"十二五"普通高等教育本科国家级规划教材

高等学校网络空间安全系列教材

iCourse·教材

信息系统与安全对抗

——实践篇

第2版

Information System and Security Countermeasures: Practice Part

罗森林

高平

苏京霞

潘丽敏

编著

高等教育出版社

"十二五"普通高等教育本科国家级规划教材
高等学校网络空间安全系列教材

iCourse·教材

信息系统与安全对抗

——实践篇 第2版

Information System and Security Countermeasures: Practice Part

罗森林
高平
苏京霞
潘丽敏
编著

高等教育出版社·北京

内容提要

本书是“十二五”普通高等教育本科国家级规划教材，北京高等教育精品教材，国家精品开放课程主讲教材，经过长期酝酿和多年教学经验总结而成。本书重点介绍操作系统攻防技术实践、TCP/IP网络通信技术实践、网络攻击基础技术实践、数据加密解密技术实践、网络防御基础技术实践等内容。

本书从信息安全与对抗的理论、技术到工程实践，引导读者系统地学习信息安全与对抗领域的核心概念、原理和方法，全面、深入地培养读者的系统思维和创新实践能力。本书可作为信息对抗技术、信息安全、计算机应用、电子信息工程等专业相关课程的主讲教材，也可供实验选修课程、开放实验课程、专业课程设计及信息安全对抗相关技术竞赛培训使用，还可供科研人员参考和对信息安全感兴趣的读者自学使用。

图书在版编目（CIP）数据

信息系统与安全对抗．实践篇／罗森林等编著．--2版．--北京：高等教育出版社，2016.5

ISBN 978-7-04-044581-7

Ⅰ．①信… Ⅱ．①罗… Ⅲ．①信息系统－安全技术－高等学校－教材 Ⅳ．①TP309

中国版本图书馆CIP数据核字（2016）第069991号

信息系统与安全对抗——实践篇（第2版）

Xinxi Xitong yu Anquan Duikang：Shijianpian

策划编辑	时　阳	责任编辑	时　阳	封面设计	张申申	插图绘制	杜晓丹
责任校对	杨凤玲	责任印制	毛斯璐				

出版发行	高等教育出版社	网　址	http://www.hep.edu.cn
社　址	北京市西城区德外大街4号		http://www.hep.com.cn
邮政编码	100120	网上订购	http://www.hepmall.com.cn
印　刷	三河市骏杰印刷有限公司		http://www.hepmall.com
开　本	787mm×1092mm　1/16		http://www.hepmall.cn
印　张	23.25	版　次	2013年1月第1版
字　数	500千字		2016年5月第2版
购书热线	010-58581118	印　次	2016年5月第1次印刷
咨询电话	400-810-0598	定　价	36.00元

物 料 号　44581-00

封面图片出处于『（C）IMAGEMORE Co., Ltd.』

与本书配套的数字课程资源使用说明

与本书配套的数字课程资源发布在高等教育出版社易课程网站，请登录网站后开始课程学习。

一、网站登录

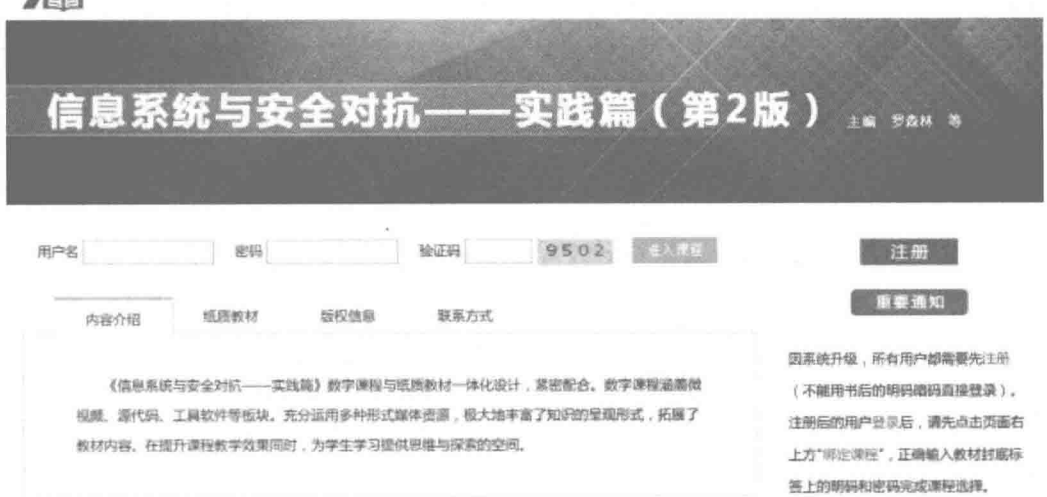
1. 访问 http://abook.hep.com.cn/186132，单击“注册”按钮。在注册页面输入用户名、密码及常用的邮箱进行注册。已注册的用户直接输入用户名和密码登录即可进入“我的课程”界面。

