章是网络信息攻击基础技术。内容包括网络攻击行为过程分析，网络攻击技术分类，安全扫描技术、计算机病毒、特洛伊木马、欺骗攻击技术、缓冲区溢出攻击、拒绝服务攻击等典型信息攻击技术。

第4章是网络信息对抗基础技术。内容包括网络安全防御行为和对抗过程分析，网络安全事件分类技术、实体安全技术、防火墙技术、入侵检测技术、蜜罐技术、身份认证技术、信息加解密技术、物理隔离技术、虚拟专用网技术、灾难恢复技术、无线网络安全技术等典型信息对抗技术。

第5章是信息安全评估与立法。内容包括信息技术安全标准、信息安全管理、信息安全评估、信息安全法律法规等。

第6章是网络对抗系统工程与实践。内容包括信息安全系统工程，数据加密解密实

践系统，防火墙技术实践系统，入侵检测技术实践系统等。

本书由罗森林、王越、潘丽敏共同撰写，其中的实践例程均经过认真的编制和调试（读者可通过邮件直接与作者联系，邮箱地址：luosenlin126@126.com）。本书在编写过程中，还得到了张蕾、陈燕颖、王坤、闫广禄、韩磊、汪俊等同学的帮助，在此一并表示衷心的感谢。同时，衷心感谢国防工业出版社编辑对本书详细、认真的修改和热情帮助，衷心感谢国防工业出版社多方面的支持和帮助。

由于时间所限，加之笔者能力范围的限制，对于书中的不足和错误之处敬请广大读者批评指正，以便使本书日渐完善。

罗森林

2011 年 4 月于北京理工大学

目　录

第1章 绪 论

1.1 信息系统与信息网络

1.1.1 信息、信息技术、信息系统

1. 信息

“信息”一词古已有之。在人类社会早期的日常生活中,人们对信息的认识比较广义而模糊,对信息和消息的含义没有明确界定。到了20世纪尤其是中期以后,随着现代信息技术的飞速发展及其对人类社会的深刻影响,迫使人们开始探讨信息的准确含义。

1928年,哈特雷(L. V. R. Hartley)在《贝尔系统电话杂志》上发表了题为《信息传输》的论文。他在文中将信息理解为选择通信符号的方式,并用选择的自由度来计量这种信息的大小。他注意到,任何通信系统的发送端总有一个字母表(或符号表),发信者发出信息的过程正是按照某种方式从这个符号表中选出一个特定符合序列的过程。假定这个符号表一共有 S 个不同的符号,发信息选定的符号序列一共包含 N 个符号,那么,这个符号表中无疑有 SN 种不同符号的选择方式,也可以形成 S 个长度为 N 的不同序列。这样,就可以把发信者产生信息的过程看作是从 S 个不同的序列中选定一个特定序列的过程,或者说是排除其他序列的过程。然而,用选择的自由度来定义信息存在局限性,主要表现在这样定义的信息没有涉及信息的内容和价值,也未考虑到信息的统计性质;另一方面,将信息理解为选择的方式,就必须有一个选择的主体作为限制条件,因此这样的信息只是一种认识论意义上的信息。

1948年,香农(C. E. Shannon)在《通信的数学理论》一文中,在信息的认识方面取得重大突破,堪称信息论的创始人。香农的贡献主要表现在推导出了信息测度的数学公式和发明了编码的三大定理,为现代通信技术的发展奠定了理论基础。香农发现,通信系统所处理的信息在本质上都是随机的,因此可以运用统计方法进行处理。他指出,一个实际的消息是从可能消息的集合中选择出来的,而选择消息的发信者又是任意的,因此,这种选择就具有随机性,是一种大量重复发生的统计现象。香农对信息的定义同样具有局限性,主要表现在这一概念未能包容信息的内容与价值,只考虑了随机不定性,未能从根本上回答“信息是什么”这一问题。

1948年,就在香农创建信息论的同时,维纳(N. Wiener)出版了专著《控制论——动物和机器中的通信与控制问题》,并创立了控制论。后来,人们常常将信息论、控制论以及系统论合称为“三论”,或统称为“系统科学”或“信息科学”。维纳从控制论的角度认为,“信息是人们在适应外部世界,并使这种适应反作用于外部世界的过程中,同外部世界进行互相交换的内容的名称。”他还认为,“接受信息和使用信息的过程,就是我们适应外部世界环境的偶然性变化的过程,也是人们在这个环境中有效地生活的过程。”维纳的

