中国信息安全产业发展白皮书

（2005—2010）

中国信息产业商会信息安全产业分会

前言

中国信息产业商会信息安全产业分会（以下简称商会）2002 年 3 月 29 日正式成立，当年，商会对我国信息安全产业进行过一次较全面的调研，并写出《我国信息安全产业调研与建议（2002 年）》。三年来，信息安全产业自身发展与环境发生了许多重要的变化，出现了一些新的情况与要求，有必要编写一本《中国信息安全产业发展白皮书（2005—2010）》（以下简称白皮书），为我国信息安全产业制定发展战略提供咨询意见，同时为信息安全产品、技术与服务的用户提供咨询服务，也为国家政府主管信息化安全部门提供参考意见。

本白皮书分成三部分：

第一部分：信息安全产业情况

第二部分：信息安全技术发展展望

第三部分：我国信息安全产业发展建议

中国信息化安全事业在近几年来得到快速的发展，这种发展首先是由于从中央到地方政府的广泛重视。国家把国家安全划分为国土安全、政治安全、经济安全和信息安全，信息化安全是其中重要的组成部分。因此，信息化安全市场得到迅速的发展，使信息化安全建设的需求在不断扩大。其次，这种发展还由于我国有一批积极进取的信息安全的创新企业，促进了信息安全产业的发展。还应当看到，我国信息化安全领域有一批敢为天下先的高水平的专家队伍和信息安全产业的商会在推动产业发展和凝聚企业发挥了较大的作用。

我国信息化已经有 20 多年的历史，而比较大规模的信息化安全建设也仅有近 10 年历史。对十年来信息化安全建设进行总结与分析，树立信息化安全新认识，并在此基础上奠定信息化安全的新起点，从而开辟信息化安全的新领域，积极培养新的发展增长点将发挥重要作用。信息化安全建设必须从出于对“安全责任”关注推进到对“安全责任”和“安全效益”的双重关注，只有坚持这种效益性安全建设方针，才能维持信息化安全产业的可持续发展。

我们需要特别说明的是，在谈到信息化安全时不可能不谈到存在的问题，在编写本白皮书时我们征求一些部门及其负责人意见，同时面向事业发展的要求尽可能客观的分析和提出建议。本白皮书不考虑各领域利益与职责关系的平衡与协调，编写本白皮书时可能存在信息与资料的遗漏。本白皮书仅仅作为商会提出的发展意见，不代表任何国家管理部门观点。如果本白皮书的某些讨论和意见与读者意见不一致或存在遗漏，请读者包涵和理解，可以与我们联系与商榷。

本白皮书由商会常务副理事长屈延文教授执笔起草，经商会理事长会议讨论和进一步修改，于 2005 年 3 月 11 日通过。本白皮书是信息安全产业的企业决策发展道路的重要参考与指导性文件，并希望作为国家、行业、地方、企业在制定“十一”五发展计划的参考文件。

本白皮书上报中国信息产业商会、信息产业部产品管理司，并抄报国务院信息化工作办公室、国家发改委、信息产业部、科技部、教育部、国家审计署、中国人民银行、认监委、银监会、证监会、保监会、工商总局、中国海关、铁道部、交通部、民航总局、国家广电总局、安全部、公安部、保密局、中办机要局、解放军总参某部、总装、国家电力总公司、电监会、国家金税工程办公室、国家金卡工程办公室、国家金盾工程办公室、国家金财工程办公室、北京市、上海市、天津市、重庆市等省市信息化主管部门等。本白皮书还下发商会所有成员单位领导。

2005 年 3 月 11 日

目录

第一部分：信息安全产业情况

第一章 我国信息安全产业概述

我国信息化安全产业大致可以划分三个发展阶段：

第一阶段：1995 年以前，以通信保密和依照 TCSEC 的计算机安全标准开展计算机的安全工作，其主要的服务对象是政府保密机构和军事机构。主要从事这方面的工作的是一些科研机构和军事机构，例如原电子工业部第 15 所、电子工业部 30 所和原邮电部数据所等研究机构及其相关企业。

第二阶段：在原有基础上，1995 年开始，以北京天融信网络安全技术有限公司、北京启明星辰信息技术有限公司、北京江南科友科技有限公司、北京中科网威信息技术有限公司、北京清华德实科技股份有限公司、上海复旦光华信息科技股份有限公司等一批从事信息化安全企业的诞生为标志的创业发展阶段，主要从事计算机与互联网的网络安全。从 1999 年起，将信息安全的工作重点逐步转移到银行与电信信息化安全建设上。2000 年我国第一个行业性质的《银行计算机系统安全技术规范》出台，为我国信息化安全建设奠定了基础和树立了示范。但是，这个时期主要提供的是隔离、防护、检测、监控、过滤等中心的局域网安全服务技术与产品，其主要面对病毒、黑客和非法入侵等威胁。到 2001 年，一时间全国成立 1300 多家从事信息化安全的企业。

第三阶段：以 2002 年成立中国信息产业商会信息安全产业分会为标志的有序发展阶段。这个阶段不仅从事互联网的信息与网络安全，而且开始对国家基础设施信息化安全开展工作，产生了许多自有知识产权的信息与网络安全产品。2002 年法论功对我国广电和信息基础设施的攻击，从反面促使了我国信息安全产业的发展。与此同时，我国电子政务、银行、证券、保险、电信、电力、铁路、交通、民航、海关、税收、工商、公安、安全、保密、机要和军队都相应开展了信息化安全建设，信息化安全建设已经在信息化全方位领域中进行，信息化安全得到了普遍的重视。在这个阶段，有大批的信息安全企业创立，同时也有大批的信息安全企业倒闭或者改做其他，一些优秀企业更加强大，企业资产得到了较大增加。与此同时，一些国内重要的 IT 企业或许多上市公司开始积极介入信息安全产业，推动了信息安全产业规模扩大。这个时期的技术与产品逐步走向产品芯片化、客户化、平台化和高技术化，并促进了信息安全管理平台的研究与开发。信息化安全的品牌和知识产权的工作得到更多的重视和加强。在企业的呼吁下，商会推动下，我国信息安全产业出台了《中国信息安全产业反不正当公约》，为建立“遵纪守法、诚信自律、公平竞争和共同监督”的市场秩序，奠定了基础。

目前，信息安全产业正在进入新的发展时期。

这个时期表现在对十年来信息化安全建设进行总结与分析，树立信息化安全新认识，并在此基础上奠定信息化安全的新起点，从而开辟信息化安全的新领域，积极培养新的发展增长点将发挥重要作用。例如，科学院与工程院的张效祥、金怡濂、何德全、蔡吉人、周仲义和沈昌祥六个院士给国务院信息化工作办公室领导的《关于积极开展银行监管信息化和银行信息化监管研讨工作的建议》，得到了国信办领导的高度重视，并批转人民银行与银监会领导阅示。国信办领导在银监会回复的报告中说，六院士的建议引起了人民银行与银监会领导的重视，银监会领导认为要启动银行监管信息化工作，希望得到国家与社会的广泛支持与帮助。在十届三次人大会期间，银监会领导在答记者会上说，提升金融风险监管信息科技水平是加强银行风险监管的重要措施之一。

这个时期主要受到未来信息化安全自主保障、监管、应急和威慑体系建设巨大需求的牵引而逐步展开的，其重要标志表现在商会的 QNS 工作室的《软件行为学》系列著作的出版发行和积极推动以多代理技术、标签技术、无第三方认证技术、监管技术、对抗技术等适合

于大范围网络环境、针对超海量数据对象和满足高智能应用与管理的新型技术与产品研发工作的开展上。同时也表现在商会推出可信网络平台（TNP）、可信应用平台（TAP）和可信计算平台（TCP）的新型市场理念上。这种可信平台的市场理念得到国家电子政务规划部门、国家金融风险监管部门、国家税务管理部门和国家涉密网管理部门等单位的高度重视。这种新的发展理念还反映在商会推出的安全管理平台企业联盟、可信计算平台（C_TCP）企业联盟、可信网络平台（TNP）企业联盟、CPK 企业联盟等标准化机构和信息安全服务等级标准企业联盟机构的创立和技术标准的制定上。

本白皮书讨论信息产业情况主要从信息安全产业的市场情况、信息安全产业企业情况和信息安全产业环境情况进行讨论。所谓信息安全产业的市场情况主要讨论信息安全产业面临的用户开展信息安全系统和工程项目建设的情况。为了使讨论分类清晰，我们将从国家基础设施信息化、电子政务、电子商务、产业信息化和城市信息化（包括人民生活信息化）需要的信息化安全建设进行分类研究，研究它们的现状和存在的问题以及今后的信息化安全建设的要求。所谓信息安全产业的企业情况主要讨论信息安全企业资产、资本市场、技术情况、服务情况。所谓信息安全产业的环境情况主要讨论信息安全市场秩序、国外信息安全企业进入中国市场情况、信息安全标准化建设情况、信息安全测评认证情况和信息安全技术法规建设情况。

第二章 信息安全产业市场情况概述

2.1 要全面、系统地认识信息化的安全问题

我国信息化安全建设任务非常艰巨，主要包括各种业务的社会公网、行业专网、互联网等信息基础设施运营、管理和服务的安全自主保障、安全监管、安全应急和打击信息犯罪为核心的威慑体系的建设，其内容包括网络系统安全建设、领域和企业的业务信息化安全建设、网络内容与行为的安全建设和用户关注的网络安全建设等方面。这些安全建设对于不同的领域和领导层面关注的内容、对象和程度各不相同。这种信息化安全需求不同方面的考虑，一方面是由于关注的威胁和风险不同，另一方面是由于关注的安全价值不相同。

信息安全企业要全面、系统地认识信息化的安全问题，将会开拓自己的眼界，看到更具有潜在市场价值领域，不断扩大企业的市场规模，而不至把企业的服务范围限制在一个封闭的狭窄空间内。开辟新的市场领域需要做多方面的准备，需要帮助用户了解这个新的市场的需求，同时，企业也需要做细致的技术准备，开发新的产品，提供新的深化服务。**信息化安全领域应当永远地保持思考、发现和创新的渴望与追求，要不断地鼓励企业的敢为天下先的进取精神。**

需要特别注意的问题是国外在中国信息化安全市场提供安全产品，主要是从用户角度考虑的，在中国信息化安全市场中通常没有从国家、领域安全考虑的高水平的安全产品，尤其是平台化的国外产品。

2.1.1 国家视角考察信息化安全问题

鉴于中国所处的国际政治、经济、外交和军事环境，国家制定了信息化带动工业化的发

展战略，反映出国家领导人对信息化安全非常重视。国家领导人关注国家主权意义上的受到侵害的网络行为、网络犯罪和网络恐怖主义行为，尤其是那些危害国家安全、社会稳定和文化侵蚀等方面的内容安全。同时，国家领导人也非常关注国家基础设施的宏观安全问题。国家领导人对信息化安全高度重视，对各领域信息化安全建设起到了巨大的推动作用。国家为了维护上述安全问题，建立相应的具备更加强大的职能的运行机构。

我国政府负责安全工作的部门对于密码、涉密网络与公共网络隔离、对信息化安全技术、产品和服务进行测评认证和市场准入应当理解为代表国家提出的安全要求。

作为信息产业部门管理信息化应当划分成两大类：即政府管理类信息化产品与系统（GOTS）和商用产品与系统管理类别（COTS）。目前在这方面管理尚没有统一管理条例和制度之前，各政府部门可以考虑制定自己的管理条例。

2.1.2 领域视角考察信息化安全问题

领域主管部门首先承担国家关注的网络行为与内容安全责任，同时还承担着制定领域信息化安全标准（例如互操作性、安全性和服务性的用户标准体系）和技术法规的责任，也承担着建立领域政府管理类产品（GOTS）配置管理服务体系的职责。领域主管部门还应当十分关注领域范围内市场秩序的建立。但是，对于许多领域来说，上述方面的领域应当关注的工作，目前开展得不是很好，缺少对领域信息化安全全面认识。

当前，领域管理部门要特别关注包括安全标签在内的技术法规和领域标准制定工作。

领域管理部门主要关心的领域发展与安全关系问题。有许多领域对其发展与安全之间的关系认识不清，认为关注信息化安全建设，影响了领域的发展。这些认识显然是错误的，产生这些认识的原因包括如下几个方面：

1、有许多领域对于发展与安全之间的关系的认识有待提高，例如有些领域的主管部门提出“发展是最大的安全”或“不发展是最大的不安全”等的观点。虽然这些观点是正确的，但是对于具体指导信息化安全建设是不够的。应当实在地对领域中安全问题进行分析，分析那些对发展构成威胁的风险是什么，根据实际情况对风险进行分类和排序，制定出领域信息化安全建设的发展规划，合理地使用资金。

2、信息化安全问题的敏感性与许多部门负责人的工作业绩相关。出现了多方面的对信息化安全建设进行干预现象，有时这些干预是相互矛盾的。一个领域的信息化安全发展事业被许多部门与人的利益所污染和损害。一个领域的信息化的事业发展规划变成了针对部门与人际关系的规划，严重地阻碍了信息化安全事业的发展。为了解决这些问题，有时又必须采取迂回的方法，通过不断地沟通和创造变化的条件取得认识上进步。

3、一些企业利益集团的反对。有些企业提供的信息化产品与技术，不包括信息化安全方面的内容，提出信息化安全要求后，这些企业认为增加了企业的成本或者丧失竞争优势，游说领域主管部门，安全建设影响了他们的发展目标和企业的利益。这些企业利益集团包括一些国外的公司。

2.1.3 企业视角考察信息化安全问题

运营商通过实施领域信息化安全标准（例如互操作性、安全性和服务性的用户标准体系）和技术法规，来体现出对国家关注的网络行为、内容安全、安全生产、业务连续性服务、网络安全问题和用户关注的安全问题的解决，同时接受国家和领域对安全问题的监管。

实施信息化建设将越来越要求对企业业务与技术组织体系结构进行改革，实现管理层次

的扁平化、时空聚焦化的低管理成本效益。当现代企业领导人在不认识信息化对企业提高企业竞争能力帮助，不明确适合信息化的业务与技术组织体系结构和信息化可能带来的负面的作用有方案能够抑制（例如企业知识产权和企业员工在上班时间做非预期的工作）之前，有见识的企业领导人是不会匆忙上信息化的。从这个意义上看，信息化安全建设必须与企业的风险监管信息化结合起来，这种结合是促进企业信息化事业发展的因素。所以，企业应当关注业务运营系统安全建设。

从事信息化安全的企业，要了解企业领导人关注的问题，才会不断扩展信息化安全建设的市场。

2.1.4 技术保障部门视角考察信息化安全问题

近 10 年来开展的信息化安全建设主要是针对技术支持部门关注的网络与系统的安全问题，也是专家们关注的安全问题，主要包括计算机病毒、黑客入侵、非法访问、蓄意代码等网络攻击事件引起的安全问题。技术保障部门关注的焦点是信息化系统的正常运行。

在数据与系统（软硬件、网络等）安全保障上能够做到具有安全防护，便于安全管理，不仅进行了局域网范围的安全保障建设，同时也考虑“大范围的网络环境的”安全建设。在安全应急处理方面，能够确保业务连续性；在安全监管方面，实现了针对行为与内容的监管，实现可信网络平台（TNP）建设。

在企业进行业务与技术组织体系结构调整时，要区别技术保障部门和风险监管部门的差别。风险监管中心应当属于一种业务组织机构，作为运营中心工作。

2.1.5 用户视角考察信息化安全问题

用户关注的安全主要是：隐私防护、权益维护、信息安全和可信接入等问题。我国信息安全企业对普通用户的信息安全问题关心的不够。

在国家和基础设施关注的信息化安全得到了普遍的重视，但是在中国还要特别注意关注普通百姓的信息化安全问题，尤其关系到政府、企业面对社会的服务系统要特别注意安全问题，在一个越来越重视人权、民主的现代社会里，应当得到特别的重视，否则会面对严重的社会问题和法律问题。例如在发达国家，我们可以看到一些面向公众的社会服务系统（例如银行信用卡系统等）都具有非常高的安全保护就是例证。

为了解决用户关注的安全问题，信息安全企业应当对公共网络可信接入专用网络的服务、信息客体在网络中传输的安全保障、标签路由与交换通信、信息安全标签、无第三方认证密钥管理和活性客体传输机制等提供服务和支持。

2.1.6 必须关注信息化安全服务的综合性、高技术性和对策性特点

信息安全产业有其鲜明的特点，虽然产生于信息化和信息系统，依然与通常的 IT 服务有许多区别。

信息化安全的基本特征是服务性的。这种服务性与一般软件的服务性是不同的。一般应用系统或产品的服务主要是维护和培训，通常服务是非对策性的、非动态的和比较固定的。信息化安全服务是对策性的、动态性的、不断产生新内容的和似乎永远不能成熟等特性。信息化安全服务范畴几乎包括了整个信息化所包括的所有产品和系统，其服务的综合性和复杂

性是显而易见的。信息化安全服务是最高技术的服务，无论从设计角度和使用的角度都要求深入、熟练和非常专业。**我们可以骄傲地说，信息化安全服务是世界上最伟大的服务业，也是最困难的服务业。**

信息化安全的环境性。信息化安全产品与系统不是孤立存在和使用的，产品与系统使用的好坏及其效果与它们所处环境密切相关。这种与环境的相关性大大增加了信息化安全服务的难度。

信息化安全服务的主体性、客户性和可信性。信息化安全不是单纯地提供一些安全产品与系统，不能采用同样的产品与系统服务于各种不同的用户，商会在 2002 年调研报告中谈到发展策略时，第一个提出的对策就是“客户化”。这种客户化要求不仅仅是由于不同行业与领域对信息化安全的要求不同，而且面对的威胁性质也可能不同，更重要的是信息化安全责任与效益也要求有针对性的服务。信息化安全服务提供的产品与系统发挥作用了吗？这个问题始终是用户关注的问题。如何做到让用户对企业提供的安全产品与系统具有可信性认可是信息化安全服务极其重要的问题。我们需要再一次的呼吁企业与用户注意，提供信息化安全服务功能和能力与为用户建立可信性的服务是两类不同性质的服务。不能提供客户化和可信性服务的安全企业必将要丧失其客户群或市场领地。

信息化安全服务有很强的时间性、变化性、及时性、动态性、非成熟性和对策性。通常的 IT 产品服务主要是面对产品的可靠性和应用培训中产生的问题进行服务，这种服务结构总体来说是静态的，是完全预期的。现代计算机服务中，已经有相当的服务内容是由于计算机病毒、黑客入侵等造成的，这些服务已经不是计算机产品的供应尚能够服务的，而是信息安全企业提供的。这种危害计算机应用的攻击还在不断地翻新，新的威胁几乎天天发生。一个信息化安全产品的供应商，不能象普通的计算机产品的供应商那样，必须面对不断发生的新问题，为用户提供新的服务内容。凡是依照传统的计算机产品和应用软件供应商的服务模式提供信息化安全服务的，不可能得到用户的满意，如果不调整其服务策略，必然会丧失市场。

信息化安全服务的复杂性、综合性、深入性和高技术性。信息化安全的复杂性和综合性涉及到通信、计算机、外部设备、硬件、BIOS、操作系统、数据库系统、应用软件、系统体系结构、系统与网络防护体系、系统和网络的检测与监控体系、系统与网络备份体系、系统的应用与操作、系统与网络的管理等。上述范畴的每一项服务都是技术性很强的业务工作，何况还要涉及诸多方面的服务呢！商会在 2002 年调研报告中谈到发展策略时，提出的第二个“平台化”对策就是基于这种复杂性和综合性认识的。信息化安全服务的深入性是指威胁与防护都要对系统与网络的脆弱性有深刻的了解，对系统和网络非常熟悉的使用和长时间的接触。信息化安全服务另一个高技术性表现在服务的远程化、代理化发展趋势的要求，商会在 2002 年调研报告中谈到发展策略时，提出的第三个对策是“服务高技术化”就是基于这种认识的。

信息化安全服务的高成本性。经过商会的多年调研，信息化中的安全建设大约占有 15%到 20%的项目投入。这个投入如此之大，不能理解为信息化安全仅仅购买信息化安全产品或系统。根据我们统计，购买信息化安全产品费用一般在 5%到 10%左右，而信息化的安全服务费用大约在 5%到 15%，这主要是由于信息系统复杂程度差距较大，安全服务的成本差别也较大。但是，我们可以看出信息化安全服务大约在信息化安全建设中占有 50%的份额，而我们知道一般的信息化服务只占信息化项目建设费用的 10%左右，可见信息化安全服务与一般信息化服务的成本之间的较大差别。信息化安全产品与系统的用户除采购产品本身之外，还必须采购其服务，否则根据上面的分析，信息化安全产品与系统的采购将会变得毫无意义。那麼，企图只考虑兜售产品与系统而不为用户提供安全服务的企业，显然是一种没有实力的或对用户安全不负责的企业。一个用户如果如此购买信息化安全产品与系统，该用户

至少是对信息化安全的特点没有认识，或者说也是对自己不负责任。**信息化安全服务的复杂性、高成本特性要求信息化安全企业必须在安全服务的远程化和代理化的推进方面做出不懈努力，不断降低服务成本。**

正由于信息化安全服务的上述特性，商会正在积极调整和建议一些企业专门从事信息化安全服务，也正是这个原因商会严厉的批评不关注信息化安全服务、只管销售所谓安全产品和对客户毫不负责的企业。

2.1.7 信息化安全认识要与时俱进

信息化安全认识必须以与时俱进的态度进行调整，这是信息化安全建设的大问题，不仅企业需要改进对信息化安全的认识，信息化主管部门也应当适时地调整信息化安全的概念体系，增强责任、危机和全局意识。

例如如何划分系统和网络安全等级的问题，有几种视点：依照网络传输信息安全要求来划分网络安全级别；依照系统和网络提供安全防护服务能力等级划分系统和网络安全级别；依照系统和网络中可信性的级别来划分系统和网络的安全级别。只要把这些问题提出来，一个比较认真对待问题的人士，一定会区别它们之间的差别。在有些情况下，可以考虑依照网络传输信息安全要求划分其安全级别；在另一些情况下，可以考虑依照系统和网络提供安全防护服务能力等级划分其安全级别；但是，无论怎样划分安全等级，都必须依照系统和网络的可信性的级别来划分其安全设施发挥作用的“心中有数”程度；如果有了上述三种分类认识，在研究信息化安全标准和制定信息化技术法规方面就会有一个明确的认识体系。

再例如如何看待信息化安全标准问题。信息化安全标准不能看成僵死的东西，信息化安全的许多标准随着信息化发展，出现了非满足和不适应的新问题。例如 TCSEC 是 1985 年美国国防部提出的标准，这个标准连带它的许多附加文件，对于单一计算机和操作系统的安全建设起到过很好的指导作用。这个标准划分等级原则是依据系统提供的安全服务能力的的等级来确定的，尤其其中的“授权可信”的安全概念需要进行调整，做到对身份授权与行为可信的双重关注；改变把信息安全质量评估等级和安全功能强度等级混合在一个等级划分标准系列内而存在可操作性问题的局面。TCSEC 这个标准对于信息系统、网络、通信、微电子等信息产品存在着相当程度的不适合性，更谈不上将这个标准作为整个信息技术或信息化的安全标准。

例如如何看待信息化安全的技术法规与条例的问题。信息化新技术的发展和信息化安全威胁变化促使信息化安全认识必须与时俱进。一个信息化安全的法规和条例是在其出台的历史环境和相应认识上制定的，随着信息化建设发展，出现了一些新问题和新情况，这种发展变化要求法规与条例进行修改；同时，法规与条理出台后，在实践中也必然会发现一些与客观环境不适合的问题，也需要在实践的基础上对法规与条例进行修改。例如，我国对于政府网络的安全划分长时期是依据系统和网络中传输信息的安全级别（绝密、机密、秘密、内部和公开）划分为核密、普密和商密的。这样划分对非信息化时代曾经发挥过很好的作用，在信息化时代这种划分原则遇到了比较严重的挑战，显然围绕着如此划分系统和网络安全技术法规应当做些修改和调整，更加需要增加对网络可信性的监管或监控能力，如何调整是一个复杂的问题，需要认真研究和对待。

2.2 国家信息化安全市场分类

本白皮书讨论的信息化安全市场分类为如下的五个方面：

- 国家基础设施信息化安全领域
- 电子政务安全领域
- 电子商务安全领域
- 产业信息化安全领域
- 城市信息化（包括人民生活信息化）安全领域

2.3 国家基础设施信息化安全建设情况

国家基础设施是指保证国家政治、经济、国防和社会各领域有效运行的基础设施，涉及电信、广电、金融、电力、能源、民航、交通、政府、国防等国家系统和资产，其中国家信息基础设施是国家基础设施的重要组成部分。信息基础设施是 20 世纪 90 年代提出的概念。信息基础设施是指信息范围内的跨领域、支持承载服务的公共环境，通常包括网络通信系统、计算机网络、计算机系统和应用支持服务系统。国家信息基础设施（称之为 NII）是指由国家使用并实现政府公务或经济活动的信息基础设施的联合体，NII 应当是国防 、金融、电力、工业、商业、政府等范畴内信息基础设施的组合，例如，国防信息基础设施（称之为 DII）、金融信息基础设施（称之为 FII）等。

在本白皮书中主要对信息化及其安全建设需求强劲的国家基础设施领域进行讨论，主要包括：电信、广电、银行、证券、电力、铁路、交通、民航、政法和国防。目前，国家基础设施信息化安全建设仅仅是开始，对于大多数领域，当前主要问题依然是增强信息化安全建设的责任与危机意识，提高信息化安全认识，建立信息化安全建设高起点，对信息化安全建设需要做一个前瞻性的建设规划，建立一套安全、可信的信息系统。

2.3.1 电信网络与电信业务信息化安全建设情况

经济全球化、区域集团化的发展要求实现全球和区域实现一体化的应用平台。全球、区域和国家为此研究 GII、NII 信息基础设施的建设。GII、NII 目前主要讨论通信网络、电视网络和计算机网络的多网融合发展。面向 21 世纪的网络服务和业务平台是一个基于多种通信体制，集电信、电视、监控和计算机网络为一体的，多网融合的信息平台。每个行业在发展综合业务时都遇到了当前克服不了的困难，这些困难包括技术体制的，也包括当前用户接入网络的现实和用户的终端设备与其综合业务的发展无法配合的问题。因此业务逐渐从综合走向融合。

我国电信行业的信息化与安全建设在全国范围内是走在前面的，其信息化安全建设得到多方面的重视。

我国电信网络安全任务非常艰巨，主要包括各种业务的社会公网、行业专网、互联网等信息基础设施运营、管理和服务的安全保障、安全监管、安全应急和安全威慑。主要包括网络系统安全建设、电信业务信息化安全建设、网络内容与行为的安全建设和用户关注的电信网络安全建设等方面。这些安全建设对于不同的领导层面关注的情况是不相同的。例如作为政府领导关注电信安全，主要是关注网络中的行为与内容的安全，其焦点重要在这些行为与内容对国家安全和社会稳定的影响。作为信息产业的管理部门，主要关心整个信息产业的发

展与安全关系问题，关心电信行业运营市场秩序，关心领域的互操作性和安全性两者之关系。作为电信运营商的领导重要关注信息化与信息安全建设对运营的技术与业务组织体系结构的影响，求得企业价值最大化和风险最小化的平衡，实现风险价值化的有效评估。对电信运营技术支持部门重要关注的电信网络与系统的安全。而对于电信系统用户关注的安全主要是信息安全和公共网络可信接入用户专用网络问题。应当特别引起注意的是上述的信息化安全建设存在着越来越严重的交叉问题。

1、网络行为与内容的安全情况

电信网络的行为与内容安全已经显现出来，而且会越来越突出，尤其在考虑恐怖主义和信息战的威胁，网络行为与内容安全将会变得越来越重要。这种安全威胁主要表现在：

- 网络犯罪行为、恐怖行为和军事行为的威胁。
- 网络内容攻击，包括利用传统媒体（广播、电视、信件）、电话（包括 IP 电话）、电子邮件、聊天室（ICQ、QQ）、板报（BBS）、论坛、个人主页、专用网站、垃圾邮件以及短信息群发等实施攻击，当前主要问题是法轮功、黄色、反动网站问题。这些问题关系到国家政权、社会的稳定。

我国社会公共网络的安全管理工作取得了显著的成绩，但是还面临着对网络行为与内容监管的艰巨任务。

2、领域关注的安全情况。总体上讲电信领域的安全意识还比较淡漠，需要加强。表现在电信网络管理“七国八制”局面虽然有所改善，依然存在较大问题；电信网络互联、互通和互操作问题突出；在解决互操作性问题中，安全问题没有得到充分重视；国家许多电信网络在建设初期就没有建立网络监控体系，实现网络监控业务，欠帐太大，目前还没有看到改变的计划；电信网络长期重视传输效率与质量，缺少对安全因素引入对网络机制机理的研究；传输、信令、管理、运营信息化出现相互交叉造成的安全问题。

另外对于电信领域急需制定的安全性、互操作性和服务性标准系列，缺少整体规划。对于相应的技术法规制定工作，不能令业界满意。电信领域主管部门主要关心的发展与安全关系问题需要有更加全面的认识。

3、电信业务运营信息化安全情况

电信业务运营信息化主要是指电信业务运营、管理、计费、销售、市场、开发、维护、培训等方面的信息化建设。这些信息化建设遇到的安全问题是典型的计算机网络的安全问题，是当前电信领域信息化安全建设的一个主要方面。

4、电信网络系统安全情况

电信网络系统安全建设是近期被关注的建设内容。主要是对电信的传输网络、信令系统和管理网络施行安全建设。电信网络面对的威胁包括：

- 对基础设施网络带宽资源的攻击。插播攻击、拥塞或干扰攻击、海量通信攻击、偷用服务攻击、拒绝服务攻击、隐蔽通道攻击、传输分析攻击等、
- 对网络管理通信和通信的信令系统的攻击。例如，攻击通信的控制命令体系，修改对网络设备的操作命令。资源不可利用。
- 对基础设施的网管中心（NMC）、管制中心、调度中心、通信中心与信息中心的攻击（要特别注意防范外包服务的网络远程服务攻击）。
- 对基础设施设备破坏或接管控制性质的攻击，失去网络基础设施控制（要特别注意外包服务的网络远程服务攻击）。

我国信息基础设施网络安全建设投入在全国来说是最大的，几年取得较大成绩，但是如下的一些问题依然应当引起注意：

- 我国许多通信系统采用了 GPS 的时统进行同步，对我国通信系统安全存在很大隐患。
- 网络的管理、信令系统的安全建设有待进一步加强。

- 对网络插播攻击问题缺少检测、定位能力。对公网与专网之间的隔离情况缺少检测能力。
- 对网络大规模入侵检测和防护缺少应对能力。
- 对网络安全缺少全局的管理、指挥、监控、调度与协调能力。

5、用户关注的电信网络安全情况

电信系统用户关注的安全主要是信息安全和公共网络可信接入用户专用网络问题。但是电信行业对用户希望提供的这些安全服务要求太缺少，或者说基本上还属于空白。

针对上述问题可以做如下的建议：

- 电信运营商建立功能强大的网络管理中心。建立功能强大的网络管理中心，这个中心要对内容检查、系统管理、网络管理、网络安全管理、行为监控、代理（Agent）管理、网络远程服务监控和标准化执行实施统一分级监管。目前的管理中心自身安全等级较低，建议与管理中心纳入同一安全区域，加强管理中心的安全管理与远程管理的高安全级别与强度的安全建设。
- 完善建立功能强大的国家网络行为与内容安全管理与监管中心。在国家网络安全管理中心基础上，在内容安全过滤与检测的基础上，实施对网络行为与内容的监管，尤其支持各政府行业的专用网络行为和内容进入公共网络的监管，实施国外存在危害意图的行为的监管与控制。
- 建立符合电信业务运营信息化要求的运营中心。
- 实现标签交换、路由技术，支持用户采用安全标签技术和实施活性客体监管技术，支持采用无第三方的身份与行为可信认证技术的使用。
- 提供用户要求的不同等级和不同成本的公共网络与专用网络的可信接入服务。
- 外包服务安全建设。业务系统开发以及维护存在的外包服务，网络系统设备的提供和维护的外包服务问题都存在安全隐患，尤其是国外产品和厂商的远程服务。建议全部选用经过测评取得相应资质的国内厂商。
- 安全检测、监控、审计、追踪与定位系统建设。对于所有的网络行为和物理接触设备行为，要求采用安全日志或记录进行审计、配备必要的信道安全检测、网络配置检测、计算机行为安全检测、网络行为安全检测、信息源的追踪、定位技术产品等。
- 大规模入侵检测和防护安全建设。配置对抗分布式拒绝服务攻击（DDOS）设备与系统。有对抗大规模陌生代理入侵的能力。
- 进口设备的远程控制/维护/检测/监控/诊断等问题。目前电信系统采用的大量引进设备普遍存在远程控制问题，存在严重的安全隐患。同时，进口设备目前普遍存在隐蔽通道现象，建议逐步以国产设备替代。重要系统网络中使用的进口设备，要采取有效手段进行隐蔽通道的检测，
- 制定安全应急规范和安全应急培训。参照国家信息基础设施应急体系建设指南和国内的相关标准，建立电信系统的应急规范，并进行应急演练。同时与国内的专业安全公司和安全专家建立良好的咨询渠道。成立专门的安全机构，并进行相应的安全培训，由通过国家测评认证体系的安全审核员负责具体的安全审核工作。最后，我们还建议：电信系统以安全审核员（CISP）的培训和系统测试评估工作为龙头，有的放矢的推进电信系统信息与网络安全建设工作。

