信息安全标准研制进展

□ 李留英 / 南京政治学院上海校区军事信息管理系 上海 200433

摘要：信息安全标准已成为国际网络空间竞争的前沿和焦点，国际组织和世界各国政府均在加紧相关问题研究。文章围绕信息安全标准，分析了国内外信息安全标准的研制现状，研究了云计算安全标准和工业控制系统信息安全标准的研制进展，从而为国内信息安全标准的推进提供借鉴。

关键词：标准，信息安全，云计算安全，工业控制系统安全
DOI：10.3772/j.issn.1673—2286.2014.02.001

随着各国对网络空间的重视，信息安全的地位日益突出，信息安全标准已成为国际网络空间竞争的前沿和焦点。为保障国家安全，许多国家都在积极制定符合本国国情的信息安全标准，以更好地指导信息安全实践活动，维护国家利益。

从制定机构来看，信息安全领域的标准主要分为国际标准、国家标准、行业标准和地方标准。国际标准是由国际标准化组织或国际标准组织通过并公开发布的标准；国家标准是由国家标准机构通过并公开发布的标准；行业标准是某个行业范围内统一的标准，一般由行业标准归口部门统一管理。地方标准又称为区域标准，一般由省、自治区、直辖市标准化行政主管部门制定。

1 国际信息安全标准研制概况

国外在20世纪70年代中期开始信息技术安全标准化工作，目前有近300个国际和区域性组织制定标准或技术规则，他们工作各有特点，制定标准的层次不同，也有部分工作重叠，已经制定了大量的信息安全标准。其中以美国、英国制定的标准比较先进。

1.1 信息安全国际标准组织

目前，有许多与信息安全标准化有关的国际标准组织，如国际标准化组织（ISO）、国际电工委员会（IEC）、国际电信联盟（ITU）和Internet工程任务组（IETF）等。ISO/IEC JTC1（信息技术标准化委员会）所属SC27（安全技术分委员会）是信息安全领域代表性的国际标准化组织，主要从事信息技术安全的一般方法和技术的标准化工作，ISO/TC68负责银行业务的信息安全标准制定。IEC与ISO联合成立的ISO/IEC JTC1负责开放系统互连、密钥管理、数字签名、安全评估等方面的标准制定。

ITU侧重于通信网络标准的制定，所属SG17组负责网络安全标准，包括通信安全项目、安全架构和框架、计算安全、安全管理、安全通信服务等。SG16和下一代网络核心组负责通信安全及下一代网络安全等标准的研究。

IETF是全球互联网最具权威性的开放性技术标准化组织，主要负责互联网标准的研发和制定。IETF的实际工作包括八个研究领域，其中安全研究领域（sec-Security Area）含21个工作组[1]，IKE和IPSec都在IETF的RFC系列之中，还包括电子邮件、网络认证和密码及其他安全协议标准。

1.2 国际信息安全标准概况

从内容看，信息安全标准主要分为互操作类标准、技术与工程标准、信息安全管理与控制标准三大类。

互操作标准主要包括：对称加密标准DES、3DES、IDEA以及AES，非对称加密标准RSA，传输层

加密标准SSL，安全电子邮件标准S-MIME，安全电子交易标准SET，通用脆弱性描述标准CVE。这些被普遍采用的安全算法和协议是事实标准。

技术与工程标准主要包括：信息产品通用测评准则（ISO15408），主要支持产品IT安全特征的技术性评估，是评估信息技术产品和系统安全性的基础准则；信息安全橘皮书（TCSEC）是美国国家计算机安全中心（NCSC）于1983年提出的可信计算机系统评估准则，将安全分为安全政策、可说明性、安全保障和文档四个方面和七个安全级别（D、C1、C2、B1、B2、B3、A)；安全系统工程能力成熟度模型（SSE-CMM），定义了一个组织的安全工程必须包含的本质特征，是安全工程实施的度量标准。