信息定义包容了信息的内容与价值，从动态的角度揭示了信息的功能与范围。但是，人们在与外部世界的相互作用过程中同时也存在着物质与能量的交换，不加区别地将信息与物质、能量混同起来是不确切的，因而也是有局限性的。

1975 年，意大利学者朗高（G. Longo）在《信息论：新的趋势与未决问题》一书的序中指出，信息是反映事物的形成、关系和差别的东西，它包含在事物的差异之中，而不在事物本身。无疑，“有差异就是信息”的观点是正确的，但“没有差异就没有信息”的说法却不够确切。譬如，我们碰到两个长得一模一样的人，他（她）们之间没有什么差异，但人们会马上联想到“双胞胎”这样的信息。可见，“信息就是差异”也有其局限性。

1988 年，中国学者钟义信在《信息科学原理》一书中，认为信息是事物运动的状态与方式，是事物的一种属性。信息不同于消息，消息只是信息的外壳，信息则是消息的内核。信息不同于信号，信号是信息的载体，信息则是信号所载的内容。信息不同于数据，数据是记录信息的一种形式，同样的信息也可以用文字或图像来表述。信息不同于情报，情报通常是指秘密的、专门的、新颖的一类信息，可以说所有的情报都是信息，但不能说所有的信息都是情报。信息也不同于知识，知识是认识主体所表达的信息，是序化的信息，而并非所有的信息都是知识。他还通过引入约束条件推导了信息的概念体系，对信息进行了完整而准确的论述。通过比较，中国科学院文献情报中心孟广均研究员等在《信息资源管理导论》一书中认为，作为与物质、能量同一层次的信息的定义，信息就是事物运动的状态与方式。因为这个定义具有最大的普遍性，不仅能涵盖所有其他的信息定义，而且通过引入约束条件还能转换为所有其他的信息定义。

2002 年中国科学院、中国工程院两院院士王越教授指出，事实上定量广义全面地描述“信息”是不太可能的，至少是非常难的事，对“信息”本质的深入理解和科学定量描述有待长期进行，在此暂时给出一个定性概括性定义：“信息是客观事物运动状态的表征和描述”，其中“表征”是客观存在的，而描述是人为的。“信息”的重要意义在于它可表征一种“客观存在”，与人认识实践结合，进而与人类生存发展相结合，所以信息领域科技的发展体现了客观与人类主观相结合的一个重要方面。对人而言，“获得信息”最基本的机理是映射（借助数学语言），即由客观存在的事物运动状态，经人的感知功能及脑的认识功能进行概括抽象形成“认识”，这就是“获得信息”加工“信息”的过程，是一个由“客观存在”到人类主观认识的“映射”。由于客观事物运动是非常复杂的广义空间（不限于三维）和时间维的动态展开，因此信息的“表征”也必定是非常复杂的，体现存在于广义空间维在复杂的多层次、多剖面相互“关系”，及在多阶段、多时段的时间维的交织动态展开，进而指出“信息”，它必定是由反映各层次、各剖面不同时段动态特征的信息片段组成，这是“信息”内部结构最基本的内涵。

据不完全统计，信息的定义有 100 多种，它们都从不同侧面、不同层次揭示了信息的特征与性质，但也都有这样或那样的局限性。信息来源于物质，不是物质本身；信息也来源于精神世界，但又不限于精神的领域；信息归根到底是物质的普遍属性，是物质运动的状态与方式。信息的物质性决定了它的一般属性，主要包括普遍性、客观性、无限性、相对性、抽象性、依附性、动态性、异步性、共享性、可传递性、可变换性、可转化性和可伪性等。信息系统安全将处理与信息依附性、动态性、异步性、共享性、可传递性、可变换性、可转化性和可伪性有关的问题。

2. 信息技术

任何技术都产生于人类社会实践活动的实际需要。按照辩证唯物主义观点，人类的一切活动都可以归结为认识世界和改造世界。而人类认识世界和改造世界的过程，从信息的观点来分析，就是一个不断从外部世界的客体中获取信息，并对这些信息进行变换、传递、存储、处理、比较、分析、识别、判断、提取和输出，最终把大脑中产生的决策信息反作用于外部世界的过程。

