# 信息系统

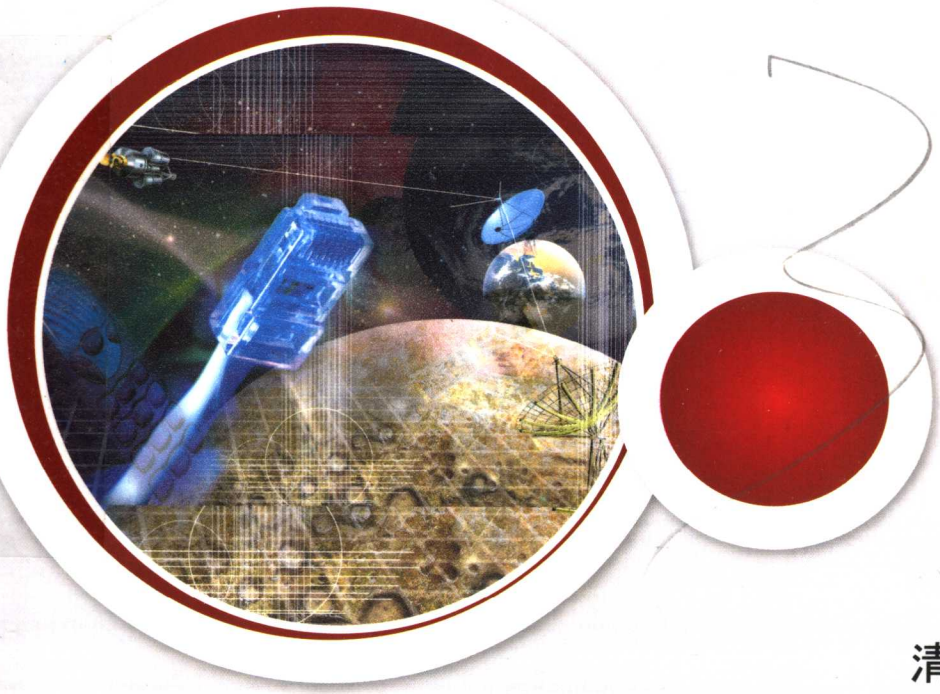
## 安全原理与应用

陆宝华 王 楠 编著

第一部分等级建设信息系统保障体系的理论与实践的指导书

第一次系统介绍可信计算基（TCB）的概念与构成

是一部学习信息系统安全理论与方法的入门读物



清华大学出版社

# 信息系统安全原理与应用

陆宝华　王　楠　编著

清华大学出版社
北　京

## 内 容 简 介

本书从信息安全等级保护的思想出发，系统地介绍了信息系统安全保障技术体系的原理。全书共分为三大部分，第一部分从第1章至第5章，是基础知识部分，介绍了信息保障体系的构成、基本的控制原理和可信计算基(TCB)。第二部分从第6章至第10章，介绍了网络、操作系统、数据库、应用软件等层面的安全保护原理和不同等级的安全保护要求，以及如何构建一个分等级的保护信息安全技术体系。第三部分为最后三章，介绍了保护系统可靠运行的技术，包括风险评估、应急响应及不同等级信息系统的安全运行维护要求。

本书适合于从事信息安全保护工作的各类人员，包括各种监管部门和运行信息系统的单位的技术人员，也适合高等院校相关专业的本科生参考使用。



**图书在版编目(CIP)数据**

信息系统安全原理与应用/陆宝华，王楠编著. —北京：清华大学出版社，2007.11
ISBN 978-7-302-16314-5

Ⅰ.信…　Ⅱ.①陆…②王…　Ⅲ.信息系统—安全技术　Ⅳ.TP309

中国版本图书馆CIP数据核字(2007)第159552号

**责任编辑**：张　瑜　闫光龙
**封面设计**：杨玉兰
**版式设计**：北京东方人华科技有限公司
**责任校对**：周剑云　马素伟
**责任印制**：李红英
**出版发行**：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　**邮　　编**：100084
c—service@tup.tsinghua.edu.cn
**社 总 机**：010-62770175　**邮购热线**：010-62786544
**投稿咨询**：010-62772015　**客户服务**：010-62776969
**印 刷 者**：清华大学印刷厂
**装 订 者**：北京市密云县京文制本装订厂
**经　　销**：全国新华书店
**开　　本**：185×260　**印张**：35.75　**字数**：863千字
**版　　次**：2007年11月第1版　　**印　　次**：2007年11月第1次印刷
**印　　数**：1～4000
**定　　价**：49.00元