信息安全管理与控制标准方面，英国标准协会（BSI）制定的BS 7799已成为世界上应用最广泛的信息安全标准。BS 7799是一项通行的信息安全管理标准，旨在为组织实施信息安全管理体系（Information security management systems，简称ISMS）提供指导性框架。BS 7799标准由BS 7799-1和BS 7799-2组成。BS 7799-1：1999《信息安全管理实施细则》于2000年采纳为国际标准ISO/IEC 17799-1：2000《信息技术-信息安全管理实施细则》。BS 7799-2《信息安全管理体系规范》详细说明了建立、实施和维护信息安全管理体系的要求。

美国国家标准技术协会（NIST）为美国政府和商业机构制定相关信息安全标准和技术指南。2003年NIST启动了为期10年的标准规划，形成了策略规划、风险管理、安全意识培训和教育、安全技术以及安全控制措施的一整套信息安全管理体系。

2005年4月，国际上正式通过了信息安全管理体系ISO/IEC 27000系列标准的开发计划。该系列的标准序号已预留到27019，其中27000至27009是基本标准，27010至27019是预留的解释性文档与文档。较著名的包括：

ISO/IEC 27000《信息安全管理体系概述和术语》，规定27000系列标准所共用的基本原则、概念和词汇。

ISO/IEC 27001《信息安全管理体系要求》规定了一个组织建立、实施、运行、监视、评审、保持、改进信息安全管理体系的要求。该标准与ISO/IEC 17799共同使用，一个组织在按照27001实施其ISMS的过程中，应首先选择17799中推荐的控制措施。

ISO/IEC 27002《信息安全管理实用规则》包括11个安全类别、39个控制目标、138个安全控制措施，是实施ISO/IEC 27001的支撑标准，阐述了组织建立信息安全管理体系时应选择实施的控制目标和控制措施集；是一个行业最佳惯例的汇总集。

ISO/IEC 27003《信息安全管理体系实施指南》，提供27001具体实施的指南，包括PDCA过程的详细指导和帮助。

ISO/IEC 27004《信息安全管理测量》，主要是测量组织信息安全管理体系实施的有效性、过程的有效性和控制措施的有效性。

ISO/IEC 27005《信息安全风险管理》，以ISO/IEC 13335-2《信息技术信息和通信技术安全管理第2部分：信息安全风险管理》为基础，描述了信息安全风险管理的一般过程及每个过程的详细内容。

其他已经发布的包括ISO/IEC 27006《信息安全管理体系审核和认证机构的要求》，ISO/IEC 27011《基于ISO/IEC 27002的电信组织的信息安全管理指南》、ISO/IEC 27035《信息安全事件管理》、ISO/IEC 27044《安全信息和事件管理（SIEM）》[2]。

随着云计算等新技术新应用的快速发展，相关的标准化工作也在逐步研制与探讨制定中，以便为技术应用提供有力支撑。

2 中国信息安全标准研制概况

相比国外，国内信息安全标准化工作起步较晚。2002年4月15日成立的全国信息安全标准化技术委员会（简称信标委）在国家标准委和工信部的共同领导下，设置了7个工作组，分别是信息安全标准体系与协调工作组（WG1）、涉密信息系统安全保密标准工作组（WG2）、密码技术工作组（WG3）、鉴别与授权工作组（WG4）、信息安全评估工作组（WG5）、通信安全标准工作组（WG6）和信息安全管理工作组（WG7）。它们对我国信息安全保障体系建设和信息安全产业的发展起到积极作用[3]。

信标委主要负责组织开展国内信息安全领域的安全技术、安全机制、安全服务、安全管理、安全评估等的标准化技术工作。目前，已经制定了一批信息安全保障体系急需的、基础的、关键的信息安全标准，为国家重大信息化工程和信息安全保障体系建设提供重要的标准支撑。

信标委的主要任务是向国家标准化委员会提出本专业标准化工作的方针、政策和技术措施的建议，同时将协调各有关部门，提出一套系统、全面、分布合理的信息安全标准体系。我国信息安全标准体系，是在跟踪分析了国际信息安全标准的发展动态和国内信息安全标准需求的基础上，提出的标准体系框架和标准体系表。其中我国信息安全技术标准总体上划分为基础标准、技术与机制标准、管理标准、测评标准、密码技术和保密技术六大类，每类按照标准所涉及的内容细分若干小类。

