北京市高等教育精品教材
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

——技术篇

Information System and Security Countermeasures: Technology Part

罗森林

编著

高等教育出版社

信息系统与安全对抗

——技术篇

本书特色

- 本书为国家精品资源共享课主讲教材、北京市高等教育精品教材，经过长期酝酿和多年教学经验总结而成。
- 重点引导读者从顶层理解信息系统与安全对抗问题，系统、全面地学习信息系统与安全对抗领域的核心概念、原理和技术。
- 配套教材为“十二五”普通高等教育本科国家级规划教材《信息系统与安全对抗——实践篇》（第 2 版）。

ISBN 978-7-04-047287-5

9 787040 472875 >

定价 45.90 元

第1章 绪 论

1.1 引 言

信息是人类社会的宝贵资源，功能强大的信息系统是推动社会发展前进的催化剂和倍增器。信息系统越发展到它的高级阶段，人们对其依赖性就越强。本章主要讨论信息系统的基础知识，内容包括信息、信息技术、信息系统、信息网络的概念，信息系统的要素分析，工程系统基础知识。

1.2 信息与信息技术的概念

1.2.1 信息的基本概念

“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20世纪中期以后，现代信息技术的飞速发展及其对人类社会产生的深刻影响，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，发信者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，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含信息的内容与价值，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，同外部世界进行互相交换的内容的名称”。他还认为，“接收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”。维纳的信息定义包含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，人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人在《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，至少是非常困难的，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”，与人的认识实践结合，进而与人类的生存发展相结合，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”并加工“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,因此它的“表征”也必定是非常复杂的,体现在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,进而指出,“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,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。

1.2.2 信息技术的概念

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长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信息技术的定义，估计有数十种之多。信息技术定义的多样化，不只反映在语言、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的、图像的、文字的、数字的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、声频及语音信息，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，以及与体现这些经验、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，以及与此相关的社会、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。

1.2.3 信息的主要表征

信息的客观表征非常广泛，源于各种各样运动状态的特征。信息的表征就是各种各样的“特殊性的表现”，也可认为是“特征的表现”。

对人而言，人可以利用感觉器官和脑功能感知有关自然界的各种信息（通过多种信息荷载的媒体）。此外，人还会融合利用人类自己创立的“符号”来进一步认识、描述、记录、传递、交流、研究和利用“信息”。以上叙述可进一步认为是人脑主宰的二重“映像”过程，即通过第一次映射，形成信息感觉及初步认识，然后进一步利用“符号”二次深化映射，形成思维结果，需要时可以较长期记忆，以备日后所需。以上分步骤可述的二次映射实际上是一个变换形成“符号”的映射。

“符号”是一个内涵非常广泛的概念，它是特定的“关系”。研究“符号”及其应用已形成专门的“符号学”学科。在此简单举例说明。语言、文字、图形、图像、音乐、物理、化学、数学等领域中都有专门的符号，如微分、积分符号，极限、范数、内积符号等。推而广之，各种定理可以认为是由符号的有序组合构成的符号集合，是广义的符号，也是客观规律的“符号”。此外，人类的表情、动作（如摇头、摆手、皱眉等）也可认为是一种符号。

又因人所能直接感知的信息种类和范围有限，因此人类不断努力扩大发现、感知信息的种类和范围的新原理、新方法，并将新获得的信息转换为人类所能感知的信息，但其基本原理

仍是映射和符号转换映射。

1.2.4 信息的主要特征

1. 信息的存在形式特征（直接层次）

（1）不守恒性。信息不是物质，也不是能量，而是与能量和物质密切相关的运动状态的表征和描述。由于物质运动不停，变化不断，故信息不守恒。

（2）复制性。信息在非量子态作用机理情况，在环境中可区分条件下具有可复制性（在量子态工作环境，一定条件下是不可精确“克隆”的）。

（3）复用性。信息在非量子态作用机理情况，在环境中可区分条件下具有多次复用性。

（4）共享性。在信息荷载体具有运行能量，且运行能量远大于信息维持存在所需的低限阈值时，信息可多次共享，如说话声可被几个人同时听到，多个卫星转播接收站可以同时接收信号、获得信息等。