# 序

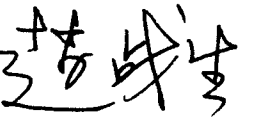
这是一本来自信息安全保障工作第一线，由多年从事网络安全监察工作的同志撰写的著作。作者将当代的信息安全技术与我国信息安全保障工作的等级保护制度的贯彻落实结合起来，根据自己长期的学习思考心得和基层实际工作体会，从信息系统安全保障体系的高度系统地展开了自己的思绪。对于一个具体事物缠身、日常工作繁忙的同志，有毅力苦读万卷书，慎思千道题，整理长考成数十万言于纸上，并愿奉献给大家共享，实属难能可贵，给人眼睛一亮的感觉。

我国信息化建设在国际信息化大潮中高速发展。信息技术越来越广泛地应用于国民经济的各个领域。信息革命带来了生产的高效率和高效益。信息安全保障成为我们追求信息化产生的利益最大化的必须。国家把信息安全与国家安全、经济安全、社会稳定列为四个重大安全问题之一。

国家信息化领导小组关于加强信息安全保障工作的意见中，提出了“国家实行信息安全等级保护，要抓紧信息安全等级保护制度建设”的要求，同时也提出了风险评估、以密码技术为基础的信息安全保护和网络信任体系、信息安全监控体系、信息安全应急处理等项基础性工作。当前，围绕着信息安全等级保护制度和各项信息安全基础性工作的试点正在推动和推广。如何认识等级保护制度和各项基础性工作的关系，如何把信息安全保障的各种技术和管理手段运用到信息安全保障体系的建设中去，成为我们必须认真思考的问题。我认为：信息安全保障的基础性工作奠定信息安全保障工作的根基。打好地基是为了盖起的信息安全保障体系这所大厦永固。盖大厦需要有科学的制度化的工作机制来组织施工并保证进度和质量。信息安全等级保护制度就是这样一个科学的制度化的工作机制。

要盖信息安全保障体系这所大厦，需要我们有一个整体的视野、系统的设计。而不能把眼光仅仅盯在用来盖大厦的一砖一瓦、一人一事上。作者给出了一个自己理解的信息安全保障体系的三维模型，从系统维、过程维和措施维涵盖了保障体系的保护对象、生存周期、保障安全技术和管理措施。这种宏观的抽象有助于我们从整体上把握我们要干什么。作者又根据自己的思考把信息安全保障的技术要求分解到各层面中，力图使其更有针对性。作者还根据国家有关信息安全保障的政策、标准以及自己的实际工作经验，诠释了等级化信息保护技术体系的建设、风险评估与风险管理、信息安全事件的响应与处置。并从等级化的思想论述了系统的安全运行维护技术和管理要求以及安全运行维护中的各类活动。这些论述把信息安全保障的概念、理论和技术与实际工作的需要结合起来，有学术而不学究，有经验而不“经验主义”，必然对我们有所启发和帮助。

信息安全保障工作的加强和落实，是一个需要以智慧和责任心为基础，运用现代技术和管理手段才能实现的艰巨任务。要完成这个任务，有许多新问题有待我们去理解、认识。世上无难事，只怕有心人。如果我们从事信息安全保障工作的同志们都像作者这样有心、认真、执着，我们将无往不胜。

国家信息安全专家 

# 前　言

我是从 1999 年末开始接触信息系统安全的，从 2001 开始，依照《中华人民共和国计算机信息系统安全保护条例》的要求，对大连市一些单位的信息系统的安全保护工作进行监督、检查和指导。一个问题一直困扰着我，信息系统的安全问题应该如何解决才是科学合理的，应该建立什么样的信息安全保障体系？我发现许多厂商(甚至是大的厂商)给用户做的安全方案几乎千篇一律，目的也很简单，只要把自己厂家生产的安全产品做到了方案中，好像他们的任务也就完成了。这一点对于厂商来说似乎是可以理解的，但是结果是不尽如人意的。许多单位采购和使用了安全产品不但没有解决安全问题，反过来却导致了安全事件。