2.3.2 广电信息化安全建设情况

1、广电网络行为与内容的安全情况

广电行业是国家政府重要的舆论宣传部门，对国家的稳定起着至关重要的作用。国家对广电行业的安全问题非常重视，尤其在 2002 年境外法轮功分子攻击鑫诺卫星后，国家与广电行业对其安全建设更加重视。广电有线电视网络已经在全国范围建成，对于敌对分子和邪教组织采用有线插播宣传的有害信息是国家广电部门应当注意的安全问题。数字电视系统的规划与开展要对数字电视系统可能引发的信息内容的安全问题要给予充分的注意，对数字电视网络管理系统安全也要给予充分的关注，要防止敌对组织企图控制有线电视和数字电视网络资源的攻击。

2、广电领域安全情况

广电领域的管理和监管部门要重视建立广播与电视专门的节目播放监控网和事故监测网络系统。

3、广电企业业务运营信息化安全情况

这里谈到的广电的企业是指中央与地方的广播与电视台站和相应的企业，广电企业的业务信息化的程度越来越高，这些业务系统与电信公共网络相连接，已经构成了与社会广泛联系的业务服务网络，存在着信息化安全威胁。有线电视的播放采用了计算机服务器系统，可能与社会的计算机网络系统连接，存在着安全隐患。

4、广电网络系统安全情况

广电网络系统包括卫星网络、无线网络、微波网络、有线电视网络和业务信息化网络系统。在上述的网络系统的管理中心多数没有安全管理系统和功能，网络的安全防护和检测能力不够，系统的备份和恢复能力不足。对于进口设备的服务和检测缺少注意，能够提供信息化安全服务的人力资源缺乏。

5、广电用户关注的安全情况

由于广播和电视节目单向性，目前用户的安全问题尚不存在。但是电视业务数字化和电视节目的双向互动系统建设，这种安全问题将会越来越突出。

广电信息化安全建设可以借鉴电信信息化安全建议。

2.3.3 银行信息化安全建设情况

银行系统包括人民银行、银监会以及下属各部门和各国有商业银行、股份制银行、政策银行以及银联等银行机构的信息系统，其安全状况直接关系到国家的经济形势和国计民生。银行业务信息化在全国范围内是走在前面的。从规划的角度看，银行的信息与网络安全建设与银行整个电子化、信息化和网络化密切相关，把金融风险监管现代化与金融电子化、信息化和网络化风险的监管密切结合起来，是搞好银行信息与网络安全建设的根本出路，这也是新巴塞尔资本协议的监管要求。强化银行网络与信息安全为银行转型改革、提高银行竞争能力与风险监管能力服务。由于目前银行信息化安全的观念依然是建立在“数据与系统（软硬件、网络等）安全自主保障”之上，整个信息化安全理念依然是在上世纪 90 年代中期发展起来的局域网安全观念。对于网络与系统的虚拟世界的“行为与内容的监管”和“大范围的网络环境的安全问题”基本上没有考虑。银行的风险观念和安全问题应当进行调整，在新起点和新高度上，进行补充总体规划，应当考虑实现可信网络平台（TNP）、可信应用平台（TAP）和可信计算平台（TCP）的建设。

1、银行网络行为与内容的安全情况

银行网络行为与内容的安全问题实际是银行风险监管的问题，银行风险监管既要检查银行和客户人员在现实世界中的人类与银行业务相关的行为结果，又要检查网络虚拟世界中用户、系统和代理的行为，实际上要对银行监管实行监管现代化的建设和银行信息化实行监管。

银行监管现代化的和银行信息化实行监管的建设任务刚刚开始，在今后十年多时间里，是银行信息化和安全建设的主要任务之一。银行行为与内容的监管可以划分为三个级别：第一个级别主要对行为的可信性、有效性、完整性、连续性、保密性以及内容的可信性、保密性和完整性进行基础性监管；第二级别是依照巴塞尔资本协议的要求对风险实行分类监管；第三级别是完成企业的综合性的风险监管，包括实现资金流量流向监管。银行建立在行为与内容上主动模式的监管才刚刚开始，其市场概念是属于领域性的。

2、银行领域业务运营信息化安全情况

对于银行领域，其信息化安全建设主要涉及国际银行支付清算系统、中国支付现代化系统、银行卡联网通用系统、全国银行电子票据交换系统、全国银行客户信用管理系统、全国银行风险监管系统、银行信息披露信息系统、国库业务系统（国库、税收财政横向联网系统等）、人民银行 OA 系统、银行领域网络系统、网管中心以及灾备支援中。由于我国银行监管局成立不久，其信息化建设的任务刚刚起步，任务十分艰巨。

我国银行领域的信息化系统建设的安全问题欠帐较多，需要进行认真规划和总体设计，将银行领域的信息化安全建设搞上去。

3、银行企业业务运营信息化安全情况

对于各商业银行，主要涉及银行价值管理信息系统、资源管理信息系统、银行产品服务管理信息系统、银行风险监管系统、银行客户管理信息系统、银行电子商务公共渠道管理系统（网络银行系统、、银行自助系统等）、银行电子商务大客户渠道管理系统、银行网关与办公系统、银行管理中心、银行运营中心系统（呼叫服务中心、电子票据中心、信息交换中心等）、银行开发中心系统以及灾备中心系统等。

由于银行系统有高度的安全意识，领导重视，银行系统的安全工作开展的较早，制定了相关的标准和规范，进行了安全规划并部分进行了实施，过去一段时间内主要实现的也是银行业务信息化安全建设。广泛采用了防火墙、入侵检测系统、VPN 和信息加密等关键安全产品建立了基础的安全防护和监控系统，但由于缺乏资金，使得安全建设仍然存在很多不足，存在许多安全隐患和问题。

4、银行网络系统安全情况

当前银行网络系统安全问题重要表现在数据大集中后的安全，其特点是数据服务大集中，前置通信中心强大的和众多本地与远端终端的中心体系结构。突出的问题是应急灾备系统建设、体系内多系统之间的隔离、生产专网与公网隔离、访问行为控制、国外外包服务、关键结点安全、大规模入侵检测与防护、进口设备的远程控制和隐蔽通道、安全培训等方面问题。其中电子银行的公共渠道和银行与大客户渠道安全与连接问题，是银行信息化安全建设、风险监管建设的重要内容。

5、银行用户关注的安全情况

银行用户关注的信息化安全问题主要是客户隐私、用户权益、信息内容安全和客户可信接入银行网等问题。

针对银行信息系统目前的安全现状，我们建议：

- 推荐《银行行为监管：银行监管信息化》和《银行行为控制：银行信息化与安全》两本书，开展银行信息化与安全建设新的学习运动，树立信息化与安全新认识，将信息化安全建设与监管信息化建设相结合。银行监管现代化建设应当结合我国国情，依据新巴塞尔资本协议提出要求，进行建设，逐步达到我国金融开放市场的监管要求，与此同时建设好银行的信息与网络安全的保障、应急、监管体系。在进行基础设施与应用体系建设时，要充分考虑到互联网目前的体制性与结构性不安全的严重问题，应当多考虑非互联网的公网技术体制。
- 全面整合银行信息化安全建设，在此基础上建立银行信息安全保障、应急和监管系统。

银行系统应在考虑建设信息安全保障体系的同时，围绕标准控制与管理中心的建设，以及数据与内容安全、计算环境安全、边界安全、信息基础设施安全、数字证书、灾备、业务行为监管以及服务等方面进行安全建设。

- 以安全观点再度审核银行应用数据大集中的安全建设问题。银行系统进行的数据大集中，使得业务系统得以进行有效的监控，但同时也造成安全风险的集中，存在许多安全问题和隐患。所谓大集中是管理、运营、控制和权利的集中，应当避免将全部资金存放在一个计算机系统之上。大集中必须建立功能强大的网络管理与标准化监管中心，对银行的数据安全、计算环境安全、围域边界安全、信息基础设施安全、数字证书与加密系统、内部人员网络行为监控、灾备中心和网络远程服务、维护等方面实施高强度的安全防护建设。同时，对银行的重点 ISP、ICP 的安全也应加以足够的重视。
- 建立功能强大的网络管理与标准化监管中心。这个中心要对数据管理、系统管理、网络管理、安全管理、蜜钥管理、内部人员行为监控、代理（Agent）管理、网络远程服务监控和标准化执行实施统一监管。目前的管理中心自身安全等级较低，建议与管理中心纳入同一安全区域，加强管理中心的安全管理与远程管理的高安全级别与强度的安全建设。
- 启动代理技术的银行主动式的银行监管系统试点工程项目。
- 银行使用卫星通信的重要系统尽快实施多星、多转发器备份、天地备份项目，为银行系统通讯提供稳定可靠的环境。
- 专网与公网的隔离安全建设。目前银行系统的专网与公网没有进行物理分离，存在严重的安全隐患。加强专网与公网的隔离检测建设。网上银行、呼叫服务中心在方便用户的同时，注意银行系统与公网相连接，增加了安全隐患。要考虑银行生产系统、服务系统、办公系统、管理系统之间的不同形式的隔离技术建设。银行网络隔离技术建议使用高安全级（相当与 HP VVOS）网关设备。
- 银行外包服务安全建设。银行的业务系统开发以及维护存在的外包服务，网络系统设备的提供和维护的外包服务问题都存在安全隐患，尤其是国外产品和厂商的远程服务。建议全部选用经过测评取得相应资质的国内厂商。
- 安全检测、监控、审计、追踪与定位系统建设。对于所有的网络行为和物理接触设备行为，要求采用安全日志或记录进行审计、配备必要的信道安全检测、网络配置检测、计算机行为安全检测、网络行为安全检测、信息源的追踪、定位技术产品等。
- 进口设备的远程控制/维护/检测/监控/诊断等安全建设。目前银行采用的大量引进设备普遍存在远程控制问题，存在严重的安全隐患。同时，进口设备目前普遍存在隐蔽通道现象，建议逐步以国产设备替代。
- 制定安全应急标准与安全应急培训。参照国家信息基础设施应急体系建设指南和国内的相关标准，建立银行系统的应急规范，并进行应急演练。同时与国内的专业安全公司和安全专家建立良好的咨询渠道。成立专门的安全机构，并进行相应的安全培训，由通过国家测评认证体系的安全审核员负责具体的安全审核工作。最后，我们还建议：银行系统以安全审核员（CISP）的培训和系统测试评估工作为龙头，有的放矢的推进银行信息与网络安全建设工作。

2.3.4 证券信息化安全建设情况

证券系统由主管的证监会、被监管的单位包括上海证券交易所、深圳证券交易所、登记结算中心、上海商品交易所、郑州商品交易所、大连商品交易所、上海期货交易所、郑州期

货交易所以及各家证券公司（128 家）、几十家基金管理公司、一百多家期货经纪公司等，其安全状况直接关系到国家和广大投资者的经济利益，影响重大。证监会领导非常重视和关注信息安全建设，颁布实施了安全管理规范。

1、证券网络行为与内容的安全情况

证券网络行为与内容的安全主要是指证券行为与内容的监管，同样可以划分为三个级别：第一个级别主要对行为的可信性、有效性、完整性、连续性、保密性以及内容的可信性、保密性和完整性进行基础性监管；第二级别是依照国际证券组织的风险监管标准的要求对风险实行分类监管；第三级别是完成证券企业的综合性的风险监管。证券系统的行为与内容的监管还处于被动模式中，或者说基本上还没有做，保留着整个领域性的市场空间。

2、证券业务运营信息化安全情况

我国证券系统在信息化建设方面走在全国的前面，从发行交易到清算全程实现了无纸化，信息安全工作极端重要。对于证券系统，其安全建设主要涉及网上业务系统、交易系统、登记清算系统、银证通系统、风险控制、监管系统、管理系统、证券 OA 系统、信息披露系统、重点网站、网络系统以及网管中心建设等方面。同时，重点 ISP、ICP 的安全也应加以足够的重视。证券系统安全建设也主要是针对这些业务系统的，由于证券信息化安全的观念依然是建立在“数据与系统（软硬件、网络等）安全保障”之上，整个信息化安全理念依然是在上世纪 90 年代中期发展起来的局域网安全观念。对于网络与系统的虚拟世界的“行为与内容的监管”和“大范围的网络环境的安全问题”基本上没有考虑。证券的风险观念和安全问题应当进行调整，在新起点和新高度上，进行补充总体规划，应当考虑实现可信网络平台（TNP）建设。

3、证券网络系统安全情况

在部分证券机构和交易所采用防火墙、入侵检测系统、VPN 和信息加密等关键安全产品建立了基础的安全防护和监控系统。但由于缺乏资金和总体建设规划，使得安全建设仍然存在很多不足，存在许多安全隐患和问题，主要体现在业务系统数据备份与恢复、专网与公网隔离问题、外包服务问题、关键结点问题、大规模入侵检测与防护问题、进口设备的远程控制和隐蔽通道问题、安全规范与培训等方面，对于突发性安全事件的快速响应不足。证券行业最突出的问题是：尚未完全建立天地互备通信系统，基于互联网的网上交易面临着更加严峻的挑战。

4、证券用户关注的安全情况

证券用户关注的信息化安全问题主要是客户隐私、用户权益、信息内容安全和客户可信接入证券网等问题。

证券信息化安全建设可以参考银行信息化安全建设的建议。

2.3.5 电力信息化安全建设情况

电力行业是国家重要的能源支柱行业，是我们日常各项工作和生活的基础和保障。如果电力行业出现问题，不仅会严重影响国民经济增长，而且还会造成社会的不稳定甚至恐慌。

电力体制改革之后，国家电网公司与南方电网公司以及五个发电集团公司，构成了厂网分家的市场竞争的局面。2002 年 5 月中华人民共和国国家经贸委 30 号令颁布的《电网和电厂计算机监控系统及调度数据网安全防护规定》，对电力系统安全建设具有重要的指导意义。由于我国电力发展的需求强劲，在发展电力生产和传输能力的同时，还必须大力发展节约电力能力和改变电力调度的控制方式，为此国家电力行业应当积极规划我国自己的“智能电力网络”的发展计划。同样由于电力信息化安全的观念依然是建立在“数据与系统（软硬件、

网络等）安全自主保障”之上，整个信息化安全理念依然是局域网安全观念。对于网络与系统的虚拟世界的“行为与内容的监管”和“大范围的网络环境的安全问题”考虑不够，需要考虑实现可信网络平台（TNP）、可信应用平台（TAP）和可信计算平台（TCP）的建设。

1、电力网络行为与内容的安全情况

电力网络行为与内容的安全主要是指建立在行为可信性、有效性、完整性和对电力资源管理与控制行为方面，面对的威胁应当属于是战略性质的，即电力系统威胁不仅要考虑一般的信息犯罪问题，更主要是要考虑敌对势力与恐怖组织对电力相关信息、通信与调度的攻击，甚至要考虑战争与灾害的威胁。

2、电力领域业务运营信息化安全情况

目前主要是指国家电监会、国家电网公司与南方电网公司管理的业务范围，“智能电力网络”的发展计划，这项发展计划必须全面地进行电力线含光纤新型电力传输线逐步替换工作，光纤通信传输线与电力传输线合为一体，对于电力调度、控制、通信和信息都会带来巨大的好处。如果解决配电线与光纤混合进入社区和家庭，对于用电的智能化管理带来革命性的变化，这种基础性的建设也必然为城市智能化社区的建设和人民生活信息化带来新的变化，对于提高人民生活水平有积极的帮助。但是，这种“智能电力网络”的发展计划也必然会带来安全方面的挑战，因此也必须对信息化安全也要进行全面规划和设计。

3、电力网络系统安全情况

对于电力行业主要考虑以下系统：各类发电企业、输电网、配电网、电力调度系统、电力通信系统（微波、电力载波、有线、电力线含光纤）、电力信息系统等。这里主要考虑到电力调度数据网（SPDNET）、电力通信网与电力信息网几个方面的安全问题。电力系统的安全建设以资源可用和资源控制的安全为中心，必须保障电力系统畅通的 24 小时服务。

目前，大多数规模较大的发电企业和很多省市的电力公司在网络安全建设方面已经做了很多工作，通过防火墙、入侵检测系统、VPN 设备等关键的安全产品的部署和实施已经初步地建立起了基础性的网络安全防护系统，并取得一定的效果，应当说是有自主特色的。但在对于已经部署的安全产品和系统合理有效的配置使用，使其充分发挥其安全防护作用方面，以及在对于突发性内外部恶意攻击等非常规的安全事件的快速有效响应所需的技术和管理措施方面，都还需要做进一步的工作。

4、电力用户关注的安全情况

电力用户关注的安全主要是使用电力的安全和有效使用电力。“智能电力网络”的发展计划不仅仅是电力领域合理配电的体系，也是节能的重要措施，所以也是广大电力用户关注的问题。但是，智能电力网络规划与建设必须要进行安全建设，维护电力用户的权益。

鉴于上述分析我们做如下建议：

- 全面整合电力信息化安全建设，在此基础上建立电力信息安全自主保障、应急和监管与监控系统。电力系统应在考虑建设信息安全自主保障体系的同时，围绕标准控制与电调、通信与信息三大系统的管理中心的建设，以及数据安全、环境安全、边界安全、信息基础设施安全、数字证书、灾备、业务行为监管以及远程服务等方面进行安全规划。在规划时要从电力应用与系统的实际出发，要考虑专用的特点，建立公共技术标准，把集中与分散合理结合起来，注意考虑一套“和平时期高效，战争时期可靠”方案出来，注意结合电力系统特点采用代理技术应用。
- 电力调度系统与其他系统和公网的隔离建设。电力调度系统与其他系统（包括：办公自动化（OA）系统和管理系统、企业电子商务和对外服务系统等）尽可能不在同一个网络上，或者如果在一个网上至少需要通过高安全级（TCSEC 的 B1 级）的电力专用的防火墙、网关或其它隔离设备等进行有效的隔离，要

按照安全域的概念严格断开，同时通过相关产品和管理手段严格控制调度系统中主机私自拨号上互联网，防止引入安全隐患。同时要采用必要产品和技术手段进行网络信道的安全检测和监控，保证关键业务系统的正常工作。应当注意，这种隔离是充分考虑了互操作性基础上的隔离技术。

- 电力调度中心、通信中心与信息中心的安全加固建设。通过多种安全产品和技术，实现各电力调度中心的信息、计算环境、边界安全的建设与加固。
- 输电网/配电网的线路安全加固建设。加强输电和配电网线路安全保护的措施，并采取一定的监控手段，保证输电/配电设备的正常运行，和输电/配电线路处于良好状态。积极开展“智能电力网络”发展计划的规划和试点工作。
- 核电站（及其他关键系统）外包服务的安全建设。核电站、大型电厂、省电力公司、电力调度中心等关键部门在将远程配置/测试/诊断/维护等服务进行外包时，尤其是服务外包给境外提供商和国内外资提供商时，应严格对其资质和可靠性进行审查，在技术服务能力相当的情况下应优先考虑国内的厂商和提供商。对特别关键系统应考虑培养内部技术人员。在确定外包服务的提供商后，应确保其获得的是为完成服务所需的最少权限。同时应通过相关产品提供的技术途径和管理方面的措施，加强对外包服务工作的操作审计和加强过程监控。
- 电力通信系统安全加固建设。电力通信系统为电力调度、内部办公自动化等多个应用系统提供网络平台。为保证各种应用系统的持续稳定运行，电力通信系统需要考虑对信道进行备份，通过微波、电力载波、地面专线、以及电力线含光纤等多种其他线路类型相结合使用，以保证关键业务系统能够不间断运行。如果需要时统，则需要考虑通信网络利用 GPS 时统在特殊情况下不可控制的问题，以及网络定位系统存在漏洞问题。因而关键系统可考虑采用国内专用定位卫星。在整个通信网络层面考虑安全审计、信息源追踪与定位问题以及大规模入侵检测和防护问题，逐渐构成电力行业网络安全的基础设施。对于向一般用户提供接入等服务的网络线路，建议与现有电力调度系统、办公自动化等系统严格隔离，避免对关键业务和内部网络造成影响。
- 另外，对于公开对外服务系统安全加固建设、办公自动化和管理系统安全加固建设、安全检测、监控、审计、追踪与定位系统建设和应急规范制定和安全应急培训采取与其他行业类似要求。

2.3.6 铁路信息化安全建设情况

国家与铁道部对铁路信息化安全建设应当说是非常重视的。由于国家在整体信息化安全观念当时没有取得突破，铁路信息化安全的观念也主要建立在“数据与系统（软硬件、网络等）安全保障”之上，其安全观念与技术主要是局域网的。现在，由于国家在“行为与内容的监管”和“大范围的网络环境的安全问题”技术领域取得了突破和进展，需要考虑实现可信网络平台（TNP）与可信应用平台（TAP）、可信应用平台（TAP）和可信计算平台（TCP）的建设。

1、铁路网络行为与内容的安全情况

铁路网络行为与内容的安全主要是指建立在行为可信性、有效性、完整性和对铁路资源管理与控制行为方面，面对的威胁应当属于是战略性质的，即铁路系统威胁不仅要考虑一般的信息犯罪问题，更主要的是要考虑敌对势力与恐怖组织对铁路相关信息、通信、调度、控制与指挥系统实施攻击，同时要考虑战争与灾害的威胁。

2、铁路业务运营信息化安全情况

铁路系统主要考虑铁路运营业务信息化（铁路车辆调度系统、电子客票系统、铁路 GIS 系统）、铁路通信系统等信息与网络安全建设和铁道部以及地方各个路局的办公自动化网络的安全建设。电子客票系统的安全建设也已经有了一定的基础，但是存在着丢票等利用信息系统的犯罪问题。铁路信息化安全建设应当特别注意不同的信息化系统在安全建设的目标、采用的安全技术有较大的不同。要特别注意信息化对铁路运营业务的变化所带来的技术与业务组织体系结构的变化，关注信息化管理中心与运营中心的建设，要关注采用多种公共网络技术（不能仅仅采用互联网）和建立必须的应急体系。

3、铁路网络系统安全情况

铁路系统具有自己独立的通信体系，这个通信体系为保障铁路调度、指挥、控制、通信与信息系统的正常运行发挥了关键作用。但是，由于铁路通信体系开展了为社会公共电信服务，增加了铁路通信与信息系统不安全因素，为此铁路系统在信息化安全建设方面已经做了很多工作，通过防火墙、入侵检测系统等关键的安全产品的部署和实施已经初步地建立起了基础性的网络安全防护系统。但在产品选择方面，目前国外产品用得较多，需要逐步改变。

4、铁路用户关注的安全情况

铁路关注的安全问题重要应当是用户权益的维护问题。

根据以上分析可以做如下的建议：

- 应当全面地对铁路信息化安全问题做出总体规划，明确信息化安全建设的目标，要特别注意信息化对铁路运营业务的变化所带来的技术与业务组织体系结构的变化，关注信息化管理中心与运营中心的建设，要关注采用多种公共网络技术（不能仅仅采用互联网）和建立必须的应急灾备体系。要认真研究“行为与内容的监管”和“大范围的网络环境的安全问题”开展可信网络平台（TNP）、可信应用平台（TAP）和可信计算平台（TCP）的建设规划和总体设计工作。
- 建立功能强大管理中心，加强内部管理与远程管理安全建设。目前的网管工作站自身安全等级较低，加强 NMC 的安全管理与远程管理的高安全级别与强度的安全建设。
- 现有信息系统安全加固建设。通过边界安全隔离（防火墙）、严格的配置管理（网管）、监控措施（入侵检测）多种安全产品和技术，实现各车辆调度中心的信息、计算环境、边界安全的建设与加固。通信系统需要考虑对信道进行备份，通过卫星、微波、地面专线等多种线路类型相结合使用，以保证关键业务系统能够不间断运行。如果需要时统，则需要考虑通信网络利用 GPS 时统的在特殊情况下不可控制问题，以及网络定位系统存在漏洞问题。因而关键系统可考虑采用国内专用定位卫星。在车辆调度网需要使用卫星通信的情况下，建议不要使用任何国外的卫星线路。而且要考虑采用双星双频多转发器的模式，实现卫星线路的备份。保证车辆调度这一关键业务的不间断进行。
- 铁路内部调度与外部网络隔离建设。铁路系统内部的车辆调度网是铁路行业最为关键的业务网络，必须保证与外界任何网络完全隔离和断开，保证关键业务系统的正常工作。
- 另外，对于公开对外服务系统安全加固建设、办公自动化和管理系统安全加固建设、安全检测、监控、审计、追踪与定位系统建设和应急规范制定和安全应急培训采取与其他行业类似要求。

2.3.7 交通信息化安全建设情况

我国公路交通信息化建设目前规模较小，主要包括高速公路计算机计费系统、公路 IC 卡电子栏杆系统、公路通信系统、公路交通监控系统。我国交通信息化网络化建设了一些孤立的信息化系统。没有构成规模网络体系，没有建立公路交通安全保障监控系统。为我国交通信息化安全建设提供了后发优势。应当充分借鉴先发行业经验与教训。

1、建立我国交通数据管理信息系统。其建设内容包括：

1）调研近五年我国重大交通事故，形成汇总分析资料。

2)研究我国车辆和船舶安装运行信息记录仪等车船信息技术应用情况并做出需求分析。

3）研究国际和国外先进国家有关交通安全的监测管理与技术并做出分析。

4）研究交通（公路、水路）安全监测模型、应急对策、预警方案和有关措施，包括旅客运输、普通货物运输（主要为集装箱运输和重型货车运输）、危险品运输和特种运输。

5）研究建立与第 4 项密切结合的交通信息资源数据库（车辆库、船舶库、运输企业库及其他有关资源库）、交通电子图库、危险品数据库、专家知识库（提供应急对策、优化调度指挥方案）、多媒体监控及模拟演示技术。

6）研究一套规范化的监测车辆和船舶运行的信息采集技术、GPS/GSM 实时定位技术和通信传输系统技术。

7）建立的监测、预警、应急处理集成系统分区域、分线路、分专题进行实验和示范，并试制中试产品。

8）建立车船运行信息记录仪等有关信息技术的检测中心的技术研究。

9）该系统的标准化、有关政策法规体系研究

2、统一规划我国交通信息化安全建设总体框架。在交通信息安全保障、应急、监管等方面实施整体规划。

3、建立针对运输车辆和船舶运行全过程的监测、预警和应急处理系统。形成一套较完整的监测、预警、应急处理体系和信息交换/服务平台。

4、建设国家交通安全监管中心。

5、建设我国交通信息安全自主保障体系。

6、制定我国交通信息安全自主保障规范。

7、制定信息化安全应急标准与规范。

8、开展信息化安全培训，普遍提高公路领域的信息化认识。

2.3.8 民航信息化安全建设情况

中国民航是我国信息化、电子化建设起步较早、规模较大、应用广泛的行业之一。中国民航在信息系统建设的同时，对信息安全也给予了相当的重视和关注。近期由民航总局组织召开的信息化建设及信息安全建设讨论会上，各大航空公司、机场等均对信息安全提出了更高的需求。

因业务方向、服务对象各异，中国民航的信息系统涉及范围较广。

中航信主要经营电子客票系统，该系统在全球范围销售客票，系统的实时性、稳定性要求极高。目前，已在位于东四的中航信计算中心和位于西坝河的结算中心建立了互为备份的的数据中心。

中航油、中航材分别运营油料管理系统和航空器材管理系统。以上两系统用户量有限，对系统数据的完整性作了一定的保护。

各大航空公司主要运行本部办公自动化信息系统以及航务管理系统，航务管理系统通过由空管局运行维护的民航地空数据链（ACARS）提供的数据，对飞机提供全程跟踪服务。

各大机场主要负责运行基于大型局域网的离港系统和安检系统。

空管通信部门负责航空通讯保障，包括平面和对空通讯，同时，运营覆盖全国管制部门和机场与世界其它国家联网的自动报转网。

总体来看，中国民航在信息化建设的同时，对信息安全建设也投入了相当的精力，基本保障了民航各信息系统的可靠、稳定运行。但是，随着技术的不断发展，新的非法攻击手段的不断出现，民航信息系统难以抵御来自网络层和应用层的非法攻击以及保障系统稳定可靠的运行，面临较大的运行风险。我们认为，民航主要面对的威胁应当是战略性的有组织的集团（敌对势力与恐怖组织）的攻击，重点在于对网络、设备与系统的管理能力和控制能力的把握。

中国民航各信息系统的安全建设基本是基于应用系统的，没有形成一个整体、统一的安全防护体系和网管中心，抗打击能力较弱。各应用系统也存在相当的安全风险和漏洞。空管通讯系统备份不足，没有实现多星多转发的安全自主保障。电子客票系统、飞行调度系统、离港系统、安检系统等与民航业务正常运行关联密切的应用系统还运行在较为脆弱的平台之上。我国空管系统在依据 CNS/ATM 新航行系统的建设中要特别注意安全的建设。对原有的路基导航系统也要实施安全建设。

针对中国民航信息系统目前的安全现状，我们建议，中国民航应在考虑建设信息安全保障体系的同时，重点做好如下应急建设：

- 全面整合民航信息化安全建设，在此基础上建立民航信息安全保障、应急和监管系统。使用卫星通信的重要系统尽快实施多星、多转发器备份和天地备份项目，为空管通讯提供稳定可靠的环境。在考虑建设信息安全保障体系的同时，围绕标准控制与管理中心的建设，以及数据安全、环境安全、计算边界安全、基础设施安全、数字证书、灾备、业务行为监管以及服务等方面进行重点建设。
- 加强专网与公网的隔离与检测建设。
- 另外，对于公开对外服务系统安全加固建设、办公自动化和管理系统安全加固建设、安全检测、监控、审计、追踪与定位系统建设和应急规范制定和安全应急培训采取与其他行业类似要求。

2.3.9 政法信息化安全建设情况

我国政法系统的网络安全建设的任务除加强自身信息化安全保障、应急和监管建设外，与其它行业不同的重要建设内容是，建立打击网络犯罪与敌对势力的网络破坏力量的威慑体系。

计算机安全的基本理念是攻击和防护都必须以软件作为代理。网络犯罪和破坏是人在计算机中的代理软件完成的，那么防护、打击与执法也必须在网络中，也必须通过其代理完成。不可能设想，犯罪和破坏在网络内，而防护、打击和执法在网络外边。

我国政法系统信息安全建设，原建设重点在于自身工作的信息化，其安全建设缺少统一规划。我国政法系统信息基础设施尚未建立，对网络的监管非常不够。尤其对建立我国打击网络犯罪与敌对势力的网络破坏力量的威慑体系缺少认识，投入也严重不足。

- 制定我国政法系统的包括安全保障、安全应急、安全监管和安全威慑等方面的信息化安全建设总体规划。
- 建立我国政法系统信息共享的具有高度安全性的政法专网系统。

- 建立功能强大的网络管理与标准化监管中心。建立功能强大的网络管理与标准化监管中心，这个中心要对内容检查、系统管理、网络管理、安全管理、行为监控、代理（Agent）管理、网络远程服务监控和标准化执行实施统一分级监管。目前的管理中心自身安全等级较低，建议与管理中心纳入同一安全区域，加强管理中心的安全管理与远程管理的高安全级别与强度的安全建设。
- 建立国家统一的打击网络犯罪的“数字警察”威慑体系和侦察体系。打击公共信息网络的犯罪行为，建立公共信息网络监控网络中心是完成此项任务的必要条件。但是打击犯罪和发现犯罪是两个概念。由于其犯罪行为在公共网络上的社会性，通常黑客在现实社会中没有刑法规定的犯罪行为，其犯罪仅仅通过网络，通常对网络实施直接攻击。应当说其打击行为应当看成一种执法行为，是公安业务的组成部分。打击犯罪，就要确定犯罪现场。由于基础设施信息化，利用人员的金融行为（存取钱）、居住行为（旅馆）、通信行为（电话、上网）和交通（乘坐飞机与火车、汽车等）作为人员在社会中定位重要信息源是现实的。显然，如果没有实施安全监控和服务的网络化，要实现打击网络犯罪的快速反应是不可能的。在网络经济中，其犯罪在网络中，定位也要在网络中。利用网络 IP 地址或电话号码以及移动通信的无线定位系统，定位罪犯的位置。为定位，要有跟踪网络犯罪活动的能力。打击网络犯罪，要有罪证。要记录网络犯罪的活动和行为。要有对海量的网络活动中发现异常的能力，与罪犯通信能力和警告罪犯的能力。要有统计和分析的能力。为打击犯罪有通告、上报指挥中心的能力。通过作战指挥打击网络犯罪，形成快速打击网络犯罪的能力。**当代计算机犯罪是软件化的，犯罪是通过代理软件实施犯罪，而打击犯罪的公安力量在网络外面，也存在着公安业务与网络犯罪之间巨大的时间不匹配。要想真正有效的打击网络软件的犯罪，公安业务也必须实现网络软件代理化，以公安业务代理软件去对抗网络犯罪的代理软件，才是根本出路。我们把公安干警与其打击犯罪业务代理软件构成的体系称之为“数字警察部队”。**
- 建立国家统一的打击对抗敌对势力与恐怖组织的“数字安全”威慑体系。打击信息恐怖主义的威胁力量，主要任务是打击针对国家要害行业信息专网上的有组织犯罪行为和恐怖主义的犯罪行为。由于其攻击的隐蔽、间谍、恐怖、政治目的等特性，其打击行为应当看成是一种国家安全业务组成部分。根据我们的了解，各行业专用网络均将建立自己的信息安全保障体系，没有实施针对此类敌对势力的打击威慑力量建设。在网络上打击敌对势力活动，与打击一般网络犯罪活动有所不同。因为这种敌对势力的攻击活动采用的方法与一般黑客已经不同，是一种可以采用特殊工具与手段的有组织攻击。打击活动本身也必须是有组织的，针对性的和采用一些特殊工具。敌对活动已经不单纯是信息破译、病毒和入侵等直接攻击行为，从事网络业务的敌对行为是这其特点，将网络敌对行为与在社会上从事的敌对行为结合在一起。打击活动也必须在网络世界和现实世界两个方面进行，并且以打击现实世界敌对势力和恐怖组织为根本目的。同样的道理，建立“网络隐蔽战线”的打击网络敌对势力的数字化安全部队是根本建设内容。
- 建立全国 800 兆数字机群应急、调度通信系统。
- 建立我国信息源定位系统、定位系统的漏洞检测系统和抗定位的系统。
- 制定政法系统安全应急规范和开展政法系统安全应急培训。