（5）时间维有限尺度特征。具体事物运动总是在时间、空间维的有限尺度内进行的，因而信息必定具有时间维的特征，如发生在何时、持续多长时间、间隔多长时间、时间变化率的大小、相互时序关系等，这些都是“信息存在形式”内时间维的重要特征，对信息的利用有重要意义。

需要着重说明的是，若信息系统的运行处在量子状态，复制性、复用性和共享性这 3 种特征的情况就完全不同了。事物在量子状态的运行能量水平非常微弱，能量可用 $\varepsilon=h\upsilon \cdot n$（$\varepsilon$ 为能量，h 为普朗克常数，$h=6.625\ 6\times10^{-34}$ J·S，υ 为频率，n 为能级数）表示。可以这样理解，当 $n=1$ 时求出的 ε 值是事物量子化运行存在的最低值（也可认为是一个低限阈值），如果低于此值，事物运动状态就无法保持。信息系统运行中的能量水平都远远高于此值，例如，在微波波段，$\upsilon=10^{10}$ Hz，阈值 $\varepsilon=6.626\times10^{-24}$ J；在光波波段，$\upsilon=10^{14}\sim10^{15}$ Hz，阈值 $\varepsilon=6.626\times10^{-19}$ J，这两个波段中的信息系统的运行低功率门限约为 $10^{-13}\sim10^{-14}$ 及 10 个光子能量的信号检测能力阈值，比 ε 值高得多，而信息系统正常工作状态（如高灵敏信号接收检测设备的正常运行能量水平）的能量或功率水平更要高得多。还有些信息运行形式是靠外界能量照射形成反射，由反射情况来表示信息，这些表征信息的反射能量（如反射光）也远大于 ε 值。这意味着，这些系统只有处在远离量子态的“宏观态”中才具备信息的上述特征，如果利用量子态荷载信息，即信息系统运行在量子态，则信息的上述特征就不再存在了。这对于信息的保密有利，但系统的实际运行会有巨大困难。

2. 信息在利用层次上的特征

信息最基本、最重要的功能是为人所用，即以人为主体的利用。从利用层次上讲，信息具有如下特征。

（1）真实性。产生信息不真实反映对应事物运动状态的意识源可分为“有意”与“无意”两种。“无意”是人或信息系统的“过失”所造成信息的失真，而“有意”则是人有目的地

制造失实信息或更改信息内容以达到某种目的。

（2）多层次、多剖面区分特性。信息属于哪个层次和剖面也是其重要属性。对于复杂运动的多种信息，了解其层次和剖面属性，对于综合、全面地掌握信息的运动性质是很重要的。

（3）信息的选择性。信息是事物运动状态的表征，运动充满各种复杂的相互关系，同时也呈现对象性质，即在具体场合，信息内容的关联性质对不同主体有不同的关联程度，关联程度不高的信息对主体就不具有重要意义，这种特性称为信息的空间选择性。此外，有些信息对于应用主体还有时间选择性，即以某时间节点或时间区域节点为界，对于主体有重要性，例如在地震前进行预报。

（4）信息的附加义特征。由于信息是事物运动状态的表征，即便只是某剖面信息，也必然蕴涵运动中相互关联的复杂关系。通过信息可获得其所蕴涵的非直接表达的内容（“附加义”）具有重要的应用意义。人获得附加义的方式可分为联想方式和逻辑推理方式。联想是人的一种思维功能（联想的机制甚为复杂），它比逻辑推理的作用领域更广泛。例如，根据研究课题的性质联想到企业将推出的新商品，这一过程是根据企业所研究课题蕴涵的指称对象的多种信息，综合利用逻辑推理和相关科学技术所做出的。

3. 可由获得的信息认识事物的运动过程

事物的运动是客观存在的，并具有数不尽的复杂多样性。信息的深层次重要性在于，可以通过信息所表征的状态去认识事物的运动过程。

信息可以无遗漏地表征事物运动过程的核心状态，以及信息中蕴涵的由状态到运动过程的要素，是可以由信息认识事物运动过程的基础。挖掘信息内涵，从而认识事物运动过程的过程可表示如下：

