第1章　信息内容安全是当今形势发展的需要

1.1　信息与信息内容的性质与作用

什么是信息，这是一个既简单又复杂的问题，它的简单性导致人们陷入了“画鬼容易画人难”的尴尬境地，它的复杂性又使得人们进入了“知其然而不知其所以然”的迷宫。因此在众多的信息论著作中，对信息的定义和描述，种类繁多，观点纷纭。但是就信息的本质而言，在当今信息时代，我们仍然有必要简单地分析一下信息的基本属性。

众所周知，世界的本质是物质的，而物质是运动的，这种运动又有其内在的规律性。世间万物，都有反映和被反映的特征，这种特征形成了时空运动状况差异的运动机制。如何反映这些差异，这就是信息的本质属性。

信息之所以受到当今社会的高度重视和得到广泛应用，是其特有的属性所决定的。一方面人们对其特性可以归纳为普遍性、客观性、无限性、动态性、可度量性、可传递性等诸多正面特性，另一方面还可以归纳出其不完全性、异步性、可伪性、衍生性等负面的特性。总而言之，信息的意义在于可以极大地影响人们的认识与行动，所以这种影响既可以是正面的、积极的，也可以是负面的、消极的。也正因为这种原因，必须对信息的两重作用都要给予足够的重视。信息的作用效果取决于信息的四要素：信息内容以及信息量、针对性和适时性。这一点对信息的正面作用和负面作用都是一样的。由此可见信息内容是十分重要的。因此确保信息内容的安全是一个极为重要的课题。我国刚刚走上信息化建设的道路，在信息化建设中也取得了

一定的成果。但由于我国还处于发展中国家正在跨越工业化走向信息化的历史进程中，许多涉及的政策法规包括信息安全的政策法规研究时间短、起点低、范围小，至今仍缺乏有效的理论基础，一些基本的概念尚未明确，对信息安全政策法规的研究，其水平还不高，因此，探讨信息内容安全问题的含义及内容是极其有意义的。

1.2 信息社会导致了对信息内容安全问题的格外关注

信息社会化是当今社会、经济、文化发展的必然趋势，它涉及信息的生产或使用两大方面。但是如果从这两个方面进行考察，可以得出不同的涵义。

信息生产的社会化，与劳动社会化、生产社会化的涵义相类似，它是指信息的获取、变换、传递等活动越来越具有社会性，分工细化，专业化加强，协作日益发展。因此，最终的信息产品或服务，成了越来越大的社会集体的劳动成果，很难说是某个人或少数人单独劳动的产物。这样理解的信息社会化，对一切信息都是适用的。在现代条件下，即使是绝密情报信息的生产，也离不开有关人员的配合和社会提供的必要手段。

信息使用的社会化，与信息共享的涵义相类似，说的是信息越来越向社会公开，让更多的人所利用。毫无疑问，应当公开和可以公开的信息，应该放手供社会上需要者利用，才能最大限度发挥这种信息的效用。不符合国家保密法规规定的不适当的保密制度和办法，诸如认为保密范围越大越好，任意扩大保密范围，以及信息资源拥有单位或部门，视信息资源为部门私有，因一些部门长期处于分割状态而拒绝信息共享等等现象，都会严重阻碍信息的流通，使信息拥有者“消化不良”，使信息需要者“营养不良”。这对信息资源是一种巨大的浪费。但是，相当一部分信息资源在一定的时间周期内有保密性，不能外传，是不能随便提供给任何人共享的。例如，涉及国家安全和国家秘密的信息，个人隐私，企业商业秘密和专利等。所以，并非任何个人的、企业的和国家的信息都可以向社会公开，这类需要保密的信息在其使用方面就要遵守国家法律法规的约束和规定。至于非保密信息，需视具体的内容来决定它在使用中有没有必要社会化。很明显，特定的信息只对它的需要者有使用价值,对其他人即使让他们‘共享”,他们也不会感兴趣。使用信息是要花费财力、物力或时间和精力的，把财力、物力或时间和精力用在不需要的信息上，也是一种浪费。所以，就加密信息和不为使用者所需要的非密信息来讲，提倡其使用的社会化

是毫无意义的。

目前流行的对信息社会化的一种理解，恰恰是属于上述的后一种。其理论依据是：商品经济越发达，越要求信息在社会中公用和共享。固然，商品经济的发展促进了信息的商品化，采取商品形态的信息日益增多。但是,事实上,即使在商品经济很发达的资本主义国家，非商品化信息大量存在。在商品经济的发展过程中，存在商业秘密，这也不容抹煞。社会主义的有计划商品经济在我国的发展，必然会促进一部分信息商品化，但不会出现商品化信息在量上超过非商品化信息的情况。商品化信息只对花钱购买它的经营者才谈得上有使用社会化的意义，而对购买不到或未曾购买它的社会成员来说,仍不能“公用”“共享”这种商品化了的信息。