最后，我们还建议：政法系统以安全审核员（CISP）的培训和系统测试评估工作为龙头，有的放矢的推进政法系统信息与网络安全建设工作。

2.3.10 国防信息化安全建设情况

军网安全建设在保密等领域取得较大成绩，但从信息安全建设的全局看，还存在一定问题，发展不平衡，至少，某些军事部门对我军信息安全的认识，存在一定问题。我军信息安全建设，目前尚处在起步阶段，与要求相比存在一定差距，应当急起直追。我们认为，军网安全建设应当处理好如下三个方面的关系：

- 我国军网的自身安全建设（应当清楚，虽然军网是个专网，但是从战争与反恐的角度来看，军网是非封闭的，可开放的。），要从保障、应急两个方面去努力建设。
- 我军网络对抗的军事威慑力量建设，研究网络对抗的技术、装备与战术，不仅仅是学习一些黑客的攻防技术。网络对抗是双方的多种功能代理的作战协同体系的对抗。所谓网络对抗是通过真实作战人员的直接对抗操作或主要通过各自代理系统向对方系统和对方网络代理系统发起攻击。对抗可以实施多种的战术，战术优劣仍然是胜负重要因素。双方有攻击，也有防护。在很大程度上，消灭对方的网络代理系统是网络对抗的重要，甚至有时是主要内容。双方产生网络作战代理的能力，不断补充被消灭的网络代理系统是胜负的关键因素。
- 启动我军对网络“国土防护”的安全保卫力量的建设。我们不能设想，在敌对势力的军事组织攻击我国电信、金融、电力等通信网络基础设施时，由于我国军队没有准备，在旁边看，而束手无策的局面出现，要研究参与国家网络国土防护的战术、技术、装备和人员训练等一系列新问题。）

由于军网的安全建设的特殊性，我们仅提出上述概念性意见，供参考。

2.4 电子政务信息安全建设情况

在这里我们仅仅就政府一些重要部门的电子政务信息安全建设情况进行描述，不可能对政府的所有部门的电子政务建设进行介绍。

2.4.1 电子政务信息化安全概述

我国的电子政务的工作较大规模的建设开始于“金字系列工程”，尤其是“金桥工程”、“金税工程”、“金关工程”、“金企工程”、“人民银行内联网工程”等。在十五期间实施的国家发改委的“国家电子政务纵向网络工程”、公安部以及政法部门的“金盾工程”和当前正在实施的“金财工程”都是重要的电子政务的建设工程。在启动“金字系列工程”时，1999 年在当时的国家经贸委和信息产业部的支持下，启动了“政府上网”工程，经过一段时间的努力，各政府机构的网站纷纷建立，为社会提供行业信息服务。为不断升温的“电子政务”建设奠定了初步的基础。

电子政务当前主要建设内涵应当包括：

- 政府面向社会的网络服务业务；
- 政府监管现代化业务的开展；
- 实现政府办公业务现代化与网络化。

其中以政府监管现代化与政府的网络服务业务开展为重点。当前，尤其以监管现代化为重点。建设目的是形成政府网络服务和政府网络监管的能力，并逐步实现这些能力的成熟。其中政府办公业务现代化与网络化在电子政务中是比较容易实现的，建设目标也较明确。

商会认为，我国的电子政务建设是在当前严峻的国际政治与安全的大环境中建设的，电子政务的建设要有利于国家驾御信息化和国家政权的巩固。要研讨电子政务信息化开放服务的同时，必须强调信息化的控制。我国当前电子政务的本质是实现网络政治、网络经济、网络公安、网络安全、网络工商、网络银行、网络税收和网络军事等一切政府行业的网络政权的建设。是国家政权在网络时代的基础建设，是国家政权建设的新内容和新任务。建立国家网络政权是电子政务的中心思想。

商会认为，电子政务要抓网络服务、网络监管和网络安全建设（包括威慑力量建设）三件事。由于网络监管和网络安全建设严重滞后，要重点抓。要把国家监管现代化和国家信息安全建设结合起来，不能孤立抓电子政务的信息安全建设。

我国的电子政务首要问题是总体的规划，首先要确定我国电子政务的目标、任务、发展阶段规划、策略、原则进行描述。要区分政府的向社会服务、政府内部服务和国家权力业务三个方面的工作，实施这些网络的业务分离。总体规划提出统一的公共操作环境平台标准和网络认证基础设施要求，提出了分网实施的可信和非可信的信息安全等级制度。要建立面向互联网络和经济信息专用网络的两个信息安全监控网络。各政府部门的业务系统、办公系统、服务系统等的建设，将依据统一的总体规划各自独立实施。这种规划工作要通过政府用户标准化系列和技术法规系列的制定、通过测评认证和监管/监控工作的部署来落实和通过建立面向管理和服务的配置管理体系的建设保障，不仅要管理与服务于现实社会的人类行为，还要管理和服务于网络世界中的行为。

电子政务的用户标准化系列的建设问题。这个用户标准系列包括互操作性标准、信息化安全标准和技术服务标准。电子政务的信息化互操作性标准是政府部门考虑的第一个标准化

工作。主要是由于过去国家各政府部门各自独立建设电子政务系统当作各自单位的自有系统建设的做法，忽略了电子政务建设的社会性、公共性。在新世纪，不能采用孤立的信息化建设策略，任何企业与部门的信息化建设都具有社会性、公共性和综合性，这一点是与以往的信息化建设最大的区别，关于电子政务的互操作性标准和公共办公环境的标准化工作可以认为尚未开始。电子政务的信息化安全标准是政府部门考虑的第二个用户标准化工作，其任务相当艰巨，但是政府有关部门和标准化组织对于这个问题的认识存在较大差距，从某种角度看，还没有开始，缺少基本的规划和部署。电子政务的信息化技术服务标准是政府部门考虑的第三个标准化工作，这项工作关系到安全和管理的重要问题，也是由于各种原因，尚没有一个了解该问题的标准机构为此工作。总之，中国信息化标准化工作目前是远远落后信息化要求的。

我国电子政务的技术法规建设问题。为了维护电子政务的网络秩序和贯彻国家有关电子政务的标准化体系，必须出台相应技术法规。建立和完善电子政务技术法规体系是电子政务发展成熟的表现。对于我国电子政务急需出台的技术法规包括：政府网络与系统安全标签技术法规、电子印鉴技术法规、电子签名技术法规、电子政务互操作性法规、电子政务系统安全法规、电子政务网络系统行为监管法规和电子政务的技术服务法规等。技术法规的建设问题，其首要的任务依然是做一个好的规划。

我国电子政务的信息化互操作性问题。信息化互联、互通和互操作问题是当代信息化第一位的系统问题，实际上就是要求建立某个范围内统一的运营和管理平台。我国电子政务的互操作性问题，应当包括各行业的监管信息化的平台建设、政府网络服务的统一平台和政府办公业务系统公共办公环境。

我国电子政务的信息化安全建设问题主要是指信息化系统及其承载数据的自身安全问题。电子政务的信息化安全分范畴和分级别划分问题。

我国电子政务的信息化管理和监管问题。电子政务的信息化管理问题之所以特别强调是应当把电子政务使用的系统列入为 GOTS 类管理，而不属于 COTS 类管理。这两类信息化产品和系统由于其完全不同的安全要求，GOTS 类产品的安全重点是从国家安全角度考虑的，而 COTS 类产品的安全重点是从用户的安全角度考虑的，所以要求的管理和监管也是不同的。

下面我们将分别针对监管信息化、政府网络服务和办公业务自动化的安全问题进行讨论。

2.4.2 监管现代化和信息化情况

2.4.2.1 监管信息化概述

建立监管现代化体系最根本的理由是服务实现了网络化，可以说“服务在网络里”，是毫微秒级光电速度。而监管是人工的，靠看打印结果实施监管，可以说“监管在网络外面”，其速度是人工的阅读速度。这种“服务在网络里”和“监管在网络外面”之间的巨大速度不匹配，造成了监管的虚假性。在号称规范成熟的美国金融界，“安龙事件”发生，充分说明了这个问题。在中国，信誉是当前的突出问题时期，网络外面的人工监管问题就更加严重，更加虚假。监管现代化体系建设的主要任务是监管业务要进网，主要监管原始数据和原始行为，而不是主要监管经过修改的资产负债表。建立国家信息化监管现代化体系，是一个国家的综合系统工程，涉及到政府监管当局、税收、财政、工商、海关、商业、政法、银行、证券、保险、投资、融资、租赁、社会和企业等多方面领域，直接为国家创收、金融安全、用好资金和社会稳定服务。

当前，税收、金融和政法等方面的监管系统的建设是国家监管现代化建设的重点。

2.4.2.2 税务监管信息化情况

我国税收等行业安全监控体系建设是国民经济安全监管的重要组成部分，是政府的主要的创收项目。税务管理部门监管企业的商业和税收情况，监管的对象是企业和个人，税收与及其监管对象数量巨大，监管的内容繁多，而且面向广大非可信社会用户。

我国税收与及其监管情况目前停留在通过可视化系统实现对人类在现实社会的税收活动与行为管理与监督上，是一种被动模式的监管。国家税务网络是建在国家电信公共网络上，用户通过它实现交纳税和各种检验业务，实行的是随路安全监管。这种被动模式的监管需要大量的人力，监管力度较差，安全性问题严重。所以必须建立主动模式的税务监管现代化体系，普遍地使用代理化的税务征管体系，其税务业务系统实行代理化服务，税务监管实行代理化监管，实行税收高智能的业务应用与管理，全面实现简单业务的事务处理代理化，实现税票比对、分类、统计、查询代理化处理，增加人工辅助决策能力。在上述主动征管业务系统基础上，实现税务系统的行为与内容监管、分类属性监管和综合监管。

税收业务网络结构包括生产干网和内部结点网络，税收活动通过税务系统的终端进入系统。另外，税收业务还可以直接面向社会，通过与公共网络进入体系，实现税务服务。从这个网络结构来看，建设专门的监管使用的监控网络系统和监控网络的运营管理系统是必要的。

所以说，税收监管现代化和信息化建设任务依然艰巨，是信息化建设的重要新领域，为信息安全产业开辟了新的市场前景。信息安全产业商会的企业，应当积极向我国税务领域推荐可信网络平台（框架）概念，借鉴《银行行为监管：银行监管信息化》及《银行行为控制：银行信息化与安全》两本书介绍的信息化安全和监管思想，用新的理论和认识武装税务领域的用户，把我国税务领域的信息化安全和监管信息化工作推进到一个新的水平。

2.4.2.3 金融监管信息化情况

金融监管现代化系统是促进和保障金融业务发展、规避和化解金融风险以及确保金融电子化安全发挥效益的最重要的建设。

金融安全监管的对象是银行、证券、保险和非金融机构开展的金融业务。主要监管资金的使用情况，包括资金流向、流量，同时监控信息与系统的安全性。传统安全监管工作主要是事后检查和审计、这项工作主要通过查账进行，监管是靠人工完成的，效率低下。另外，利用计算机打印出结果实施审计和检查，对于现代计算机犯罪已经是靠不住的。已经多次发生金融计算机犯罪在打印数据上做文章，使计算机打印的结果和计算机内部的实际数据不一致的来掩盖犯罪。实行我国的金融监管，在信息化和网络化的时代，银行监管必须实现现代化、自动化、信息化和网络化。仅靠人的眼睛和头脑实施事后处理的金融监管是不可能的，也是靠不住的。监控网络结构包括银行监控网的干网和接入网络建设，监控网络的系统建设以及监控网络的运营管理系统建设。国家金融监控网络建设主要实现实时监管资金的流向、流量和信息与系统的安全性，该系统应当具有商业银行行长、人民银行行长和国家领导人可以控制的三级实时预警系统。建立金融监管现代化体系是国家信息化监管现代化体系最重要的组成部分之一。

首先，金融风险监管要建立统一的认识体系平台，这种新认识体系的探索表现在金融学方法、管理学方法、计算机科学方法和系统工程方法学的结合。这种结合体现在新的综合认识体系平台上，既坚持了银行、证券和保险风险监管的国际组织以及各国的金融风险监管当局标准（例如银行的巴塞尔资本协议、证券的证监会国际组织 IOSCO）和保险的（IAIS））

对风险监管的标准要求，从金融学宏观理论探讨银行风险监管；又发扬了系统工程学方法清晰的优势，从微观分析风险因素研究银行风险监管；既体现了管理学方法监管制度建设的重要作用，又突出了监管信息化中计算机科学理论指导意义，还为经济学家、金融学家、系统工程学家、管理学家、信息科学家采用各种方法学在这个认识体系平台上发挥作用提供动力，实现了宏观与微观统一和制度与技术的结合。

其次，要明确金融风险监管信息化与信息化监管的要求。我们认为要有非常明确的监管信息化目标：实现主动模式风险监管模式；为克服银行信息化中出现的“服务在网内，监管在网外”的严重弊端和满足监管业务要进网的要求。要了解监管信息化的对象，对监管信息的的内容和系统在网络虚拟世界中的行为，有清晰的认识，实现可信网络平台（TNP）建设。

第三，监管信息化要有明确的分类：实现行为条件的基础监管：银行信息系统业务和技术行为与内容监管。银行行为属性分类监管：在银行业务系统行为与内容可信性、有效性、完整性、保密性和连续性监管的基础上，实现了信用风险、市场风险和操作风险的分类监管。银行行为标题综合监管：行为与内容综合性监管、银行资金流量流向监管、信息自下而上汇总监管、政策自上而下传导畅通性监管等。

第四，要紧紧抓住监管信息化的时代特点：“大范围网络环境、超海量数据与对象、高智能应用与管理”。

所以说，我国金融监管现代化和信息化安全建设任务非常艰巨，《银行行为监管：银行监管信息化》及《银行行为控制：银行信息化与安全》两本书介绍的信息化安全和监管思想对全国金融系统有普遍的指导意义，在金融领域应当率先学习与研讨，通过这个学习运动建立信息化安全的新认识和新起点，开辟信息化安全建设的新领域新市场。信息安全产业商会的企业，应当积极向我国金融领域推荐可信网络平台（框架）概念，把我国金融领域的信息化安全和监管信息化工作推进到一个新的高度。

2.4.2.4 财政监管信息化情况

财政监管现代化系统是保持国家财政稳定、规避和化解财政风险以及确保财政信息化安全发挥效益的最重要的建设。

目前实施的“金财工程”（也称之为国家财政管理信息系统，英文缩写为 GFMIS）是财政部领导根据党中央国务院对财政部要求的指挥、决策和管理政府财政系统体系。GFMIS 是利用先进的信息技术，支持以预算编制、国库集中收付和宏观经济预测为核心应用的政府财政管理信息综合系统，覆盖各级政府财政管理部门和财政资金使用部门，全面支持部门预算管理、国库单一账户集中收付、宏观经济预测和办公自动化等方面的应用需求。为了支撑部门预算管理和国库集中收付制度改革，按照建立我国公共财政系统框架的总体要求，建设先进的政府财政管理信息系统，有利于预算管理的规范化，提高国库资金的使用效率，提高政府财政管理决策的科学性，增大财政管理的透明度，有利于加强廉政建设。GFMIS 系统体系结构依然属于传统联机事务处理（OLTP）和联机分析处理（OLAP）可视化管理信息系统。

GFMIS 安全威胁包括敌对国家和国内外组织、敌对犯罪分子以及黑客的攻击，造成政府财政管理信息的泄露、篡改和删节，造成政府财政管理信息需要使用时不可用等。GFMIS 实施了信息保障技术框架防护措施。在信息化安全建设方面做了较多的考虑，但是由于信息化安全的观念依然是建立在“数据与系统（软硬件、网络等）安全保障”之上，整个信息化安全理念依然是在上世纪 90 年代中期发展起来的局域网安全观念。对于网络与系统的虚拟世界的“行为与内容的监管”和“大范围的网络环境的安全问题”基本上没有考虑。金财工

程的风险观念和安全问题应当进行调整，在新起点和新高度上，进行补充总体规划。实现可信网络平台（TNP）建设。

从金财工程的总体方案中看不到财政信息化系统的监管体系，显然需要对财政信息化系统制定监管信息化的总体规划，要做到在网络虚拟世界中对财政行为实施全面监管，对现实世界中财政方面人类活动实现辅助监管。

所以说，财政监管现代化和信息化建设任务是艰巨的，是信息化建设的重要新领域，为信息安全产业开辟了新的市场前景。信息安全产业商会的企业，应当积极向我国财政领域推荐可信网络平台（框架）概念，借鉴《银行行为监管：银行监管信息化》及《银行行为控制：银行信息化与安全》两本书介绍的信息化安全和监管思想，用新的理论和认识武装财政领域的用户，把我国财政领域的信息化安全和监管信息化工作推向新高度。

2.4.2.5 海关监管信息化情况

“金关工程”实施十周年来，海关信息化的建设应当说取得的很大的成绩，在报关、过关、检验、税收、监管等业务信息化建设方面达到了较高的水平。“金关工程”在信息化安全建设方面做了较多的考虑，由于历史的原因，信息化安全的观念是建立在“数据与系统（软硬件、网络等）安全保障”之上，同样，对于网络与系统的虚拟世界的“行为与内容的监管”和“大范围的网络环境的安全问题”基本上没有考虑。海关系统的风险观念和安全问题应当进行提升和补充，在认识提升的基础上实现海关监管信息化建设。

海关监管信息化建设同样可以借鉴《银行行为监管：银行监管信息化》及《银行行为控制：银行信息化与安全》两本书介绍的信息化安全和监管思想。

2.4.2.6 政法监管信息化情况

“金盾工程”是政法系统重要电子政务工程，其宗旨是科技强警，在网络建设方面构成全国政法系统内的专用网络体系，并期望实现体系内的信息共享和交换。从现在看来，该工程基本上完成了国家公安部门的信息化一些基本内容的建设，但对于公安部门发挥更高工作效益重要系统还没有建设。对于法院、检察院、司法部门和国家安全部门信息化建设需要新的支持。国家政法监管现代化建设基本是空白，需要更多的支持，例如可以考虑启动全国范围的政法可信网络建设和建立国家监管基础设施。

以打击公共网络的信息犯罪为例。打击犯罪，首先要发现犯罪。快速有效打击网络犯罪必须具备如下三个条件：1、互联网监控体系必须是网络监控体系，监控本身必须组成全局网络系统。2、必须建立“网络警察”的打击网络犯罪的数字化警察部队。实现网络代理技术应用。把网络警察代理软件与芯片永久或动态嵌入到被监控的设备与系统中，实现网络远程的监管服务。3、网络信息内容的检查与监控，例如对法轮功、黄色、反动网站的检查和监控。为解决问题，除积极考虑过滤器方案外，还应当考虑实现网络代理技术应用。把监控代理软件动态嵌入到被监控的设备与系统中，实现网络远程的监控服务，建立网络主动监管体系。

这些监管信息化的新领域，为安全产业开辟了新的市场前景。

2.4.2.7 政府信息化安全监管情况

政府信息化安全问题本身就需要监管，这主要是由于广泛存在着业务与技术风险，包括政府网络服务越来越普遍的开展与国际与国民的联系，可信与非可信因素复杂地交织在一起；包括政府内部的腐败和变节分子从事非法活动，需要对其进行严厉打击；包括政府网络

大量的从事非政府业务活动，需要实现网络内的管理等。政府业务信息化促使了越来越多办公业务在网络上实施，而在网络从事办公业务的管理制度和管理方法却没有进入网络，而在网络外面。也就是说政府的网络中的行为需要实行管理，以维护政府网络的办公秩序与安全。另外，国家关于对于政府人员的守法、保密规定以及要求实施政府办公网络与社会公共网络分离的规定，如果不实行严格的监管，事实证明了这种网络隔离要求在相当程度上是不能确保的。

通过对政府信息化的行为监管、行为控制和行为认证等措施，逐步实现政府网络的可信性。同时，这些信息化监管的新领域，为安全产业开辟了新的市场前景。

2.4.3 政府网络服务信息化安全情况

政府网络服务是电子政务建设的另一个重点，尤其对于地方政府就显得更加重要。政府提供网络服务类型越来越多，例如政府批准程序的网络虚拟服务厅、政府信息网络发布系统、政府网络信访系统等。目前这些系统主要建立在互联网和其他社会公共网络之上，其安全考虑还相当少，即便考虑某些信息安全建设，也主要是针对网络与系统自身的安全建设，例如防病毒、防黑客入侵等。

我们应当建立一种新的观念，信息化安全不仅仅涉及到国家安全、基础设施安全才是最重要的，对于社会稳定和公共服务领域的信息化安全同样是非常重要的，因为公共服务的安全直接涉及到政府对公众的信誉和法律方面问题。政府网络服务需要安全建设是要保证政府网络服务行为的可信性、有效性、完整性和连续性。所以，除保障服务的自身安全之外，要保障政府网络服务系统不构成对公众用户的隐私和权益的损害。如果政府需要对公众用户实施行为监管或监控，应当严格依据法律规定实施。

政府提供的安全服务是通过有关政府部门，例如公安、安全、保密、机要和司法等有关部门提供的信息安全服务。这些安全服务包括信息化安全产品市场准入服务、信息化安全测评认证服务、信息化安全管理与监控服务、信息化安全预警服务和信息化安全法律服务等。

目前我国政府网络服务的信息化安全建设也只能是刚刚起步，还有大量的工作需要去做。

2.4.4 政府办公业务信息化安全情况

政府办公业务信息化实际上已经取得的突出的成绩，这主要表现在各政府部门范围内的信息化建设。

政府办公业务信息化存在的问题包括：

1、关于建立公共办公环境问题。建立公共办公环境（Commen Office Enviroment，COE）问题是政府部门办公业务信息化的关键问题，包括办公业务流程控制、批准程序、文件管理、电话管理、会议制度、布告制度、电视电话会议等相关内容。在信息化建设方面涉及到办公业务之间互联、互通和互操作和安全性。这种公共办公环境的建立首先是在一个政府部门领域，例如人民银行从总行到各分行支行以及与银监会和各商业银行之间的办公业务的公共办公环境的建立。例如国家财政、税务、工商、海关、政法等各领域范畴内的办公业务自动化和信息化中公共办公环境的建立。然后才是建立跨政府部门领域的互联、互通和互操作环境问题。为解决这些问题，各政府部门还需建立相应的办公内联网系统。

2、关于办公业务信息实现共享制机制问题。政府办公业务信息共享与交换问题是一个老大难问题，在政府内部信息共享也存在着评价、评分甚至定价问题，否则信息提供方积极

性是很难被调动起来，也不能促进各部门对于提供信息的积极性提高。过去和今后一段时间内，用户通过访问方式是处理信息共享与交换的重要手段。但是，越来越多地使用代理服务方式来解决信息共享和信息交换，并且会成为主流的信息共享和交换形式。

3、关于建立政府办公系统分范畴和分级别划分问题。

4、关于网络中身份与行为可信认证问题。

5、关于网络中办公行为监管问题。网络中办公行为监管主要是对政府的权限规定、保密规定、知识产权和工作人员的行为的可信性、有效性、保密性进行监督和管理。这种监管是在网络中实施的，通过政府部门的监管代理对所管辖人员网络与系统行为实行监管。

6、办公系统安全防护问题。办公系统安全防护是指办公信息系统自身防护，这种防护在其计算机系统、计算机网络系统和通信系统中实施的。

政府办公业务信息化的安全问题，虽然得到普遍重视，但是其安全建设不规范和没有标准可以遵循，其建设、运营和管理的好坏由政府办公业务信息化安全的主管人员对信息化安全的认识水平来决定，应当说问题还是相当普遍和严重的。

2.4.5 政府信息化安全应急体系建设情况

政府信息化安全应急体系建设目前还没有提到议事日程上，要建立面向政府部门的信息化安全的应急体系。作为国家级的应急体系的建设必须与政府部门的档案机构和制度结合起来，建立电子档案备份基地，建立档案备份数据库体系和介质备份体系。

2.5 电子商务信息安全建设情况

2.5.1 电子商务信息化安全概述

电子商务的问题千头万绪，有企业的问题，有银行的问题，也有政府相关部门的问题。可以看到许多企业的电子商务模式，业界讨论电子商务的 B-to-B，B-to-C，B-to-E 和 I-to-I 等各种模式，以及如何将电子商务与企业的资源计划、企业信息化建设结合起来。国外电子商务一开始就使企业与银行表现出最大的热情，而且以企业联盟形式进行探索。例如电子商务发展趋势构成以企业或企业集团为中心的联盟或商会是一种发展趋势。在国际互联网络上不是没有电子边界，而是建立了明显的市场的电子边界，实施企业的核心网络、内联网络、外联网络和国际互联网络，组成多层次会员机构。例如，汽车行业的电子商务，由通用汽车公司、福特汽车公司、克来斯乐汽车公司联合发起，后由日本的尼桑公司和法国的雷诺公司加入，于 2000 年成立的专为电子商务而成立的合资公司 COVISINT(Cooperation Visibility Integration)，就是这种模式开展 B-to-B 的统一的市场交易的电子商务平台重要案例。世界著名的 EDS 和 ORACLE 公司作为这个联盟电子商务平台建设的主要技术支持机构，这个发展计划并没有达到预期的目标。美国和其它发达国家对于电子商务的市场环境、法律环境、推进全球发展和一致性原则作了大量的工作，例如在 20 世纪 90 年代颁布《全球电子商务框架》、《关于电子商务的宣言》和《电子商务国际宪章》等框架体系，为促进电子商务发展提供了动力。为了推动电子商务的实际推进，各国纷纷出台 “电子签名法”、“电子印鉴法”、“电子票据法”、“电子标签法”、“网络监听监控法”和网络代理等相应技术法规。

我国电子商务的发展与世界电子商务发展一样，走过一段弯路。我国电子商务作为政府的早期计划是国家经贸委和信息产业部于 1996 年和 1998 年分别启动的“金企工程”和“金

贸工程”，试图在经贸委的领导下建立从国家到省、市的一系列的网络商品交易中心，启动电子商务的发展。由于要求企业参与的理由和企业参与的需求力不够，该工程出现经营困难。当时的国家经贸委很快认识到电子商务的建设主体应当是企业。国家经贸委支持国家 520 家大型企业以企业集团的方式建设行业的电子商务平台。国家经贸委于 2000 年已经启动了家电和车床两个行业的电子商务平台计划。国家经贸委和信息产业部后来认识到，电子商务平台应当建立在国家大型企业与企业集团网络信息公共操作环境平台的基础上。除国家政府部门关注电子商务的发展外，地方对电子商务的发展也十分关注，例如北京、上海等省市希望通过建设城市与地方的电子商城，建立互联网络上的超级市场，促进企业电子商务的发展，探索我国电子商务的发展道路。行业主管部门也在积极探索电子商务的发展模式，其中我国进出口电子商务建设一马当先，国家进出口的电子商务源于国家外经贸部的 EDI 建设和“金关工程”，是我国的进出口商会的贸易网，提供在线信息发布、在线交易和在线服务的平台，进出口的配额管理服务，于 2000 年建立了中国国际电子商务中心。除此之外，金融行业积极推进电子银行（银行电子商务）发展计划，取得了实在的成果。

我国与世界一起逐步认识到电子商务的主要形态是网络服务的商业模式，也就是说，电子商务的发展不能仅仅靠一种网络经济模式，而要基于当时的情况。从网络服务的角度来看电子商务，有许多网络服务可以比网络购物更容易实现电子商务的商业概念。也正是在这个基础上，我们提出了基于网络远程服务的网络经济商业模式和更加广义的电子商务观念，呼吁企业家不要把电子商务概念仅仅捆绑在网络购物和网络银行上（B-TO-B，B-TO-C等），走更加宽广的电子商务的发展之路。企业家应当解放思想、实事求是，结合企业的实际情况，革新电子商务观念，提出适合时代特点的网络服务的信息平台化发展思路。可以“哪壶开了，提哪壶”，条件成熟的先做。

网络经济的基础是网络远程服务。这些网络（远程）服务包括：网络支付、网络银行、网络台账、网络购物、网络收税、网络公安、网络炒股、网络调度（电力）、网络教育（学生）、网络认证、网络会议、网络培训（技术）、网络设计（产品）、网络扫描、网络测试、网络监控、网络维护（电器）、网络诊断、网络管理（系统或业务）、网络咨询、网络安装（软件）、网络备份、网络恢复和网络浏览等等，涉及到国家政治、经济和社会的许多方面，但主要还是涉及到网络经济发展。这些网络服务没有国界、可以在远程实施。

这种基于网络服务的电子商务与国家基础设施信息化、产业信息化、城市信息化、人民生活信息化和电子政务密切相关，实现它们之间的互联、互通和互操作。正是由于这种网络服务的电子商务和互联、互通和互操作对信息化安全提出更高的要求。

电子商务的安全概念划分为如下的五个方面：

- 安全交易、运营、管理等模式。
- 安全保障，研究数据在语法意义上安全和系统（包括软硬件）自身安全。
- 安全监管，研究数据在意义范畴上内容安全和系统在网络虚拟世界中的行为安全。
- 安全应急，研究系统在异常或灾害情况下如何维护系统工作的连续性及其采取的应急响应。
- 安全威慑，打击网络犯罪和网络恐怖主义，建立网络虚拟世界安全与秩序。

2004 年 11 月，国务院第四次信息化领导小组会议专门研究了我国电子商务的发展计划，为我国电子商务发展提供指南。

2.5.2 企业电子商务信息化安全情况

企业电子商务建设实际上是企业公共渠道现代化和信息化的建设。我国企业电子商务建

设已经有相当的发展，建设一些发挥网络服务优势的电子商务服务系统，例如，全国或地方税收网络系统、报关和退税网络系统、工商信息系统、电费收费网络系统、电信或移动电话计费收费网络系统、公路交通计费收费网络系统、汽车维修网络系统、铁路售票收费网络系统、民航售票收费网络系统、家电维护和服务网络系统、汽车加油计费收费网络系统、闭路电视收费网络系统、远程教育网络系统等等。但是，对于大多数企业而言，其电子商务概念依然是在互联网上建立了一些网站式的信息发布系统、广告系统，并没有建立起互动式的网络业务服务系统。

目前，企业电子商务系统实际上是彼此分离的“烟囱式”的信息系统，不能实现网络业务的交换、共享、协同和控制，相互之间难于在业务与安全范围内实现互联、互通和互操作必须实现相融操作环境（COE）建设。

所有这些电子商务建设都面临着普遍的信息化安全问题，要区别面向企业电子商务平台安全建设和面向公共渠道的安全建设。对于面向平台安全建设大致需要建立如下安全体系：

1、企业电子商务的安全自主保障体系建设。

2、企业电子商务的监管体系建设，这种监管体系是采用多代理监管技术。

3、企业电子商务的安全应急与业务连续性建设。

对于面向渠道安全建设要特别强调终端系统安全防护、监控、监管，其中必须包含定位、检测和取证的能力。

企业电子商务的安全问题的需要差别较大，有明显的客户化要求，同时是信息安全产业重要的市场领域。

2.5.3 银行电子商务信息化安全情况

银行计算机系统的发展已经历了三个阶段：计算机辅助管理阶段（20 世纪 50 年代—80 年代中后期）；银行电子化阶段（20 世纪 80 年代中后期—90 年代中期）；以网络银行为标志的电子商务阶段（从 20 世纪 90 年代中期至今）。当前，出现了各种新型的电子网络服务，如以自助方式为主的在线银行服务（PC 银行）、自动柜员机系统（ATM）、销售终端系统（POS）、家庭银行系统（HB）、企业银行系统（FB）、移动银行等，通过电子化渠道替代了大量的手工操作。随着银行电子化的发展，电子货币转账逐渐成为银行服务中的主要业务形式，电子信息取代传统的现金支付和票据转账结算。电子货币以分布在金融机构、服务网点的金融专用终端（如 POS 或 ATM）和计算机网络为物质条件，以提款卡、银行卡、IC 卡为媒介，使货币以电子数据的形式在银行网络间进行传递，从而形成电子货币流通系统。