信息→[信息直接关联特征域关系，信息存在广义空间域关系，信息存在时间域关系，信息变化率域关系]→一定条件下指称对象的运动过程（片段）

由于运动的复杂多样性，因此上述各域还需要再划分成子域进行研究。

“信息直接关联特征域关系”涉及下列子域：关联对象子域，如事、物、人及联合子域，如人与事、事与物、人与物等；关联行为子域，如动作、意愿、评价、评判等；动作状态性质子域，如确定性、非确定性、确定性与非确定结合性等。

“信息存在广义空间域关系”包括三维距离空间子域、物理空间子域、事理空间子域、人理空间子域、生理空间子域。各子域仍可再进行多层次子域划分及特征分析，如物理（广义的事物存在的理）空间子域中包括数学空间、物理空间、化学空间等各子域。

“信息存在时间域关系”常需要分成多种尺度的时间子域。

“信息变化率域关系”可进一步划分为以下几个子域：广义空间多层变化率子域，$\frac{\partial}{\partial x},\frac{\partial}{\partial y},\cdots,\frac{\partial}{\partial \theta},\frac{\partial}{\partial r},\cdots,\frac{\partial^2}{\partial x^2},\frac{\partial^2}{\partial y^2},\frac{\partial^3}{\partial x^3},\cdots$；时间域多层变化率子域，$\frac{\partial}{\partial t},\frac{\partial^2}{\partial t^2},\frac{\partial^3}{\partial t^3},\cdots$；时空多层变化率子域，$\frac{\partial^2}{\partial x\partial t},\frac{\partial^2}{\partial t\partial x},\cdots$。

利用以上所介绍的四元组关系框架对信息（或信息组合）进行分析，并通过类比和联想，可以得到信息所代表的运动过程的一些预测。例如，运动过程是否存在质变阶段或量变过程，是否会有重大新生事物产生，运动过程是否复杂等。

4. 信息组成的信息集群

一种状态的表征往往需要用多条信息来表示，其包含的信息量（未考虑其真伪性、重要性、时间特性等）可用香农（Shannon）定义的波特、比特等表示，但这些表征的还只是状态相对简单的信息片段，可称为“信息单元”。客观世界中还存在着由信息单元有机组成的信息集群，它表征更复杂的运动状态和过程，是信息单元的自然延伸，但它们还没有专门名称，在此暂用与汉语语义学中“言语作品”类似的“信息作品”来表述，它还需结合思维推理、逻辑推理进行判断、理解和认识。理解信息作品对人类社会发展是有意义的，尤其在信息作品是由人有目的地策划、组织形成的情况下。信息作品的表现形式有多种，如文字、图像、多媒体影像等。如果信息作品表征较长的过程，则信息作品内包含的信息单元数量就会非常巨大。

1.3 信息系统及其功能要素

1.3.1 信息系统的基本概念

自 20 世纪初泰罗创立科学管理理论以后，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。

M. 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”。

N. M. 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、中国工程院王越教授给出的信息系统的定义是：帮助人们获取、传输、存储、处理、交换、管理控制和利用信息的系统称为信息系统，信息系统是以信息服务于人的一种工具。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的总称。

1.3.2 信息系统的理论特征

现代信息系统内往往嵌套多个互相交织的子系统，基于自组机理，各子系统的自组织机能有机集成构成系统的自组织机能，这是系统理论所描述的典型系统。例如，现代通信系统包括卫星通信系统、公共骨干通信网、移动通信网等，卫星通信系统又包括卫星（包括转发器、卫星姿态控制、太阳能电池系统等）、地面中心站系统（包括地面控制分系统、上行信道收发系统等）、小型用户地面站（再分子系统等）。移动通信网系统、公共骨干通信网都由多层子系统组成。上述各类通信系统组成为“通信系统”，它正以通信功能为基础，融入具有更广泛服务功能的网络系统，以服务社会及人类发展。