正确的结论是，从生产上来理解信息社会化，是有意义的，而从使用上来理解信息社会化，应有条件，不能泛指一般信息，只能限于一部分有内容需要的特殊信息，即其内容为接收者所需要而又可以公开的信息。

信息不但是管理的基础，而且它本身还是管理的对象。信息与物质和能源一样，是一种资源。资源需要开发和利用，也需要管理。信息政策与法规，就是把信息作为管理对象，对信息与信息内容及其安全进行管理的一种形式。

1.3 信息内容安全问题的法律环境

国外最早的信息立法，产生于18世纪欧洲的瑞典。1776年瑞典发表了《出版自由法》，是目前业界认为迄今为止的世界上最早的一部信息立法。直至1969年,瑞典又成立了“官方文件公开化安全保密工作委员会”。但是，正像世界上很多事情一样，往往最早产生于欧洲，然后中心又从欧洲转移到美洲，信息政策和信息立法也是这样。它一开始产生于欧洲，但真正兴起信息立法是20世纪的事情。因为《出版自由法》是对传统信息的立法，而现代信息法是与电子化联系起来的。从发达国家来看，现代信息政策与立法主要兴起于20世纪70年代。1967年,美国颁布了《信息自由法》，强调信息要自由流通。世界上大部分国家或地区信息立法都产生于20世纪70年代，从时间顺序上排列如下：

1973年,瑞典出版了《数据资料管理法》,此法于1979年、1981年又做了两次修改。从中可以看出，瑞典在信息立法方面是有基础的。1976年,美国颁布了《在阳光

下的政府法》，内容就是政府的一些公开政策应该让群众了解，群众有权了解政府信息。政府的会议文件在开会时是保密的，但开完后成了历史时应让群众了解。1978年，法国颁布了《信息科学归档文件卡片与自由法》，其用意是归档文件应当让公众有自由查阅权。1984年，英国颁布了《数据保护法》，针对数据需要公开但又有安全、保密的问题，用该法律规范了解决这两方面的矛盾的办法。加拿大作为一个发达国家,也先后颁布了《个人隐私法》和《查询信息法》。

各国所颁布的这些法规虽然名称不一样，但含义却是一样的。一方面，信息为了要自由流通，所以要公开；另一方面，信息内容又涉及私人的秘密、企业的秘密和国家秘密，必须通过一系列法规包括隐私法，来解决信息内容的保密问题。

与发达国家相比较，发展中国家在信息立法方面起步较晚，比较早开展这方面工作的有巴西。 1984年，巴西就颁布了《国家信息政策与其他措施法》。

到了20世纪70~80年代，信息在国际间的流动加强了，特别是随着软件和信息内容传播业的发展，提出了信息也即信息内容产权的问题。所以，不仅是每个国家有了自己的信息法规，而且国家之间共同的法规也提出来了。 1971年,联合国提出《世界知识产权组织关于保护计算机软件的示范条例》。1985年，经济合作与发展组织的国家通过了一个《过境数据流的宣言》，因为数据出现跨国流通后，涉及各国的政策。这一法规是在经济合作与发展组织的范围内解决信息跨越国境的问题。

以上可以看出，涉及信息内容的一系列政策与法规问题是在20世纪70年代随着信息管理、信息资源共享、信息公开化，以及保密和隐私问题而提出来的。

以加拿大为例，该国政府高度重视信息立法问题，包括就信息内容安全问题涉及的立法问题给予了足够的重视，目前已经有了8个方面的立法：

（1）《查询信息法》，该法要求政府的一些公开的信息应该让老百姓查询、共享。

（2）《隐私法》，信息公开化会涉及一些私人、法人和企业的秘密，此法是解决私人及企业的保密问题的。

（3）《政府信息交流政策》，该法要求政府的信息要互相交流。

（4）《政府安全保密政策》。

（5）《文牍削减法》,此法的规定就是对文件太多加以限制。因为信息太多了,就干扰、污染了必要的信息。

（6）《统计法》。

（7）《档案法》。

(8)《图书馆藏书管理法》。

后3个法是专业法。

从以上背景我们可以看到，到目前为止，世界各国都对信息内容安全给予了足够的重视，并采取了多种形式的信息立法方式来加以调整。所谓信息内容安全的政策与法规、条例，都是根据客观实际需要，针对具体问题制定的法。比较具体的主要有两个,一是《查询信息法》,政策信息大家可以查询另一个是《隐私法》,解决保密问题。其他是关于信息交流的。从信息政策和法规的发展，可以看出它是一个过程，它是为具体问题的需要所制定的一些政策法规和条例。这些规则性的东西，旨在加强对信息的管理。