2. 课程绑定：单击“我的课程”页面右上方的“绑定课程”按钮，正确输入教材封底防伪标签上的 20 位密码，单击“确定”按钮完成课程绑定。

3. 在“正在学习”列表中选择已绑定的课程，单击“进入课程”按钮即可浏览或下载与本书配套的课程资源。刚绑定的课程请在“申请学习”列表中选择相应课程并单击“进入课程”按钮。

账号自登录之日起一年内有效，过期作废。

使用本账号如有任何问题，请发邮件至：ecourse@pub.hep.cn。



二、资源使用

与本书配套的易课程数字课程资源按照章的结构组织，包含教学课件、微视频、例程软件等资源。

1. 教学课件：教师上课使用的与课程和教材紧密配套的教学 PPT，可供教师下载使用，也可供学生课前预习或课后复习使用。

2. 微视频：内容基本覆盖重要知识点，能够让学习者随时随地使用移动设备观看比较直观的视频讲解。这些微视频以二维码的形式在书中出现，扫描后即可观看。相应微视频资源在易课程各章的“微视频”栏目中也可观看。

3. 例程软件：实践篇中各实验用到的工具软件和生成的例程软件，包含所有的源代码。

前　言

信息系统在社会中起到“增强剂”和“催化剂”的作用，信息安全问题是信息系统所固有的本征矛盾发展的问题，在极大推动生产力发展的同时，人们对信息网络的依赖程度也日益提高，也因此使国家和社会面临着日益严重的信息安全威胁。国家政治、经济、文化、社会和生态建设中各领域面临着非传统的安全挑战，国家安全和社会稳定受到新的安全威胁，并表现得更为尖锐和复杂。“没有网络安全就没有国家安全”，信息安全保障体系的建设、信息安全与对抗综合实力的加强依赖于人才，人才是关键和亟需的。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。

目前，全国有多所高校建立了信息对抗技术和（或）信息安全专业，本书符合现代社会和科技发展对人才培养的需求，是各高校急需解决的共性的、长期发展的问题，也是北京理工大学军工优势和特色的充分体现。本书同《信息系统与安全对抗——理论篇》（国家级规划教材，国防特色优秀教材，国家精品开放课程主讲教材）、《信息系统与安全对抗——技术篇》（北京高等教育精品教材，国家精品开放课程主讲教材）、《信息安全与对抗实践基础》（工业和信息化部“十二五”规划教材）一起，构成了上下贯通、互为延伸，适合于高素质信息安全人才培养的配套教材。

北京理工大学是1998年教育部首批批准建立信息对抗技术专业的学校，其学科专业、教学科研、实践创新、人才梯队的建设已初见成效。本书在充分理解、掌握信息系统安全对抗理论与技术的基础上，总结多年的教学科研、人才培养经验，充分考虑研究型教学的特点，让学生能够有效运用信息安全与对抗技术，发挥学生的主观能动性，重点培养学生的系统构建、工程实施、实践动手以及创新意识和思维能力。首先，本书定位于研究型培养模式，信息安全对抗是信息系统中不可缺少的重要功能组成，在系统构建之初就应置于顶层来考虑，且需要贯穿于系统的整个生命周期。本书基于广博、丰厚和繁杂的专业知识，充分结合理论分析、系统工程设计与实践方法，内容上体现理论技术的前瞻性和可持续发展。其次，本书内容系统、先进、有实效。信息安全问题本身是一个系统性问题，遵守“全量大于各分量之和”的原理，单就分门别类的具体技术讲解，很难理清脉络，容易“只见树木，不见森林”。本书结构上从信息系统出发，层层推进，在注重信息安全与对抗学科领域的核心思想、原理和方法的基础上，加强系统工程思想和创新实践能力的培养；内容上基于信息安全对抗基础、先进性技术和系统工程设计，充分考虑学生的兴趣（既有理论内容又有技术应用的系统设计与实践，还有需要思考的创新性内容）和讲授内容的灵活性（既可作为独立的理论教材，又可用于辅助的实