每一种信息系统研发完成后仍会不断进行局部改进（量变阶段），当改进已不能适应需要的情况下，则要发展一种新类型（质变阶段）。如此循环一定程度后，会发生更大的结构性质变（系统体制变化），如通信系统中的交换机变为程控式交换机，进而又向路由式交换机发展。这种变化发展“永不停止”，符合系统理论中通过涨落达到新的有序原理。

信息系统作为为人类社会服务的系统，伴随社会进化而发展，并有明显共同的进化作用，且越发展越复杂、越高级。信息系统发展的核心因素是进化机制的进化，即信息系统发展机理的发展变化可引起系统根本性的发展。

每一种信息系统的存在、发展都有一定的约束，新发展会产生新约束，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”。这里所说的“获得”和“代价”都是指时空域中广义的“获得”和“代价”，如“自由度”“可能性”“约束条件”等的增减（当然，功能、范围、质量等的增减也包括在内）。

1.3.3 信息系统的功能组成

任何信息系统都是由下列部分交织或有选择交织而组成的。

（1）信息的获取部分（如各种传感器等）。任何一种信息系统，其内部都要利用一种或多种媒体荷载信息运行，以达到发挥系统作为工具的功能。人类不断地依靠科学和技术改进信息获取部分的性能并创造新类型的信息获取器件，同时信息获取部分的重要突破也会给人类社会的发展带来重大影响。

（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时间间隔内，为了能够多次利用，信息需要以多种形式存储，同时要求以快速、方便、无失真、大容量、多次复用等作为主要性能指标。

（3）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、接发设备等）。这部分以大容量、低损耗、少干扰、稳定性、低价格等作为改进的持续目标。

（4）信息的交换部分（如各种交换机、路由器、服务器等）。这部分以时延小、控制容易、安全性高、容量大、多种信号形式和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”、信号编解码、调制解调、信号压缩与解压缩、信号检测、特征提取识别等，统称信号处理）。信息处理是通过荷载信息的信号提取信息表征的运动特征，甚至推演运动过程，逆向运算难度很大，因此被认为是信息科技发展的瓶颈，近年来虽有很大进步，但尚不具备发展出所需要的类似人的信息处理能力，以实现人与机器的更紧密结合。要实现这种结合仍需要漫长艰难的过程，这也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）。随着信息系统的复杂程度急剧增加，信息的管理控制部分也变得更加复杂（例如，信息系统复杂的拓扑结构分析是信息管理、监控领域的数学难题）。随着信息系统及信息科技进一步融入社会，还诞生了多种依靠管理信息对其他领域进行管理的管理系统，如现代服务业的管控系统，同时其管理控制的学科基础也由于与社会科学的交融而逐步综合化。信息的管理控制部分还涉及社科、人文等方面的复杂内容，造成需求与实际水平之间的差距，使得矛盾更加明显。例如，电子商务系统的管理控制涉及法律，多媒体文艺系统的管理涉及伦理道德、法律等领域。总之，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。

信息的应用领域日益广泛，需要提供的服务功能也越来越高级、复杂。在很多场合下，由信息系统的管理控制部分包含与应用服务关联功能的工作模式已不能满足应用需要，因此对应用进行支持的专门部分应运而生，称为应用支持部分（它与管理控制部分有密切联系）。

以上各部分都有如下特征：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、支持，以形成主功能部分，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，形成信息科技、信息系统与社会互相促进发展的局面，发展中充满了机遇和挑战。

1.3.4 信息系统的要素分析

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，还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，目的都是为了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，它是信息系统得以正常运作的基本条件。

（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、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《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。国家标准《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。标准中针对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《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应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GB/T 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）计算设备

计算设备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，基本上不会存在其他安全问题。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存在于磁盘驱动器方面，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。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。网关或路由器的威胁主要有物理破坏、后门、设计缺陷、配置篡改等。

（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

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。同其他的传输介质相比，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威胁。

（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，发射端需要安装发射转换装置，接收端需要安装接收转换装置。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等。