有必要澄清两个概念，一是银行电子商务的内涵大于网络银行，或者说，网络银行只是银行电子商务的标志性服务渠道之一。银行电子商务系统向客户提供上述服务的渠道主要有三种：

- POS 机和 ATM 机，这些端末设备基于银行内部结算网络，主要应用于与银行签约的特约商户，实现个人、商户和银行间的资金流动。
- 呼叫中心，主要提供账务查询、挂失服务和代理销售等服务，实现客户与银行之间互动服务。
- 网络银行，是银行在互联网上开辟的金融服务窗口，目前客户通过上网浏览方式已经能够实现账务查询、转账以及网上支付功能。

网络银行的出现使银行服务完成了从传统银行到现代银行的一次变革。网络银行与企业银行、家庭银行、电话银行、自助银行等，都是在电脑及其通讯系统上进行操作的，但网络银行的软件系统是在银行服务器上运行，各种金融服务不会受到终端设备及软件的限制，具有更加积极的开放性和灵活性。简单地说，传统银行为客户提供服务的手段主要有分支机构、商业网点，以及电话、传真和其他通用通讯工具等。网络银行为客户提供的主要服务手段包

括：互联网、PC、电话、IC 卡、可视电话和银行分支机构等，以各种代理商（如股票经纪人或房地产代理商等）为信息来源基础的网络银行服务，将成为传统银行的有力竞争途径。银行服务的整体实力将集中体现在前台业务受理和后台数据处理一体化综合服务能力及其整合技能上。

第二个需要澄清的概念是网络银行。巴塞尔银行监管委员会（BCBS，1998）指出，网络银行是指那些通过电子通道，提供零售与小额产品与服务的银行。这些产品和服务包括：存贷、账户管理、金融顾问、电子账务支付，以及其他一些诸如电子货币等电子支付的产品与服务。但是，随着身份认证、信息安全等技术的发展，网络银行的服务内容已经从零售、小额业务发展到批发、大额业务，并整合原来相对独立、面向网上购物的在线支付功能，逐渐发展成为全功能银行（现金收付业务除外），其用户不仅有个人、中小企业，还包括大型集团公司，部分机构甚至将银行电子商务系统作为跨机构、跨地区的资金管理平台，延伸到公司内部使用。

银行电子商务的安全问题包括如下的五个方面：

1、银行电子商务的交易安全。交易安全问题是通过一整套的交易协议来保证。

2、银行电子商务的安全保障体系建设。

3、银行电子商务的监管体系建设，这种监管体系是采用多代理监管技术。

4、银行电子商务的安全应急与银行业务连续性建设。

6、打击金融犯罪威慑体系建设（包括反洗钱、诈骗等各种犯罪行为）。

电子银行的安全与监管方面详细论述可以借鉴《银行行为监管：银行监管信息化》及《银行行为控制：银行信息化与安全》两本书介绍的内容。

2.5.4 政府电子商务信息化安全情况

政府电子商务系统主要是指在企业、银行和社会电子商务系统上实行商业目标的管理、监督、税收、法律、安全等方面的职能。这种职能是针对网络中的商务行为的。主要存在三个方面的问题：

1、平台建设。国家的工商、税收、海关、防伪、法律、公安等政府管理系统不可能建设在成千上万相互分离的企业的电子商务平台上。企业的电子商务平台也不可能建设在政府行业的电子商务的管理平台上。企业电子商务平台和政府电子商务平台，必须在统一的公共操作系统环境上实施建设，以解决企业电子商务平台与政府电子商务管理系统平台之间的互联、互通、互操作问题。国家的工商、税收、海关、防伪、法律、公安等政府管理系统要求在全国统一电子商务平台上实施建设。总之，电子商务的建设必须在公共的基础、公共的标准、公共的规范、公共的核心实现、公共的 API 服务、公共的工具、公共的测评认证范围内实施建设，保证不同的系统之间的互联、互通、互操作和安全性，积极吸纳大量 IT 厂商开发千差万别的应用系统，为电子商务发展服务。国家的电子商务平台应当建立在国家大型企业与企业集团网络信息公共操作环境（COE）平台的基础上。

2、在网络内实行监管的技术体制，即建立多代理监管技术体制。

3、政府电子商务系统的安全问题。这些安全建设一方面是面向电子商务平台的，其建设要求可以借鉴电子政务；另一方面是面向社会客户的，其安全建设可以借鉴银行公共渠道的信息化安全建设。

2.6 产业信息化安全建设情况

2.6.1 产业信息化安全概述

通过近 20 年的信息化的建设，我国产业信息化取得了可观的成绩，包括产品设计自动化、生产过程自动化控制、企业资源管理系统、企业产品与服务管理信息系统和企业渠道管理信息系统以及企业电子商务系统等。当前，产业信息化和网络化建设目前主要向多网融合的通信平台、具有广泛安全机制的信息交换平台和一体化的应用平台的建设发展。在这些平台上，将建设新一代的产业应用信息系统，向更加开放的社会安全服务的方向发展，建立产业的网络商会，建立行业统一的电子商务市场，加强企业之间的合作。企业的信息化与产品的设计、生产、储运电子化和自动化相结合，企业信息化要与企业电子商务相结合，更加与企业业务发展相结合，强调信息化建设的效益性。当前企业的信息化大致可以划分为如下的几个方面：

- 企业价值管理信息系统
- 企业资源管理信息系统
- 企业风险监管信息系统
- 企业产品与服务信息系统
- 企业渠道管理信息系统
- 行业领域网关信息系统
- 企业办公信息系统

企业信息化更加强调向多系统和多代理体系结构发展，多系统的平台建设是企业信息化建设的焦点。

运营商通过实施领域信息化安全标准（例如互操作性、安全性和服务性的用户标准体系）和技术法规，体现出对国家关注的网络行为与内容安全、安全生产问题、业务连续性服务问题、网络安全问题和用户安全问题解决，同时接受国家和领域对安全问题的监管。

实施信息化建设时，越来越要求对企业业务与技术组织体系结构进行改革，实现管理层次的扁平化、时空聚焦化的低管理成本效益。现代企业领导人在不清楚信息化对企业提高企业竞争能力帮助，不清楚适合信息化的业务与技术组织体系结构和信息化可能带来的负面的作用有方案能够抑制（例如企业知识产权和企业员工在上班时间做非预期的工作）之前，有见识的企业领导人是不会匆忙上信息化的。从这个意义上看，信息化安全建设必须与企业的风险监管信息化结合起来，这种结合是促进企业信息化事业发展的因素。所以，企业应当关注业务运营系统安全建设。

我国信息安全产业中的企业，要了解企业领导人的关注的问题，才会不断扩展信息化安全建设的市场。

2.6.2 产业信息化安全情况

产业信息化建设划分为企业内部信息化建设、渠道信息化建设和领域信息化建设。其内部信息化建设主要包括企业价值管理信息系统、企业资源管理信息系统、企业风险监管信息系统、企业产品与服务信息系统和企业办公信息系统。这些企业信息系统建设虽然也有对外的联系，仍然是相对封闭的系统。

企业渠道管理信息系统主要理解为企业的电子商务系统，包括公共渠道和大客户渠道的

信息化建设。其公共渠道安全建设与电子商务信息化安全基本一致，大客户渠道的信息化安全要保持与大客户信息化安全建设一致。

行业领域网关信息系统涉及到行业内部多企业或者企业与行业主管部门的联系与合作，但是这种合作与联系必须是安全的，所以应当进行信息化安全建设。

产业信息化安全建设有两个特殊的问题：

1、企业知识产权保护。企业的产品（软硬件）、系统、解决方案、工艺、流程、结构、技术所有的设计文档、图纸、模型、资源、手册、说明书、规范标准和程序代码等为企业私有的东西，都属于企业知识产权保护的内容。而这些内容在信息化时代，基本都记录在计算机系统和数据库系统之中。如果企业对这些珍贵资源不实行保护，很可能被内部或外部的人员所盗窃。另外，对于从事安全工作的企业，对于设计、开发、生产、培训、维护、服务、市场等部门不实行必要的隔离、防护和监控，很可能造成对自己和客户的安全威胁。这种管理不安全的威胁，如果涉及到客户的利益，还会涉及到法律方面的问题，给企业带来更大的损失。企业要建立比较严格的档案管理体系。

2、企业员工网络业务与技术行为监管。为了管理信息化后企业员工的网络行为和考评人员的网络行为的可信性、有效性等要求，必须对员工的网络行为进行监管和对其网络行为的结果（内容）进行监管。同时，实行人性化的对在办公时间从事非预期行为的监管，并将这些监管与员工的绩效考评和工资待遇联系起来。

如果一个企业领导不实行上述两个方面的建设，企业信息化建设是具有非常大的风险的。

2.6.3 产业信息化安全应急体系建设情况

除少数企业和有特殊要求的企业外，企业除建立自身的备份与恢复系统之外，企业信息化安全应急体系建设通常应当纳入到行业和地方、城市建设的应急、灾备基地或支援中心的建设中。在灾备和应急基地内设置或租用专门的服务器，相当于开展信息化保险业务，化解或分散企业信息化风险。

2.7 城市信息化安全建设情况

城市信息化安全建设应当包括城市基础设施信息化、城市电子政务、城市电子商务、人民生活信息化、智能社区信息化、家电设施网络化、城市呼救服务和城市应急信息化等方面的安全建设。

2.7.1 城市信息化安全概述

城市信息化的总体工作，在建设规划时必须注意如下的一些原则问题：

1、城市信息化必须为城市发展的总体战略目标服务，以实现城市的总体发展目标为宗旨。不能为信息化而信息化。要特别注意信息化的综合工程，建立城市领导的信息化。

2、城市的信息化不能孤立建设，以为城市信息化仅仅是银行企业自己的事情，而不考虑如何与其他方面的信息化衔接是行不通的。尤其城市的信息基础设施、电子政务、电子商务和银行公共渠道信息化建设更要考虑信息化衔接问题。主要考虑的内容是互操作性、安全性和服务性等方面的用户信息化标准建设。

3、城市信息化建设要处理好城市信息化的一般规律和城市信息化的特点与专门要求关系，处理好采用成熟技术与时尚技术的关系。

4、要建立城市信息化建设好坏的评价指标体系，了解现实与发展目标的差距。

5、要对城市信息化建设的复杂性做出正确评估，了解缩小与发展目标差距的有利与不利条件，确立克服困难的措施与对策。

6、要建立一个切实可行的前瞻性总体发展框架，制定信息化发展路线图。

7、要建立城市信息化总体的运营体系结构、系统体系结构和技术体系结构。

8、城市信息化建设要落实在关键和影响全局的项目建设上，要明确项目建设清单，制定项目建设计划。

信息化规划关注的问题是信息化对社会生活方式和工作方式的改变，关注信息化在人民生活、基础设施、产业、政府、商务等领域普及、成熟和深入的程度。关注产业、社会、政府整体服务能力提高，关注通过信息化促使生产力和生产关系的变革。信息化从抽象的角度看，主要考察信息化对管理层次扁平化和时间空间的会聚和聚焦的程度和广度，是信息化真正有效性的更本性标志。

以上八点意见是作者在几十年信息化的经验与教训的基础上总结出来的，同样适合于信息化安全建设的规划。

城市信息化的安全建设也要做总体规划，同样应当依据上述八点原则进行。

2.7.2 城市基础设施信息化安全情况

城市基础设施与国家基础设施有范围和领域的差别，城市基础设施许多是与国家基础设施衔接的，作为国家基础设施网络的结点。但是城市基础设施也有自己的特殊内涵，其信息化建设与国家基础设施信息化建设也是衔接的，其信息化主要包括城市交通、城市供电、城市供水、城市供暖、城市供气、城市排污、城市绿化、城市大气环境、城市气象、城市道路、城市管道、城市管线、城市教育、城市文化、城市卫生、城市商业、城市社区、城市旅游、

城市宾馆、城市消防和城市治安等诸多方面的信息化建设。城市基础设施信息化安全建设覆盖整个信息化领域。

城市基础设施信息化安全建设主要宗旨是保持其可靠安全的运行，维护基础设施的财产和安全。

城市基础设施信息化安全建设主要是将信息化、网络化和电子化密切地结合起来，建立一定范围的有效监控体系。所有这些安全措施都要求有最快的物理与网络的定位、检测和取证能力。

2.7.3 城市电子政务安全情况

城市的电子政务建设业主同时考虑省市党委会、省市人大、省市政府、省市政协四个方面。另外，城市电子政务的信息化的建设与中央政府的电子政务建设的重点有所不同，城市电子政务的建设首要的重点在于建设政府的网络服务系统，其次政府的监管信息化建设，第三是做好办公业务的自动化。城市政府的网络服务系统要求特别注意有关信访服务建设，要特别加强政府与市民通过网络的互动联系的建设。另外，要重视政府信息发布和披露系统建设，为企业和社会个部门提供发展服务。

城市的电子政务的安全建设应当与国家电子政务的安全建设要求一致的。目前城市电子商务的安全建设对交易安全提出了明确要求外，对于系统和网络的安全保障和网络行为与内容的监管还基本没有考虑。

2.7.4 城市电子商务安全情况

城市电子商务是国家电子商务的组成部分，要突出城市特色的电子商务。但是城市电子商务安全建设应当与国家电子商务安全建设要求是一致的，只是更加强调终端系统安全防护、监控、监管，必须包含终端设备的物理和网络中定位、检测和取证的能力。但是目前的电子商务的系统与设备的这方面的情况还基本是个空白，应当在新系统升级、换代和新产品的研发中，将这些安全的要求考虑进去。

2.7.5 人民生活信息化安全情况

人民生活信息化和网络化是 21 世纪的新型生活方式的特征之一。通信、电视与计算机网络，尤其是互联网和移动通信为人民生活信息化开辟了许多新的方式。人民生活信息化情况发生了巨大的变化。现代人们生活的不仅仅包括衣食住行，还包括娱乐、商务、学习、交际等多方面的活动。在现代生活中，信息化大大改变了活动的方式，这些现代生活方式不仅仅是固定的，而且还是移动的，向更加便捷和舒适方向发展。

例如在出行方面，人们外出依靠汽车、火车和飞机。从个人生活模式中，驾车上班、外出旅游已经是一种主要的生活方式之一，汽车电子化和信息化要求在不断地提高。文化、娱乐、休闲和体育活动是现代人的不可缺少的生活内容，文化、娱乐和休闲场所的信息化和网络化建设大大提高了这些设施的利用效率。电子游戏、网络游戏、网络下棋、倾听网络音乐也是现代的生活方式。教育与学习活动是现代人的重要的生活内容，网络读书、网络教育是改变现代人学习方式。社会交际和人们相互交流活动是现代人不可缺少的生活内容，通信和计算机网络原来被主要应用于人类的业务和社会活动。许多现代人打电话交谈已经变成生活

组成部分，例如打手机、发短信息、网络聊天非常盛行，甚至在网络上谈恋爱也变成了值得注意的问题。这些新型交流活动早已不是仅仅由于工作的需要，而是生活的需要。现代人的金融活动和商业活动也离不开信息化，商业与金融业的电子化设备使用和信用卡越来越普遍使用，大大改变了人们在这些领域的行为方式、能力和状态。

上述人民生活信息化同样存在着比较突出的安全问题。利用电话、手机等进行诈骗犯罪和散步谣言和反动宣传，在互联网上建立建立色情网站和邪教网站进行危害社会和国家安全的非法活动，在网络上开展非法赌博活动和敌对活动，利用冒牌商业和金融网站骗取钱财，散布大量的垃圾信息或邮件骚扰人们的正常生活，其花样数不胜数。**这些关系到现代个人生活方式的信息化，其安全主要是开展网络及其设备的行为与内容监管，任何网络上设备及其行为都是可以定位、检测、认证和取证的。**

2.7.6 智能化社区信息化安全建设情况

智能化社区信息化属于人民生活信息化组成部分，同样是城市信息化的组成部分，特别是城市基础设施信息化重要单元。智能化社区信息化安全首先应当保障城市基础设施信息化的安全。除此之外，社区生活信息化网络化还包括自己独立的内容，例如社区安防系统、自动抄表系统、社区商务服务系统、社区社会保障和就业服务系统、社区文化、教育、娱乐系统、社区消防管理系统、物业管理系统等等。这些信息化也要注意安全建设，尤其关系到人民生命财产的信息化建设，其安全更为重要。

2.7.7 家电设施网络化安全建设情况

家电设施网络化与信息化建设属于人民生活信息化组成部分。

家电设备的信息化网络化，包括电视、电话、手机、电冰箱、微波炉、洗衣机、家用安防报警系统、家用消防报警系统、家用门警系统、家用求助护理系统等家电设备的信息化和网络化。我们知道，以前控制都是面向具体的对象，控制本身没有网络化。控制网络市场前景非常巨大，并以维护和服务为契机，建立全国和地方的家电信息网络系统，号称将来世界第一大网络。该网与 IP 网衔接。人民生活环境信息化网络化和家电设备信息化网络化，采用的设备出自成千上万的企业，如何才能构成互连、互通和互操作的网络，上世纪 90 年代以来，提出了家电设备互联、互通和互操作的网络平台化体系结构概念。发达国家是在电力网络、闭路电视网络、电信网络、计算机网络都已经发达之时进入互联网络时代的和网络经济时代，发达国家的信息化网络化的解决方案有许多是不符合我国的国情。在我国，家电信息化网络化并不可能建立在计算机网络上，我国的现时的国情是电力网络、闭路电视网络、电信网络、计算机网络发展非常不平衡。我国在城市和农村刚刚实现了电力网络，电视网络和电话网络还是基本的，而计算机网络主要用于单位，进入家庭的覆盖面还相当低。可能进入家庭的光纤网络已经包括有线电视网络、电信网络的网络、计算机网络和智能化社区与建筑的监控网络。考虑到电力线，如果不走多网融合的技术发展道路，第五根网络线进入家庭。电力线含光纤为多网融合提供了新的思路，我们已经看到了一种新的发展趋势。家庭信息化的网络带宽已经不是什么主要问题。

家电设施网络化安全建设也刚刚提到议事日程之上，其安全建设，应当在社会与用户可以接受的范围内进行规划设计，在家电及其网络中配置必要的安全措施，例如主体认证、安全流程、报警、紧急处置等。

2.7.8 城市呼救服务信息化安全建设情况

在城市范围内建立一个统一的应急救助体系。我们知道，已经在全国各城市，建立了面向分类事件的呼救系统，例如 110 系统、119 系统、120 系统和 122 系统以及全国各行业的呼救和呼叫系统有几十个。显然有必要建立统一呼叫号码，解决统一呼叫救济问题。如何建立这样一个紧急呼救系统呢？

这个统一呼叫救济系统必须是实时坐席值班系统或呼叫中心系统。

这个统一呼叫救济系统具有服务、调度、指挥的功能，能够分派任务，快速转到行业呼救系统上和具有全部存档、记录和过程重演功能，这些都是一个救济指挥中心和服务中心的必备功能。

这个统一呼叫救济系统必须保障业务连续性和资源的可用性，具有较高的备份与恢复能力，具备良好的网络管理（包括配置管理）、系统管理、应用管理、数据管理和安全管理能力。这些管理能力集中于管理中心。

这个统一呼叫救济系统具有多种技术体制的通信能力，有内部的专用通信网络、公共通信网络和公共数字集群（例如 800 兆数字集群）通信网络。各种通信设施与系统集中于通信中心。采用以话音为主的通信技术体制，并且具备最广泛的终端设施与系统相连。

必须建立一个适合社会救助的应急救助体系的总体的框架结构，这个结构应当按照层次进行划分，例如如下的层次结构：管理中心在体系的最内层，其次称之为为核心层，服务中心、通信中心、信息中心、监控中心、指挥中心在这个层面上。在往外层是建立在内部网络上的呼叫中心，在网外层是公共网络。在整个总体结构中还应当加入应急支援基地和安全威慑力量，并且与国家信息安全威慑力量结合起来。

2.7.9 城市应急信息化体系建设情况

国家和城市基础设施安全应急体系应具有足够的预警能力、控制能力和协调管理能力，通过建立由国家控制运行的和行业控制运行的技术支撑系统提供应急支援和服务，保证应急响应时间短、涉及区域和行业范围可控、可有效实施事件影响隔离，保证安全威胁事件对国家信息基础设施损害最小。

作为国家和城市信息基础安全应急体系的近期目标和长远发展，建设国家和城市信息基础设施安全应急支援体系和服务中心，建立较完备的国家和城市信息化安全应急协调机制、管理体系、技术体系、培训与教育体系。

建立城市应急支援中心与基地是解决地方安全应急能力的重要办法。在城市内建立应急支援体系，在平时用来指导城市安全应急工作，提高城市安全应急能力。在危机时刻发生时，城市应急体系为城市内一切机构提供应急问题处理支援，并协调整个城市地区的应急资源和能力。

要求城市范围内各重要部门建立静态或动态灾备中心体系，此类灾备中心的建设应当保持分布特性和异地特性。灾备中心，作为运营的工作中心的备份中心。在这个中心，可以实现设施、系统（包括全部应用系统）和数据库系统全方位的备份和恢复体系。在这个中心，还可以只建立数据备份中心，作为统一访问控制与管理的数据库系统，建立所谓的数据仓库体系。

要建立移动中心，这种移动中心是一种车载形式的灾备应急系统，通常包括通信中心的车载系统、运营操作中心的车载系统以及管理中心的车载系统，同时还包括车载的指挥系统。移动应急体系，具有所有可能的通信系统（有线通信系统、无线通信系统、卫星通信系统等），

计算机系统、应用系统、数据库系统，其中最大的特点是具有应急的各种通信接入系统。可以在危机发生时，将移动系统开入任何工作地点，进入工作中心的角色。

第三章 信息安全产业企业情况

3.1 信息安全产业企业情况概述

近 10 年，中国信息安全产业得到快速的发展，这种发展当然首先得益于国家领导人对信息化安全的重视，这种重视是与国家在世界政治、经济和军事的大环境的态势息息相关。我国信息安全企业虽然发展不平衡，从总体上看我国信息安全产业已经走过了创业期，进入了开拓期或发展期。信息安全产业从由几个国家的研究机构主要从事数据加密和单纯计算机系统安全研究发展到国家的一批研究机构、大学院系和一大批高科技中小企业共同从事信息、计算机系统和互联网络安全，到现在形成主体企业团队全面服务于国家基础设施信息化安全建设与运营，逐步走向成熟发展阶段。

2002 年商会提出“六化，三加强”（产品客户化、技术平台化、服务高技术化、市场规范化、企业规模化、资本多元化和加强信息安全测评认证工作、加强信息安全产业的总体规划与基础研究和加强推进国家基础设施安全建设）发展策略以来，企业依照自身的发展规律，在技术方面，产品客户化、技术平台化和服务高技术化要求信息安全企业适合新的市场的要求和建立更加有效的标准化工作；在市场方面要求建立一个更加规范的市场环境，这种环境包括反对不正当竞争、建立合适的技术法规和监管体制；在企业规模化和资本多元化方面，要求信息安全企业规模做大。这个“六化，三加强”发展策略对于指导信息安全企业发展发挥了一定的作用，主要表现在信息安全产品在客户化服务方面取得了一定的进展，在平台化方面取得了共识，为下一阶段成立企业标准化联盟，从事信息安全产品平台化奠定了基础。但是，在服务的高技术化方面进展不大，在市场的规范方面建设虽有进步，但有限。在企业规模化和资本多元化建设方面，许多企业做了有意的探索，有一定的进展，依然存在许多问题。

企业进入开拓或发展期，不仅带来的是新的产品问世和新市场领域开拓，同时还伴随着企业资产结构和规模的扩大。在发展阶段，有的企业衰落了，有的企业在原地艰苦地维持，有的企业适时地调整了企业方向寻求新的发展，而有的企业一军突起，逐步做大了，成为信息安全企业主体团队，整个产业结构在市场大浪冲击下逐步调整和改变了。

3.2 信息安全产业企业资产情况

随着我国信息安全产业迅速发展，我国信息安全企业的资产规模也得到了飞速发展，企业资产成倍的增长。信息安全产业进入了开拓期或发展期的一个重要标志是信息安全产业的企业资产得到了迅速发展。其中许多信息安全企业在营业额达到数千万元后，企业资产结构开始发生较大的变化，在这种变化中，有一些企业的股东之间发生了较大的冲突和矛盾，企业走向了衰落的态势，还有一些企业对于企业的资产结构的调整和企业的资产扩张采取了谨慎的态度，使企业安全地度过了这个发展阶段。

企业产权结构总体上看逐步趋向合理，在这个期间信息安全的许多企业都在积极寻求新的投资，新的资本投入必然带来新的企业管理和新的市场理念。这种新的管理与市场理念是适合投资商原服务领域和产品特征的，其中有些投资商原理念是适合信息化安全市场的，有

些是不适合信息化安全市场的。正因为如此，调整后的信息安全企业往往要对信息化安全认识需要一段时间，这一段时间的对于企业来说，有的是丧失机遇发展停滞，有的是把握了机遇继续发展，有的是调整了市场方向开辟新的领域。

3.3 信息安全产业的资本市场情况

初期我国信息安全产业的企业主要是创新企业，基本是一些中小企业，其企业资本结构主要依靠国家、地方政府的投资和民营资本，这些企业的资产规模都不大。这些企业在发展中，要求不断扩充其资产的规模，寻求新资本投入。首先看国外投资，目前国外战略投资资本在投资信息安全市场还受到一定的限制。再看国内投资，国内资本市场较活跃的资本，目前对投资 IT 行业或信息安全产业，其困惑较多，投资者对信息安全产业生疏，苦于选择好的项目，而信息安全企业通过出让股权融资，又担心最终丧失企业发展的原创力，改变企业的建设宗旨与目标。近几年来，一些上市公司，尤其是 IT 的一些上市公司，开辟新的市场领域，许多都考虑了从事信息化安全业务。目前在这些公司中。对于国内外的资本市场，理论上讲，应当是对我国的信息安全产业是开放的，但是在实际操作中，由于信息安全产业的企业比较年轻，资本规模小，企业尚为成熟，上市融资目前还比较困难。

为了解决我国信息安全产业融资困难，我们在 2002 年商会的产业调研报告中，曾经提出我国信息安全产业资本投资要走向多元化，对外国投资商投资我国信息安全产业，尤其是国家基础设施安全，仅应当允许在董事会的资本运营层面参与工作，在中方股东控股条件基础上，外国投资公司可以参股，实施投资。对于总经理层面及其相关的事物实施限制。同时还提出鼓励有良好金融背景的金融中介投资机构收购有前途的信息安全企业，使我国信息安全企业在资本市场上有依靠，而不是孤立的，构成纵向融资和财务管理的良性环节。也提出在商会的参与下，与商业银行、金融投资机构、融资租赁机构和有实力的实业公司共同成立信息安全产业投资委员会或信息安全产业发展基金，改变整个信息安全产业的资本市场现状。现在看来，这些建议依然是可以参考的。作为商会，应当积极促成信息安全产业发展基金的建立。

3.4 信息安全产业的技术情况

在传统信息安全技术方面，几年来，信息化安全在传统技术与新技术两个方面都取得了显著的进步，在开发自主信息安全技术与产品方面，在国家各方面的大力支持下，取得了骄人的成绩。

我国在数据加密和加密设备研究方面具有世界先进水平的。例如，我国由江南计算机研究所和科学院等单位参与和自主开发的十几万亿次的计算机和具有数百 T 以上规模的存储设备就是世界先进水平的。在数据保密性、完整性等研究方面取得了重要突破。信息资源可用性技术（数据备份技术等）越来越多地得到重视与应用。在这个期间，信息隐藏及其发现技术的研究也取得了相当的进步，建议将信息隐藏技术与数字标签技术结合起来，会进一步扩大信息隐藏技术的应用领域。

在身份认证、数字证书及其管理技术在局域网和区域网方面取得了相当的应用成果，但是在大范围网络环境内和超海量主体和客体的认证技术方面，包括推行 PKI 技术路线，没有取得期望的应用成果。但是我国在认证理论研究方面取得了世界领先的成果，其重要的标志是 CPK 密钥管理算法和行为认证理论提出。

在系统和网络的防护技术（包括隔离技术、网闸技术、防火墙技术）和抗病毒防的护技

术方面也取得了显著的进步。系统与网络的防护技术可以采用系统结构方法（包括安全路由器、防火墙、代理服务器、安全网关、访问控制服务器和 VPN 技术等），并已经得到普遍采用。近几年提出的网闸技术对于非实时的办公网络业务来说，隔离专用网络和公共网络是一个创举，得到了许多用户的认可。我国在防护墙技术开发方面也取得了显著进步，中低端的防火墙产品基本实现了国产化，已经有我国自主的终端用户的软件防护墙技术产品、局域网的百兆防火墙技术产品和区域网的千兆防火墙技术产品，并得到普遍的使用。在高端防火墙技术方面研发方面也取得了相应的进展。系统和网络资源可用性技术（信道备份、系统备份、系统恢复、抗拒绝服务攻击技术等）被广大用户关注和得到普遍地应用。

在系统和网络安全检测与监控技术方面同样取得了显著的进步。系统与网络漏洞扫描，我国已经可以解决几千个漏洞检测工作。在入侵检测方面，我们的产品与技术也在许多方面超过国外同类产品，具有很强的市场竞争能力。在隐蔽通道和信息隐藏检测技术方面也取得了初步的成果。

特别需要说明的是，我国自主开发的防火墙技术、入侵检测技术目前达到了千兆水平。这意味着，我国防火墙、漏洞扫描、入侵检测、网络防病毒、网络加密和服务器安全模块等已经或正在开始从软件形式产品向嵌入式硬件板式、IC 卡式和芯片式的方向前进了一大步。在信息安全专用芯片和 ASIC 芯片的研究也取得了突破。

从应用和市场角度看，影响市场开拓的主要技术问题依然是客户化、平台化和服务高级化。

第一个问题依然是客户化。信息化安全产品客户化取得了一定成绩，但是依然存在着许多必须注意的问题。所谓客户化不仅仅指不同客户的信息化安全要求与目标有所不同，更重要的是网络与系统防护与客户的应用越来越相关。在系统与网络防护中，如果说以往主要关心系统与网络基础层面的防护问题，而现在越来越多要求更加关注应用层面的安全防护问题，这种应用防护问题甚至已经深入到业务行为的相关性和信息内容的语义范畴。

第二个问题是信息化安全技术产品的平台化（互操作性的标准化技术）。平台化虽然取得共识，但是进展有限。为了解决多厂商信息安全产品互连、互通和互操作问题还许努力，距离产生生产力，提供初步的产品至少还有一段时间，暴露了我国信息安全总体研究和基础研究的薄弱。我国信息安全产业最先关注管理平台的建设，表现在多厂商和多类别的信息安全产品的互动和互联、互通和互操作。商会在 2002 年就安排企业从事信息安全管理平台的建设。积极推荐国际标准化组织 DMTF 提出的公共信息模式（CIM）的管理平台概念，不久，商会又推荐 CISCO 公司的 CIC 作为管理平台体系结构样板，要求我国企业积极借鉴，并指出今后几年是实现管理软件和管理平台产品国产化的最好机会，呼吁抓住机遇。同时，商会已经安排几家信息安全企业在从事这方面的研发。信息产业部的发展基金也在信息安全管理平台上给予了有力支持。

第三个问题是信息化安全服务高技术化推进工作。在信息化安全服务方面我们积极提倡服务网络化和高技术化，不断提高信息化安全网络服务的能力。所谓服务的高技术化就是提倡网络服务代理化，把安全网络的代理体系建设看成企业提高网络服务水平重要措施和降低服务成本的重要措施。但是，我们企业在推进网络服务代理化方面缺少必要的理解和敏感性。所以我们再次呼吁商会的企业积极开展网络服务代理化的研究与开发工作，全面提高企业的服务能力与竞争能力。

除上述三个问题以外，还存在者许多新领域未开发的突出问题。

第四个问题是大范围网络环境安全技术问题。整个信息化安全理念依然是在上世纪 90 年代中期发展起来的局域网安全观念，对于“大范围的网络环境的安全问题”基本上没有考虑或考虑远远不够。

第五个问题是网络与系统的虚拟世界的行为与内容的监管、认证和控制问题。以往信息

化安全的观念依然是建立在“数据与系统（软硬件、网络等）安全保障”之上，对于网络与系统的虚拟世界的“行为与内容的监管”基本上没有考虑。

面对新领域的开拓问题，必须积极推进信息安全新技术的研究与开发工作。通过商会在2001年之后的安排，在可信计算平台（TCP）技术、可信网络平台（TNP）技术、可信应用平台（TAP）技术、多代理技术、标签技术、无第三方认证技术、监管信息化技术、网络对抗技术和多代理计算网格技术研究与开发工作取得了一定的进展。在推进上述信息化安全新技术的总体推动者是商会的QNS工作室。