针对这个问题，我不断学习和研究。读书、看资料向人请教，几年下来，我读了大约上千万字的书刊和资料，终于觉得自己在这方面有了心得、体会甚至是体系思想，觉得自己有发言权了。并不断地向身边的人宣传自己的观点。

2005 年夏，一个厂商的技术人员建议我把这些心得体会写成书。我很犹豫：一是时间，我的工作很多也很忙，能否允许我拿出时间来完成这样的任务；二是关于信息系统安全的书已经很多了，还有必要去写吗；第三，我不是学者，这些心得体会是否达到了一定的学术高度，是否是幼稚的、错误的，等等。但我又很动心，所以利用所有可利用的时间，跑各类书店浏览这方面的著作。我发现，虽然信息系统安全方面的书不少，但是讨论安全体系的书却不多，特别是结合等级保护进行的安全体系建设方面的书就更难看到。虽然书的种类很多，但多数书的内容可以分为这样几类：一是介绍防火墙等安全产品的，二是介绍 PKI 等密码应用的，三是介绍黑客入侵知识的。而对信息系统安全的基础知识系统进行全面介绍的却不多。利用工作之便，我也和许多从事网管或安全的人士进行过讨论，我发现，很多人对于安全体系没有理解，他们所做的安全就是花钱买“盒子”，对于为什么要买这些盒子，他们的理解是不够深刻的。

我觉得有必要把自己的想法，与更多的人进行分享。我开始进行梳理，并规划了这部书的体系结构。

这部书计划分为三册：技术保障、管理保障和工程保障，我认为一个信息安全保障体系应该从这三个方面来考虑。(但是，能否完成这个计划，还是个未知数。)

我提出了以下几个方面的观点和想法。

(1) 三维信息安全保障模型：特别是将作为时间函数的过程作为模型中的一维。

(2) 将信息安全的属性，分为三类，第一类是信息自身的安全属性——机密和完整性；第二类是信息利用的安全属性——可用性、可控性和不可否认性；第三类是信息利用的责任属性——可追究性。

(3) 应用程序，不仅本身可能具有脆弱性，还可能会导致管理方面的漏洞。

(4) 将信息安全技术明确地分为三大类。计算机安全技术类、密码技术类和信息隐藏

技术类。并给计算机安全技术下了定义：将计算机科学理论及相应的软、硬件用于保障信息系统安全的技术。

本书讨论的是技术保障，在技术保障中，将内容分成三大部分。

第一部分是基础知识部分，从第 1 章到第 5 章。目的是尽可能全面和系统地介绍信息系统安全的基础知识，这样做的目的是有利于初学者。

第 1 章是绪论，对于一些基本的概念和知识进行了介绍，算是读这本书的一个准备。

第 2 章介绍了等级保护的一般原理。

第 3 章介绍了在信息系统安全中的基本控制理论和安全模型。对于访问控制和信息流控制及相应的安全模型作了尽量通俗的介绍。

第 4 章，对可信计算基(TCB)进行全面系统的介绍。在其他的著作中很少看到对可信计算基的详细介绍。之所以这样做，是有这样的两点考虑：①信息系统的安全保障体系的建设，说到底是要构建信息系统的可信计算基；②许多标准中大量地引用这一概念，却很少有介绍这一概念的著作，而使得一些阅读标准的人不明就里。这一描述是基于 CC 及对我国专家提出的等级保护通用标准等资料进行分析做出的。

第 5 章，考虑到读者阅读的方便和本书的体系要求，简要地介绍各类计算机安全技术、现代密码技术和信息隐藏技术。这方面的著作很多，所以这些知识的介绍没有做过多的推敲，只是简要的介绍，需要进阶的读者可以再细读其他的著作。

第二部分从第 6 章至第 10 章，介绍的是保护“信息”安全的技术体系。对信息系统进行了分层分析并提出了相应的保护方法。这些知识在许多其他书中也有介绍，但为了反映本书的思想，并为了读者阅读的方便，同时也是考虑到这部书可能要作为培训的教材，所以对这部分内容还是做了介绍。在此基础上，结合美国国家安全部(NSA)提出的《信息保障技术框架》(IATF)和我国相关的信息安全等级保护方面的一些标准和指南编写了“信息”保护技术体系分等级的建设方法。