我们以前不太注意信息是有周期的，实际上，信息内容安全政策与法规是从信息周期出发而制定的。信息从开发、采集、加工、存储、归档、传播、利用,最后废弃，是有一个周期的。从信息采集一使用—废弃,到新的信息来代替它,是一个周期,信息管理要适应这个周期的变化，而且要根据信息周期变化的不同阶段的特点以及客观的需要，制定不同的政策法规，来加强对信息的管理。这是从信息本身的特点来看的。另外，尽管各个信息法规是针对具体问题的，但政府的信息政策法规，有一个协调完整的体系问题，各个法规要相互不矛盾。如档案法要和政策查询法一致，相互协调成为一个完整的体系。还有一点就是，信息内容安全立法都是为了保护国家的利益，如《过境数据流的宣言》解决信息跨国境问题，也是为了保护国家利益。一方面使信息能够为每个国家共享；另一方面，它要保护每个国家的主权和独立的利益。因为现在还有国家的界限，即使像欧盟组织内的国家，虽然由于经济发展的需要要实行共同市场、共同货币，但国家还存在，也有各自不同的利益。政策法规就是要保护这种东西，其中包括过境信息流问题，也即信息内容问题。我们研究涉及国外信息内容政策与立法问题，是为了解决我们国内的问题。近年来国家有关部门已经加大了国家信息立法的研究工作，预料“十五”期间国家将在信息立法工作上有较大突破，其中也包括涉及信息内容的主要法规。我们相信，随着我国信息化进程的加快，建立健全我国的信息化法律环境，将会有力地推动我国经济的发展。

1.4 信息内容安全是国家信息安全政策的重要组成部分

1.4.1 信息政策与信息安全政策

关于信息政策的概念，学术界作了不少探讨，其中下列意见比较具有代表性：

(1)美国学者认为，一切用以鼓励、限制和规范信息创造、使用、存储和交流的公共法律、条例和政策的集合即为信息政策。也可以说，信息政策是一个由信息的生命循环圈的监视和管理的指导原则、法令、指南、规则、条例、手续而构成的相关政策群体。

(2)日本学者认为，信息政策是包含了通讯政策、信息通讯政策、传播政策的全部内容，并且具有广泛射程的发展性的概念。

(3)我国不少学者都提出：信息政策是指国家用于调控信息业的发展和信息活动的行为规范的准则，它涉及信息产品的生产、分配、交换和消费等各个环节，以及信息业的发展规划、组织和管理等综合性的问题。信息政策着重解决信息总供给与总需求的平衡问题和信息产业结构优化问题，从而实现信息产业协调发展的政策。因此信息政策是一个国家或组织在某段时间内为处理信息和信息产业中出现的各种矛盾而制定的具有一定强制性规定的总和。

从以上学者们给出的定义可以看到，信息政策包括了国家信息安全策略的内涵。由于信息概念的广泛性与不确定性，字面含义可理解为消息、情报、新闻、知识等，这决定了信息政策研究客体的复合性。同时，学术界对信息理解有广义和狭义之分，不同的理解，对信息政策的概念有不同的定义。若把信息放在经济领域来理解，就必须解决信息的供求问题，信息从生产到消费整个过程的控制以及产业的规划、组织、管理等问题。若从管理学的角度来理解，信息政策是国家根据需要制定的有关发展与管理信息事业的方针、原则和办法。信息安全包括信息内容安全是其中不可或缺的组成部分。

还应该看到的是，由于各国的信息业发展及信息化、社会化水平不一样，造成各国信息政策不同。这是由各国国情不一样所造成的。然而尽管各国对国家信息政策理解的角度和侧重点不一样，但当今各国都对信息安全特别是政府信息资源安全给予了高度重视。信息事业的发展战略和目标不断变化，信息业的外延不断延

伸，造成了信息政策概念的变化发展。美国早期信息业的发展战略，也是主要局限于科技信息方面，信息政策的内容基本上还以传统的科技信息政策的系统建设和工程规划为主，对于信息活动的指导仅限于宏观管理，这就是小信息政策概念。20世纪90年代以后，以美国为代表的发达国家在社会生活各个领域全面推进信息化建设，掀起了新经济的热潮，对制定国家信息政策包括信息安全政策提出了更加紧迫的任务。中国的信息产业建设起步较晚，信息化水平还不高，过去有一段时间在国家信息政策的阐述上更多涉及信息基础设施建设，如信息产业、信息高速公路、信息资源与供求方面的问题，而对于个人隐私、跨境数据流、信息安全等涉及较少，这是很不妥当的。这反映了我们信息安全意识比较弱和我国信息化水平较低。可喜的是我国政府特别是高层领导及时注意到这个具有重大意义的问题，现在已经对信息安全问题给予了高度重视。我国科技工作者也在自己的实践中努力耕耘，力争在这个领域为我国信息化建设发挥保驾护航的作用。