在可信计算平台（TCP）技术研究与开发方面。我国的TCP研究工作在国家上是处于领先地位的，在这方面开拓者是武汉瑞达公司，随后联想公司、浪潮公司以及科学院和军方等相关企业与研究机构也积极参与其工作。我国从事可信计算平台（TCP）工作也是最认真的，可见我国对信息化安全问题关注程度比跨国公司要高得多。

在可信网络平台（TNP）和可信应用平台（TAP）技术研究与开发方面。QNS工作室、银长城公司、天融信公司、武汉瑞达公司、中科网威公司和启明星辰公司等商会的企业积极参与到TNP或TAP研究与开发工作中来。

在代理技术的研究与开发方面，自2001年来，QNS工作室特别宣传了代理技术，是调整我国信息安全产业结构的实际技术准备步骤，这些工作首先是从我们选定的大学与科研机构开始，取得了初步的结果，例如在国防科技大学、解放军信息工程大学、北京大学、武汉大学、华中理工大学、中山大学、华南理工大学、南京大学、成都电子科技大学、南京航天航空大学、信息产业部54研究所、信息产业部15研究所等单位中一些课题组、教授及其学生在进行这方面的研究。QNS在商会的骨干企业中积极推行与宣传多代理技术研究工作。

在标签技术研究与开发方面主要研究与开发单位有信息产业部54研究所、华为公司等。

在无第三方认证技术研究与开发方面有QNS工作室、武汉瑞达公司、北京大学、解放军信息工程大学、北京沃奇公司、北京密海公司等。

在多代理计算网格技术研究开发方面有QNS工作室、国防科技大学和信息产业部15研究所等。

在监管信息化技术研究与开发方面有QNS工作室、武汉瑞达公司、天融信公司、启明星辰公司、国家计算机网络与信息安全管理中心等。

从总体看，信息化安全技术发展，传统技术方面我们遇到了攻坚和标准化困难，在新技术方面我们面临着创新的严峻挑战，才仅仅开了一个头，从总体看实力还相当薄弱，需要彻底改变局面。

3.5 信息安全产业的服务情况

我国信息安全服务的开展取得了初步的成绩，主要包括培训、咨询、评估、测试等方面。但是，由于信息化安全的服务综合性、复杂性、环境性、主体性、时间性、对策性和高技术等特点，信息安全的企业服务要求相当高，信息安全企业必须面对一轮一轮新的攻击威胁面前，必须实施及时的对策服务。目前看来信息化安全服务从总体上看是不能令人感到满意，需要大大改进。

有些信息安全企业咨询服务不是从用户的需求出发，不是认真研究用户的安全问题，而是千方百计地引导用户购买自己的产品。有些企业不能做到培养用户的信息化技术人员，提高信息化安全的认识，通过这种信息化安全认识的提高，与用户共同研讨信息化的安全问题的解决。

有些信息安全企业的风险评估服务留于形式。一个好评估服务除主要找出存在的问题之外，就是能够引导企业走向自我评估工作展开，培养出自我评估的人才和能力。培养企业的

自我风险评估能力和帮助企业建立自我评估的制度、机构和人才，才可以说风险评估没有留于形式。这种要求如同银行领域的巴塞尔资本协议要求那样，鼓励企业积极开展内部评估工作。安全企业评估工作意义和价值不仅仅在于评估本身，而在于向企业提供风险评估的方法、程序和工具。

有些信息安全企业售前技术服务的主要问题表现在不能给用户提供体系化的总体方案服务，仅仅提供安全产品层面的技术服务。

有些信息安全企业售后技术服务存在比较严重的问题和不足。有些企业销售信息安全产品如同销售 PC 产品一样，仅仅做些使用方面的培训，甚至更加糟糕，将产品买给用户后，对用户没有起码的服务，造成用户的巨大损失，败坏信息安全产业的整体形象。

有些信息安全企业在信息化安全出现应急事件和灾难时，不能提供需要的服务，尤其是一些外国企业，这方面表现最差。有些国内企业由于其经营思想不正确，在用户要求提供应急服务时，表现裹足不前。我国的许多安全企业之所以有较大的发展和进步，其最本质的原因是服务搞得好。

解决上述问题方法和途径就是大力加强信息安全技术服务人员的培训和需要建立信息安全服务等级价格体系和测评体系。

第四章 信息安全产业环境

4.1 在国家宏观经济调控中快速发展信息安全产业

为维护国家经济快速稳健发展，国家将长期实行宏观经济调控政策。国家将以科学发展观统领各项事业的发展，改变与控制经济发展的速度、方式和结构，建立资源节约型和环境保护型经济。在社会与自然各方面实行统筹，构建和谐社会。

在国家宏观经济调控中，如何实现快速发展我国信息安全产业呢？ 建设资源节约型经济，信息化与安全可以发挥重要的作用，例如商会推荐在电力系统中实行智能电力网的建设计划。建设环境保护性经济、灾害预警、实现安全生产、安全交通、社会秩序的监管、技术监督信息化和构建和谐社会，信息化与安全都会发挥重要的作用。信息安全产业界为国家经济宏观调控和经济健康发展将做出贡献。

4.2 我国信息安全产业发展的基础环境

信息化安全的基础环境是国家实施了信息化带动工业化的发展战略。从本白皮书第二章的讨论中看出，我国行业和企业的信息化的发展是相当不平衡的，在地区分布上看也不平衡。从应用角度看，对于一些发展比较先进的行业，信息化建设的问题主要是需要整和，需要将信息化与行业及企业的技术与业务组织体系结构改革结合起来，实现业务运营中心的信息化建设同时要积极规划管理中心的建设。在企业应用系统的开发中，需要启动价值管理信息系统领衔，带动资源管理、产品服务管理、风险监管、渠道管理、办公业务信息化的建设。中国信息化建设的任务和目标正在改变，从以局域网、城域网、区域网为主体的信息化应用体系建设，逐步过渡到大范围网络环境、超海量数据与对象和高智能应用与管理的信息化体系的建设。在信息化的新时期采用多系统和多代理的系统平台的体系结构是其新的特点。在这样的信息化的时代，在以互操作性和代理化为信息化建设的主要特征，其信息化安全建设任务就非常重要，从而构成信息化总体技术包括：互操作性技术、安全性技术和服务性技术。

正因为如此，在中国信息化安全事业得到中央到地方政府的广泛重视，国家把国家安全划分为国土安全、政治安全、经济安全和信息安全，信息化安全是其中重要的组成部分。所以，我国的信息化安全的基础环境是非常良好的。

4.3 我国信息安全产业发展的国际环境

我国信息安全产业发展的国际环境还是比较严峻的，这主要表现在国外信息安全企业进入我国情况。国外企业进入我国信息安全产品市场的一个典型代表是美国 ISS 公司。该公司 1997 年开始进入我国。一进入我国就受到国家安全部、公安部和信息产业部的重视，对其销售将 IP 地址捆绑、美国密钥等问题提出整改，同时要求 ISS 公司的产品进入我国必须进行测评认证。直到现在 ISS 公司，公开对抗上述要求，违背我国信息安全产品认证管理办法，

其信息安全产品已经在电信、电力和部分银行使用，并相当长一段时间产品伴有“回传问题”，是我国信息安全建设一大隐患。

目前，一些外国信息产业公司从事信息安全，也改变了策略，不谈国家、政府、敏感行业的信息安全，以保护人的信息隐私为理由，面向民营企业、股份制企业、外资企业、社区建设和城市建设，又一轮发起进入我国信息安全市场浪潮。国外 IT 企业在我国从事信息安全业务的有：IBM 公司、CISCO 公司、HP 公司、Microsoft 公司、ISS 公司、CA 公司、RSA 公司、SUN 公司、NAI 公司、赛门铁克、VeriSign 公司、EDS 公司、CheckPoint 公司、韩国安浪等上百家公司在我国从事信息安全业务。最近许多国外公司到我国来洽谈建立网络中心和服务中心的事项，企图进入我国信息安全服务市场，这方面的代表是 Microsoft 公司、VeriSign 公司、EDS 公司等。安全服务关系到国家安全大事，应当十分谨慎。

关于国外企业投资我国信息安全产业，已经有美国、日本、韩国、澳大利亚、以色列、新加坡、欧洲一些国家的信息安全企业到中国来洽谈产业投资事项。

我国国家基础设施、敏感行业的信息安全建设直接关系到国家的安全，在我国信息安全产业基本能够提供信息安全技术与产品情况下，应当以“自主可控”与“趋利避害”原则为指导，限制在国家基础设施、敏感行业使用国外信息安全产品。所谓“自主可控”是指信息安全技术、产品与服务的发展必须立足我国信息安全产业。所谓“趋利避害”是指信息安全建设也必须实施必要的国际合作，保持适合我国国情的国外合作渠道。

我们要克服某些部门管理人员的错误思想:“认为信息安全产品与服务采用国内产品与国外产品一个样，谁的产品好就用谁的”和“中国没有必要搞基础设施安全，只需搞应用层和端到端的安全，基础安全可以让外国公司来搞的错误主张”。信息安全产品与服务不仅仅比功能与性能，比高技术，信息安全是集技术、人员、操作、管理为一体的综合体系，信息安全的本质在于“可信和可用”。只有发展我国的信息安全产业，才会有可靠的并用得上的服务能力。我国信息安全产业是我国面对信息犯罪、网络敌对势力破坏与信息战威胁的强大现役与预备役防护的主要力量。

我们提醒一些用户，信息化安全建设服务是最重要的。每当我国出现安全方面的应急事件时，这些外国企业有的纷纷撤出中国，有的被美国总部限制不能提供服务。总之，需要他们提供安全服务的时候，他们都跑得无影无踪，到这时才想到我国信息安全企业提供服务时，已经来不及了。历史的事实一再告诉我们，信息化安全服务必须建立在国内企业服务基础上。

商会将积极与国家商务部等有关部门合作，在 WTO 规则和信息安全作为技术壁垒等封面，为促进民族信息安全产业发展与国际合作做出新的贡献。

4.4 我国信息安全产业发展的法律环境

我国信息安全产业发展的法律环境目前还不是很好，主要表现在我国信息化和安全技术法规建设离信息化与安全建设的要求相差较大。有些法规应当是国家制定的，有些技术法规应当是行业制定的。

商会建议：

1、要对信息化与安全的技术法规进行总体规划。

2、对已有技术法规进行清理和评估，要了解这些技术法规的使用状况和适应程度。已经出台的信息化安全技术法规、条例等已经推行多年，取得了一些效果，但是我国信息化安全认识、技术条件、环境条件、投资情况以及威胁情况发生了许多变化，有些效果还存在问题，显然应当根据变化情况，以与时俱进的态度，对于这些行政或技术法规进行修改或升级，不能长时间让这些技术法规和条例处在一种不适合的状态中。

3、对期望建设的法规要进行调研，了解制定这些新法规的需求、条件、环境、用户和

企业等方面情况，确立新法规建立方法和制度，分清轻重缓急，有计划地大力推进。

4.5 我国信息安全市场秩序情况

中国信息安全产业经过认真讨论，并逐字修改和律师审议和修订，于 2004 年初，经全体会员大会表决，一致通过《中国信息安全产业反不正当公约》，并正式出台。中国信息安全产业终于有了建立在“遵纪守法、诚信自律、公平竞争和共同监督”基础之上的行业公约。对于规范信息安全市场秩序，改善竞争环境，共同促进产业的健康发展，将发挥作用。

商会将组织和开展用户对信息安全企业遵守《中国信息安全产业反不正当公约》评估活动这种评估活动不是为了排名次，而是征求用户对企业“遵纪守法、诚信自律、公平竞争和共同监督”的意见。

市场秩序依然存在着许多令人关注的问题。

1、关于建立信息化安全产品和服务等级制度。目前信息安全市场的产品质量与提供功能服务相差很大，许多质量与功能不合格的产品与一些优秀的产品在市场领域处在一个竞争位置上是很不公平的，所以建立信息化安全产品和服务等级制度的对于维护信息安全高水平产品和服务非常必要。商会将向国家认证认可委员会和各测评机构建议，应当全力推进信息安全分级测评认证工作，从根本上维护国家信息化安全的市场秩序。

2、关于规范信息化安全服务价格问题。

许多信息安全产品供应商对于信息化安全服务缺乏认识，以销售成熟 IT 产品（PC 等）方式，销售信息化安全产品与系统，大打价格战，以非常低的价格冲击信息安全市场。这些企业错误地估计了形势，忘记了所从事事业的神圣性，以为可以象一般民用产品，可以任意冲击信息化安全的市场价格。这些信息化安全企业以损人利己开始，最终以危害用户和国家信息化安全和害己告终。商会再一次提醒这些企业，你们从事的事业关系到国家和用户安全，不要把国家信息化安全建设当儿戏，我国的信息化安全市场的行为是有监管的，一旦造成国家信息化安全灾难时，是有人追究责任的！

为了维护信息化安全产业的健康发展，商会将配合国家发改委价格司，专门研究规范信息化安全服务的成本价格体系。

3、关于在产业内部建立仲裁机制和机构。

4.6 关于信息安全标准化建设情况

我们要在提倡科技创新的同时，还要提倡应用成熟发展策略。科技创新和应用成熟是对立的统一，相辅相成。应用成熟要求科技创新更具有持续性，对科技创新提出了更高的要求，是科技创新应用发展策略。同样很难设想，IT 产品得不到长期应用支持，产品会得到成熟发展。因此，IT 产品只能在持续应用和长期服务才能得以发展，用户的对信息技术的成熟应用是带动我国信息产业发展最有力的支持。“科技创新和应用成熟”可持续发展的辨证思路，是掌握对立统一规律，促进产业发展的重要的指导思想。

在用户信息标准体系发展时代，是又一次出现我国自己制定 IT 发展战略的机遇，我们应当抓住。我们有如下的网络经济技术基础标准体系必须自己制定：

1、信息安全标准体系标准系列

2、网络服务的技术标准体系

3、信息应用平台标准体系（互操作性标准体系）

正由于这些标准在参照国际标准的基础上必须自己制定，不可替代，所以出现了我国自己制定发展战略的机会。我们应当一方面重视基础与核心技术研究，同时更应当关注当前发展的机遇。要抓住当前的发展机遇，加快研究我国自己的网络远程服务的平台，切实解决我国信息化急需解决的问题。

4.7 关于信息安全产品测评认证情况

要加强我国信息系统安全建设，促进我国信息安全产业的发展，安全测评认证是安全建设的龙头工作，国家对安全测评认证工作十分重视，于 1996 年，由国家安全部、国家公安部、国家保密局、中办机要局、解放军保密委和信息产业部等单位联合成立了国家信息安全测评认证管理委员会，并在该委员会的领导下成立了中国信息安全产品测评认证中心及相应的授权分支机构和实验室机构（但目前依然缺少行业性和专业性测评认证）。我国信息安全测评认证体系是与我国信息安全产业同步发展的，同样取得了可喜成绩，已经开展了信息安全产品、系统和服务的测评认证工作。已经通过信息安全测评认证的有几百个产品。测评的产品类型包括：操作系统、安全隔离计算机、计算机安全模块、防火墙、系统与网络漏洞扫描、入侵检测、安全审计、安全加密、VPN、CA 等产品。出版了《政府信息安全产品采购指南》是我国信息安全测评认证从创业走向业务发展的里程碑。从 2003 年起已经依照 ISO/IEC15408（GB18336）开展分级测评工作。

但是长期以来我国信息安全测评认证工作存在着多部门和多证管理问题，虽然有理顺测评认证管理体系普遍要求，但是解决这个问题是相当复杂的。除中国信息安全产品测评认证机构之外，还有公安部负责的信息安全产品市场准入发证和检测工作、国家保密局负责的安全服务资质检测与发证工作和国家商用密码检测与批准工作。另外，军队还有专门为军队负责的信息安全测评认证工作。在 2004 年，经过几个部委的协商，将信息安全认证的发证工作统一到国家认证认可委员会，信息安全产业的企业期待认证认可委将测评认证工作，尤其是已经开展的分级测评认证工作，推进到更高的水平上，而不要给企业增加新的负担，希望能够做到在信息化条件下提高其执政能力。但是，从产业发展角度来看，这个问题并没有解决，统一发放信息安全产品、系统和服务的证书，出发点或者说从理论上看也许是可行的。但是，由于信息化安全的综合性、复杂性，涉及的领域非常多，我们很难设想，在当前国家有关部门的技术水平和管理水平条件下，实际能够胜任这项工作。仅仅从发证来说，目前还不可能做到一个单位发证，例如电信网络上网证，银行应用系统上网证、电力部门的上网证等行业上的应用测评认证，大概就不能仅仅通过统一测评认证的发证工作来代替，更何况保密系统、机要系统和国家公共安全的执法部门管理证书也是不能替代的。对于国家安全部门，有通过测评认证渠道及其监控手段实施防范敌对实力破坏的职责，国家认证认可机构是很难分担其相关职责的而硬性占有其渠道和手段的。其次，即便对于一个领域范围，也存在着多方面的安全管理问题，例如许多经济部门都同时存在安全生产、打击犯罪和信息化安全的多重管理问题，而且这些安全部门都有各自不同的国家管理部门（例如国家安全生产管理部门、公安部、保密局和安全部）在管理。所以，信息化安全的测评认证并不能简单地看作质量问题，信息化安全也不仅仅是用户角度的安全，还涉及到国家安全、打击犯罪、对敌斗争、基础设施安全、企业安全、安全生产等多方面的重大问题，每一个方面都存在着艰巨的管理问题。何况还要将测评认证工作推进到网络化服务的新阶段，对测评认证提出新的技术和管理要求，如此众多的领域的信息化与安全配置管理体系建设与运营，由一个国家认证认可部门统一管理是很难完成的。如何建立一个现代化的、高效率的和满足各方需求的测评认证体系，现在看来，依然是一个相当复杂的理论课题、高技术体系、系统工程、管理工程和社会工程，

应当用科学发展观统领国家信息化安全测评认证体系的建设。

我国信息安全测评认证体系的建设当前存在的主要问题是：由于信息安全测评认证是一个高技术领域的业务，对于人员素质有很高的要求，提高我国信息安全测评认证人员素质和服务质量以及提高服务效益是一个长期建设任务，要建立“金钢钻工程”。上述不足，在2002 年底开始的分级测评工作中表现的十分突出。整个体系提高测评业务服务能力十分迫切，学习与培训任务艰巨。提高测评认证服务能力要通过开展更高水平的业务工作来推动。分级测评暴露出来的普遍能力不足的问题，必须要加以解决。另外，目前推出的测评认证模式也是传统的，对网络时代的测评认证以及企业强烈要求的测评认证服务前移呼声和标准化规定的测评认证的网络服务模式没有研究或缺乏认识或没有必要的敏感性。其解决的办法是积极建立国家信息安全测评认证配置管理体系，国家测评认证配置管理体系宗旨是开展测评认证的网络服务业务、提供测评认证的前移服务。第三，信息安全测评认证实验室建设没有实现专业化或专业体系建立进展缓慢。必须建立芯片、硬件、操作系统、数据库管理系统、通信网络设备与系统、自动化控制设备和互操作性等专业领域的安全实验室。开发测试工具、配置工具、防护工具、攻击工具、监管工具、维护工具、诊断工具和监控工具等，同时还具有信息安全教育与培训中心的职能。信息安全测评认证的配置管理体系将会对国家测评认证机构的面向社会的前台服务提供基础支持，是信息安全测评认证的基础设施工程，应当加紧立项、规划和建设。

4.8 关于信息化安全产业基地

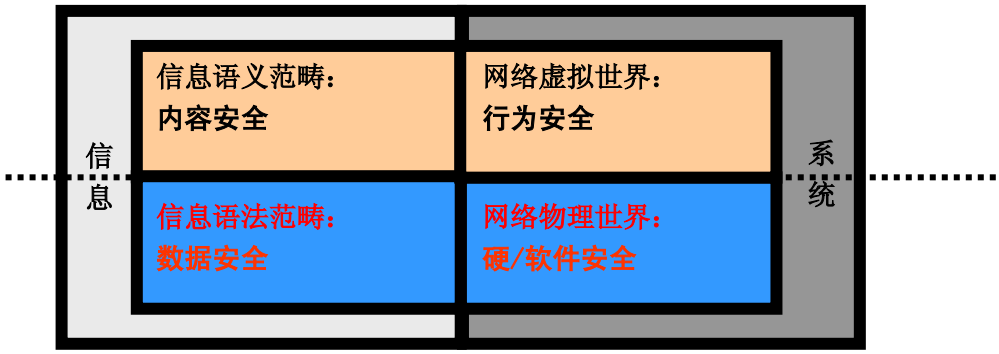
几年来国家和各地建立了一批信息安全产业基地。这些产业基地建设对于信息化安全建设和信息安全产业发展的推动作用作用相差很大。有些基地对推进当地的信息安全产业发展起到了积极作用，有些基地对发展信息安全产业和推进当地信息化安全建设作用不大，并没有实现建立基地的初衷。有些基地建设的初衷就存在问题，例如有的考虑到房地产原因，没有经过详细地论证；有的对当地信息安全产业的目标、方向、定位、原则、政策和市场发展前景研究不够，对基地的赢利模式研究缺少论证；有的是对信息安全企业利益、服务、工作便利性等问题考虑不周；有的基地建设中还夹杂着其他因素和问题，使信息安全企业对产业基地望而却步。

但是信息安全产业需要基地建设，因为信息安全产业同样存在产业链和产业生态环境等一系列保障的支持，信息安全产业的相对集中，对于整体产业会起到降低成本，促进发展的环境和态势。商会正在积极与有关部门策划，形成几个国家级基地的建设。

第二部分：信息化安全技术发展展望

第一章 信息化安全技术发展概述

建立新的安全概念、树立新的信息化安全认识对于我国信息化安全事业和信息安全产业的发展是非常重要的。信息化安全观念的发展经历过两个世界和两个范畴发展时期。所谓两个世界是指网络物理世界和网络虚拟世界，所谓两个范畴是指信息的语法范畴和语义范畴。第一个发展时期的安全观念称之为网络物理世界软硬件和信息的语法范畴的安全观念，也称之为传统的安全概念。信息语法范畴安全观念主要是指数据安全，主要包括数据保密性、数据完整性和数据可用性等安全问题，主要采用数据编码，而不涉及信息语义或内容。网络物理世界安全观念是指系统、网络（软硬件）安全，主要包括访问控制、系统完整性和系统可用性安全问题。第二发展时期的安全观念称之为网络虚拟世界行为和信息的语义范畴的内容安全观念，也称之为现代可信概念。信息语义范畴安全观念主要是指信息的内容安全，包括内容可信性（真实性）、内容保密性、内容完整性和内容危害性等内容安全问题。网络虚拟世界行为安全主要包括行为可信性、行为有效性、行为保密性、行为完整性和行为连续性等行为安全问题。把传统的安全观念和现代可信观念合在一起，便构成现代信息化安全新概念。上述叙述可以用如下的图来表示。



可信观念演变也经过一段较长认识过程，早期的可信概念反映在美国国防部的 TCSEC 标准中（1985），其基本可信概念是“授权可信”，表现在保密性、完整性和可用性定义中，破坏这些安全属性均被定义为“非授权”获得、篡改等行为上。这种可信观念是只看身份和权限，而不看表现。现代的可信概念应当是“既看身份与权限，又看行为表现”，最终落实在行为可信概念上。所谓行为可信是建立在多行为或历史行为的考察（监管、认证和控制）之上。现代可信概念已经定义在可信计算平台联盟 TCPA 的可信定义上，也表现在商会推出的可信网络平台 TNP 或可信应用平台 TAP 定义上。

如何看待网络与系统的安全与可信的问题，是需要认真研究的。一个系统是安全，在技术领域中是认为该系统采用规定的安全功能和安全服务能力，至于提供的这些安全功能和服务能力是否真的安全，系统的用户并不能真正建立起一种信心。而一个系统是可信的，该系统不仅提供了安全功能与安全服务能力，而且还提供系统被用户考察是可信的能力，做到让系统的用户和管理者建立起一种安全的信心，让用户认为系统不仅是安全的，而且还认为是可信的。可信这个概念是有主体概念的，是主体认为可信的，而不是仅仅因为存在某种能力而可信的。安全是可信的必要条件，但不充分。

可信概念还表现在对事前的预警、事中的监督和事后的审查全过程中。

第二章 信息化安全传统技术发展展望

2.1 信息化安全传统技术概述

信息化安全传统技术是指针对网络物理世界软硬件和信息的语法范畴的安全观念或称之为经典安全概念的安全技术。

信息语法范畴安全观念主要是指数据安全，主要包括数据保密性、数据完整性和数据可用性等安全问题，主要采用数据编码，而不涉及信息语义或内容。网络物理世界安全观念是指系统、网络（软硬件）安全，主要包括访问控制、系统完整性和系统可用性安全问题。从这个传统信息化安全技术定义概念来看，不要认为传统的信息化安全技术已经过时了，传统信息化安全技术依然有无限的发展空间。

为了信息化安全产业的持续发展，必须将信息化安全建设从由于安全责任原因搞信息化安全建设推进到由于信息化安全效益搞信息化安全建设。从仅仅关注“安全责任”到“安全责任”和“安全效益”双重关注是信息安全产业的最重要的理念。

传统信息化安全产品与技术发展要比较全面地实现平台化是今后若干年的主要的工作，信息化的安全不能停留在提供单一产品和单一技术服务上，要提供综合与体系化的服务。平台化是信息安全产业为用户提供综合与体系化服务方案的关键，不仅系统与网络防护需要实现平台化、安全检测与监控需要实现平台化、安全审计需要实现平台化、安全认证需要实现平台化和安全管理需要实现平台化。

平台化发展战略是我国信息安全企业及其商会当前最重要关注的问题。

2.2 数据安全技术

数据安全技术包括数据保密技术、数据完整性技术和数据可用性技术。数据保密性技术主要包括通信与信息处理和存储等环节的数据加密技术、文件加密技术。

数据完整性技术在计算机系统和网络中得到广泛的重视。

数据可用性技术包括数据备份与数据恢复技术，也得到广泛的重视。

在数据安全技术方面目前尤其以手机的通信加密问题引起人们的注意。根据目前的手机通信的机制，主要有 GSM、CDMA 和 3G 移动通信值得注意。

早期开展的保密手机中主要是 GSM 的，其中把语音通信和数字通信区分开，其语音延时大约为 2 秒时间，但是 MODEM 的延时大约为十几秒；由于传输体制的原因，对于语音和数字通信，优先于语音通信，在数字通信时容易产生断线和被挤掉问题。所以，GSM 加密手机由于这些原因迟迟不能使用。最近，一些公司利用自主技术，采用 GSM 的语音信道，不使用 MODEM，实现了数字通信与语音通信在延时一致突破，都仅为 2 秒。但由于其专利技术需要得到大多数企业和信息产业部门标准化的批准与认可，同样存在着推广和开拓市场困难的问题。

后来，国家有关部门提出对 CDMA 加密手机的研发支持，国内有许多大企业参与开发，目前正在进展中。

3G 手机的加密问题仅仅被理论提出，目前还没有得到有效实施。

需要明确的是通信保密手机所采用的加密算法并不是用来认证用的密钥管理算法，保密

通信和认证都需要密码体系，但是它们是完全不同的东西和完全不同的领域。

2.3 信息隐藏与发现技术

信息隐藏与发现技术是一种在时间和空间两个方面利用正规资源承载和检测附加信息的技术，在通信领域称作隐蔽通道技术。在模拟信号通信时代，这种隐蔽通道的信息隐藏技术就已经存在，对正常的信号传输进行二次和附加调制，在二次和附加调制中隐藏传输的信息，这种调制可以是频率的，也可以是幅度的，甚至包括背景信号或噪声的调制。把这种隐蔽通道技术扩展到计算机系统和网络系统中，划分为隐蔽存储通道技术和隐蔽时间通道技术。在隐蔽存储通道技术表示在计算机的系统空间、客体存储空间、尤其在图像、文字、图形等文件中，利用其资源隐藏信息的技术。隐蔽时间通道技术表示利用计算机处理频率或计算机网络和公共通信、电视等网络通道的带宽资源搭载隐藏信息的技术。有时，将隐蔽存储通道技术和隐蔽时间通道技术混合使用。

在计算机和网络系统中隐蔽通道(Covert Channel)是一种以允许违背合法的安全策略的方式进行操作系统进程间通信（IPC）的通道。其隐蔽通道同样划分隐蔽存储通道(Covert Storage Channel)与隐蔽时间通道(Covert Time Channel)。隐蔽存储通道是指在系统中包含着一种载体，它允许一个进程直接或间接写一个存储位置，而另一个进程可以直接或间接读这个存储位置。例如，在系统上这种问题主要表现在全局变量上、进程头、文件头、系统参数等资源的占有上，利用这些资源进行特殊的通信或信息交换；同样可以表现在用户的存储空间上，例如对于图像信息，从不同的层面观察（微观和宏观）看到不同的信息内容。即便是文字格式的信息，也可以约定从不同的层面看到不同的信息，例如从微观看是字符矩阵表格，从宏观看人物的头像。又例如，在网络系统中主要表现在数据包头或信元头或用户数据存储空间的剥夺上，达到传输隐藏信息目的。隐蔽时间通道是指在系统中包含着一种载体，它允许一个进程向另一个进程以调制其使用系统资源的方式传递信号，而第二个进程在响应时间内，可以观察这个调制资源的信号，并作出相应动作。例如，隐蔽时间通道在系统上主要表现在 CPU 的时间剥夺方式或者使用资源的方式与频率所约定的隐藏信息。又例如，在网络上主要表现在传输频率的剥夺上或某种数据包出现的方式和频率所约定的隐藏信息。一定带宽的隐蔽通道在操作系统中是很难避免的。这种带宽可以通过实际测量与工程计算的方法得到。衡量信息隐藏技术的技术指标主要包括隐蔽通道的容量或带宽以及隐藏的信息的存在形式，其存在形式可以是明文、密文或压缩格式的。

隐蔽存储通道和隐蔽时间通道检测技术或者说信息隐藏的发现技术是一件非常困难的工作，利用隐蔽存储通道和隐蔽时间通道隐藏信息是一件比较容易做到的事情，但是发现隐藏信息就非常困难。

信息隐藏检测技术之所以重要不仅仅是由于信息隐藏技术可能危害国家安全，也由于代理系统可以以数据格式或者文档形式存在，作为入侵的手段，引起安全部门的关注。

2.4 系统与网络防护技术

系统和网络的安全防护技术包括应用防护技术、系统防护技术和网络防护技术（这里没有考虑物理防护技术）。已经使用的应用防护技术包括：应用程序接口（API）安全技术、隐蔽 API 技术和应用层门卫技术。已经使用的系统防护技术包括：可信计算基（TCB）、抗篡改、抗旁路、自主访问控制、强制访问控制、强制行为控制、标识与鉴别（用户鉴别、机

器鉴别）、客体重用、系统备份与恢复技术、系统抗拒绝服务技术、系统防信息泄露技术等。已经使用网络防护技术包括：网络安全体系结构、安全网络设备、安全网络协议和安全网络服务构成的多层次防护结构。具体包括网络可信计算基（NTCB）技术、互联网应用防护技术（例如套接字（SOCKS）、互联网密钥交换协议（IKEP）、安全 SSL、安全 S/MIME、媒体加密器和互联网安全（IPSec）和互联网网络安全技术（例如 DNSIX 网络协议、RFC-1108 RIPSO、CIPSO、安全路由器、防火墙、代理服务器、网关、访问控制服务器、服务器软件防火墙、VPN 技术等）、门卫技术、网络抗拒绝服务技术、网络防信息泄露与截获技术等。

解决信息化安全传统技术主要问题就是系统与网络安全防护的发展趋势。其宗旨是推进系统与网络防护技术的客户化、平台化。

推进信息化安全产品客户化，组织信息安全防护高端产品的研究与开发，加强面向应用层面的安全防护问题研究，深入探讨客户业务行为和信息内容的语义方面的安全防护研究。

推进信息化安全技术产品的平台化（互操作性的标准化技术）。积极推荐国际标准化组织 DMTF 提出的公共信息模式（CIM）的管理平台概念，推荐 CISCO 公司的 CIC 作为管理平台体系结构样板，要求我国企业积极借鉴。成立系统与网络安全防护产品企业联盟、系统与网络安全检测与监控产品企业联盟和安全管理平台产品企业联盟作为推进此项工作的主要措施。

2.5 系统与网络安全检测、监控技术

已经在市场上得到使用的系统和网络安全检测技术包括：已知脆弱性检测、已知病毒检测器、已知蓄意代码检测、配置管理检测、隐蔽通道检测、通信断路检测、通信连接检测、内容检测、布线系统检测、WEB 检测、代理服务器检测、访问控制服务器检测、内联网络检测、网络协议测试与检测、网络服务测试与检测等。