第三部分从第 11 章至第 13 章，讨论的是安全运行维护体系，关于审计知识、防病毒知识、备份知识等，许多书中都分别做了介绍，这里没有进行介绍，但信息安全事件的分类和分等级及响应和处置，是一些书中没有考虑到的。本书总结了许多这方面的技术资料并结合国家出台的一些指南和我们在工作中的体会与实际作法而进行了编写，应急响应基本上是依据我们的实际工作的总结写出的，病毒事件的应急响应，得到了瑞星公司的技术专家的帮助。

当然，对于书中的错误包括观点的错误，我是不敢否认的，信息安全学体系是浩繁的海洋，我只看到了这海洋中的一滴水，冒然提出的东西有可能是贻笑大方的甚至是错误的，希望读者批判地阅读吧。

技术保障一章中，王楠完成了计算机安全技术中防火墙、IDS、UTM、隔离与漏洞扫描等内容和数据库安全中的部分内容，还有一些与程序语句有关的内容是在她的帮助下完成的，其余的部分由我完成。

这部书得到了很多人的帮助，首先要感谢天融信、启明星辰、三〇盛安等安全公司，他们提供了大量的资料。

要感谢上海柏安公司的张照龙先生，他给我提供了许多他们在风险评估中的方法和第一手资料；同时也要感谢北京凝瑞公司的赵峰先生对风险评估的方法论等方面给了我很好

的帮助。

感谢赵战生老师、贾颖禾老师和崔书昆老师等专家平时给我的帮助和指导。

特别要感谢我的领导、兄长梁明同志，给我创造了极为宽松的工作环境，给了我足够的空间去研究和学习信息系统安全知识。

书成稿后，王晓宇，一个刚毕业的计算机专业大学生，作为第一读者，给我提出了很好的修改意见，并帮我校对了前六章，也是对这部书的难易程度的一个检验，在此表示感谢。

作　者

# 目　录

# 第 1 章　信息系统安全保障体系概述

## 1.1　信息系统安全介绍

随着信息技术的发展，特别是以计算机和通信技术相结合的网络技术的发展，使得社会对信息系统的依赖越来越强。应当说，信息系统已经是现代社会运转的重要基础设施，离开了这样一个基础设施，整个社会将会发生极大的动荡。但信息技术的发展从一开始就忽略了一个极为重要的问题：安全。

近年来，关于各类安全事件的报道可谓层出不穷，每年都会有一些让人心惊肉跳的消息见于媒体。计算机病毒和人为入侵造成的损失每年都以百亿美元计，而且这一定是不完全的统计。可以说信息安全问题，已经是涉及国家安全、社会稳定和经济建设安全的重大问题。美国在克林顿政府时期就有人说，国家安全就是国土安全加上信息安全。

对于一个组织来说，一方面它的信息安全是国家信息安全的组成部分，另一方面，也是它内部安全的重要组成部分，甚至，对于一些组织来说，信息安全是这个组织的生命线。所以，如何解决组织的信息安全问题，是组织面临的一个重要问题，甚至是涉及组织生存与发展的重要问题。构建合理的信息安全保障体系，对于一些组织来说是头等重要的大事。

### 1.1.1　什么是信息

信息是当今社会使用频率最高的词之一。什么是信息呢？应当说目前还没有一个很统一的关于信息的定义，目前在全世界关于信息的定义有百种之多。

1928 年，哈特莱(L. V. R. Hartley)在《贝尔系统技术杂志》上发表了一篇题为《信息传输》的论文。在这篇论文中，他把信息理解为选择通信符号的方式，且用选择的自由度来计量这种信息的大小。哈特莱认为，任何通信系统的发信端总有一个字母表(或符号表)，发信者所发出的信息，就是他在通信符号表中选择符号的具体方式。

