信息安全问题刍议

文／王寅生·哈尔滨市信息产业局

“十一五”期间，电子政务和社会信息化建设将带动企业信息化发展。企业信息化与工商、税务、社保、医保和金融等部门的互联互通。跨区域、跨行业的信息服务平台（如网上支付、信用体系、第三方认证）的网上信息消费、服务消费和产品交易，成为了信息时代的“寻常事”。

因此，基于互联网络的信息技术热点应用，冲击着政治、经济、文化和生活领域。网络时代的到来，使得信息安全问题，成为了迫切需要解决的、复杂的、具体的而且现实的问题，也成为了我们在每一天的工作和生活当中必须面对的和不容忽视的问题。健全政策法规、建设网络环境、净化网络行为、规范安全标准、搭建产业基础、推进基础产业、强化技术保障、完善信息安全基础设施等方面工作，是今后信息化建设和信息产业发展的信息安全保障。

一、电子政务的信息安全需求

电子政务改变了传统的生活模式和工作流程，提高了效率。但是，病毒破坏、黑客入侵、重要信息泄漏等危害越来越大。

国家规定“涉及国家秘密的计算机信息系统，不得直接或间接与国际互联网或其它公共网络联接，必须实行物理隔离”。即使用终端隔离、信道隔离、网络和服务器隔离等多种技术来构建内外网；阻断内外网的物理传导，不能从外网侵入内网，防止内网信息泄漏到外网；隔断内外网的物理辐射，内网信息不通过电磁辐射或耦合方式泄漏到外网；隔离内外网的物理存储，防止残留信息窜到外网；内外网的信息要分开存储；严格限制使用软盘、光盘等可移动介质。

对于政务内网，即政府部门内部的关键业务管理系统和核心数据应用系统，需要采用包括身份鉴别、访问控制、特殊协议和通讯技术、访问控制、数据保密、数据完整、数据校验、防止否认、审计管理、可用性和可靠性等安全措施。

对于政务外网，即政府部门内部以及部门之间的各类非公开应用系统，需要CA认证、加密传输、防火墙技术、VPN、漏洞检测与在线黑客监测预警、实时审计、网络防病毒、自动备份恢复等安全技术。包括公钥管理基础设施（PKI）、密钥管理基础设施（KMI）和授权管理基础设施（PMI）。

对于与互联网相联的外网，面向社会提供一般应用服务及信息发布。以防火墙、代理服务器、入侵检测等安全技术进行逻辑隔离，阻止黑客和内部用户的入侵和破坏，满足信息安全要求。但是，这些技术难以解决进口计算机核心软硬件的后门和漏洞等问题。

二、信息安全管理体系与信息安全产业基地建设要求

目前我国的信息安全管理，依靠传统的管理方法和手段来实现，缺乏现代的系统管理技术，技术手段有限。

国际标准BS7799和ISO/IEC17799是流行的信息安全管理体系标准。其中的管理目标为数据的保密性、完整性和可用性要求，具有自组织、自学习、自适应、自修复、自生长的能力和功能，保证持续有效性。通过“计划、实施、检查、措施”四个阶段周而复始的循环，应用于其整体过程、其他过程及其子过程，例如信息安全风险评估或者商务持续性计划的安排等，为信息安全管理体系与质量管理体系、环境管理体系等的整合运行提供了方便，在模式和方法上都兼容，成为统一的内部综合管理体系。包括按照可信网络架构方法，编制信息安全解决方案，多层防范、多级防护、等级保护、风险评估、重点保护；针对可能发生的事故或灾害，制定信息安全应急预案，建立协调机制、规避风险、减少损失；根据相应的政策法规，在网络工程、数据设计、建设和验收等阶段实行同步审查，建立完善的数据备份、灾难恢复等应用，确保实时、安全、高效、可靠的运行效果。

2000年国家863信息安全产业（东部）基地落户浦东张江高科技园，形成了国内最大规模的国家级信息安全产业基地。其中包括国家信息安全基础研究中心，主要研究电子政务等重大信息化工程，构建信息安全支撑平台和信息安全应用平台。国家信息安全工程研究中心，承担国家科技攻关电子政务和信息安全重大专项课题，

承担多项信息安全标准起草任务。国家863计划反计算机入侵和防病毒研究中心，承担“网络病毒防治关键技术”和“电子物证保护及分析技术”等项目，建立“计算机病毒库”、“计算机漏洞”和“打击计算机犯罪侦查技术研究”等实验室。上海交大信息安全学院，研制防火墙、网页防篡改系统、内容监管系统、安全邮件系统等，人才培养和科研开发同步进行。

三、信息安全发展所面临的问题与挑战

1．信息安全建设资金投入不足

信息化投入占总资产的0.75%，与国外大企业8%至10%相差甚远；用于系统开发、IT产品采购、信息安全的费用并不宽裕。2004年对信息安全的平均投入占IT预算的总体比在亚太地区为17%。

2．用人机制僵化，难以引进优秀人才

信息化人才特别是信息安全人才匮乏且流失严重。企业每百人中，信息技术人员还不到一人，其中信息安全技术骨干人才更是稀缺，严重制约着信息安全建设。

3．“信息孤岛”问题严重

系统集成、资源共享和信息安全水平低，缺乏总体规划、总体设计和过程控制。亚太地区80%的公司受到过计算机病毒攻击，40%的站点不修复补丁导致了不安全，25%的站点由于财政紧张受到安全威胁。

4．信息安全技术的基础薄弱

国内IT产业和信息安全技术的产品结构不合理、基础薄弱、技术水平低，不能满足信息化建设需求。除PC机、财务应用软件外，高端技术和产品受控于国外企业。

5．网络安全在不断发展

网络安全，已经从网络层建设开始向应用层的内容建设过渡，新要求的内容安全，即通过内容安全设备，例如通过互联网控制网关，用户可以降低安全风险、杜绝不良信息、节约网络资源、提高工作效率，使得人们在互联网上的行为得到一定的管理和约束。目前，中央明确了加大“信息安全”建设力度。我国网络安全方面的投入，将在2010年突破100亿元，其中增长最快的将是网络内容安全设备。

6．信息安全问题，将是信息产业的产业安全问题

除了需要在计算机网络的应用层研发和推广网络安全产品以外，还需要在网络层和协议层等技术底层研发具有自主知识产权的关于管理和通信等协议的网络安全产品，构建基于TCP/IP等协议构架上的Internet/Intranet网络安全体系，研发具有自主知识产权的基础软件，建立信息安全的（软件）产业基础。国家要鼓励和发展具有自主知识产权的软件产业和集成电路产业，建立信息安全的基础产业。