由于信息政策在概念上就具有复合性、广泛性和复杂性的特点，又涉及生产、流通使用和反馈的各个方面，所以其内涵离不开涉及信息内容的政策。应该说国家信息政策的总体目标是促进信息资源充分开发和有效利用，促进经济和社会的发展，但值得强调的是，国家信息政策的制定离不开国情，与国家的总体发展目标、体制、经济、社会状况、文化背景及信息化水平等有关。不同的国家根据自己的国情制定不同目标的信息政策，研究内容的多寡及侧重点也有所不同，其中涉及信息内容政策和法规更有比较大的区别。

发达的资本主义国家，信息化水平高，市场自由化程度高，公民信息意识强，信息政策内容较多地关注私营企业信息产品的开发、信息技术的自由竞争、协调私有企业的融合发展和投资兴建信息基础设施，但也会保障一些国有的信息系统和信息基础设施的建设。如美国强调信息自由化，目前还没有公开的、统一的信息政策，但对信息政策问题进行了大量研究，其内容范围除涉及信息本身的版权、通讯、信息技术、跨国信息传送外，还研究且通过了不少对各种信息机构的信息活动进行约束的信息政策，注重协调政府和私人机构的调节，形成了比较完整的信息体系和自发调节机制，其各联邦政府也重视信息法律的制定。而日本由于能源和资源贫乏，视信息为资源和重要的竞争要素，充分发挥信息技术，扶植信息产业和促进信息传播，构成以科技信息政策和信息传播政策为主体的国家信息政策。在发展中国家，由于信息化水平低下，经济自由性缺乏，公民信息意识薄弱，国家信息政策的功能更多地是在宏观上改善信息环境，通过各种措施调整信息系统的结构和协调信息

工作，加强信息基础设施建设，发展信息技术，发展包括提供信息内容服务在内的多种信息服务业。对关于政府和私人的信息活动调节机制关注较少，对个人信息权益、信息产权和信息内容安全较少涉及，信息技术和信息产业方面还处于国家垄断，信息市场的自由机制不完善，信息法制不健全。所有这些都成为发展中国家在跨越“数字鸿沟”中必须解决的问题。

1.4.2 信息内容安全是符合我国国情的信息安全政策的要素

我国信息政策研究是从科技信息政策着手的，而科技信息政策本身就尚不健全,缺乏系统性。我国信息化水平较低,公民信息意识也十分薄弱,随着科技发展和信息业的崛起，信息政策内容上存在的许多薄弱环节已显露出来，如政府信息缺乏保障，信息机构难以协调，信息基础设施建设资金缺乏，信息犯罪和污染问题突出等。综合我国国情,借鉴外国经验,我国应加快制定信息产业政策,完善有中国特色的信息政策内容体系。我认为信息安全政策应包含以下内容：

（1）信息资源保障政策。包括国家、政府信息资源建设指导政策，国家信息基础设施建设政策，资金投入和信息人才保障政策，信息机构管理政策。

（2）信息产业发展政策。包括计算机产业政策，软件业和数据业政策，信息技术政策，信息服务政策和信息市场指导、管理政策。

（3）信息交流与合作政策。包括信息资源共享政策，信息工作、信息技术及信息标准统一指导政策，国际、国内信息交流与合作政策。

（4）通讯、广播政策。包括国家邮政、电信网络建设指导政策,有线电视和无线广播网络建设和管理政策，信息传送与扩散政策。

（5）信息安全、保密政策。包括政府信息资源保密政策,保障个人隐私政策,信息系统和信息网络安全政策，信息内容安全政策，知识产权法规政策，跨国数据流控制与管理政策。

信息政策的内容是变化发展的，并与国家的政治、经济利益紧密相连，已经从单一的学术研究扩展到国家主权问题、信息安全问题和信息经济学方面的问题。隐私权、信息安全保密、越境数据流、信息立法越来越成为信息政策研究的重点。学术理论界也不断完善信息政策的内容体系，我希望有更多学者加入到这项工作中来，为确立有中国特色的信息政策体系而努力。