践类教材，讲授时可根据学生的情况灵活运用）。此外，注重教材使用的附加效果，在社会更大的时空范围内持续加强“提升信息安全意识，普及信息安全知识，实践信息安全技术，共创信息安全环境，发现信息安全人才”。

本书主要内容包括操作系统攻防技术、基于 TCP/IP 的网络通信保障技术、网络攻击和检测基础技术和系统、数据加密解密技术和系统、网络防御基础技术和系统、网络应用安全技术和系统、无线网络攻防技术和系统等。

本书由罗森林、高平、苏京霞、潘丽敏共同撰写，其中第 2.2 节、第 3 章、第 4.3 ~ 4.7 节由高平撰写，第 4.8 节由苏京霞撰写，第 5 章、第 6.7、6.8 节由潘丽敏撰写，其余各章节由罗森林撰写。罗森林负责全书的章节设计、内容规划和统稿。本书的实践例程均经过认真的编制和调试，读者可直接与作者联系获取。

本书在编写过程中得到了北京理工大学仲顺安、杨翌祥、赵昊、刘畅等教师和张蕾、陈燕颖、王坤、闫广禄、韩磊、韩龙飞、郭亮等同学多方面的帮助，在此一并表示衷心的感谢。同时，衷心感谢高等教育出版社多方面的支持和帮助。

由于时间所限，笔者能力有限，对于书中的不足和疏漏之处，敬请广大读者批评指正，以使其更加完善。

罗森林

2016 年 1 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 基本概念

微视频：信息系统与信息网络

1. 信息的概念

“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宽泛且模糊，对信息和消息的含义没有明确界定。到了20世纪尤其是20世纪中期以后，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，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符号表（或字母表），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号序列的过程。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，必须有一个选择的主体作为限制条件，因此这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》一文中提出了在信息认识方面取得的重大突破，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，发明了信息编码的三大定理，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，只考虑了信息的随机不定性，未能从根本上回答信息是什么的问题。

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,同外部世界进行相互交换的内容的名称”。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。”维纳的信息定义包括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。例如,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,信息则是信号所承载的内容。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,但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,其定义是事物运动的状态与方式。因为这个定义具有最广泛的普遍性,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。对信息本质的深入理解和科学定量描述有待于长期进行。王越教授对“信息”暂时给出了一个定性、概括性的定义:“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”,能够与人类的认识实践相结合,进而与人类的生存发展相结合,因此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。对人类而言,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,经人的感知功能及大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”。由于客观事物的运动是在非常复杂的广义空间(不限于三维空间)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、多剖面的相互“关系”,及在多阶段、多时段的时间维的交织动态展

开；进而，信息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的，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，但不是物质本身；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。但随着生产活动和科学实验活动的深度和广度的不断发展，人类信息器官的功能已明显滞后于行为器官的功能。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做斗争的实际需要。到了这个时候，人类才把关注的焦点转到扩展和延伸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相应的定义，估计有数十种之多。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，而且也反映了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相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的支持下，用以获取、加工、存储、变换、显示和传输文字、数值、图像、视频和音频以及语音信息，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等认识自然和改造自然的过程中所积累起来的获取信息、传递信息、存储信息、处理信息和使信息标准化的经验、知识、技能，以及将体现这些经验、知识、技能的劳动资料有目的地结合的过程。

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，还包括与此相关的社会、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来，管理科学、方法与技术得到迅速发展；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。比较流行的信息系统定义有以下几种。

《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，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具有各种不同功能和特征的信息系统之总称”。

任何信息系统都是由下列部分交织或选择交织而组成的。

① 信息的获取部分（各种传感器等）。任何一种信息系统，其内部都要利用一种或多种媒体承载信息运行，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，这是信息系统重要而基本的功能。应该注意的是，人类不断地依靠科