1948 年，美国数学家仙农(C. E. Shannon)在《贝尔系统技术杂志》上发表了一篇题为《通信的数学理论》的论文，在对信息的认识方面取得了重大突破，堪称信息论的创始人。这篇论文以概率论为基础，深刻阐述了通信工程的一系列基本理论问题，给出了计算信源信息量和信道容量的方法和一般公式，得到了著名的编码三大定理，为现代通信技术的发展奠定了理论基础。仙农发现，通信系统所处理的信息在本质上都是随机的，可以用统计方法进行处理。仙农在进行信息的定量计算时，明确地把信息量定义为负熵：“随机不定性程度的减少。”这就表明了他对信息的理解：信息是用来减少随机不定性的东西。

1948 年，就在仙农创立信息论的同时，维纳(N. Wiener)出版了专著《控制论：或关于

动物和机器中控制与通信的科学》，创建了控制论。后来人们常常将信息论、控制论和系统论合称为“三论”，或统称为“系统科学”或“信息科学”。

维纳从控制论的角度出发，认为“信息是人们在适应外部世界，并且这种适应反作用于外部世界的过程中，与外部世界进行互相交换的内容的名称”。维纳关于信息的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，但也有局限性。由于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，但维纳关于信息的定义没有将信息与物质、能量区别开。

1975 年，意大利学者朗高(G. Longo)在《信息论：新的趋势与未决问题》一书的序言中认为“信息是反映事物的形式、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”。

据不完全统计，有关信息的定义有 100 多种，它们都从不同的侧面、不同的层次揭示了信息的特征与性质，但同时也都有这样或那样的局限性。

1988 年，我国信息论专家钟义信教授在《信息科学原理》一书中把信息定义为：事物的运动状态和状态变化的方式。并通过引入约束条件推导了信息的概念体系，对信息进行了完整和准确的描述。

为了进一步地理解信息的定义，在此作以下的讨论。

“信息不同于信号，信号是信息的载体，信息则是信号所载荷的内容。”

“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。”当然，在计算机里，所有的多媒体文件都是用数据来表示的，计算机和网络上信息的传递都是以数据的形式进行，此时信息等同于数据。

“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，知识是由信息抽象出来的产物，是一种具有普遍和概括性的信息，是信息的一个特殊的子集。也就是说：知识就是信息，但并非所有的信息都是知识。”

从上面的讨论，我们可以把一般意义上的信息定义为：信息是事物运动的状态和状态变化的方式。如果引入必要的约束条件，则可形成信息的概念体系。这一定义，在我国已被普遍接受。

不论我们能不能给信息下一个准确的定义，但是，作为信息一定应该具有以下四大属性。

(1) 在收到信息前，对于收信者来说信息是未知的。

(2) 信息一定可以消除主体对一事物的未知性或不确定性。

(3) 信息是可以量度的。

(4) 信息是可以产生、传递、存储及处理的。

### 1.1.2 信息的分类

信息是一种十分复杂的研究对象，为了有效地描述信息，一定要对信息进行分类，分门别类地进行研究，由于目的和出发点的不同，信息的分类也不同，比如：

(1) 从信息的性质出发，信息可以分为语法信息、语义信息和语用信息。

(2) 从信息的过程出发，信息可以分为实在信息、先验信息和实得信息。

(3) 从信息的地位出发，信息可以分为客观信息和主观信息。

(4) 从信息的作用出发，信息可以分为有用信息、无用信息和干扰信息。

(5) 从信息的逻辑意义出发，信息可以分为真实信息、虚假信息和不定信息。

(6) 从信息的传递方向出发，信息可以分为前馈信息和反馈信息。

(7) 从信息的生成领域出发，信息可以分为宇宙信息、自然信息、社会信息和思维信息等。

(8) 从信息的应用部门出发，信息可以分为工业信息、农业信息、军事信息、政治信息、科技信息、经济信息、管理信息等。

(9) 从信息源的性质出发，信息可以分为语音信息、图像信息、文字信息、数据信息、计算信息等。

(10) 从信息的载体性质出发，信息可以分为电子信息、光学信息和生物信息等。

(11) 从携带信息的信号的形式出发，信息还可以分为连续信息、离散信息、半连续信息等。

还可以有其他的分类原则和方法。

### 1.1.3 信息安全

对于安全解释，在线词典上的说法：安全是避免危险、恐惧、忧虑的量度和状态。

从对信息的分类可以看出，信息安全是一个很大的概念，或者说是一个很大的范畴，只要存在着信息，就存在信息安全的问题。传统的电话通信存在信息安全问题；广播电视存在信息安全问题；报纸出版业也存在信息安全问题。所以说这是一个大的范畴，不是我们要讨论的问题，我们要讨论的是信息系统的安全问题。现在一般定义上的信息安全还是针对计算机信息系统的安全。