综上所述，国家信息政策含义是变化发展的。随着社会信息化的发展状况、公民信息意识的不同，随着学科的发展和科技时代的进步，国家信息政策总在不断地

调整和改变，其中变化之一就是涉及信息安全的内容更加丰富了，内涵更加广泛了，其中信息内容安全政策已经成为一个重要的组成部分，由此带动了一个范围十分广阔的研究领域。

1.5 当前信息内容安全面临的主要问题

鉴于我国信息技术和信息产业发展与技术先进国家存在较大的差距，我国信息化建设需要的大量基础设备依靠国外引进，这种状况在今后相当长的时期内不能彻底改变。引进设备中的核心芯片和系统内核逻辑编程都掌握在他人之手，无法保证我们的安全利用和有效监控。

目前我国信息与网络安全的防护能力处于发展的初级阶段，许多应用系统处于不设防状态，当务之急是要用我国自己的安全设备加强信息与网络的安全性，大力发展基于自主技术的信息安全产业。而自主技术的发展又必须从信息与网络安全的基础研究着手，全面提高创新能力。而我国的信息与网络安全研究尚处于忙于封堵现有信息系统安全漏洞的阶段，宏观安全体系研究上的投入严重不足，不能从根本上解决我国的信息与网络安全问题。目前，我国还需从整个安全体系的高度开展强力度的研究工作，从而为解决我国的信息与网络安全提供一个整体的理论指导和基础构件的支撑，并为信息与网络安全的工程奠定坚实的基础，推动我国信息安全产业的发展。

据美国信息内容安全软件公司（Contents Technologies）在日本的分公司对日本所进行的调查表明，日本企业一方面担心公司内部的机密信息通过电子邮件泄露出去，而另一方面却忽略为防止发生泄密而导入安全措施，并且对“信息安全性”的理解甚为肤浅。仅就电子邮件的安全而言，就包括与电子邮件内容等相关的安全性问题。例如当通过电子邮件公司的机密被泄漏，或者不适合发表的信息外流时，就存在着信息安全性的问题。

据调查结果显示，与黑客的攻势及病毒猖獗相比较，企业用户对信息内容安全性的意识相差甚远。例如，认为对通过电子邮件故意泄露公司内机密的事件，有必要采取某种对策的企业高达44.4%，而实际采取对策的企业却只有区区的10.7%。对于通过电子邮件收发个人用途的大容量影视数据从而导致系统发生故障的问题，

有40.3%的企业认为有必要采取措施，而对此实际上采取了措施的企业也只有10.7%。对于信息安全性的概念回答“知道其含义”的占34%,回答‘曾经听说过’的占53%,回答‘不知道’的占13%。经解释信息安全性的概念后重新提问其必要性后，有98%的被调查者回答“应该引进信息安全性对策”。

主办此次调查的机构负责人指出，“有太多企业认为只要设置了防火墙，安全性对策就可以高枕无忧了。”“如果将安全性概念比做入境手续，那么用来阻止病毒及黑客入侵的防火墙就相当于检查护照的入境审查。当然，光靠入境审查还不够，应该设置用来确认电子邮件的内容及其收发路径的海关。”

如果设置了针对电子邮件的“海关”，通过确认电子邮件的内容，可以避免出于故意或者由于电子邮件软件的误操作而导致机密信息向外部泄露。为了使“海关”能够发挥正常的功能，很重要的一点是严格规定有关电子邮件的公司内部规则。据本次调查表明，已经制订了公司内部有关电子邮件使用规定的企业为48.1%,还不到半数。

该调查表明，多数企业对“信息安全性”有关问题的认识水平亟待提高,对信息内容安全知之甚少。企业如此，政府机关和个人的情况也类似。不少单位和个人屡屡发生的安全事件，国内外敌对势力利用安全漏洞，破坏信息内容，网站被黑客入侵时有发生，也从反面告诉我们，信息内容安全，已经成为当今信息安全的一个重大问题。

第2章　信息内容安全概念的递延和发展

根据《汉语大词典》（罗竹风主编）的解释，“安全”有两层含义：其一是指“平安，无危险”；其二是指“保护、保全”。“保密”则指：“保守事物的秘密，不使泄漏。”所以，信息内容安全也具有上述两个方面的含义，但在具体的工程应用和社会实践中情况就比较复杂。

随着全球信息化的飞速发展，我国大量建设的各种信息化系统已经成为国家关键基础设施，其中许多业务需要与国际接轨，诸如电信、电子商务、金融网络等。随着网络信息安全已成为亟待解决、影响国家大局和长远利益的重大关键问题，随着信息安全保障能力已经成为 21 世纪综合国力、经济竞争实力和生存能力的重要组成部分，信息内容安全问题日益重要，成为世纪之交世界各国在信息安全领域奋力攀登的制高点。如果解决不好将全方位地危及我国的政治、军事、经济、文化、社会生活的各个方面，使国家处于信息战和高度经济金融风险的威胁之中。