“科学”是扩展人类各种器官功能的原理和规律，而“技术”则是扩展人类各种器官功能的具体方法和手段。从历史上看，人类在很长一段时间里，为了维持生存而一直采用优先发展自身体力功能的战略，因此材料科学与技术和能源科学与技术也相继发展起来。与此同时，人类的体力功能也日益加强。信息虽然重要，但在生产力和生产社会化程度不高的时候，人们仅凭自身的天赋信息器官的能力，就足以满足当时认识世界和改造世界的需要了。但随着生产斗争和科学实验活动的深度和广度的不断发展，人类的信息器官功能已明显滞后于行为器官的功能了，例如人类要“上天”、“入地”、“下海”、“探微”，但其视力、听力、大脑存储信息的容量、处理信息的速度和精度，已越来越不能满足同自然作斗争的实际需要了。只是到了这个时候，人类才把自己关注的焦点转到扩展和延长自己信息器官的功能方面。

经过长时间的发展，人类在信息的获取、传输、存储、处理和检索等方面的方法与手段，以及利用信息进行决策、控制、指挥、组织和协调等方面的原理与方法，都取得了突破性的进展，当代技术发展的主流已经转向信息科学技术。

对于信息技术，目前还没有一个准确而又通用的定义。为了研究和使用的方便，学术界、管理部门和产业界等都根据各自的需要与理解给出了自己的定义，有数十种之多。信息技术定义的多样化，不只是反映在语言、文字和表述方法上的差异，而且也有对信息技术本质属性理解方面的差异。

目前比较有代表性的信息技术的定义主要有以下几种：

（1）信息技术是基于电子学的计算机技术和电信技术的结合而形成的对声音、图像、文字、数字和各种传感信号的信息，进行获取、加工处理、存储、传播和使用的能动技术。

（2）信息技术是指在计算机和通信技术支持下用以获取、加工、存储、变换、显示和传输文字、数值、图像、视频和声频以及语音信息，并包括提供设备和提供信息服务两大方面的方法与设备的总称。

（3）信息技术是人类在生产斗争和科学实验中认识自然和改造自然过程中所积累起来的获取信息、传递信息、存储信息、处理信息以及使信息标准化的经验、知识、技能，以及体现这些经验、知识、技能的劳动资料有目的的结合过程。

（4）信息技术是在信息加工和处理过程中使用的科学、技术与工艺原理和管理技巧及其应用；与此相关的社会、经济与文化问题。

（5）信息技术是管理、开发和利用信息资源的有关方法、手段与操作程序的总称。

（6）信息技术是能够延长或扩展人的信息能力的手段和方法。

3. 信息系统

自20世纪初泰罗创立科学管理理论以后，管理科学与方法技术得到迅速发展，在它同统计理论和方法、计算机技术、通信技术等相互渗透、相互促进的发展过程中，信息系统

作为一个专门领域迅速形成和发展。同“信息”、“系统”的定义具有多样性一样,信息系统这种与“信息”有关的“系统”,其定义也远未达成共识。比较流行的定义有:

《大英百科全书》把“信息系统”解释为:有目的、和谐地处理信息的主要工具是信息系统,它对所有形态(原始数据、已分析的数据、知识和专家经验)和所有形式(文字、视频和声音)的信息进行收集、组织、存储、处理和显示。

巴克兰德(M. Buckland)认为信息系统是“提供信息服务,使人们获取信息的系统,如管理信息服务、联机数据库、记录管理、档案馆、图书馆、博物馆等”。

达菲(N. M. Dafe)等认为信息系统大体上是“人员、过程、数据的集合,有时候也包括硬件和软件,它收集、处理、存储和传递在业务层次上的事务处理数据和支持管理决策的信息”。

中国学者吴民伟认为信息系统是“一个能为其所在组织提供信息,以支持该组织经营、管理、制定决策的集成的人机系统,信息系统要利用计算机硬件、软件、人工处理、分析、计划、控制和决策模型,以及数据库和通信技术”。

中国科学院、中国工程院两院院士王越教授给出的信息系统的定义是:“帮助人们获得信息、传输信息、处理信息和利用信息的系统称为信息系统,是以‘信息’服务于人的一种工具。‘服务’一词有着越来越广泛的含义,因此信息系统是一类各种不同功能和特征信息系统之总称”。任何信息系统都是由下列部分交织或选择交织而组成。