4）终端设备

常见的输入输出设备主要有键盘、磁盘驱动器、磁带机、打孔机、电话机、传真机、识别器、

扫描仪、电子笔、打印机、显示器和各种终端设备等。

（1）键盘。键盘是计算机最常见的输入设备。常见的主要威胁有电磁辐射泄露信息和人为滥用造成信息泄露，如随意尝试输入用户密码。

（2）磁盘驱动器。磁盘驱动器也是计算机中重要的输入输出设备。其主要威胁有磁盘驱动器的电磁辐射以及人为滥用造成信息泄露，如复制系统中重要的数据。

（3）磁带机。磁带机一般用于大、中、小型计算机以及一些工作站，既是输入设备也是输出设备。其威胁主要有电磁辐射和人为滥用。

（4）打孔机。打孔机是一种早期使用的输出设备，可用于大、中、小型计算机。其威胁主要是人为滥用。

（5）电话机。电话机主要用于话音传输，严格地讲，它不是信息系统的输入输出设备，但电话是必不可少的办公用品。在信息系统安全方面，主要威胁是滥用电话泄露用户密码等重要信息。

（6）传真机。传真机主要用于传真的发送和接收，严格地讲，它不是信息系统的输入输出设备。在信息系统安全方面，主要威胁是传真机的滥用。

（7）麦克风。在使用语音输入时需要使用麦克风。其威胁主要是老化和人为破坏。

（8）识别器。为识别系统用户，众多的信息系统都使用识别器。最常见的识别器有生物特征识别器、光学符号识别器等。主要威胁是人为破坏摄像头等识别装置，以及识别器设计缺陷，特别是算法运用不当等。

（9）扫描仪。扫描仪主要用于扫描图像或文字。其主要威胁是电磁辐射泄露系统信息。

（10）电子笔（数字笔）。在手写输入法广泛使用的今天，电子笔或数字笔作为一种输入设备越来越常见，其主要威胁是人为破坏。

（11）打印机。打印机是一种常见的输出设备，但是部分打印机也可以将信息主动输入计算机。常见的打印机有激光打印机、针式打印机、喷墨打印机三种。打印机的主要威胁有电磁辐射、设计缺陷、后门、自然老化等。

（12）显示器。显示器作为最常见的输出设备，负责将不可见的数字信号还原成人可以理解的符号，是人机对话所不可缺少的设备。其威胁主要是电磁辐射泄露信息。

（13）终端。终端既是输入设备又是输出设备，除了显示器以外，一般还有键盘等外设，基本上与计算机的功能相同。常见的终端有数据、图像、话音等类别。其威胁主要有电磁辐射、设计缺陷、后门、自然老化等。

5）存储介质

信息的存储介质有许多种，常见的主要有纸介质、磁盘、磁光盘、光盘、磁带、录音/录像带，以及集成电路卡、非易失性存储器、芯片盘等存储设备。

（1）纸介质。虽然信息系统中的信息以电子形式存在，但许多重要的信息也通过打孔机、打印机输出，以纸介质形式存放。纸介质存在保管不当和废弃处理不当导致的信息泄露威胁。

（2）磁盘。磁盘是常见的存储介质，它利用磁记录技术将信息存储在磁性材料上。常见的磁盘有软盘、硬盘、移动硬盘等。对磁盘的威胁有保管不当、废弃处理不当、损坏变形等。

（3）磁光盘。磁光盘利用磁光电技术存储数字数据。对其威胁主要有保管不当、废弃处理不当、损坏变形等。

（4）光盘。光盘是一种非磁性的、用于存储数字数据的光学存储介质。常见的光盘有只读光盘、一次写入光盘、多次擦写光盘等种类。对其威胁主要有保管不当、废弃处理不当、损坏变形等。