信息内容安全特别是网络环境下的信息内容安全与保密是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题。从技术角度看，网络信息安全与保密是一个涉及计算机科学、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边缘性综合学科。而信息内容安全则是网络信息安全与保密的重中之重。特别是随着全球信息基础设施和各国信息基金设施的逐渐形成，国与国之间变得“近在咫尺”。网络化、信息化已成为

现代社会的一个重要特征。网络信息本身就是时间，就是财富，就是生命，就是生产力。实际上，网络的快速普及、客户端软件多媒体化、协同计算、资源共享、开放、远程管理化、电子商务、金融电子化等已成为网络时代必不可少的产物。

事物总是辩证统一的。科技进步在造福人类的同时，也带来了新的危害。从某种意义上讲，网络信息系统的普及，就像一个打开了的潘多拉魔盒，使得新的邪恶与罪孽相伴而来。涉及信息内容的各种犯罪活动已经严重地危害着社会的发展和国家的安全，也给人们带来了许多新的课题。网络信息内容的保密、安全和健康便是这些众多新课题中最具代表性的课题。

2.1 信息域的划分决定了信息内容不同的安全级别

在每个机构内部，通常将要进行处理的信息依据其功能被划分为以下几种：管理、人事、后勤等，一些可能是公用的，而另一些则是秘密的。秘密信息又可以分为许多类型：个人隐私，公司内部的商业秘密，政府执法信息、秘密信息、绝密信息以及受限制的敏感信息等具有不同密级的信息，如上划分的信息可用性又称“信息域”。

政府部门与商业机构都有其需要保护的公共信息与秘密信息，任务和环境决定了保护具体信息的方式与程度。例如在美国政府国家安全局发布的《信息保障技术框架》中明确提出了联邦政府专用信息的密级级别：无密级、秘密、机密和绝密在各个级别之中还可能有用于某些特定团体的子级别。

多数机构对于其专有信息的保护都有比公共信息保护更为严格的要求，首先，对这些信息的访问是受控制的，在涉密的政府领域，这个要求通过秘级划分、特殊限制与“应需可知（need to know）”的标志得以实现。除了访问控制之外，还需要更严格的技术性安全措施。级别越高，采取的安全措施越严格。依据访问控制、需要和保护需求对信息进行划分便产生了不同的信息类别，又称信息域。机构将实施具体的机制进行信息化分，并在信息域之内或之间进行有意义的信息流动。

在协作环境中或跨不同级别的信息域之间进行信息保护具有挑战性。共享信息的机构需要取得对信息的敏感级别和保护信息的方法的一致性意见。不同机构

对信息域的敏感程度有不同的理解，信息共享的各方需要进行协商，并在此基础上提出一个各方均满意的解决方案因此专家和管理部门都提出了有关信息资源与边界的概念。这就是说信息资源具有其物理和逻辑位置，而所谓边界就在其间所以必须研究确定应该保护哪些资源，使其不受外界影响，确保在最恰当的地方采取保护措施并获得最好的效果。所以一般认为“边界”可以定义为受一个单位某一位置策略控制的信息和信息系统的边缘。

为了实现有效的信息保护，美国国防部牵头定义了名称为“深度防御”的信息保障战略，具体如表 2.1 所示。

表2.1　　信息保障框架

人　员	技　术	操　作
培训	深度防御技术框架域	分析
意识	安全标准	监视
物理安全	获得IA/TA	入侵检测
人员安全	风险分析	警告
系统安全管理	证书与信任	恢复

备注：IA：Information Assurance（信息保障）TA：Technicalassurance （技术保障）

信息基础设施是具有许多脆弱性的复杂系统。为此，信息保障技术框架在深层防御战略的基本原理中采用了多个信息保障技术解决方案。在攻击者成功地破坏了某个保护机制的情况下，其他保护机制能够提供附加的保护。采用层次化的保护策略并不意味着需要在网络体系结构的各个可能位置实现信息保障机制。通过在主要位置实现适当的保护级别，便能够依据各机构的特殊需要实现有效保护。另外，分层策略允许在适当的时候采用低级别的保障方案以便降低信息保障的代价，同时也允许在关键位置（例如边界）明智地使用高级保障解决方案。所以信息保障并非是一个静态概念，而是一个持续性的适应过程。

2.2 全面地把握信息内容安全的内涵

长期以来，人们把信息安全理解为对信息的机密性、完整性和可获性的保护，这固然是对的，但这个观念是在20多年前主机时代形成的，因此它是面向单机、面向数据的。20世纪80年代进入了微机和局域网时代，计算机已从专用机房内解放到分散的政务或商务桌面乃至家庭，由于它的用户和网络结构比较简单、对称，所以既要依靠技术措施保护，还要制定人人必须遵守的规定。因此，这个时代的信息安全是面向网管、面向规约的。