信息的获取部分(各种传感器等)包括在内。任何一种信息系统其内部都要利用一种或多种媒体荷载信息进行运行,以达到发挥系统作为工具的功能,故首先应通过某种媒体获取“信息”并根据需要将其记录下来,这是信息系统重要基本功能部分。应该注意到的是:人类不断地依靠科学和技术改进信息,获取部分的性能和创造新类型的信息。信息获取部分科学技术的重要突破会对人类社会的发展带来重大影响。

信息的存储部分(如现用的半导体存储器、光盘等)。因“信息”往往存在于有限时间间隔内,因此为了事后多次利用“信息”就需要以多种形式存储“信息”,同时要求快速、方便、无失真、大容量、多次复用性为主要性能指标。

信息的传输部分(无线信道、声信道、光缆信道及其变换器,如天线、接发收设备等)。这部分以大容量、少损耗、少干扰、稳定性、低价格等为科学研究技术进步为持续的目标。

信息的交换部分(如各种交换机、路由器、服务器)。这部分以少时延、易控制、安全性好、大容量,多种信号形式多种服务模式相兼容为目标。

信息的变换处理部分(如各种“复接”,信号编解码、调制解调、信号压缩解压、信息检测等,统称信号处理领域)。这部分被认为是信息科技发展的瓶颈,近年来虽有很大进步,但尚不具备发展需要的类似人的信息处理能力,实行人与机器的更紧密结合,实现这种结合,科学技术有漫长艰难的发展征程,但它是人类努力追求的目标之一。

信息的管理控制部分(如监控、计价、故障检测、故障情况下应急措施、多种信息业务管理等)。这部分功能的完成,除了随信息系统的复杂化而急骤增加变为更加复杂和困难外(如信息系统复杂的拓扑结构使管理监控领域科技基础涉及到数学难题),随着信息系统进一步融入社会,其管理控制的学科基础也发生了社会科学之进入交融而综合化。其管理控制功能也包括社科人文的复杂内容,导致“需要”与“实际水平”之间差距矛盾更加明显。例如电子商务系统的管理控制涉及法律,多媒体文艺系统涉及管理及伦理道德、

法律等领域,因此信息的管理控制部分的发展涉及众多学科,具有重要性、挑战性及紧迫性。

信息系统的各个功能部分都有以下特征:软件、硬件相结合、离散数字型与连续模拟型相结合、各种功能部分交织融合支持形成主功能部分,如存储部分内含处理部分,管理控制部分内含存储、处理部分等。以上各部分发展都密切关联科学领域的新发现、技术领域的创新,并形成了信息科技与信息系统及社会之互相促进发展,“发展”中充满了挑战和机遇。

信息系统具有如下理论上的特征:①现代信息系统一般叠套多个相互交织作用的子系统;②信息系统符合系统理论中通过涨落达到新的有序原理;③信息系统作为人类社会及为人服务的系统,伴随社会进化而发展,并有明显共同进化作用,且越发展越复杂、高级;④每一种信息系统的存在发展都有一定的约束,新发展又会产生新约束,也会产生新矛盾,如性能提高是一种“获得”,得到它必然付出一定的“代价”。

1.1.2 信息系统要素分析

信息系统从不同的角度划分,其要素的性质也不同。如可以划分为系统拓扑结构、应用软件、数据以及数据流;也可划分为管理、技术和人三个方面;也可划分为物理环境及保障、硬件设施、软件设施和管理者等部分,其划分方法可根据不同的应用进行。无论采用哪种划分方法,都是利于对信息系统的理解、分析和应用。下面根据最后一种划分方法分析信息系统的要素。

1. 物理环境及保障

1)物理环境

物理环境主要包括场地和计算机机房,是信息系统得以正常运作的基本条件。其中:

(1)场地(包括机房场地和信息存储场地):信息系统机房场地条件应符合国家标准GB 2887—2000中的有关具体规定,应满足标准规定的选址条件;温度、湿度条件;照明、日志、电磁场干扰的技术条件;接地、供电、建筑结构条件;媒体的使用和存放条件;腐蚀气体的条件等。信息存储场地,包括信息存储介质的异地存储场所应符合国家标准GB 9361—89的规定,具有完善的防水、防火、防雷、防磁、防尘等措施。