（5）磁带。磁带主要用于大、中、小型机或工作站，由于其容量比较大，多用于备份系统数据。对其威胁主要有保管不当、废弃处理不当、损坏变形等。

（6）录音 / 录像带。录音带或录像带也是磁带的一种，主要用于存储话音或图像数据，这类数据通常是由监控设备获得的。其威胁主要是保管不当或损坏变形等。

（7）其他存储介质。除以上列举的一些常见的存储介质以外，还有磁鼓、IC 卡、非易失性存储器、芯片盘、Zip Disk 等介质，它们都可以用于存储信息系统中的数据。对这些介质的威胁主要有保管不当、损坏变形、设计缺陷等。

6）监控设备

依据国家标准规定和场地安全考虑，重要的信息系统所在场地应有一定的监控规程并使用相应的监控设备。常见的监控设备主要有摄像机、监视器、电视机、报警装置等。对监控设备而言，常见的威胁主要有断电、损坏或干扰等。

（1）摄像机。摄像机除作为识别器的一个部件以外，还主要用于环境场地检测，记录对系统的人为破坏活动，包括偷窃、恶意损坏和滥用系统设备等行为。

（2）监视器。在信息系统中，特别是交换机和入侵检测设备中常带有监视器，负责监视网络数据出入情况，协助管理网络。

（3）电视机。电视机同显示器一样，主要输出摄像机或监视器所捕获的图像或声音等信号。

（4）报警装置。报警装置就是发出报警信号的设备。常见的报警信号可以通过传呼机、电话、声音、图像等多种方式表现。

3. 软件设施

组成信息系统的软件主要有操作系统（包括计算机操作系统和网络操作系统）、通用应用软件、网络管理软件以及网络协议等。在分析信息系统风险时，软件设施的脆弱性或弱点是考查的重点，因为虽然硬件设施有电磁辐射、后门等可利用的脆弱性，但是其实现所需的花费一般比较大，而对软件设施而言，一旦发现脆弱性或弱点，几乎不需要多大的投入就可以实现对系统的攻击。

1）通用操作系统

操作系统安全是信息系统安全最基本、最基础的安全要素，操作系统的任何安全脆弱性和安全漏洞必然导致信息系统的整体安全脆弱性，操作系统的任何功能性变化都可能导致信

息系统安全脆弱性分布情况的变化。因此从软件角度来看，确保信息系统安全的第一要务便是采取措施保证操作系统安全。

常见的操作系统有以下几种。

（1）UNIX：UNIX 是一种通用交互式分时操作系统，由贝尔实验室于 1969 年开发出来。自从 UNIX 诞生以来，它已经历过多次修改，各大公司也相继开发出自己的 UNIX 系统。目前常见的有加州大学伯克利分校开发的 UNIX BSD、AT&T 开发的 UNIX System、SUN 公司的 Solaris、IBM 公司的 AIX 等多种版本。

（2）DOS。DOS 即磁盘操作系统，是早期的 PC 操作系统。常见的 DOS 有微软公司的 MS DOS、IBM 公司的 PC DOS、Norton 公司的 DOS 系统以及我国的 CCDOS 等。

（3）Windows/NT。Windows 即视窗，是微软公司的一系列操作系统，其中常见的有 Windows 3.x、Windows 95/98，以及 Windows NT、Windows 2000、Windows XP、Windews 7 等。

（4）Linux。Linux 类似于 UNIX，是完全模块化的操作系统，主要运行于 PC 上。目前有 Red Hat Linux、Slackware、OpenLinux、TurboLinux 等多种版本。

（5）Mac OS。Mac OS 是苹果公司开发的 PC 端 Macintosh 的专用操作系统。

（6）OS/2。OS/2 是 1987 年推出的与以 Intel 80286 和 80386 微处理器为基础的 PC 配套的新型操作系统。它是为 PC DOS 和 MS DOS 的升级而设计的。

（7）其他通用计算机操作系统。除以上的计算机操作系统以外，还有 IBM 公司的 System/360、DEC 公司的 VAX/VMS、Honeywell 公司的 SCOMP 等操作系统。

2）网络操作系统

网络操作系统同计算机操作系统一样，也是信息系统中至关重要的要素之一。

（1）IOS。IOS 即 Cisco 互联网络操作系统，提供集中、集成、自动安装以及管理互联网络的功能。

（2）Novell Netware。Novell Netware 是由 Novell 公司开发的分布式网络操作系统。Novell Netware 可以提供透明的远程文件访问和大量的其他分布式网络服务，是适用于局域网的网络操作系统。