20世纪90年代进入因特网时代以后，每个用户都可以连接、使用乃至控制散布在世界上各个角落的上网计算机，因此因特网的信息安全内容更多，更为强调面向连接、面向用户(“人”)。因为在这个崭新的世界里，人与计算机的关系发生了质的变化。人、网、环境相结合，形成了一个复杂的巨系统。通过网上的协同和交流，人的智能和计算机快速运行的能力汇集并融合起来，创造了新的社会生产力，丰富着大量应用（电子商务，网上购物等）和满足着人们的各种社会需要（交流、学习、医疗、消费、娱乐、安全感、安全环境等）。在这个复杂的巨系统中，“人”以资源使用者的身份出现，是系统的主体，处于主导地位。而系统的资源（包括硬软件、通讯网、数据、信息内容等）则是客体，它是为主体即“人”服务的。与此相适应，信息安全的主体也是“人”(包括用户、团体、社会和国家)，其目的主要是保证主体对信息资源的控制。可以这样说：面向数据的安全概念是前述的保密性、完整性和可获性，而面向使用者的安全概念则是鉴别、授权、访问控制、抗否认性和可服务性以及在于内容的个人隐私、知识产权等的保护。这两者结合就是信息安全体系结构中的安全服务功能，这些安全问题又要依靠密码、数字签名、身份验证技术、防火墙、安全审计、灾难恢复、防病毒、防黑客入侵等安全机制（措施）加以解决。其中密码技术和管理是信息安全的核心，安全标准和系统评估是信息安全的基础。信息安全的体系结构如图2.1所示。

图 2.1　信息安全体系构架示意图

现代的信息安全涉及个人权益、企业生存、金融风险防范、社会稳定和国家的安全，它是物理安全、网络安全、数据安全、信息内容安全、信息基础设施安全与公共和国家信息安全的总和。信息安全的完整内涵是和信息安全的方法论相匹配的，信息安全系统是一个多维、多因素、多层次、多目标的系统。因此，有必要从方法论的角度去理解现有的信息安全模式。总的说来，至少有以下两种方法必须考虑：

(1)分析与综合的辩证思维方法。要在分析过程中从整体上把握好分析要素的内部矛盾，例如：在威胁分析中的环境灾害与人员失误、无意疏忽与有意破坏、外部人员与内部职员、窃密篡改与拒绝服务、个人行为与有组织的信息战等关系；在脆弱性分析中的软件、协议缺陷与嵌入后门、网络层、系统层、应用层薄弱环节的关联等；在攻击分析中的利用技术漏洞与社会工程、行为模式与隐蔽方式等关系。在综合方法上则应该面向过程，着眼发展风险管理的综合方法：立足于尽量减少风险，实行资产评估,风险估算,重点选择,综合平衡,政策制定,系统实施,审计监管等的全过程和全面质量管理。对于安全评估的综合方法，则应该面向设计过程，强调系统总体评价。在评估标准上掌握好传统与现实、国际通用互认和中国特点的关系。在保护轮廓内掌握好安全功能和保障的关系。

(2)从系统复杂性的观点理解和解决安全问题。信息内容安全是过程、政策、标准、管理、指导、监控、法规、培训和工具技术的有机总和。这需要在不同层面上面向目标，用定性与定量相结合、技术措施与专家经验相结合的综合集成方法加以解决。对信息内容的管理则要从源头、传递、网关、服务网站和用户层面进行综合治理。我们处在网络调整发展和科技突飞猛进的时代，要以创新精神跟上网络和安全技术的新发展。有关影响信息内容安全的过程和因素参见图2.2。

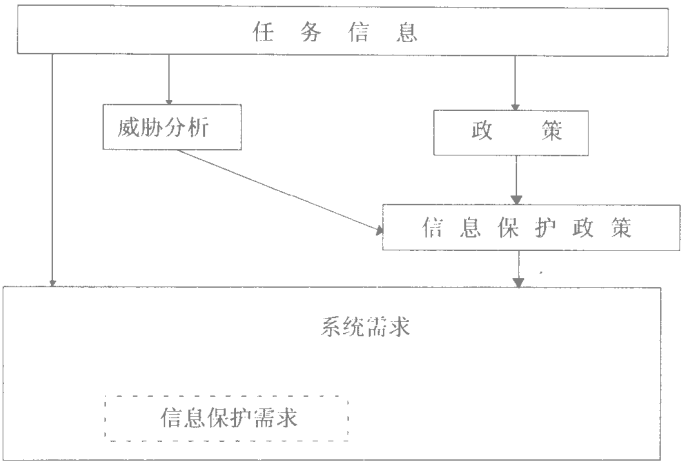

图2.2 系统任务、信息安全威胁和政策对确定信息保护需求的影响示意图

信息安全技术是具有对抗性的敏感技术，面对日益迫切的需要，惟一的出路就是自主研究和开发，同时必须密切跟踪国际信息安全技术的新进展，才能知己知彼，为我所用。在技术创新上以下发展值得注意：