已经使用的系统和网络的安全监控技术包括：包过滤技术、状态包过滤技术、内容过滤与监控技术、软件行为（应用）监控技术、已知入侵检测与监控技术、隐蔽通道检测与监控、网络远程监控技术、分布式监控技术等。

传统的入侵检测（IDS）是对入侵行为实行实时检测和监控的技术产品，该项技术有从适合局域网到适合大范围网络环境的发展过程，有对入侵行为定位和追踪的要求，有与安全审计密切结合的要求和入侵检测作为安全管理的核心联动其他安全产品实现综合的防护要求。

安全检测与监控产品在把握发展趋势方面要注意如下几个方面：

从安全检测与监控产品技术发展趋势来看，从对单一行为的检测，要开辟多行为的检测，只有积极开展大范围、多主体和多行为的检测，才能把所有主体和客体的相互关系搞清楚，才能把一个主体行为踪迹搞清楚，才能真正将安全检测与监控产品建立可信基础之上，把信息安全检测与监控的工作推进到宏观与统计的新高度。换句话说，安全检测与监控需要提高到可信检测与监控新概念。可信检测与安全检测的最大区别就是可信检测是“用户心中有数”的安全检测，而不仅仅是实现了一些安全功能和提供了一些安全服务。

从客户关注的行为检测与监控问题来看，把入侵行为检测与内部行为监管密切的结合起来也是系统与网络安全检测与监控的重点问题，需要引起系统与网络检测与监控产品的供应商注意。

从安全检测和监控体系结构看，信息安全检测与监控技术产品的平台化是当前发展的一个重要的关注点。所谓安全检测与监控平台化实际上将安全检测和监控产品组网，构成大范围的安全检测与监控系统。对于具有地区、国家甚至国际范围的运营网络环境系统，建立大范围的安全检测与监控体系是非常重要的。目前的安全检测与监控等产品主要针对局域网建

设的，作为局部网络环境防范外部入侵的重要的技术手段，也是建立大范围网络安全预警体系手段。

安全审计是信息安全检测的重要系统，几乎所有的计算机操作系统都提供审计服务，我们把这种审计称作为“结点审计”，这些结点审计相互之间是孤立的。可以提出一个问题：一个网络的审计，尤其是大范围网络环境的审计，可以认为网络审计等于所有的网络结点审计的和吗？其答案显然是否定的。因为把所有结点的审计结果加起来要远小于整个网络的审计，因为每个结点的审计都仅仅孤立地进行审计，而没有考虑结点相关性的审计，就是说这种结点审计是“前后文无关”的，而整个网络的审计是在网络范围内“前后文有关”的。从传统意义上讲，更有效的审计体系是将所有的结点审计系统组成审计网络，并进一步建立研究相关性的全局审计系统。从这个意义上看，审计系统的建设也要实现平台化，因为一个网络环境内审计系统仍然是多厂商和多类别的。我国信息安全企业为了满足用户更有效的安全管理，建立审计网络平台系统依然是下阶段的重要工作内容。

2.6 安全管理平台技术

信息安全管理建立平台，就是要把入侵检测、防火墙、脆弱性检查、蓄意代码检查、计算机病毒检查等安全产品与系统建立互动、互操作的统一管理平台。信息安全产品在上世纪 90 年代问世以来，经历过独立发展、客户化发展（不同客户领域需求的安全产品，例如划分成电信、金融、政府等领域的产品）、更加便捷应用（可视化）的发展阶段。当前，信息系统安全产品正在实现互动和统一管理发展阶段，还积极与系统管理、网络管理等产品融合，把安全管理纳入到大管理体系框架之内。管理系统和管理平台正在向更加智能化和应用便捷化方向积极迈进。还正在积极调整安全观念，与行为监管体系相联系，促使安全管理更加有效和具有证据化。

2.7 病毒、蓄意代码检测与消除技术

计算机和网络病毒以及蓄意代码检测与消除技术是当前用户最经常关心的技术。传统的计算机和网络病毒检测技术主要依靠行为结果判断、模式识别与匹配等方法来发现病毒的存在。国家还建立了病毒预警和服务体系，来消除其影响，维护计算机和网络系统的正常运行。但是这些发现能力和预警、服务体系的建设的现代化程度还需要提高。

显然需要将这些传统的计算机和网络病毒以及蓄意代码检测与消除技术与多代理技术结合起来，需要将模式检测发现与行为检测与发现技术集合起来。

2.8 身份认证技术

身份认证技术是现代网络安全技术最重要的内容之一，无论是可信计算平台、可信网络平台、可信连接标签、代理活动和交易活动都需要代理认证技术。配合使用的系统包括数字签名、电子印鉴、标签认证、代理认证、数字证书管理、密钥管理等系统。在网络世界的认证系统中，都以逻辑参数作为鉴别的主要依据。目前主要存在三种认证体系：

其一，基于 PKI 技术实现的认证系统。PKI 是一种第三方在线认证的系统，其运行主要靠两个部件：层次化的 CA 机构和在线运行的证书库。由于其实行的是 CA 证书管理和采用

的密钥管理算法规模小，对于处理数量巨大的证书管理和认证工作，需要建立非常复杂的多层次 CA 体系结构，需要建立高带宽的网络系统。所以认证管理能力低，管理成本高。另外，该方法不适合网络世界中代理、进程、主体的身份认证。

其二，基于 IBE 算法实现的认证系统。IBE 算法是 Don Boneh 和 Matthew Frankin 提出基于标识的加密算法（Identity Based Encryption）算法。其特点是取消了第三方认证的 CA 机构，颁发的是 ID 证书。但依然保留了在线认证服务，需要保留大量的用户证书，仍然需要建立在线的证书数据库系统。因此，其认证管理能力低，管理成本比 PKI 大大减少。该方法吸引着国际上许多人的关注。但是，该方法仍然不适合网络世界中代理、进程、主体的身份认证。

其三，基于 CPK 算法实现的认证系统。CPK 是我国密码学和信息安全著名专家南相浩教授 1999 年提出的基于标识的公钥算法，也称之为组合公钥算法，是无第三方认证技术，无须在线认证数据库系统的支持，颁发的是 ID 证书。由于采用了种子矩阵算法，只需要保留很少的公钥参数，甚至可以在手机等小终端上得到普遍的使用，其认证规模极大。该方法仍然适合网络世界中代理、进程、主体的身份认证。CPK 认证体系要远远优于 PKI 和 IBE 体系。南相浩教授提出的 CPK 密钥管理算法至少比美国最近提出的 IBE 方法领先几年，已经引起了国际人士的关注。

2.9 业务连续性技术

银行业务连续性主要讨论业务部门和技术部门应当处理应急事项以及总体方面应当处理的问题。银行业务连续性管理信息系统主要帮助实施业务连续性计划和业务连续性管理两个方面的任务。从方法模型来看有如下的一些体系：故障诊断和容错模型与分析、软件系统异常处理模型与分析、备份系统模型与分析、外部威胁与攻击应急响应模型与分析、恢复模型与分析、业务连续性管理模型与分析等。

建立应急体系：到上世纪 90 年代，对于信息系统可靠性的要求更高了，建立一般的灾备中心还嫌不够，在积极策划建立应急处理体系，建立专门的应急通信系统（例如 800 兆数字集群通信系统）和各种车载移动指挥系统、通信系统和信息系统。

实现业务连续性管理：从可靠性概念到业务连续性概念，将服务的不间断性或连续性问题扩展到相关业务领域，不仅仅是信息技术系统的可靠性、备份恢复、灾备中心、应急中心等建设问题，而且是包括业务系统在内的不间断服务和业务工作在危机中的处理能力，使可靠性工作直接有了效益。其中，非常重要的概念是合理布局业务体系，反对片面追求业务过分集中局面。

美国 2001 年 911 事件之后，业务连续性问题概念变得更加突出，对金融性行业和经济的重要机构提出了更高的业务连续性发展计划。2002 年 FSA 对世界上一些重要的金融财团进行了考察与调研，得出了一些很有启示的结果，反映出了业务连续性管理（BCM）的一些新的概念。业务连续性概念包括如下一些内容：

- 业务连续性管理 BCM 结构（认识、角色、责任、机构和预算）
- 灾害对业务影响分析（对业务结果和过程的影响）
- 业务连续管理计划（恢复位置、时间、功能、过程等）
- 应急响应和恢复管理（预案框架、测试、演练和危机管理计划）
- 业务连续性的信息技术系统和电信系统
- 业务连续性的外包服务
- 业务连续性决策
- 业务连续性的相关性等

第三章 信息化安全新技术发展展望

3.1 信息化安全新技术概述

信息化安全新技术是指针对网络虚拟世界行为安全和信息的语义范畴的内容安全观念或称之为现代可信概念的安全技术，也可以是传统信息化安全问题通过行为可信概念或方法解决问题的技术。这些新技术概念不仅仅考虑网络提供的安全功能和安全服务能力，同时还要考虑提供让网络用户和管理者建立可信性的能力和主体建立可信认识的服务和支持。

在这里介绍技术不仅是未来信息化安全主流技术，也是信息化的主流技术，包括可信计算平台技术、可信网络平台技术、多代理技术、数字标签技术、无第三方认证技术、监管信息化和信息化监管技术、网络对抗技术、多代理计算网格技术和多系统与多代理系统体系结构技术。

3.2 可信计算平台（TCP）技术

可信计算机平台联盟（Trusted Computing Platform Alliance，简称 TCPA），是一个开发安全计算机，研发计算机安全技术的开放式机构。2001 年 2 月，创新的行业规范“可信计算平台（Trusted Computing Platform）”出台，成为计算机安全领域一个重大飞跃。目前 TCPA 已经重新改组为 TCG。

提起 TCP 使人们很容易想起美国国防部的 TCSEC 评估准则中定义的 TCB（Trusted Computing Base）的概念。这种 TCB 安全核的概念对于操作系统和在其上建设的数据库管理系统（DBMS）以及应用系统的建设都是有意义和有效的。在操作系统的安全观念中也按照角色（例如管理员、超级用户、普通用户等）给予一定的引用系统服务的权力。也就是说，在 TCSEC 中也提出可信概念实际上是一种特权概念。只要是系统管理员或超级用户，就认为是可信的。但是 TCPA 的可信概念是建立在行为基础上的。

TCPA 可信的行为定义：

即一个实体如果其行为总是以期望的方式和意图发生的，那么这个实体可以是可信的。

从这个定义可以看出，可信不再是一种角色的特权，而一种是信誉。这是一种进步：

- 可信概念定义为行为可信概念
- 建立在可信测试、可信报告、可信管理等基础上的可信平台模式概念
- 可信平台概念强调系统的完整性
- 可信平台概念重视行为的完整性

在可信计算平台概念中引入了子系统身份鉴别、加密、子系统实体、可信平台模式、平台完整性、验证平台身份与完整性、抗篡改、CC 测评和其它服务。

一般地讲，计算平台是指包括计算机、服务器、终端设备和网络设备等在内的在网络范围内的，能够实现共享、交换、通信任务的支持运营、或管理、或开发或应用的环境系统。TCPA 定义的可信平台概念为：一个平台对于本地用户和远程实体是可信的，那么该平台是可信平台。如此平台模式称之为可信平台模式(TPM)。其工作原理为，通过不断的可信测量递交的可信报告，实现一个实体与预期值的充分匹配，来了解信息平台的可信程度。

TCP主要实现系统完整性，这种可信概念通过建立几个可信的根来实现的，其中包括可

信测量根RTM、可信测量报告的根RTR和可信存储根RTS等可信概念。 “可信测量根”和“可信报告根”联合起来提供了平台的当前计算环境的测量数据。可以访问这些测量结果而且将结果与期望的值比较，考察平台操作是否是期盼的。如果测量结果与期盼值充分匹配，那么这个实体可以在平台上进行可信计算。由于这种测量和报告可以长期记录，为维护系统完整性提供了必须的信息。所以，TCP对发现计算机病毒、特洛伊木马甚至代理入侵都有决定性的意义。但是，这个TCP计算模型实际上是跨国公司的方案，对于大多数国家，因为没有计算机核心技术系统软件技术，仍然没有国家的信息安全。但是，大多数国家可以采用另一种方案，即设计可信平台的测试模块和TPM模块，对计算机硬件、BIOS、操作系统、应用系统等实施测试，并保存测试报告，从而对系统实现监控。从上面的讨论中，看出现代计算机的安全概念在进步，这种安全观念在于建立一种新的体系，即计算机的安全应当由用户来决定，而不能由计算机或操作系统厂商或厂商所在国家来控制和决定。只有这种安全观念才是目前国际秩序所需要的，而不是由哪个霸权国家所控制。

3.3 可信网络平台（TNP）和可信应用平台（TAP）技术

可信网络平台（TNP）和可信应用平台（TAP）框架是中国信息安全产业组织---中国信息产业商会信息安全产业分会提出的概念（2002 年准备并提出，于 2004 年 12 月 18 日正式发布），该概念作为今后几年商会推荐给信息安全产业的企业为客户服务的市场概念。我国信息安全产业中的许多公司已经或开始以此概念为用户提供系统体系结构整体方案和产品。

早期的可信网络概念出自于 TCSEC 的网络解释（TNI），在这个解释中，现在看来是把安全概念与可信概念混淆了，因为它认为一个可信的网络必须可信网络设备、可信网络结构、可信网络协议和可信网络服务。从现在看来这些概念实际上网络的安全概念，即一个安全的网络可以认为包括：安全的网络设备、安全的网络结构、安全的网络协议和安全的网络服务。因为，这些概念实际上还是考虑网络提供的安全功能和安全服务能力，而不是提供了让网络用户和管理者建立可信概念的能力，没有为网络的使用主体建立可信认识提供服务和支持。要做到安全可信，就是要求既提供的安全功能和安全服务能力，又提供让用户和管理者建立可信概念的服务和能力。本白皮书认为：

一个网络和应用是可信的，使用和管理这个网络与应用的所有用户能够考察到这个网络和应用系统中的行为与行为的结果总是预期和可控的，那么网络和应用系统对于使用主体是可信的。在网络与系统上针对业务与技术的行为与行为结果提供行为控制、行为监管、行为认证、行为管理和行为对抗的充分能力，并建立相应的体系是维护网络的可信性根本措施。

在以下的各节的新技术讨论中，都涉及到可信网络平台和可信应用平台的建立。

3.4 多代理技术

代理做如下的定义：代理是具有代理性、自治性、社会性、协同性、交互性、移动性与适应性等特性的网络环境内有组织群体应用进程。多代理是将代理群体依照一种组织模式构成具有分工、相互协同和实现制定总体目标的系统体系。

代理（Agent）技术诞生于上世纪 70 年代，但到 90 年代中后期开始迅速发展的信息技术，在本世纪，尤其是在 2001 年 911 事件之后，得到更大的重视。代理是一种研究人类在网络虚拟世界中虚拟主体行为的技术，它是为人类利益服务的一种具有自治性、社会性、协

同性、交互性、移动性与适应性等特性的新型软件的体系结构和系统。代理技术，尤其是多代理技术的发展，使软件不仅仅作为工具为人类所使用，而且成为网络世界中代表人类在其中自治活动的主动虚拟主体，并能联合起来构成有组织群体为其“主人”服务。是计算机科学与技术中继计算技术、网络技术、对象技术和可视化技术之后，带动 IT 全局发展的更高层面的新技术，它为 IT 发展带来一个新的时代：代理时代。

当代信息化的发展一大问题是信息看不过来，甚至在有些方面到了没人看的程度。解决这个问题，采用代理技术是主要出路。信息化发展到综合信息化的时代，大范围和大规模挖掘信息与数据，采用代理技术是主要的出路。建立信息化的主动发展模式，是推动信息化服务的主要思路，采用代理技术也是主要出路。在国家基础设施实现大范围的安全建设，传统的计算机局域网技术已经不能满足要求，采用代理技术是基本出路。代理技术也是摆脱目前 IT 发展疲软重要出路。代理技术几乎可以应用于所有领域。

911 事件后各发达国家在重新反思其信息化发展战略，研讨新型的系统体系结构是其中重要内容。例如，传统的雷达信息处理系统、电力调度系统、铁路与交通的信息综合处理系统、经济监管系统以及银行的计划采用的数据大集中系统在设计体系结构时，都会采用被动的、统一管理集中控制体系结构。且不说单一厂商大型计算机依赖问题，从基本的生存性问题看就非常严重。这种体系结构在和平时期使用的越好，到战时，一、二枚精确制导导弹打击便可以瘫痪大范围的指挥与控制。原来的非主动的分布式系统在战时似乎可以解决可靠性问题（实际上并没有真正解决），但不能解决和平时期的高效问题。我们必须找到**“和平时期高效，战争时期可靠”**的新型体系结构——主动模式分布式的网络体系结构。我们呼吁：传统典型的信息系统体系结构，尤其军事、电力、民航、交通、电信、金融等国家基础设施的信息系统，需要实施主动模式的革新。

我们只要从下面的一个不完全的代理技术发展情况的清单，便可以看到这种逼人的态势。

- 美国国土安全战略，对国家基础设施信息化将要实行更加严格的监管与控制，其主流技术是代理技术。
- 2003 年由布什总统签发的美国网络空间国家安全策略之中，谈到新技术发展对国家网络空间安全的影响时，首先提到光学计算和智能代理技术。
- 美国国防部研究未来新型战争模式 C4ISR 研究中，深入研究了以代理技术为核心的信息战、网络对抗和新型战争模式中广泛采用代理技术。美国 DOD 讨论了代理网格平台技术、新讨论的 GIG 发展规划中也十分关注代理技术应用与发展。
- 美国能源部（DOE）提出了新一代智能能源网络总体规划概念，广泛考虑多代理技术的采用，期待国家电力网络的调度、通信和信息的一种可靠、高效的新型的体系结构诞生。
- 美国情报部门（例如 FBI）在世界范围的情报收集中大量采用代理技术。
- 美、英国科学研究机构正在研究利用大规模数据挖掘与采集中，在科学实验中，广泛采用代理技术，寻求代理化帮助。
- EPRI 披露，欧洲能源、电力也在积极规划智能电力网格新型的体系结构。
- 金融（银行、证券、保险、信托、租赁等）风险监管考虑采用代理技术。
- 在互联网内容与行为监管方面:美国和欧洲互联网的安全技术主要是网络内容与行为的监管技术。
- 世界个 IT 跨国公司对代理技术研究十分敏感与迅速。认为 Agent 技术的发展是最重要的发展，是 21 世纪软件最重要的发展战略。ECFO 杂志于 2000 年对世界著名科学家、技术权威、工业界的领袖们进行了主题为“什么技术在未来五年时间改变应用模式、组织结构和行为”，在最后调查结果中，Agent 技术得到了极大的重视。一些有

远见的科学家认为在未来十年内，操作系统、网络系统、数据库管理系统、智能家电系统、社会服务应用的各类软件系统都要按照 Agent 技术发展要求重写。许多跨国公司都纷纷建立自己的 Agent Factory 产业基地，做了大量的投入，积极迎接代理时代的到来，并以此根本摆脱 IT 发展当前的困境。

世界 IT 标准化组织已经和正在产生大量代理技术发展的工业标准：

- -ITU 新的电信网络安全体系结构中，要求广泛采用代理技术
- -FIPA 是世界著名的代理技术研究的标准与规范的组织，直到 2002 年出台了 94 个规范及其草案。
- -OMG 是世界最大的研究对象技术软件组织，著名的分布式计算产品 CORBA 就采用了代理技术，CORBA 成为了美国国防部 COE 计划的基础平台模式，
- -OMG 与 FIPA 组织共同制定了代理通信语言标准，在代理技术领域进步中发挥了积极作用。
- -RFC 和 ITU 是两个把 Agent 技术应用网络管理最成功的组织、他们的 SNMP 和 CMIP 在网络管理应用中得到了最广泛应用。
- -目前被 W3C 组织以及 IT 跨国公司发展起来的 Web Services 计划中也非常重视采用 Agent 技术，企图采用 Agent 网格技术，企求更大突破。
- -研究 CALL CENTER 服务标准 COPC 也采用 Agent 技术。
- -分布式管理任务组 DMTF 提出了公共信息模式 CIM 对统一资源管理平台发挥了积极作用。
- -最近两年为建立新的可信计算平台概念的 TCPA 联盟，把采用代理技术作为一个基本点。
- -家电网络研究以及个人代理助理软件系统也都在积极出台的 Agent 平台体系结构和标准。

总之，Agent 技术的标准化工作快速进展。

3.5 数字标签技术

数字标签或数字标识是解决安全问题的基本方法之一。在公共网络中讨论客体的安全采用信息伴侣体系与采用信息的数字标签体系有异曲同工的作用。在网络使用信息标签，使得信息在网络中得到认可，对信息在网络上旅行路径得到了基本认定，没有数字标签的文件与信息，将会被查处与质疑。数字标签概念在多个方面被得到应用，请看如下的讨论。

1、安全数字标签技术

数字标签系统最早还是从美国军方在 1991 年提出的 RFC 1108（Revised Internet Protocol Security Option）和由美国国防部情报局和情报委员会 DoDIIS 提出的“DoDIIS Network Security For Information Exchange"安全网络标准（DNSIX），研究可信网络与不可信网络的通信与信息交换引起的。在 TCSEC 中网络安全，主要是讨论可信网络的安全问题，没有涉及非可信网络的安全。通过这个安全标签的选项标准的提出，试图解决可信与非可信网络的信息交换的安全问题，其思路依然延续 TCSEC 中阐述的原则、对策和方法。DNSIX 是针对 TCP/IP 网络的。非可信网络当然首选互联网。其文档是公开的。该标准涉及 DIA-CMW 安全标准的网络环境，CMW 安全级可以认为在 TCSEC 的 B1 安全级与 B2 安全级之间。RIPSO 为 IP 基本安全选项（BSO），说明了敏感标识和一组保护属性标志（PAF）。RIPSO 还提供附加安全选项（ESO）。在此基础上，又提出了 CIPSO：新生标准中的公共互连网协议（IP）安全选项（CIPSO）预期会采用 MIL—STD—2045—48501，“公共安全标记”，该项新生标准是：“可信系统互操作性组（TSIG）受限环境的可信信息交换[TSIX（RE）1.1]”。例

如 HP 公司的开发的 MaxSix 就是基于 DIA-CMW 安全标准的网络。又例如原 DEC 公司开发的 SEVMS 操作系统也是支持 DNSIX 标准的网络。

美国商务部/国家标准的和技术研究所于 1992 年提出政府开放系统互连的标准安全标识轮廓，并在 1995 正式颁布执行信息传输中标准安全标签的标准（FIPS 188）。

互联网网络工作组于 1993 年，在 RFC1457 中提出过互联网安全标识框架（Security Label Framework for the Internet），后来 1997 年提出互联网安全标识 Internet Security Label (ISL)。对安全标签的研究工作一直没有停止。

为什么在计算机中实现强制访问控制（MAC）得不到用户的认可，而在网络中实现这种安全标识或标签的传输中却可以得到用户和厂商的认可，其中的原因建议读者去认真思考。需要说明的是这种安全标识或数字标签概念是需要网络设备支持的。通常一个概念如果仅仅需要厂商在产品上进行改变进行支持，通常是可行的，如果一个概念需要用户的应用软件需要改变才能实施，通常是非可行的或很难实行的。

2、通信领域的数字标签技术

数字标签工作，不仅仅在安全方面得到重视，而在网络传输的机理方面也在研究。在网络上传输的客体要打上标签，表明走过的路径。在电信领域中利用标签技术改进交换、路由、寻址的技术。在上个世纪后期到本世纪的出，IETF Network Working Group 提出的多协议标签交换（Multiprotocol Label Switching，(MPLS)），目的在于改变传统的交换和路由技术，采用标签交换与路由技术，提高网络传输的效率和质量，甚至提高网络传输的安全机理。另外 IETF’s IPng Working Group 也在积极从事类似的工作，为 IPV6 提供数字标签。另外，主动网络的研究者积极为其提供活性标签技术（Active protocol label）研究成果。在通信领域的标签中，如果保留对于标签的记录信息，自然可以发挥客体在网络传输的路径定位的作用，当然也就对网络安全起到保障支持作用。

3、建立在标记语言上数字标签技术

XML 是可扩展的标记语言可以作为客体的数字标签使用。我们需要说明的是对于文档编辑和应用软件应当具备建立数字标签的功能。

4、代理数字标签技术

其中DAML（DARPA Agent Mark-Up Language ）是美国国防部使用的代理标记语言，可以作为数字标签使用。DAML= XML + 语义Web。语义Web是在这个网页中定义一种语义结构，为在网页（Web page）中内容能够被代理和人都能读方法，定义的语义的语言DAML、RDF、XML、WSDL等。语义Web是在当代WEB中能够使计算机与人均可读的良义定义信息内容的语义方法学，在Web中定义一种数据，使得在各类应用中更有效的发现、自动化、集成和重用。如此可以发挥与延伸Web的能力，达到数据共享、被自动工具与人处理的更高境界。

与上述的代理可读的数字标签不同，将数字标签技术与代理技术结合起来，实现活性客体的传输、处理，是本书中提出了概念，这个代理本身可以作为一种活性的标签使用。

将数字标签与代理技术结合在一起，可以更加强化客体在网络中的传输安全，提高客体在公共网络中传输的防护能力。

5、基于 CPK 的数字标签技术

代理安全技术的核心概念依然是代理的识别与认证，采用的技术只能是不必须是第三方的 CPK 密钥管理技术。在商会的咨询机构 QNS 工作室中，正在积极研究基于 CPK 的标签技术、基于 CPK 的代理技术和基于 CPK 的活性标签与活性客体技术。

3.6 无第三方认证与行为可信认证技术

认证主要包括对主体、客体和服务的认证。认证的方式可以划分为有第三方认证和无第三方认证两种方式。当前关注的是无第三方和非在线认证模式发展。目前，主要有两个无第三方认证体系：IBE 认证系统和 CPK 认证系统。IBE 认证体系实行在线认证，不适合网络世界中代理、进程、主体的身份认证，规模小，使用资源较大；而 CPK 认证系统实行非在线的认证形式，适合网络世界中代理、进程、主体的身份认证、规模大、使用资源小。

但是这样的认证体系仍然不属于可信认证的体系。所谓可信认证是一种针对主体的多行为或者相当长一段时间内行为的考察得出的可信性结论，行为可信认证需要建立在行为监管的基础之上，而行为可信认证又为身份控制提供新的行为可信控制机理。

我们需要研究代理和多代理的可信认证、标签可信认证和其他对象的可信认证技术。

3.7 监管信息化和信息化监管技术

当前监管信息化和信息化监管主要任务是监管业务要进网。建立国家监管现代化体系，涉及到政府监管当局、财政、税收、工商、海关、商业、政法、银行、证券、保险、投资、融资、租赁、社会和企业等多方面领域，直接为国家创收、金融安全、用好资金和社会稳定服务。当前，税收、金融和政法等方面的监管系统的建设是国家监管现代化建设的重点。

有如下监管技术：

1、行为监管技术

行为监管技术定义：行为监管技术是为防范风险，对行为的输入、过程与输出、行为产生的环境、行为特性和与其它内容与行为关联性（空间关联性、时间关联性和其它环境属性相关性）进行综合研究、分析、监控、管理，并发现问题点的技术。

行为监管技术包括：行为隐蔽技术、行为踪迹变化技术、行为踪迹消除技术、行为可信性技术、行为完整性防护技术、行为可信认证技术、行为控制技术、行为一致性检查技术、行为协同控制技术、行为有效性确认技术、行为输入条件满足性判定技术、行为过程记录跟踪技术、行为输出条件满足性判定技术、行为环境标识与识别技术、行为分类技术、应用系统行为监控技术、终端行为监控技术、网络行为监控技术、计算机系统行为监控技术、网络定位技术、网络跟踪技术、网络远程控制技术等。

2、内容监管技术

内容监管技术定义：内容监管技术是为防范风险，对内容本身、内容产生的环境、内容变化过程、相关行为特性和其它内容与行为关联性（空间关联性、时间关联性和其它环境属性相关性）进行综合研究、分析、监控、管理，并发现问题点的技术。

内容监管的对象包括：格式内容（主要为应用系统数据库记录内容等）、字符文档内容（字符文件内容）、图形内容、图像内容、加密信息内容和隐藏信息内容等。

内容监管技术包括：内容保密性技术、内容完整性技术、内容可信判定技术、内容分类技术、内容摘要技术、内容标识与识别技术、内容载体（客体）标识与识别技术、应用系统内容监控技术、终端内容监控技术、网络内容监控技术、内容过滤技术、键盘记录技术、屏幕抓取技术等。

3、监管代理技术

监管代理技术定义：监管代理技术是一种从事信息内容与系统行为监管任务的代理技术。

监管代理技术包括：代理分类技术、代理组织体系结构、代理通信技术、代理数据采集

技术、代理行为监控技术、代理操作技术、代理管理技术、代理协同技术、代理识别技术、代理安全技术、代理移动技术等。

4、监管代理服务技术

代理服务技术定义：代理服务技术是一种从事与监管任务相关的服务代理技术。

监管代理服务技术包括：代理可信网络安装服务技术、代理可信网络配置服务技术、代理可信网络管理服务技术、代理可信网络测试服务技术、代理可信网络监控服务技术、代理可信网络诊断服务技术、代理可信网络维护服务技术、代理可信网络培训服务技术等。

5、监管代理平台技术

监管代理平台技术定义：监管代理平台技术是一种为监管的探针、信息采集器、监视器和具有操作与控制功能的代理部件、子系统和系统实现互联、互通和互操作的系统。

监管代理平台技术包括：多代理系统互操作性标准化技术、代理网格平台技术、网络配置可信管理平台（TCP）技术、系统配置可信管理平台技术、安全资源管理平台技术、凭证与密钥管理平台技术、系统裁减技术等。

6、监管技术机制

监管技术机制定义：监管技术机制是面对监管需求组合监管技术的方法与结构。

这些监管技术产生的监管服务主要包括如下的一些内容：

风险监管服务定义：风险监管服务是银行风险监管需求要求的监管服务，这些服务提供风险的信息采集、测试、分析、评估、预案、设计、接受、管理、控制、优化、规避、化解、应急等服务功能，实现对信息与系统及其行为与内容的完整性、可信性、有效性和一致性监管。

对风险监管服务进行分类归纳，提出行为可信认证服务、行为控制服务、行为保密性服务、行为完整性服务、行为可信性服务、行为有效性服务、内容可信性服务、内容完整性服务。

1、行为可信认证服务

行为可信认证服务是银行风险监管的重要的服务，是实现主体身份识别的基础上对主体行为的预期性和可满足性的度量。行为可信性认证是在主体身份认证的基础上，不仅识别身份、权限、授权、口令甚至用户的生物特性，更关注主体的表现行为的可信性。网络行为可信性度量在过去是很困难的，但是在代理技术信息时代，这种主体的行为可信性度量便得可信和有效。应当明确，行为认证是建立在行为监管基础之上的，没有行为监管，就不可能实现行为可信认证。把认证的主体的各种行为可信性加以汇总，分析和进行统计，从而实现行为可信认证。

2、行为可信控制服务

行为可信控制服务是银行风险监管的重要的服务。行为可信控制是建立在传统的访问控制（自主访问控制、强制访问控制、强制行为控制）基础上，增加行为可信控制功能与服务。行为可信控制服务是通过对权限的改变和增加或改变监管力度来实现的。所谓改变权限是指主体行为的权力和范围将受到控制，还可以改变行为的优先级。所谓改变监管力度是对其行为增加监管范围和强度。如果没有行为监管和行为可信认证，行为可信控制服务是不能实现的。显然，可信性高的主体，监管力度应当较低，因为监管本身也是付出代价和成本的。

行为可信控制是将传统的访问控制、行为监管、行为可信认证等组合实现的。

3、行为保密性服务

行为保密性服务是银行风险监管重要服务。行为保密性服务是对行为的输入、行为过程和行为的输出实施保密服务。采取行为过程隐蔽技术，行为过程冗余技术、行为输入/输出改变技术、行为踪迹变化技术、行为踪迹消除技术、行为踪迹变化技术、行为踪迹消除技术、虚拟行为、改变行为控制方式等技术，与行为控制技术与行为认证技术联合，共同组成行为

保密性服务。

4、行为完整性服务

行为完整性服务是银行风险监管的重要的服务。行为完整性服务是防护行为过程的执行文件的完整性，防止行为对象管理与控制被其它行为过程的接管，改变管理控制主体，防止其它行为参与行为过程的管理控制。

5、行为可信性服务

行为可信性服务是银行风险监管的重要的服务。行为的可信性是依据主体行为历史记录的预期特性和可满足性来度量的，这种度量表现在行为符合法律、符合规定、符合预期、符合满足性要求，这种行为不仅表现与钱相关的事务中，例如借贷、还贷、合同执行、电话费用、电费、交通费用和社会活动其它费用信用情况。这种行为还表现在其它行为符合规定的满足性度量（例如违约概率、错误概率、违纪概率、异常概率等）。

6、行为有效性服务

行为有效性服务是银行风险监管的重要的服务。行为有效性服务要确认行为输入或输出非空和行为输入或行为输出的结果或目标的满足性。监管行为有效性必须实现对行为的输入和输出监管，监管行为输入和输出的目标条件的满足性。本书，在软件行为学方法的指导下给出了行为有效性的度量方法和满足性度量方法。