学和技术改进信息，获取部分之性能并创造新类型的信息。信息获取技术的重要突破会对人类社会的发展产生重大影响。

② 信息的存储部分（如半导体存储器、光盘等）。信息往往存在于有限的时间内，为了能够多次利用，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、多次复用性为其主要性能指标。

③ 信息的传输部分（无线信道、光缆信道及其变换器，如天线、收发设备等）。这部分以大容量、低损耗、抗干扰、高稳定性、低价格等为目标。

④ 信息的交换部分（如各种交换机、路由器、服务器等）。这部分以低时延、易控制、高安全性、大容量，多种信号形式、多种服务模式相兼容为目标。

⑤ 信息的变换处理部分（如各种复接器、信号编解码器、信息检测器等）。这部分可被认为是信息技术发展的瓶颈，近年来虽有很大进步，但尚不具备类似人的信息处理能力。要实现人与机器更紧密的结合，还需要漫长、艰难的发展征程，但这是人类努力追求的目标之一。

⑥ 信息的管理控制部分（如监控、计价、故障检测、故障情况下的应急措施、多种信息业务管理等）。这部分功能除了随信息系统的复杂化而急剧增加，变得更加复杂和困难（如信息系统复杂的拓扑结构使管理监控领域的科技基础涉及数学难题）外，随着信息系统进一步融入社会，其管理控制的学科基础也与社会科学发生交融而逐步综合化。管理控制功能包括社科人文的复杂内容，导致“需要”与“实际水平”之间差距更加明显。例如，电子商务系统的管理控制涉及法律，多媒体文艺系统的管理控制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：软硬件相结合，离散数字型与连续模拟型相结合，各功能部分交织、融合、支撑，形成主功能部分，如存储部分包含处理部分，管理控制部分包含存储、处理部分等。以上各部分的发展都与科学领域的新发现、技术领域的创新密切关联，并形成信息科技与信息系统及社会互相促进发展的局面，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、越高级；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”，得到它必然要付出一定的“代价”。

从功能的角度分析，信息系统由下列部分交织或有选择地交织而组成，即信息的获取、存储、传输、交换、处理、管理与控制和应用部分。

1.1.2 信息系统要素

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；还可以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。无论采用哪种划分方法，目的都是要有利于对信息系统进行理解、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，它们是信息系统得以正常运行的基本条件。

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《计算机场地通用规范》（GB/T 2887—2011）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、噪声、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《计算机场地安全要求》（GB/T 9361—2011）的规定，具有完善的防水、防火、防雷、防磁、防尘措施。

② 机房：《计算机场地安全要求》（GB/T 9361—2011）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。标准针对A、B、C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、防鼠害等方面做出了具体规定。

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《计算机场地通用规范》（GB/T 2887—2011）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。信息系统在灾难应急方面应符合国家标准《计算机场地安全要求》（GB 9361—2011）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，并应制定相应的应急计划，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，在此将存储介质和环境场地所使用的监控设备也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，基本上不会存在额外的安全问题。常见的计算机有大型机、中型机、小型机和个人计算机（即 PC）。PC 的电磁辐射和电磁泄露主要在磁盘驱动器方面，理论上讲，虽然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（switch）：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（router）：网关或路由器设备的威胁主要有物理破坏、后门、设计缺陷、修改配置等。

④ 中继器（repeater）：对中继器的威胁主要是人为破坏。

⑤ 桥接设备（bridging equipment）：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。与其他传输介质相比，光缆虽较昂贵，但对电磁干扰不敏感，并且有更高的数据传输速率。在光缆的两端，通过光端机来发射并调制光波的实现数字通信。常见的主要威胁有人为破坏、搭线窃听和辐射泄露等。

④ 卫星信道（收/发转换装置）：卫星信道是在多重地面站之间运用轨道卫星来转接数据的通信信道。在利用卫星通信时，需要在发射端安装发射转换装置，在接收端安装接收转换装置。常见的威胁有对信道的窃听和干扰，以及对收/发转换装置的人为破坏。

⑤ 微波信道（收/发转换装置）：微波是一种频率为 300 MHz ~ 300 GHz 的电磁波，具有很高的带宽和相对低的成本。在进行微波通信时，发射端按安装发射转换装置，接收端安