(1)在信息安全系统的构建、模式、评估方面。风险管理技术已由传统的相对固定的模式向灵活的不断反馈、不断演进的弹性模式转化，强调可测量的方法体系，形成所谓“有适应能力的风险管理模式”。10年前，信息安全系统构建理念是“自上而下’即顶层设计。从因特网的历史特点和发展现实出发，需要先‘自下而上”，接着“上下结合”，然后再在网络的确定范围内从全局上规划，构成安全体系。系统安全不能做到一劳永逸，需要动态地构建模型。在安全功能、服务的配置上，过去是先从整体定义入手，但是因特网是个多元化的应用环境，而且日新月异，因此现实的解决办法是‘分而治之”。各种应用，各个部门，先在统一的规范下“从我做起’或者分层分步实施。这在相当一段时间内，是推动网络发展、激励安全应用的现实途径。

(2)新的安全协议不断出现，有的已趋于成熟，例如大家熟知的IPv6已被公认安全性较强，又能比IPv4提供更好的互联互通功能，很有可能进入主流，如何使我们的安全产品能同时支持IPv6已提到日程上。

(3)树立新的实体安全观念。几年前，针对因特网网中网的特点出现了基于“入口防守”的概念或防火墙，它发展很快，迅速普及，目前仍是因特网安全的主要卫士。但防火墙无论从基本概念或实际功能都不可能完全满足安全的多种需要，随着

网上人口大量增加和信息流量直线上升，一些新思路、新设施应运而生：

智能化实时安全监控系统：包括基于统计偏离的实时入侵检测（针对内外入侵等）和基于违规的实时检测（针对用户违规调阅网上资源如黄色材料等）。系统在识别入侵以后随即做出反应，或与防火墙配合进行控制。

自适应网络安全检测软件：能主动地找出系统的安全隐患，对风险做出半定量的分析，提出堵塞漏洞的方案，自动地随着计算环境的变化，通过入侵模式识别，对系统安全做出校正，这样就由被动防守转向了主动防守。

积极防御的反黑客工具：能在一定条件下对入侵进行取证乃至追踪，这是由被动防御转向积极防御乃至自卫反击的一种新技术。

智能"代理"发展很快，"代理"在用户控制的范围内散布和移动在各关键部位。代理的功能由管理者定义，它们在统一政策的统帅下执行指定的任务，代理具有部分的自治和自保护功能，代理之间还可以交换风险信息并协同工作，检测出入侵后向中心报告并发生警号，它在一定程度上解决了管理的集中性和防卫的分散性的矛盾

各种信息安全设施日趋综合化、集成化和智能化，如防火墙的联防，混合防火墙的出现，防火墙与入侵检测和安全代理的联用等。

基于反应时间的入侵对抗技术：鉴于因特网的网络接入点和脆弱点呈指数型增长，安全观念由"御敌于国门之外"向"运动战"的方向发展。这种模型认为入侵是不可避免的，问题取决于检测到入侵所需的时间和做出反应的时间。在这里，人机结合的智能系统将扮演关键的角色。

(4)重视密码技术的研究和开发。据报道，目前密码技术研究速度比10年前加快了10倍，密码技术的实现越来越集中在芯片技术上（智能IC、纳米技术）。由于密码大量普及到商业和个人用途，商用密码、密钥托管、密钥恢复、可信第三方等是当前的热点，新的密码算法SSO口令和信息掩蔽技术不断出现。

(5)现有系统的安全增强。众所周知，目前操作系统、应用程序和信息处理芯片等组件是由西方几家大公司主导的，为保证自主的安全功能，各国都在寻求出路，其中包括设置安全外壳、打安全补丁、设置统一的安全接口界面、优化操作系统内核、发展自由软件等。将各组件作为黑箱，用控制论的方法来解决问题。系统安全性的测评认证工作是信息安全的重要保证。

(6)基于个人和基层的信息安全技术。移动通信个人化、计算机个人化及家庭政务化是世界潮流，这里实际上就是"网络空间"和"现实空间"的接口和界面，它的信息安全问题日益凸显，提出了以个人认证作为基本逻辑单元的安全思