(2)机房:在国家标准GB 9361—88中将计算机机房的安全分为A类、B类、C类三类,其中:A类——对计算机机房的安全有严格的要求,有完善的计算机机房安全措施;B类——对计算机机房的安全有较严格的要求,有较完善的计算机机房安全措施;C类——对计算机机房的安全有基本的要求,有基本的计算机机房安全措施。国家标准中针对A类、B类、C类三类机房,在场地选择、防火、内部装修、供配电系统、空调系统、火灾报警及消防设施、防水、防静电、防雷击、防鼠害等方面作了具体的规定。

2)物理保障

物理安全保障主要考虑电力供应和灾难应急。

(1)电力供应:供电电源技术指标应符合国家标准GB 2887《计算机场地技术要求》中的规定,即信息系统的电力供应在负荷量、稳定性和净化等方面满足需要且有应急供电措施。

(2)灾难应急:设备、设施(含网络)以及其他媒体容易遭受地震、水灾、火灾、有害气

体和其他环境事故(如电磁污染等)的破坏。信息系统的灾难应急方面应符合国家标准GB 9361—89 中的规定,应有防火、防水、防静电、防雷击、防鼠害、防辐射、防盗窃、火灾报警及消防等设施和措施。并应制订相应的应急计划,应急计划应包括紧急措施、资源备用、恢复过程、演习和应急计划关键信息。应急计划应有明确的负责人与各级责任人的职责,并应便于培训和实施演习。

2. 硬件设施

组成信息系统的硬件设施主要有计算机、网络设备、传输介质及转换器、输入/输出设备等。为了便于叙述,在此也将存储介质和环境场地所使用的监控设备包含在硬件设施之中。

1) 计算机

计算机是信息系统的基本硬件平台。如果不考虑操作系统、输入/输出设备、网络连接设备等重要的部件,就计算机本身而言除了电磁辐射、电磁干扰、自然老化以及设计时的一些缺陷等风险以外,基本上是不会存在另外的安全问题。常见的计算机有大型机、中型机、小型机和个人计算机(即 PC 机)。PC 机上的电磁辐射和电磁泄漏主要在磁盘驱动器方面,虽然理论上讲主板上的所有电子元器件都有一定的辐射,但由于辐射较小,一般都不作考虑。

2) 网络设备

要组成信息系统,网络设备是必不可少的。常见的网络设备主要有交换机、集线器、网关、路由器、中继器、网桥、调制解调器等。所有的网络设备都存在自然老化、人为破坏和电磁辐射等安全威胁。

(1) 交换机:交换机常见的威胁有物理威胁、欺诈、拒绝服务、访问滥用、不安全的状态转换、后门和设计缺陷等。

(2) 集线器(HUB):集线器常见的威胁有人为破坏、后门、设计缺陷等。

(3) 网关或路由器:网关设备的威胁主要有物理上破坏、后门、设计缺陷、修改配置等。

(4) 中继器:对中继器的威胁主要是人为破坏。

(5) 桥接设备:对桥接设备的威胁常见的有人为破坏、自然老化、电磁辐射等。

(6) 调制解调器(Modem):调制解调器是一种转换数字信号和模拟信号的设备。其常见威胁有人为破坏、自然老化、电磁辐射、设计缺陷、后门等。

3) 传输介质及转换器

常见的传输介质有同轴电缆、双绞线、光缆、卫星信道、微波信道等,相应的转换器有光端机、卫星或微波的收/发转换装置等。

(1) 同轴电缆(粗/细):同轴电缆由一个空心圆柱形的金属屏蔽网包围着一根内线导体组成。同轴电缆有粗缆和细缆之分。常见的威胁有电磁辐射、电磁干扰、搭线窃听和人为破坏等。

(2) 双绞线:双绞线是一种电缆,在它的内部有一对自绝缘的导线扭在一起,以减少导线之间的电容特性,这些线可以被屏蔽或不进行屏蔽。常见的威胁有电磁辐射、电磁干扰、搭线窃听和人为破坏等。

(3) 光缆(光端机):光缆是一种能够传输调制光的物理介质。同其他传输介质相