7、内容完整性服务

内容完整性服务是银行风险监管的重要的服务。与传统的数据完整性服务有许多共同之处，但是在主动模式中最大的不同是，为了维护内容的完整性，可以“守护代理”对内容的完整性实施监管与防护。

现代文字、文档和超文本的电子文本信息的软件通常可以支持相当能力的开发或者使用某些“宏”程序，使用这种“宏”程序为文本文件实行“防护代理”的工作，维护内容的完整性，例如电子邮件、微软公司 OFFICE 文件、PDF 文件等都可以设计这种维护内容完整性的服务。

另外，还可以设计专门的维护内容完整性、保密性的监管代理，只要任何文本类应用软件启动运行，该内容监管代理便启动实施监管，而且可以监管一类这样的文本文件。

8、内容可信性服务

内容可信性服务是银行风险监管的重要的服务。主要研究客体提供的信息内容是否可信，按照通俗话说，给出内容的真实性的评估。这里所说的行为的可信性主要是给出内容真实性度量。内容可信的度量的方法主要是考察主体在历史上提供的文件、报表等信息内容的真实性度量的统计与分析。这种可信性的度量与行为可信性度量依据不同，行为可信性度量主要依据行为的预期性和行为输入和输出条件的满足性，而内容的可信性主要考察内容的真实性或“说假话”或“犯错误”的概率。这种说假话或犯错误，应当在一切可能的方面进行考察。当然，本书关心的是主体在网络活动中说假话的概率和说假话达到条件。

3.8 网络对抗技术

建立网络对抗的威慑力量是信息化安全重要领域。安全威慑体系主要针对有组织犯罪、有较大和很大资源的攻击者对我国基础设施信息系统发出的攻击威胁，通常意义上防护或保障体系已经不能防止这种威胁的发生，提供对攻击者实施打击的力量和能力是非常必要的，让任何攻击者在实施攻击时要三思而行，不能轻易去从事攻击。从另一个方面，说明了企业或行业安全，不仅仅是这些部门的事情，还是国家，尤其是国家政法部门（例如，公安、安全、保密、司法、检查、法院等）和军事部门的共同的事情，在必要时，能够用得上。

我们归纳如下三种威慑力量的建设。

第一种威慑力量是打击公共信息网络的犯罪行为的力量。网络犯罪和破坏是人在计算机中的代理软件完成的，那么防护、打击与执法也必须在网络中，也必须通过其代理完成。不可能设想，犯罪和破坏在网络内，而防护、打击和执法在网络外边。

第二种威慑力量打击信息恐怖主义的威胁力量。主要任务是打击国家要害行业信息专网上的有组织犯罪行为和恐怖主义的犯罪行为。

第三种威慑力量是在战争中实施网络对抗的力量。所谓网络对抗的战争形态，是指双方建立一支多种功能代理的作战协同体系，建立网络中的虚拟组织和军队。双方有攻击，也有防护。在很大程度上，消灭对方的网络代理系统是网络对抗的重要，甚至有时是主要内容。

建立“网络警察” 的打击网络犯罪的数字化警察部队，建立数字化安全部队打击网络敌对势力与恐怖势力和建立能够实施网络对抗的数字化师或数字化军是三个独立发展的国家主权意义上的威慑体系建设。相互之间不要替代、相互依存。

网络对抗技术可以包括：代理生存与消除对手技术、模式发现与模式隐藏技术、行为发现与行为隐藏技术、行为控制性与反控制的技术、行为特性对抗技术、攻击入侵技术 （例如“黑客”模式攻击方法、“战争”模式寄寓“和平”工作模式之中的攻击方法、快速有线插播攻击方法、卫星通信攻击方法、无线通信攻击方法等）、定位与反定位技术、追踪与反追踪技术、行为对抗组织输送、配置技术、行为对抗能力评估（红/蓝测试）等。

3. 9 多代理计算网格技术

代理网格定义如下：

代理网格是多代理系统实现“系统协同”的公共要求，实现分离代理系统之间协同任务，创建、合并或联合这些分离代理系统，构成更大的代理系统的协同联合体的框架或机制称之为代理网格（Agent Grid）。

多代理计算网格技术是一种新型的功能强大的具有主动特性的，充分利用资源和可实施不确定分布式计算的技术。

分布式计算主要有如下的三种模式：

第一种是“网络计算机”模型。计算机网络主要是解决不同站点计算机通信、资源共享和数据交换的问题。而网络计算机主要解决把一个网络看成一台计算机进行超级计算的问题。把多台计算机通过网络连接成一台计算机进行并行和分布式计算是网络计算机的主要工作概念。也称之为并行虚拟机（PVM）分布式计算平台模型。这种分布式网络计算机概念，已经有许多成功的应用，例如城市交通控制、科学计算、军事领域、虚拟现实等。

第二种是基于中间件技术的 CORBA 分布式计算模型。CORBA（Common Object Request Broker Architecture）是 OMG 提出的厂商独立、操作系统独立、语言独立网络基础设施独立解决信息平台互操作性问题规范和标准，其核心是对象请求代理（ORB）部件。ORB 是一个机制，利用这个机制，其中的对象可以彼此相互发出请求和接收响应，并且把这种机制跨越在网络的计算机之间。公共对象请求代理体系结构(CORBA)是一个集成广泛对象系统的结构，通过它实现网络计算结点连接。不管计算机网络的拓扑结构是什么类型，中间件运行结点是网络的逻辑中心，扭转网络计算的请求与响应之间的相互关系。

第三种分布式计算模式是多代理计算网格模式。

代理网格是利用软件部件和系统，为快速与动态构建配置和创立新功能。代理网格要求包括如下：

- 代理是人在网络虚拟世界中虚拟主体，可以划分成不同角色，代理可以在任何地方与任何时间得到人给予的信息。
- 网格基础设施和服务必须能够区分数以百万计、千万计的代理，代理活动可以

不受设备和组织边界的限制，代理要求实现整个生存期管理。代理应当能够动态发现和与其它代理共同体的代理建立通信。

- 代理是可移动的，如果一个代理消失，其它代理将代替它，实现代理的移动管理。代理网格有维护其范围、状态的能力。代理的能力是可扩展的。在代理联合体中的本地服务被网格服务启动，但不被代替。
- 在异构代理系统的联合体中，代理之间的互操作性应当被支持。提供代理与非代理软件(对象已有应用)之间的互操作性机制或方法。
- 最小化的部件再工程（通过包装、代理、翻译和其它互操作性服务等）
- 一个网格设计者要明确：网格提供什么服务?什么语言？什么协议？提供什么特性?例如，扩展性、互操作性、一致性、安全性、可靠性等如何控制？如何管理？如何维护？

1、代理网格系统有群体组织协同的特点

群体组织体系中的代理个体基本上包含协同部分、功能部分与行为信息基。所谓协同是群体为了维系其组织关系的能力，每一个代理在组织中都承担一个角色，通过这些角色的关系，实现组织的群体功能。协同关系是群体的组织机制。所谓功能部分，是群体组织中每一种角色的业务功能的能力。行为信息基是代理行为的依据和研究行为的特征的描述。代理的群体特征是由群体组织模式、组织行为模式描述的。而组织行为模式又划分成组织行为协同和组织业务功能两个方面。

2、代理网格系统具有有效使用资源特点

代理系统（尤其是监管代理、管理代理、服务代理）的运行环境是在被监管对象、被管理对象和被服务对象上。代理系统把平台系统和门户系统建立在己方的运行环境中，而把信息采集和前端处理子系统放到“别人”的计算机上。也就是说代理系统的终端体系是非封闭的，把客户的个人计算机系统作为企业系统的终端。作者认为，代理技术比资源共享、网络计算机（NC）等技术更有可能解决信息与信息系统资源的利用问题。代理技术出现本身就阐明了为“主人”的利益服务，强调代理性为第一特性，有在市场机制中显然具有可操作的利益概念。

3、有限不确定计算特点

现代分布式计算具有不确定计算模型的，大概只能是建立在一定范围上的多代理分布式计算体系了。任何一个了解计算机科学读者都知道，不确定计算概念是计算机科学中比较复杂的问题，其中有 “NP 等于 P 吗？” 著名的问题。这种计算概念在单一的电子计算机上是不可能实现的。但是，在一个大范围的网络环境内，有成千上万台计算机和服务器的条件下，利用具有自我复制能力的移动多代理系统，这个问题变得很容易实现。我们可以回想，在单一计算机上，对于大量的枚举算法，在一个分叉点处，首先选择一个分叉计算，在计算条件不满足时，实行回退方法，对于任何一个编过计算或应用软件的技术人员来说，这是多么熟悉的事情。在所谓的并行处理计算机上，也仅仅研究出了同时计算几百种（甚至上千种）情况算法，也不能称作为不确定计算模式。但是具有自我复制能力的移动多代理系统，在处理这类问题时，碰到一个情况或分叉点，便可以产生一个相同能力的代理，始终可以保持在有限范围内做到不回退，从理论上讲，如果不考虑网络传输上的时间损失，几乎可以说在这个范围内 NP = P，实现了将指数性复杂性变成了线形复杂性。如果说到极端，如果把全球的所有计算机系统作为这个具有自我复制能力的移动多代理系统计算环境，那么通常意义下的不确定计算都将化解为确定模式的计算。当然，在现实世界中这种计算模型会遇到网络传输、国家边界、单位领地等许多概念的限制。但是，移动多代理系统至少为我们开辟了一种可能性，只是这种不确定的计算范围有多大的问题。

3. 10 信息系统体系结构技术与方法

归纳管理信息系统发展阶段的历史，可以看到如下的 5 个管理信息系统发展阶段：

1）单系统的主机应用模式的管理信息系统发展阶段

从 20 世纪 70 年代开始的管理信息系统主要采用面向主机系统，采用字符终端的信息系统，应用的表示是自己规定的，其界面主要是文字形式的。工作对象主要是业务计算和一些项目的管理。

2）单系统的客户器-服务器两层应用模式的管理信息系统发展阶段

两层客户器-服务器应用模式采用了计算机局域网分布式概念，起源于 20 世纪 80 年代，采用图形界面和菜单方式实现操作，开始启动全面可视化进程，计算机可用性得到了很大提高。这个时候应用的表示服务与应用服务以及数据管理服务分离了。

3）单系统的三层应用模式的管理信息系统发展阶段

希望将表示服务、应用服务和数据管理服务全面分离，起源于 20 世纪 90 年代。这种分离最大的好处是表示服务实现了规范化，多个管理信息系统的数据管理可以综合在一起，建立数据仓库体系，实现数据共享工程。还没有实现应用系统在互操作性上的综合应用。

4）多系统互操作性平台式综合管理信息系发展阶段

众多的企业信息化建设管理信息系统，虽然表示服务和数据共享实现了某种程度的综合。但是，应当说这个时期的信息化应用主要还是部门型的，面向单个业务和项目管理。尤其那些多厂商开发应用系统，几乎不能实现系统之间的互联、互通与互操作。于是在 20 世纪 90 年代后期，开始建立互操作性平台系统，以解决企业范围内的综合业务管理。需要说明的是，综合管理信息系统不能通过建立一个超级综合信息系统来解决，必须要求建立在互联、互通、互操作的基础上，走多系统互操作性平台化的道路。

目前，正在走向一个新的发展阶段：

5）多代理平台模式的代理化管理信息系统（Agent-MIS）发展阶段

前面谈到，管理都是人的直接管理或人通过管理信息系统提供的信息对人类在物理世界中的业务活动进行管理。但是，如果这种人工或人通过管理信息系统提供信息的管理发展到更大范围时，这种管理模式就会越来越没有效果。因为需要建设更大范围的互操作性平台，需要更多人去采集、阅读海量信息。为了解决这些问题，越来越需要网络虚拟主体的帮助，越来越需要实现服务代理化。大量的代理服务又需要实现代理平台体系结构（主动模式），实现更低成本的互操作性、安全性和可管理性。

鉴于上述分析，我们提出了系统开发的新型体系结构概念：多系统和多代理网格体系结构。

新世纪的系统开发已经不再把应用的开发作为工作的重点，随着应用开发的规范化，应用开发已经比较容易，现代系统开发的重点是面向多系统的平台开发。由于代理化的发展，许多系统已经转化为代理系统，而这种代理系统的开发也是多代理系统的开发，对于多个多代理系统的开发重点，也逐步转移到了多代理平台的开发上。于是有如下的两个重点体系结构模型：

- 新世纪系统的开发将面向多系统（重点是多系统平台开发）。
- 新世纪的开发是面向多代理网格体系结构的（重点是多代理平台开发）。

应用开发已经逐步转移到门户系统的开发中，而所谓门户，实际上是统一应用体系的内部站点。

体系结构是信息化总体设计最重要的概念。信息化总体设计同样需要采用比较规范和标准化的方法（*Standardized Approach to IT* Architecture）。推荐给读者的方法是从采用

IEEE 610.12 为标志的开创的体系结构方法（1990）。后来这种方法又被在 IEEE STD 1471 标准（2000 年）发扬光大。

首先，在实践方面，这种体系结构方法应用于美国军方的 DII COE 计划实践中，在 1996 年产生了 C4ISR 体系结构框架第一版本（C4ISR Architecture Framework V1.0）。到 1997 年产生了 C4ISR 体系结构框架第二版本（C4ISR Architecture Framework V2.0）。在这以后，美国国防部依据 C4ISR 体系结构框架第二版本重新命名为美国国防部的体系结构第一版（DoD Architecture Framework, Version 1.0），于 2000 年开始，到 2003 年 8 月正式发布，作为在整个国防部范围内的信息化总体设计的标准化方法。在这个体系结构文件中定义了两个全视图产品（AV1，AV2），七类运营视图产品（OV1，OV2，OV3，OV4，OV5，OV6a，OV6b，OV6c，OV7）,11 类系统视图产品，（SV1，SV2，SV3，SV4，SV5，SV6，SV7，SV8，SV9，SV10a，SV10b，SV10c，SV11）和两个技术视图产品（TV1，TV2）。利用这些体系结构产品，已经产生了 DII COE、SHADE（数据共享工程）、LISI、JTA（联合技术体系结构）、JOA（联合运营体系结构）、JSA（联合系统体系结构）、CADM 和 UJTL 等成熟的综合体系结构产品系列。与此同时，美国国防部考虑到全球化需要，又在上述研究的基础上，又进一步提出 GIG 体系结构的概念和标准化方法。

其次，这种体系结构方法还使用在美国政府的电子政务的体系结构设计中，称之为联邦企业体系结构（Federal Enterprise Architecture，简称 FEA ），是由美国政府的管理与预算办公室（The Office of Management and Budget ，OMB） 提出的。这个总体体系结构方法虽然借鉴了美军的体系结构方法，但是非常具有一般政府信息化的特点。它主要是站在美国总统的角度，以公众服务为中心来看美国电子政务的体系结构的（即不是美国政府信息化的全部）。于本世纪初开始，通过一段时期的不断研讨和修改，在 2003 年到 2004 年之间，先后提出了 FEA V1.0 所有文件。这个体系结构的标准化方法提出了业务引用模式（The Business Reference Model V2.0， BRM，美国政府全局电子政务的业务模型）、执行引用模式（The Performance Reference Model V1.0， PRM）、服务引用模式（The Service Component Reference Model V1.0 ，SRM）、数据引用模式（The Data Reference Model V1.0 ，DRM）和技术引用模式（The Technical Reference Model V1.1，TRM）体系结构模式范畴。美国 FEA PMO 对于 2005 年以及后的年代，如何加强信息化体系结构标准化方法研究与应用同样做出规划，制定了行动指南。显然这个体系结构的标准化方法还在进一步完善，例如需要将这种方法运用到各领域中去，不能仅仅停留在白宫角度看电子政务。

上述的体系结构方法对于中国的信息化体系结构设计也产生了很好的借鉴作用。在中国的信息化实践中，尝试这些体系结构的标准化方法，也有了自己的认识与体会，这种体会尤其表现在在中国信息化建设的特点中，逐步找到了适合中国国情的体系结构标准化方法。信息化体系结构设计不是固定不变的教条，有着其深刻的国情、文化和领域性质，不同的领域其体系结构的实际内涵是不同的。体系结构定义与领域的相关性，可以从美国军方和电子政务的不同的体系结构组成中看出。但是，这种标准化的体系结构方法是各领域都应当学习和借鉴的，只是不同的领域，其体系结构的内涵不同，因而也会产生不同的体系结构的领域标准化方法。

上述体系结构的标准化方法对于一些新的技术发展没有做考虑，例如本书阐述的信息化业务应用代理化的发展和代理技术的广泛发展，对体系结构带来的变化就没有考虑，尤其对多代理技术发展起来的群体计算、群体软件新型理念就没有研究，或者说缺乏认识，或者说没有达成共识（因为标准化通常总要晚于技术发展趋势的）。

第四章 信息化安全理论研究展望

4.1 信息化安全理论研究概述

我国信息化安全领域从事业开创起就非常重视理论研究，我国有一批非常杰出的数学家和密码学专家，我国也具有一批优秀的计算机科学家、计算机专家、通信专家、系统工程专家和信息化专家。但是，信息化安全横跨信息化的几乎所有领域。例如谈到计算机安全，实际上属于计算机的理论学科，其研究的对象属于计算机软硬件及其系统的安全；研究通信的安全，实际上属于通信的理论学科，其研究的对象属于通信设备、协议、服务和网络结构的安全；这样算来算去，除密码学还算作安全的理论学科外，信息化的安全都是依托在其他学科的理论基础上，而没有自己独立的安全理论体系。在我国信息化安全作为一级学科，从其应用的重要性，从国家需要来说，是理所当然的。但是，作为一级学科没有自己的独立理论仍然是一个巨大的遗憾。令人欣慰的是，自从《软件行为学》系列著作问世以来，这个局面可以说已经或者正在发生改变，行为学理论研究的对象不是研究软硬件或系统的问题，而是研究系统中各种主体的行为，不再依赖系统本身，属于系统之外的理论基础研究。也就是说，信息化安全在有了行为学理论之后，终于有了自己的独立理论体系。

我们这里介绍的信息化安全理论研究，仅仅是商会最为关注的信息化安全理论的研究内容，并不是指所有的信息化安全理论研究。

4.2 软件行为学系列著作

《软件行为学》系列著作出版表明了中国信息安全领域，在理论研究方面跃居到世界先进水平，现代科学理论研究工作需要多学科融合，需要一批有才华人士组成的团队，更加需要有广泛经历和具有规划和设计学科的总体框架能力的学科带头人。软件行为学学科是由中国计算机科学工作者提出的，反映中国信息化巨大实践所具有的挑战性，也为中国的计算机科学家提供了最多的机会。我们之所以相信软件行为学提出是正确的是由于其应用体系的产生，表现在《银行行为监管：银行监管信息化》和《银行行为控制：银行信息化与安全》和《网络行为对抗学》所描述的广泛新型的应用上。《软件行为学》系列著作出版发行将会带动一大批计算机科学工作者对软件行为学的研究，也必将产生大量理论和实际成果，丰富这个学科领域并不断完善这个应用基础理论体系。同时，还表现出抓住机遇和正确选择的理论研究对实践工作的巨大的指导作用，为当代体系化的理论研究的科学选题、研究作风、研究模式、研究组织体系提供一种新的存在现实（当然不是唯一的），对传统科研存在模式与形态提出挑战。

1、《软件行为学》

软件行为学是屈延文教授在上世纪 90 年代中期提出的计算机科学的理论课题。《软件行为学》创立了行为语义学，建立了群体软件组织、模式、系统与平台结构，为信息系统代理化应用发展和行为控制、行为监管、行为认证和行为对抗等重要领域奠定了理论基础框架。

计算机研究行为，必须对行为的语义进行描述，这种行为的语义描述是计算机可读的，而不是仅仅人类可读的。而以往的语义学是语言的语义学，并没有现成的对行为语义描述的方法。我们研究了当今国际上对行为研究的各种文献和成果。仅仅看到对单一主体的单一行

为输入/输出条件满足性的行为方法（与 20 年前研究过的结论没有什么进步），另外还看到在欧洲，正在将人类行为的研究成果硬性搬到计算机中来，这个方面的研究被称之为人工智能学派，也可能是由于一些计算机科学家对现代信息化发展失去掌握能力和了解，在当代需要多学科融合时代，这些科学家对提出新的理论课题能力减弱了。也看到美国，虽然对代理技术与系统研究很多，但是在代理体系的理论研究非常薄弱，使屈延文教授看到了自主提出理论框架和进行学科总体设计的机会。通过几年研究终于找到了行为语义研究的形式化数学方法。

软件行为学是抽象研究软件行为的语义学，不仅研究主体对客体的行为，还研究多主体行为之间的相互关系。软件行为学将成为计算机科学的新兴的应用基础理论，是计算机与网络安全的基础理论体系；是网络虚拟世界行为监管、网络对抗、打击网络犯罪、代理技术的计算机科学的理论基础；同时还是网络网格技术的应用理论基础；即讨论软件的微观行为，又讨论软件的宏观行为；既讨论软件的个体行为，又讨论软件的群体行为。

在《软件行为学》中建立了软件群体行为的理论框架，描述与论证了网络中群体有组织软件体系资源使用能力、不确定计算能力、主动服务能力和自身生存能力，研究了群体中单一代理和多代理行为，论述了类型表达式、行为树、行为信息基和多行为的行为表达式语义学方法，为形式语义学应用发展也做出了新的贡献。在《软件行为学》中详细地阐述了行为协同、伴侣行为、行为控制、行为监管、行为认证和行为对抗六大行为模式。

从多个应用领域讨论了多代理系统体系结构，提出了代理网格、代理网格平台、多代理、代理网络和规范代理等多层次的系统体系结构，同时还建立了一种分类型的规范代理组织结构，为代理程序设计和代理软件工程规范奠定了基础，把面向对象、面向模式，面向代理和面向行为的程序设计有机地结合起来，为程序设计理论丰富了新的方法。

2、《银行行为监管：银行监管信息化》

《银行行为监管：银行监管信息化》是软件行为学系列著作之一，为风险监管建立了统一的认识体系平台，这种新认识体系的探索表现在金融学方法、管理学方法、计算机科学方法和系统工程方法学的结合。这种结合体现在新的综合认识体系平台上，既坚持了巴塞尔资本协议对风险监管的标准要求，从金融学宏观理论探讨银行风险监管；又发扬了系统工程学方法清晰的优势，从微观分析风险因素研究银行风险监管；既体现了管理学方法监管制度建设的重要作用，又突出了监管信息化中计算机科学理论指导意义，还为经济学家、银行家、系统工程学家、管理学家、信息科学家采用各种方法学在这个认识体系平台上发挥作用提供动力，实现了宏观与微观统一和制度与技术的结合。

《银行行为监管：银行监管信息化》首次为风险监管建立了统一的认识体系平台，并为监管信息化与信息化监管描绘了解决方案指南。

《银行行为监管：银行监管信息化》提出了完整的银行风险监管信息化与信息化监管的方案指南。有如下五个特点。

- 监管信息化目标：实现主动模式风险监管模式；为克服银行信息化中出现的“服务在网内，监管在网外”的严重弊端和满足监管业务要进网的要求。
- 监管信息化的对象：监管信息的语义范畴的内容和系统在网络虚拟世界中的行为。
- 监管信息化特点：“大范围网络环境、超海量数据与对象、高智能应用与管理”。
- 监管信息化的分类：实现行为条件的基础监管、银行信息系统业务和技术行为与内容监管。 银行行为属性分类监管：在银行业务系统行为与内容可信性、有效性、完整性、保密性和连续性监管的基础上，实现了信用风险、市场风险和操作风险的分类监管。银行行为标题综合监管：行为与内容综合性监管、银行资金流量流向监管、信息自下而上汇总监管、政策自上而下传导畅通性监管

等。

- 监管信息化的结构：方法监管、结构方法监管、行为监管、结构行为监管和多结构行为监管。

3、《银行行为控制：银行信息化与安全》

《银行行为控制：银行信息化与安全》是软件行为学系列著作之一，首次确立信息化总体技术范畴，并将信息化从局域网安全引入大范围网络环境安全。

国家或行业甚至大型企业的信息化都应当摆脱信息化没有总体框架指导的弊端。信息化不等于建立通信系统、计算机系统。计算机专家、通信专家和其它信息技术专家并不自然等于是信息化的专家，因为信息化逐步产生出自己固有技术领域：

- 互操作性技术
- 信息化安全技术
- 用户技术标准化技术
- 技术法规体系
- 测评认证技术体系
- 信息化监管/监控技术体系
- 信息化配置管理体系等技术领域。

在新世纪，任何国家、行业和企业应当重视基础与核心技术研究，同时更应当抓住当前发展机遇，在高水平的总体设计的指导下实施信息化，切实解决信息化急需解决的问题，并要培养一大批信息化的总体人才。

国家网络国土安全也必须建立总体发展的框架，信息化安全总体方法学理论是信息化方法理论与实践体系中的重要组成部分，为信息化发展的总体目标服务。在新世纪，信息化安全不仅仅要求防护信息语法范畴数据和网络物理世界的软硬件的安全，而是更加关注信息的语义范畴的内容和网络虚拟世界的行为的安全；信息化安全在总体结构上不仅仅要求在一个企业或一个部门中实现，而是要求在全球范围、国家范围内实现一体化体系建设；本书提出在国家范围内建立安全保障、安全监管、安全应急和安全威慑体系，就是在这种认识上提出的安全总体框架，具有普遍的指导意义。

4、《网络行为对抗学》

《网络行为对抗学》是软件行为学系列著作之一。网络行为对抗承担的任务是打击网络犯罪、打击网络恐怖主义和在网络上实现信息战对抗。在人类社会中打击犯罪和战争已经有几千年的历史，而在网络中打击犯罪和信息战还仅仅是开始，在网络虚拟世界中的战争是什么样子，虚拟世界中军队是什么？虚拟军队的组织和行为特点是什么？还没有可供借鉴的经验和理论。本书探索如果发生信息战的网络对抗，计算机系统和通信系统能够支持做些什么。

《网络行为对抗学》是一部正在撰写的内部出版的书籍，包括网络行为保密学、代理执法学、数字警察学、数字隐蔽对抗、对抗网络恐怖和信息战网络对抗学等研究内容。

4.3 认证管理算法理论

CPK 密钥管理算是认证理论与技术的创举，它与《软件行为学》中提出的行为可信认证概念一起，共同建立新型的身份与行为可信认证体系。我们需要研究代理和多代理的可信认证、标签可信认证和其他对象的可信认证的理论方法，将认证理论系统化，建立更加完善的认证管理算法理论体系。

4.4 计算网格理论：多代理网格操作系统

计算网格理论是讨论研究真正的网络操作系统问题理论研究，其分析如下：

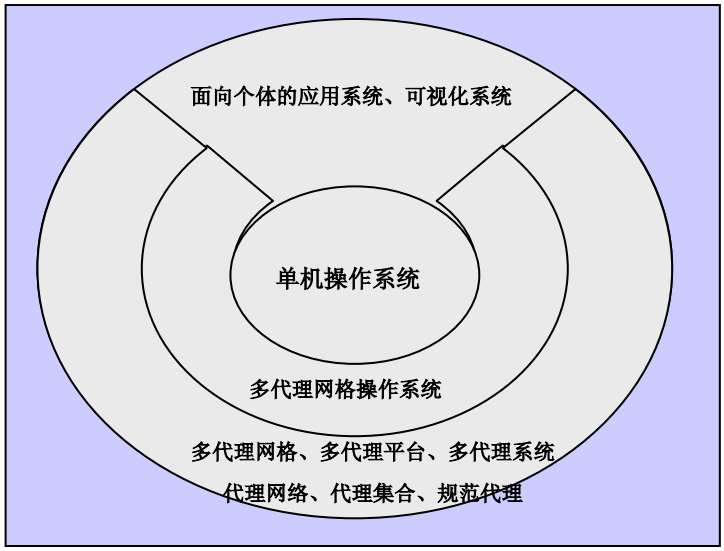
现代单机操作系统的核心概念是进程和子进程或进程与线程，这种进程、子进程与线程在操作系统有其相应的类型概念或结构框架。有了这种框架，用户就可以很方便地建立进程、子进程或线程这些实体。计算机运行支撑也是依据进程、子进程或线程为单位在进行的。计算机单机操作系统也只有支持一组进程、子进程或线程规范组合体运行控制的小规模的组合形式，例如有“作业”形式、“组”形式和“会话”形式等。

如果在这样的单机操作系统上建立代理或多代理系统将是一件非常复杂的事情，其大致步骤为：由于代理是由一组进程、子进程或线程依据代理协同机制和功能机制建立的规范组合体，用户在这样的操作系统环境下如果需要创建一个代理，用户根据代理的结构，在应用层面通过创立进程、子进程和线程的方法，通过使用专门的服务将它们捆绑在一起，通过同步和进程通信机制实现代理内部结构或者代理之间的信息交换。同样，如果构建一个多代理体系，也必须通过许多微观的服务和动作，才能将许多代理构成一个群体的组织结构。所以，我们可以看到在单一计算机上的操作系统，通过比较微观的进程或线程概念，来建立代理和多代理的群体软件的应用模式将是一件非常复杂的工作。

也就是说在现代单机操作系统中没有一个代理结构的类型，为用户直接构成代理、多代理和更高级代理群体对象提供服务，也没有支持代理和多代理运行的运行支持环境和服务。所以，信息化的发展需要建立一种以代理和多代理为核心概念的网格操作系统，为用户提供方便的代理和多代理建立、运行和控制的便捷的服务机制。真正的网格操作系统要系统化地支持代理网格、代理网格平台、多代理、代理网络、规范代理和进程等多层次的系统体系结构形成。我们可以设想，一个使用网络操作系统用户，可以面向模式和面向对象，方便地建立任何需要的群体软件的组织模式体系结构。

我们可以得出结论：计算网格操作系统将代理或多代理概念作为网络系统的核心概念，为了区别旧式的操作系统概念，我们称之为**多代理网格操作系统。**

另外，这个网络操作系统将多代理作为网络系统的分布式计算的核心概念，支持动态体系结构配置和在配置领地范围内不确定计算。用代理概念建立网络操作系统显然比 PVM 概念引入到操作上更加有普遍意义，而且还完全包含了 PVM 概念，是真正的计算网格的体系结构。我们认为，在 IT 企业中推荐开发这样的新型的网络操作系统是有必要的。



有志向的软件创新企业，应当抓住研发支持代理或多代理概念的多代理网格操作系统，抓住又一次产生一个新的“微软公司”的发展机遇。

4.5 代理程序设计与代理软件工程理论

代理程序设计起初是比较简单的，代理通常是软件代理，是孤立的简单代理软件系统。例如黑客开发的简单的攻击软件、特洛伊木马软件和计算机病毒软件等。另外，还包括数据采集软件等。

面向代理的程序设计（AOP）是面向模式的程序设计。面向模式的程序设计，从应用模式出发，尤其是从分布式并发应用模式出发，依照模式框架和相互关系设计体系结构，模式中体系部件其存在的价值全是围绕模式要求的，其程序设计的特点是始终围绕模式的概念、框架、部件关系按阶段求精，细化的。依照这个模式设计概念，设计功能，设计结构，设计实现等。这方面最应当注意的成果是 OMG 组织的 UML 和 MDA。

面向代理的程序设计更高级的阶段是面向有组织群体模式的程序设计。有组织群体模式是指“一个狼群”， “一个数字警察大队”，“税务局”，“商业银行监管组织”和“一个数字化军”等等有组织群体的业务模式。这种应用模式可以是社会性的，协同工作模式的。在设计与实现时，也要紧紧围绕其群体模式实施。有组织群体体系结构，如果再考虑动态性、可移动性等特性，应当认为群体模式的能力比单一个体系统能力强大得多，高级得多。这方面最应当注意的成果是各种面向代理的建模方法，其中 OMG 组织的 Agent –UML 比较引人注意。

面向代理的程序设计是基于面向对象的程序设计的。代理与对象是两个即有联系而又有区别的概念。不要认为有了代理概念，对象概念过时了。对象概念是类型概念的实例概念，类型是对具有共同性质的事物集合，有数据对象与在这些对象上的操作集合。类型是这个集合的总称，而对象是这个集合中的一个实体。所以面向对象的本质是面向类型。有人说，对象是静态的，而代理是动态的，这是不确切的。在对象概念中，尤其把对象概念引入到操作系统之后，一个对象已经可以是一个进程（例如，在 Windows NT 中，对象概念就包含进程），而进程显然是动态概念。把握对象概念和代理概念，最重要的是从它们的定义出发。在这方面，FIPA 研究可以被借鉴。

把握对象概念和代理概念，最重要的是从它们的定义出发。另外，FIPA 为面向代理的技术提供了开发者指南，读者可以借鉴。

代理体系结构主要是研究多代理系统的结构。代理可以划分成管理者（Manager）、管理者代理（Proxy）和操作代理（Agent）。它们之间的连接关系可以如图 B1.4-1 所示，构成星型结构或树型结构。