### 1.1.4 信息系统

2004 年公安部、国家保密局、国家密码管理办公室和国务院信息化办公室联合下发的《关于信息安全等级保护的实施办法》(公通字 2004 第 66 号)中给信息系统作了以下的定义：“信息系统是由计算机及其相关和配套的设备、设施构成的，按照一定的应用目标和规则对信息进行存储、传输、处理的系统或者网络；信息是指在信息系统中存储、传输、处理的数字化信息。”在 66 号文中，对信息给了明确的界定。应该说明的是这里说的信息，并不是指完全的信息论意义上的信息。对于信息论意义上的信息，一定是未知的；但在信息系统中的数字化信息，并不一定是未知的。

### 1.1.5 信息系统安全

国际标准化组织(ISO)给出的信息安全(实际上是信息系统安全)的定义是：“为数据处

理系统建立和采取的技术的和管理的安全保护。保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭受破坏、更改、泄露。”我国的信息安全专家也指出，信息系统的安全是：“计算机的硬件、软件、数据受到保护，不因偶然的或恶意的原因受到破坏、更改、泄露，以及系统连续正常运行。”1994 年国务院 147 号令《中华人民共和国计算机信息系统安全保护条例》第三条中指出：“计算机信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施(含网络)的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。”这里虽然没有明确定义信息系统安全，但标明了信息系统安全所涵盖的内容。

## 1.2 信息安全保障体系的基本概念

### 1.2.1 人们对信息安全的认识历程

信息安全的发展是与信息技术的发展和用户的需求密不可分的，在不同的时代也体现出不同的特征，大体来讲，信息安全经历了一个从通信安全(COMSEC)→信息安全(INFOSEC)→信息保障(information assurance，IA)的发展阶段，也可称为：保密→保护→保障发展阶段。

通信安全的历程开始于 20 世纪 40 年代，那时人们关注的通信安全，主要关心对象是以政府和军事、外交为主，多采用加密、发射传输保密等技术手段来保护数据的机密性和可靠性。同时也关心信道的安全性。

一直到20世纪80年代，以美国国防部DoD发布的《可信计算机系统评测准则》(TCSEC，俗称橘皮书)，和 DES 算法的发布为标志。这一时期，计算机从刚刚诞生，经历了电子管、晶体管、IC、大规模 IC 几个阶段，计算机的性能日新月异，而计算机的体积，从高楼大厦般的庞然大物变得小得可以放在办公桌上。计算机的软件也开始独立于计算机硬件之外，成了独立的系统，而且从功能上又将操作系统与应用相互独立开来。编制软件也从机器码发展成汇编语言和各种高级语言。这一时期，人们对信息安全的认识停留在通信保密阶段，也就是说只认识了信息机密性的这一信息安全属性。这一阶段人们的关注点在于两个方面，一是采取加密技术和访问控制措施解决对信道中传输的信息进行加密的问题，以保护信息的机密性，使之不泄露给非授权的人。另一方面是要解决信息信道本身的安全问题，即信道不被发现和破坏。实际上，这除了对信息机密性保护外，已经意味着对信道的可用性和对信息的完整性进行了某种保护，但当时人们还没有从理论的高度来认识这个问题。

20 世纪 70 年代以后，计算机软硬件技术开始快速发展，并且开始出现了对内开放、对外封闭的计算网络。这种环境下的信息安全可以归纳为对信息系统的保护，即信息安全，典型标志是美国国防部制定的彩虹系列中的橘皮书以及欧洲四国制定的 ITSEC，TCSEC 以信息安全的机密性为主，ITSEC 则强调保障信息的机密性、完整性、可用性(即著名的信息安全三原则 CIA)。其后由于社会管理以及电子商务、电子政务等的网上应用的开展，人们又逐步认识到还应关注可控性和不可否认性。至 90 年代中期，这个时期可以大体归结为信息安全时期。