（3）其他专用网络操作系统。为提高信息系统的安全性，一些重要的系统会选用专用的网络操作系统。

3）网络通信协议

网络通信协议是一套规则和规范的形式化描述，即怎样管理设备在一个网络中交换信息。协议可以描述机器与机器间接口的低层细节或者应用程序间的高层交换。网络通信协议可分为 TCP/IP 协议和非 IP 协议两类。

（1）TCP/IP 协议。TCP/IP 协议是目前最主要的网络互联协议，它具有互联能力强、网络技术独立和支持的协议灵活多样等优点，得到了最广泛的应用。国际互联网就是基于 TCP/IP 协议进行的网际互联通信。但由于 TCP/IP 协议在最初设计时没有考虑安全性问题，因此协议本身有许多安全缺陷。另外，TCP/IP 协议的实现也存在一些安全缺陷和漏洞，使得基于

这些缺陷和漏洞出现了形形色色的攻击，导致基于 TCP/IP 协议的网络十分不安全。造成互联网不安全的一个重要因素就是它所基于的 TCP/IP 协议自身的不安全性。

（2）非 IP 协议。常见的非 IP 协议有 X.25、DDN、帧中继、ISDN、PSTN 等协议，以及 Novell Netware、SNA 等专用网络体系结构进行网间互联所需的一些专用通信协议。

4）通用应用软件

通用应用软件一般指介于操作系统与应用业务之间的软件，为信息系统的业务处理提供应用的工作平台，例如 Internet Explorer、Office 等。通用应用软件安全的重要性仅次于操作系统安全，其任何安全脆弱性和安全漏洞都可能导致应用业务乃至信息系统的整体安全问题。

（1）Lotus Notes。IBM 公司的 Lotus Notes 作为信息系统业务处理工作平台软件的代表，对其安全性的探讨目前主要集中在 Domino 服务器的安全方面。

（2）MS Office。微软公司的 Office 办公软件包括 Word、PowerPoint、Excel、Access 等软件，是目前较常见的信息处理软件。有关 MS Office 软件的漏洞较多，如 Word 的帮助功能就可以被用来执行计算机中的可执行文件。

（3）E-mail。电子邮件是互联网最常用的应用之一。邮件信息通过电子通信方式跨过使用不同网络协议的各种网络在终端用户之间传输。

（4）Web 服务、发布与浏览软件。World Wide Web（WWW）系统最初只提供信息查询、浏览等静态服务，现在已发展成可提供动态交互的网络计算和信息服务的综合系统，可实现对网络电子商务、事务处理、工作流以及协同工作等业务的支持。

（5）数据库管理系统。数据库系统由数据库和数据库管理系统（DBMS）构成。数据库是按某种规则组织的存储数据的集合。数据库管理系统是在数据库系统中生成、维护数据库以及运行数据库的一组程序，为用户和其他应用程序提供对数据库的访问，同时也提供事件登录、恢复和数据库组织。

（6）其他服务软件。在信息系统中，除了以上常见的一些通用应用软件以外，还有 FTP、TEL、NET、视频点播、信息采集等软件，这里不再赘述。

5）网络管理软件

网络管理软件是信息系统的重要组成部分，其安全问题一般不直接扩散和危及信息系统的整体安全，但可通过管理信息对信息系统产生重大安全影响。鉴于一般的网络管理软件所使用的通信协议（例如 SNMP）并不是安全协议，因此需要额外的安全措施。

常见的网络管理软件有 HP 公司的 Open View、IBM 公司的 Net View、SUN 公司的 Net Manager、3Com 公司的 Transcend Enterprise Manager、Novell 公司的 NMS、Cabletron 公司的 SPECTRUM、Nortel 网络公司的 Optivity Campus、HP 公司的 CWSI 等。

此外，信息系统还涉及组织管理、法律和法规等内容，这些内容将在后续章节中专门论述。