代理技术的发展产生了许多基于代理的系统（ABS）和平台（AOP），为了更好开发代理系统，便产生了面向代理软件工程（AOSE），其研究的问题包括：代理技术标准化体系建设、开发方法、代理程序设计语言、代理系统的开发平台、代理体系结构、代理通信语言等等。支持基于 agent 系统开发的 CASE 工具和环境，包括软件开发包(Java 类库)，Stanford 大学一组 Java 包，支持开发利用 KQML 进行通讯的软件 agent。支持基于 agent 系统开发的方法学，包括建模语言和建模过程。自 1995 年成为研究热点，取得了不少研究成果，其代表性工作包括：

- Wooldridge 等人在 1999 年提出的支持面向 agent 的需求的，称之为 GAIA 方法学
- 由 Wood 和 DeLoach 在 1999 年提出的 Multiagent System Engineering 方法学。
- 由 Wagner 在 2000 年提出 AOR(Agent-Object Relationship)方法学
- 扩展 OMG 的 UM L 语言，增加支持面向 agent 的建模功能，称之为 AUML。

代理软件工程包括代理系统工程需求分析、代理系统概念设计规范、代理系统验证技术、面向代理的分析与设计、代理本体的结构、代理部件、代理设计平台、代理运营支撑系统、代理开发工具、代理运营平台等等。

在《软件行为学》中，同样阐述一种更为规范的代理程序设计和代理软件工程的方法学和体系结构。提出了代理网格、代理网格平台、多代理、代理网络和规范代理等多层次的系统体系结构，同时还建立了一种分类型的规范代理组织结构，为代理程序设计和代理软件工程规范奠定了一种基础，把面向对象、面向模式，面向代理和面向行为的程序设计有机地结合起来，为程序设计理论丰富了新的方法。

4.6 网络虚拟世界社会学研究

在《软件行为学》著作中，有如下一段话：

“过去，软件是人类直接拿在手里的工具，用它来直接进行操作；现在和将来，代理是人类在网络虚拟世界中使用的虚拟的奴隶、仆人、管家、卫士，甚至虚拟的公务员、职员、操作员、秘书、管理员、……，并且把它们按照期望的组织模式组织起来，以群体方式为人类服务。”

过去，人类直接拿着工具劳动；后来，人类进入了奴隶社会，有些人不劳动，靠奴隶劳动生活；在后来，人类进入了封建社会；再后来，人类进入了资本主义社会；将来，人类要进入社会主义和共产主义社会，**……**。在网络虚拟世界中，人类不满足直接拿着软件工具劳动，开始在网络中使用虚拟奴隶、虚拟工人、虚拟职员、虚拟操作员、虚拟秘书和虚拟管理员了，而且比人类社会发展历史快得多的速度，进入一个网络虚拟世界中更高级的虚拟社会形态中，并不断进步。网络虚拟世界虚拟社会形态的基础学问是研究虚拟社会中成员的行为的规律。人类使用虚拟主体，不仅仅采用个体，而且采用虚拟主体的的有组织群体的方式为人类服务。专门研究网络虚拟世界中各种各样的组织形态和组织行为形态，并且研究它们社会学的各种形态。从软件行为学开始，会有越来越多人来研究网络虚拟世界社会学。

4.7 信息化安全总体框架

大力推进国民经济和社会信息化，是覆盖现代化建设全局的战略举措。我国的信息基础设施的迅猛发展为我国全面实现信息化提供了有力支持。但是，一般来说，一个国家的基础设施信息安全保障、应急、监管和威慑体系建设通常滞后于信息化的发展。没有信息安全保障、应急、监管和威慑体系就没有真正意义上的信息化，必须把国家基础设施信息安全保障、应急、监管和威慑体系建设作为一项紧迫任务，与信息化建设同步推进，投入足够的人力、物力和财力，必须实施统一的规划。

国家基础设施安全建设从建设内容来看包括安全保障、安全应急、安全监管/监控和安全威慑力量建设四个方面（不能，也不适合把所有的信息安全问题都称之为安全保障问题），之所以如此划分，是由于处理这些问题的责任主体不同。

安全保障方面，其责任主体是运营部门，所以也可以称之为自主安全保障。对数据与系统（计算机系统、通信系统、自动控制系统等）实施安全防护的体系。安全保障概念中，保障的对象应当是信息表示的语法范畴：数据和网络物理世界的硬/软件，例如计算机设备与系统、网络设备与系统、通信设备月系统、操作系统、数据库管理系统、应用软件系统等等。安全的保障的概念是数据与系统不被破坏、篡改、删除、偷窃、泄露和识别。

安全监管方面，其责任主体是系统运营管理者和政府的监管当局（行业的运营与监管职

责分离是必然的)。对信息的内容与系统（软件/硬件）行为实施监管的体系。安全监管的对象显然应当是信息表示语义范畴的内容和系统的虚拟世界的行为。从逻辑意义上观看，监管的对象显然不能是信息表示的语法范畴和系统硬/软部分。监管信息内容的危害及其影响，监管交易信息中的违反法律和规定的内容。内容的监管工作是一个传统的工作，例如电话监听、邮件监视和互联网的电子邮件内容过滤检查等。银行客户信息是隐私，必须要维护客户信息的隐私权，为客户保守必要的秘密。这种保护客户的隐私和披露客户的信息是一对矛盾。但是无论保护隐私还是披露信息，都必须实现对客户信息与交易信息的内容监管。

安全应急方面，责任主体运营管理者与相应的专业组织（国家信息安全应急组织还没有组建）和基础设施运营与管理部门。确保业务连续性和防备灾害应急响应的工作体系。有对付敌对势力、恐怖组织以及各种可能的灾害防范、应急处置的能力，维护社会的稳定，减少灾害造成的损失。

安全威慑方面，其责任主体是国家政法与军事机构。实现打击信息犯罪、打击网络恐怖行为和实现网络战争的打击力量体系。在网络政权的建设中，还要特别重视建设我国打击威胁我国信息安全的威慑体系，包括如下三种威慑力量的建设：

第一、建立打击网络犯罪威慑力量。

第二、建立打击网络敌对势力的威慑力量。

第三、建立实施网络对抗战争的威慑力量。

在进行信息安全全局项目建设时，要特别注意从能力具备这个方面进行考虑，我们认为必须包括如下的能力具备目标：

- 信息化安全、灾备防护能力
- 信息化安全监管、控制能力
- 信息安全快速反应能力
- 信息化安全威慑能力
- 信息化安全网络远程服务能力
- 信息化安全全局协调能力等。

当前，应当以监管现代化为重点。建设目的是形成政府网络监管的能力，并逐步实现这些能力的成熟。我们认为，电子政务的本质是实现网络政治、网络经济、网络银行、网络税收、网络财政、网络工商、网络安全、网络公安和网络军事等一切政府行业的网络政权的建设。是国家政权在网络时代的基础建设，是国家政权建设的新内容和新任务。

第三部分：我国信息安全产业发展建议

第一章 我国信息安全产业发展概述

在 2002 年的信息安全产业调研报告阐述信息安全产业发展的目标，现在看来基本是适合的，我们略做修改，重新描述如下：

我国信息化安全的观念依然是建立在“数据与系统（软硬件、网络等）安全自主保障”之上，整个信息化安全理念依然是在上世纪 90 年代中期发展起来的局域网安全观念。对于网络与系统的虚拟世界的“行为与内容的监管”和“大范围的网络环境的安全问题”基本上没有考虑。信息化的风险观念和安全问题应当进行调整，在新起点和新高度上，进行补充总体规划。当前现有的信息系统及其安全系统基本上都是属于国际标准机构定义的未分级安全系统，其安全功能强度均是最初级的，而且构不成体系；实现的安全服务，虽然包括了访问控制服务、安全保密服务、数据完整性服务、备份与恢复服务和部分的数字证书服务，但也属于初步的，对于系统完整性服务、安全资源可用性服务、行为完整性服务和指挥控制服务基本不能提供；我国信息安全建设的平台仅在计算机局域网上，其信息安全产品是孤立的，没有实现平台化、标准化，最多实现了单一厂商产品的互连、互通与互操作；我国信息安全建设的其安全模式是被动的；我国还没有国家基础设施的全行业甚至全国保障、监管、威慑、应急系统；我国已经具有基本规模的国家信息安全测评认证体系，但各项工作还需要加强；我国已经成立国家信息安全应急中心，其职责主要是面向社会的，虽然国家刚成立面向国家基础设施的安全应急与协调小组，但还没有建设国家基础设施信息安全应急体系，没有应急的执行、操作、指挥与产业力量，也更不具备较好处理国家基础设施信息安全的能力。

在未来一、二个五年计划内，我国信息安全产业可以实现如下的目标：

- 我国信息化安全建设不仅建立数据与系统（软硬件、网络等）安全保障体系，而且要建立网络与系统的虚拟世界的“行为与内容的监管”的现代化监管体系、建立国家基础设施信息化业务连续性和应急体系和防范网络犯罪、恐怖主义和信息战威胁的安全威慑体系。在局域网安全建设的基础上实现大范围的网络环境的安全与可信系统建设。我国基础设施安全建设实现国际安全标准 EAL4 或 EAL5 级和 SML2 或 SML3 强度的访问控制服务、安全保密服务、数据完整性服务、系统完整性服务、可信备份与恢复服务、安全资源可用性服务、数字证书管理服务、行为完整性服务和指挥控制服务。
- 这些系统的体系结构要求信息平台是建立在计算机、通信、广电、控制网络的干网、区域网上；要实现产品平台化，标准化，实现多厂商产品的互连、互通与互操作。
- 其安全系统模式采用主动安全模式，建立安全、可信的计算、网络和应用平台体系。
- 我国信息安全产业将取得如下核心技术的进步：即信息安全防护、检测和反应从软件技术完成向嵌入式硬件板式、IC 卡式和芯片式的过渡；在嵌入式操作系统上，将完全取得自主知识产权；将掌握关系到主动安全模式体系建设的代理与引擎技术体系，具有多个分行业的软件代理产业骨干集群，具有规模效益，并可以输出技术；我国将完全掌握信息安全管理平台技术，完全掌握安全网络服务平台技术和完全掌握依据国际标准 CC 测评认证的主要技术。
- 达到如下能力：信息化安全、灾备防护能力；信息化安全监管、控制能力；信息安全快速反应能力；信息化安全威慑能力；信息化安全网络远程服务能力；信息化安全全局协调能力等。
- 将为国家建立国家信息基础设施安全应急体系；加强中国信息安全产品认证体系建设；基本实现税收、金融、政法、电力、交通、民航等国家基础设施的保障、监管、

威慑、应急系统。

为我国信息化安全提供发展建议，为了全面可以提出许多内容。经过认真研究，许多建议内容是可以企业自身把握。在这里，我们仅仅提出需要国家和整个产业关注的几个最重要的问题。

第二章 谁能抓住产生又一个“微软公司”的发展机遇？

Microsoft 公司是在上世纪 80 年代在个人计算机（PC）发展的初期，研发个人计算机操作系统（DOS）以及在 80 年代末个人计算机操作系统可视化（Windows）发展机遇的推动下，一些大型操作系统供应商对个人计算机操作系统认识不够的情况下，抓住机遇发展起来的。

代理化软件技术的发展，带来的新型的网络应用模式。我们已经在前面的讨论中，呼吁有志向的软件创新企业，应当抓住研发支持代理或多代理概念的**多代理网格操作系统**，抓住又一次产生一个新的“微软公司”的发展机遇。在这里，我们希望引起信息产业界的关注如下的长远战略发展需求，即：

现在出现了为了实现代理化应用的强烈需求，用户需要一个具有代理结构的类型，为用户直接构成代理、多代理和更高级代理群体对象提供服务，也没有支持代理和多代理运行的运行支持环境和服务的新型操作系统。信息化的发展需要建立一种以代理和多代理为核心概念的网格操作系统，为用户提供方便的代理和多代理建立、运行和控制的便捷的服务机制。真正的网格操作系统要系统化地支持代理网格、代理网格平台、多代理、代理网络、规范代理和进程等多层次的系统体系结构形成。全面实现用户既可以面向模式和又可以面向对象，方便地建立任何需要的群体软件的组织模式体系结构。

从较小的概念出发，仅仅从个人服务代理系统的建设，同样需要呼唤建设个人服务代理的运行和资源支持平台的建设。这种平台支持个人服务代理在平台上运行和得到平台提供的服务资源，同时支持服务代理在平台上的移动和管理。这种代理平台还支持代理构成组织群体，确保服务的代理安全和可信性。显然这是一个巨大的市场，需要我们的企业去开拓。

多代理网格操作系统应用与发展需求在召唤有战略发展眼光的企业家投入，在召唤有水平的计算机科学家、操作系统专家和软件工程师参与。这是一个向前看的发展计划。

第三章 关于建立信息化安全新型产业基地与集团

目前国家基础设施信息化与国家信息基础设施的安全建设存在着巨大建设空白，是国家信息安全建设最大的担忧。国家基础设施信息安全不是靠一、二个行业自己解决的，单靠市场经济的方法或者启动一些项目，这项关系到国家基础设施安全与发展的大事是搞不好的。需要在国家信息化领导小组统一领导下，在国家有关综合部门、安全部门和产业部门配合下，加大宏观调控力度，发挥社会主义集中资金、集中人力能办大事的优越性，认真落实邓小平同志提出的市场经济也有计划的著名论断，采取科学规划的方法，精心布点，以搞“二弹一星”的精神，建立国家基础设施信息安全的专门防护、监管、应急与威慑力量，建设提供国家基础设施安全装备与技术的产业骨干企业体系。我们制定了一个称之为“京广线”发展战略的国家基础设施安全产业结构调整方案建议，可以实现该问题的突破性解决。选择的突破口是建立代理技术骨干产业集团。为改变我国基础设施信息安全建设状况，不能简单依靠企业按照市场机制的规律实施建设，必须依靠国家的力量，实施建设。**如果我国现在不启**

动建立代理技术产业基地或集团的专项建设，我们将会在 IT 的新时代发展中，又要落后一个时代，我们又会处在茫然追赶被动状况。

由商会负责牵头，联合国防科技大学、中国人民解放军信息工程大学、总参某部、武汉大学、国家计算机网络与信息安全管理中心、信息产业部有基础的研究所和国内一些骨干的信息安全企业，开始相当规模地推动我国代理技术产业的创立、开拓、发展工作，已经显露初步的效果。其中主要推动者为屈延文教授（信息产业部 15 所）、孙玉院士（信息产业部 54 所）、何德全院士（国信办）、王正德教授（中国人民解放军信息工程大学校长）、刘经南院士（武汉大学校长）、陈火旺院士（国防科技大学）、杨芙清院士（北京大学）、南相浩教授（总参某部 58 所）、黄达仁教授（中山大学校长）、方宾兴教授（国家计算机网络与信息安全管理中心主任）、吴世忠教授（中国信息安全产品测评认证中心主任）、林鹏教授（国家计算机网络与信息安全管理中心）、蔡红教授（国家保密局副局长）、王淮民教授（国防科技大学）等共同合作推动这样一个技术发展工作。我们认为国家基础设施代理技术产业结构的建设，必须选择一些各方面基础条件好，尤其是还保持了较好的科研基础，国家能够控制的地方和单位，以它们为基础，实施产、学、研相结合的方法，采用建立现代企业制度的方法，实现计划的建设。我们称这个技术发展推动计划为“京广线发展战略”（即主要依托北京、石家庄、郑州、武汉、长沙和广州研究机构、大学、企业）。**我们再一次呼吁国家应当积极支持这样一个新型产业基地与集团的发展计划，抓住当代信息化发展的最大机遇。**

这个计划的目标是建设面向各行业（税收、金融、政法、电信、电力、交通、民航等）代理技术骨干集团，具体建设内容：

- 建立国家基础设施信息安全产业结构调整项目总体单位
- 建立面向电信与广电的信息安全代理技术产业骨干集团
- 建立面向电力、交通、民航、铁路等领域测控系统代理技术产业骨干集团
- 建立面向金融、税收、财政、工商等经济领域代理技术产业骨干集团
- 建立面向军事与政法方面的代理技术产业骨干集团
- 建立国家基础设施信息安全实验室

国家基础设施信息安全产业结构调整项目总体单位拟委托 QNS 工作室。几年来，QNS 工作室依托信息安全产业商会所属企业、信息产业部电子 15 所、信息产业部电子 54 所和解放军有关部门等单位的雄厚技术力量。

面向电信与广电的信息安全代理技术产业骨干集团拟以信息产业部电子 54 所为核心联合国家网络安全管理中心以及电信有关科研、企业机构，建立我国第一个通信系统代理技术的安全产业骨干企业群体。

面向军事与政法方面的代理技术产业骨干集团拟以郑州解放军信息工程大学为核心，联合信息产业部电子 15 所及其政法科研、企业等机构，建立我国第一个为公安、安全、军队服务的管理、服务平台安全代理技术的产业骨干企业群体。

面向金融、税收、财政、工商等经济领域代理技术产业骨干集团拟以武汉地区的大学、研究机构和信息安全企业联合我国为经济行业服务的科研、企业等机构，建立我国第一个民口系统的信息管理、服务与互操作性平台代理技术的产业骨干企业群体。

面向电力、交通、民航、铁路等领域测控系统代理技术产业骨干集团拟以国防科技大学为核心，联合电力、铁路、交通和民航等科研单位建立国家第一个测控系统安全产业代理技术的骨干企业。

国家基础设施信息安全实验室拟在广州，建立国家基础设施信息安全保障、监管、应急和威慑系统实验基地。在广州地区建立实验基地有全国最开放的实验环境，也最容易取得市场方面的推广有利条件。拟在国家网络与信息安全管理中心广州分中心、中山大学、华南理工大学、广东安全部门科技机构和为之服务信息安全企业为基础，联合相关部门建立实验

基地，其中包括建立一个代理技术的测评认证实验室。

第四章 关于建立分类产品标准化企业联盟

通过上述的技术发展趋势研究，在本白皮书中讨论的平台化问题是信息安全产业当前最突出的影响全局的大问题，也是商会认为几年内必须重点关注的技术方面的大问题。商会认为这些平台化的标准建设不能等待国家与有关部门工作安排，商会决定在商会的统一领导下，成立以商会成员为主的标准化机构的企业联盟建立互操作性的标准系列分类产品企业联盟。经过研究，商会认为首先成立如下的分类产品标准化企业联盟：

- 系统与网络安全防护产品企业联盟。
- 系统与网络安全检测与监控产品企业联盟。
- 安全管理平台产品企业联盟。
- C_TCP 产品企业联盟。
- TNP 产品企业联盟。
- CPK 产品企业联盟。
- 信息安全服务等级标准企业联盟。

这些标准化的企业联盟应当积极配合国家信息化安全标准机构和组织，积极、主动地提出上述方面的标准的建议。

另外关于信息化安全的数字标签标准化工作也要与各领域进行积极协商，推进其标准的建立，在适当时候也要成立相应的企业联盟。

商会已经决定在商会中正式成立“信息安全产业标准化企业联盟委员会”，申请挂靠在国家信息安全标准化委员会。

第五章 关于建立现代化的信息安全产品测评认证体系

我国信息安全产品测评认证发展目标：完善发展我国信息安全测评认证体系建设，推动我国信息安全测评技术发展与进步，满足我国信息安全产业的飞速发展对信息安全测评认证的需求；完善基础、标准、规范和重点突出自主可控的具有自主知识产权的信息安全测评产品系列，建立现代信息安全测评认证研发、服务和培训体系，促进我国信息安全产业安全产品换代升级；探索建立我国信息安全产业实施网络服务模式，缩小与国外发达国家信息安全测评认证的差距，加速建立我国信息安全保障体系和国家加入 WTO 后的技术壁垒体系。

完善我国信息安全测评人证标准体系。我国在信息安全测评认证标准的建设是与国际信息安全测评认证标准化机构颁布的标准接轨的。我国在 20 世纪 90 年代，相继出台了类似美国 TCSEC 的安全标准和一些网络防护的 PP 标准，ISO/IEC 15408 （GB/T18336）作为我国的测评认证标准。总之，我国信息安全标准制定工作与需求差距很大。需要制定的标准很多，许多可由企业出面解决，但是象信息安全测评认证标准和行业的用户信息平台标准，仅靠 IT 企业是建立不起来的。我国信息化技术标准工作随着国家的重视，除继续跟踪信息基础设施的标准外，我国要在一些应用领域制定自己的用户标准体系，一些急用标准如下：

- 用户应用平台标准，参照美国国防部的 COE 标准
- 制定用户的信息保障技术框架的方案类标准
- 制定网络远程服务的 PP 标准
- 制定信息安全产品 PP 标准

- 制定信息安全服务的技术标准
- 其它信息应用类的技术标准体系

以上标准，其主要目的在于我国进入 WTO 后，实施自我保护，规范国家信息安全产业市场的急用标准体系。

完善我国信息安全的培训教育体系，有些大学设立了信息安全专业，存在着严重的师资、教材和环境建设问题。许多大学的大学生学习信息安全采取的是黑客的方法，自己喜爱，靠天才和灵感，学习不系统，不全面。信息安全必须实施工程概念，要学习标准和规范，开展信息安全测评技术理论、标准、规范、方法与工具研发和教学，只有如此才能把信息安全工作从少数天才人员的艺术工作中解放出来，变成普通工程师能够从事的大众工作。形成从本科、硕士到博士研究生的培养机制，为我国信息安全测评认证工作的全面长期开展，提供应用实践和理论研究的组织和人才保证。

完善国内信息安全测评产品开发体系。必须建立芯片、硬件、操作系统、数据库管理系统、通信网络设备与系统、自动化控制设备和互操作性等专业领域的安全实验室。开发测试工具、配置工具、防护工具、攻击工具、监管工具、维护工具、诊断工具和监控工具等。建立一些面向行业（例如金融、电信、电力等）测评认证机构，实行面向行业特点的测评认证工作，与国家测评认证机构一起，相互支援和补充，构成更加完整的测评认证体系。

完善国内信息安全测评认证服务体系。测评认证的网络化服务是大势所趋，是 IT 企业实施服务低成本的主要措施之一，但是对于信息安全的网络化服务必须建立在可信的基础上，根据我国的特点，参考国外网络远程服务的管理办法，建立配置管理体系或中心（SSA-CM）是好方案。积极建立国家信息安全测评认证配置管理体系，国家测评认证配置管理体系宗旨是开展测评认证的网络服务业务、提供测评认证的前移服务。信息化配置管理体系的建设是国家或者领域进行信息化标准控制的体系。信息技术与产品的市场准入制度，在网络时代的控制，不是将“市场准入的证书”或者“测评认证的证书”挂在墙上，仅仅完成了所谓“法律概念”上的认证认可工作。国家的某些检测与测评机构，目前热衷于权利意义的批准程序，喜欢给企业和用户发证。但是他们忘了现代的信息化的测评认证工作是一种高水平的技术工作，需要有“金刚钻”，需要的实在的能力建设。测评认证工作实际上就是指导用户信息化建立方案的机构，也是引导信息产业发展的机构，更是信息化的服务与管理机构。我们再次建议，要建立国家、行业和领域的配置管理体系，实现和提高政府管理和指导信息化的能力（这也应当属于一种执政能力）。建立测评认证配置管理体系的网络服务活动，全面支持信息产业公共工业化的标准、质量、技术、工程、文档、核心实现、管理等方面远程服务工作，促进信息安全产业进步、换代和升级。信息产业提供的网络远程服务必须通过 SSA-CM 管理监控，纳入政府管理产品类（GOTS）。

第六章 关于建立我国信息安全产业发展和维权基金

信息安全产业的发展需要国家的重视与支持，需要持续发展的信息化安全的市场支持，需要一个强有力产业组织：商会和产业的骨干企业集团积极参与，需要发挥政府部门建立的信息安全产业基地或开发区作用，需要商业银行、金融投资机构和有实力的实业公司资金投入支持。

应当将安全产业商会、政府扶持产业发展资金投入、政府部门建立的信息安全产业基地和商业银行、金融投资机构及有实力的实业公司资金投入结合起来，共同组建我国信息安全产业发展基金。商会正在积极与有关方面密切协商。

在当前的市场环境中，同样存在着信息安全产业维权基金成立要求，商会也正在积极探索。

第七章 关于建立和完善企业技术与业务体系架构

我国信息安全产业已经进入开拓或发展期，建立和完善企业技术与业务体系架构是许多企业继续提高自身创新、研发和生产能力的重要举措，是企业进入规模发展的必经之路。另外，信息安全产业面临着多代理技术应用的巨大挑战，有许多新的技术需要我们去探索和研究。商会建议，有条件的企业应当针对自身特点，在树立良好的企业文化氛围中，在建立和完善企业管理体系中建立自己的技术与业务体系架构。

第八章 信息化安全建设的关键课题建议

根据前面分析与研究提出如下的信息化安全建设的关键课题建议；

8.1 信息化安全的理论课题

信息化安全作为一级学科必须建立自己的独立学科理论，《软件行为学》系列著作问世为建立这个理论学科奠定了基础。但是目前软件行为学理论学科框架，虽然已经有了一个详细的描述，但是软件行为学学科还需要更加细致描述与论证，需要更多地具体理论成果，需要数百个博士论文的正确结论来丰富它，需要一大批计算机科学工作者对软件行为学的研究，不断完善这个应用基础理论体系。同时，我们也可以感受现代科学研究的新风格、新模式和新机制。

我们认为可以在如下一些方面开展信息化安全理论课题的研究工作。

- 密码学理论研究
- 认证管理算法理论研究
- 软件、系统与网络行为学理论研究
- 网络行为控制理论研究
- 网络行为监管理论研究
- 网络行为认证理论研究
- 网络行为对抗理论研究
- 网络行为保密理论研究
- 网络数字警察学理论研究
- 网络信息战对抗理论研究
- 计算网格理论研究
- 多代理网格操作系统理论研究
- 面向模式的程序设计理论与方法研究
- 类型程序设计理论与方法研究
- 面向群体的程序设计
- 代理程序设计与代理软件工程理论研究
- 网络虚拟世界社会学研究
- 信息化安全总体理论研究

8.2 信息化安全的技术课题

信息化安全的技术的研究包括两个方面：信息化安全传统技术和信息化安全新技术。信息化安全传统技术是指针对网络物理世界软硬件和信息的语法范畴的安全观念或称之为经典安全概念的安全技术。信息化安全新技术是指针对网络虚拟世界行为安全和信息的语义范畴的内容安全观念或称之为现代可信概念的安全技术，也可以是传统信息化安全问题通过行为可信概念或方法解决问题的技术。

在信息化安全的传统技术方面研究包括：

- 数据安全技术
- 信息隐藏与发现技术
- 系统与网络防护技术
- 系统与网络安全检测、监控技术
- 安全管理平台技术
- 病毒、蓄意代码检测与消除技术
- 身份认证技术
- 业务连续性技术

在信息化安全的新技术方面研究包括：

- 可信计算平台技术
- 可信网络平台技术
- 多代理技术
- 数字标签技术
- 无第三方认证技术
- 监管信息化和信息化监管技术
- 网络对抗技术
- 多代理计算网格技术
- 多代理网格操作系统技术研究
- 多系统与多代理系统体系结构技术。

8.3 信息化安全的应用课题

我国信息化建设对 Agent 技术有无与伦比的市场需求，我们看一下在未来十年时间内我国必须要建设的一些全国性的信息化系统。而这些系统都必须采用代理技术，而且是主要的体系结构技术。

1、建立监管现代化和代理化体系，例如：

- 立项支持建立税收监管现代化系统
- 立项支持建立银行监管现代化系统
- 立项支持建立证券监管现代化系统
- 立项支持建立保险监管现代化系统
- 立项支持建立财政监管现代化系统
- 立项支持建立电信监控网络系统
- 立项支持建立电力监管/监控网络系统
- 立项支持建立民航航空管制监管/监控网络系统
- 立项支持建立铁路监管/监控网络系统

- 立项支持建立政法监管现代化系统
- 立项支持建立互联网内容与行为监管现代化系统
- 立项支持建立涉密网监管现代化系统
- 立项支持建立网络对抗现代化体系建设
- 立项支持建立全国网络数字警察体系

2、建立标签通信系统和安全标签网络系统，例如：

- 建立政府部门的信息安全标签体系
- 建立军事部门信息安全标签体系
- 建立互联网的信息安全标签体系
- 建立商务信息安全标签体系
- 建立金融企业的信息安全标签体系
- 建立文化类信息安全标签体系

3、建立无第三方身份与行为可信认证体系，例如：

- 建立个人服务代理无第三方身份与行为可信认证体系
- 建立企业服务代理无第三方身份与行为可信认证体系
- 建立企业的服务代理的无第三方身份与行为可信认证体系
- 建立政府行为监管代理的无第三方身份与行为可信认证体系
- 建立企业行为监管代理的无第三方身份与行为可信认证体系
- 建立管理代理的无第三方身份与行为可信认证体系
- 建立测试代理的无第三方身份与行为可信认证体系
- 建立军事代理的无第三方身份与行为可信认证体系
-

4、建立现代化的全国网络预警与应急体系，例如：

- 立项支持建立国土安全预警系统
- 立项支持建立全国卫生预警系统
- 立项支持建立全国农业预警系统
- 立项支持建立全国林业预警系统
- 立项支持建立全国金融风险预警系统
- 立项支持建立全国电力等能源预警系统
- 立项支持建立全国环境预警系统
- 立项支持建立全国自然灾害预警系统
- 等

5、建立现代化的全国网络定位与反定位体系，例如：

- 立项支持建设计算机网络定位系统（URL，Uniform Resources Locator），在互联网的 WEB 系统以及设备 BIOS、OS 等系统上建立定位资源系统）包括 IP 电话定位、计算机（含 PDA）拨号上网定位、入侵源定位、DDOS 源定位。
- 立项支持建立和完善我国通信网络的定位系统，该系统要综合处理电话定位、移动电话定位、干扰源定位、插播定位、入侵源定位和 DDOS 源定位等功能。
- 立项支持建立我国自主产业 BIOS 基础上采用 Agent 技术体系的网络定位系统。
- 立项支持开展对基础设施网络有关定位系统的漏洞检测研发工作。
- 立项支持建立 GPS 反干扰与插播的检测系统。
- 立项支持建立电话定位系统漏洞检测系统。
- 立项支持建立移动通信的基站定位系统漏洞检测系统。

- 立项支持建立计算机网络定位系统漏洞检测系统。
- 等

6、建立服务高技术化和代理化体系，例如：

- 立项支持建立电子政务信息化系统之间的互操作性服务平台
- 立项支持建立电子商务信息化系统之间的互操作性服务平台
- 立项支持建立金融信息化系统之间的互操作性服务平台
- 立项支持建立财政信息化系统之间的互操作性服务平台
- 立项支持建立政法系统信息化系统之间的互操作性服务平台
- 立项支持建立产业信息化系统之间的互操作性服务平台
- 立项支持建立个人助理服务平台与系统
- 立项支持建立测试、管理服务平台与系统
- 立项支持建立网络远程服务平台与系统
- 立项支持建立科学试验服务平台与系统
- 等

要完成上述如此特点的全国性、大范围的信息化系统，采用的主流信息化的体系结构将是代理技术体系。如果没有一个规模产业的支持，这些与国家基础设施安全、可信、有效利用密切相关的建设，将是不可能的。这些系统的建设，可以说比任何其它信息化建设都要求自主开发，很难采用国外的同类产品。

8.4 信息化安全的产业发展课题

- 建立国家基础设施信息安全产业结构调整项目总体单位和实现可信网络平台总体框架和标准化工作。
- 建立面向电信与广电的信息安全代理技术产业骨干集团和实施可信网络平台系统自主开发。
- 建立面向电力、交通、民航、铁路等领域测控系统代理技术产业骨干集团和实施可信网络平台系统自主开发。
- 建立面向金融、税收、财政、工商等经济领域代理技术产业骨干集团和实施可信网络平台系统自主开发。
- 建立面向军事与政法方面的代理技术产业骨干集团和实施可信网络平台系统自主开发。
- 建立国家基础设施信息安全实验室和实施可信网络平台系统自主开发。
- 建立金融信息安全测评认证机构
- 建立电力信息安全测评认证机构
- 建立国家信息化安全配置管理中心
- 建立金融信息化安全配置管理中心
- 建立电力信息安全配置管理中心
- 建立电信安全配置管理中心

结束语

我国信息安全产业发展虽然取得了较大成绩，但是依然存在很多问题。信息安全产业发展面临产业结构调整、开拓新市场领域，实现全面的技术创新的艰巨任务。同时存在着基础、市场、法律、政府指导等多方面的环境问题。信息化安全标准与技术法规建设还相当滞后，有待进一步的加强。商会相信，在国家与各级政府的大力支持下，在全体信息安全产业同人的共同努力下，我国信息安全产业一定会取得更加辉煌的成绩。

参考文献

中国信息产业商会信息安全产业分会，《我国信息安全产业调研与建议（2002 年）》
中国信息安全协会，《中国信息安全年鉴（2002—2003）》
中国信息产业商会信息安全产业分会 2002 年到 2004 年的简报
中国信息产业商会信息安全产业分会，中国信息安全产业反不正当公约