在我国，另一个与信息安全标准有关的组织就是中国通信标准化协会下设的网络与信息安全技术工作委员会，下设四个工作组，即有线网络安全工作组（WG1）、无线网络安全工作组（WG2）、安全管理工作组（WG3）、安全基础设施工作组（WG4）。

我国信息安全标准工作处在积极学习先进、努力结合实际、力图创造具有自主特色的国家标准的形势下。为了更好地贯彻《国家信息安全标准“十一五”规划》，推进我国信息安全工作，引进了国际上著名的ISO/IEC27001：2005《信息安全管理体系要求》和ISO/IEC17799：2005《信息安全管理实用规则》、ISO/IEC15408：1999《IT安全评估准则》、SSE-CMM《系统安全工程能力成熟度模型》等信息安全管理标准。

为深入贯彻落实国家信息安全等级保护制度，配合信息安全等级保护的实施和推进，根据《信息安全等级保护管理办法》（公通字[2007]43号）和《信息安全等级保护测评工作管理规范（试行）》，制定发布了GB 17859-1999《计算机信息系统安全保护等级划分准则》、GB/T 25058-2010《信息安全技术信息系统安全等级保护实施指南》、GB/T 22239-2008《信息安全技术信息系统安全等级保护基本要求》、GB/T 22240-2008《信息安全技术信息系统安全等级保护定级指南求》以及GB/T 25070-2010《信息系统等级保护安全设计技术要求》等。各重点行业，根据需求积极推进等级保护的实施。

目前，信息安全标准化工作正按照《国家信息安全标准“十二五”规划》要求，加强信息安全国家标准战略研究，开展信息安全标准体系的整体规划和顶层设计，加快新技术新应用标准研究和信息安全国际标准的转化（主要是国际ISO/IEC 17799和ISO/IEC 13335的采标工作），对促进信息安全工作起到了良好的推进作用。

3 新技术新应用信息安全标准研制现状

随着云计算、物联网、大数据等新技术的应用，对云计算安全标准的研究日渐增多。目前，云计算领域还缺乏统一的国际通用标准和指南。

3.1 云计算安全标准研制现状

国际标准化组织ISO的SC27于2010年启动《云计算安全和隐私》，目前已经确定了云计算安全和隐私的概念体系框架，出台了ISO/IEC 17788《云计算-词汇》和ISO/IEC 17789《云计算-参考框架》；SC27/WG1组制定了ISO/IEC 27017《基于ISO/IEC 27002的云计算服务的信息安全控制措施实用规则》，为云服务客户和云服务提供者双方提供云服务特定的安全控制及其实现指南；SC27/WG5组制定了ISO/IEC 27018《公共云计算服务的数据保护控制措施实用规则》[4][5]。该标准适用于所有机构和组织。SC27/WG4组制定了ISO/IEC 27036-5《供应商关系信息安全第5部分：云服务安全指南》。

ITU-T于2010年成立了云计算焦点组，从电信角度为云计算提供支持，发布了《功能要求和参考架构》、《基础设施和网络云》和《云安全、威胁和要求》等7份报告。2011年12月之后，云计算焦点的工作逐渐分散到云计算工作组SG13和云计算安全组SG17，SG17主要承担云计算安全方面的工作，关注《云计算高层安全框架》、《云计算运行安全指南》等。

云安全联盟（CSA）是一个成立于2009年的非赢利组织，发布的《云计算关键领域安全指南》是业界最重要的参考文献。2011年4月开始，CSA与ISO和IEC开始一起进行云计算安全标准的研究。

为配合美国云计算战略，2010年NIST成立了包括云计算安全工作组在内的5个云计算工作组，牵头制定云计算标准和指南。目前已经发布多个研究成果，如SP800-144《公有云中的安全和隐私指南》，《云计算安全障碍和缓解措施列表》、《美国联邦政府使用云计算的安全需求》、《美国政府云计算安全评估与授权的建议》等[6]。美国政府高度重视云计算安全和隐私，于2011年发布《联邦云计算战略》，启动联邦风险和授权管理项目（FedRAMP），以规范企业的云服务质量。

欧盟于2009年开始云计算研究工作，欧洲网络与信息安全局（ENISA）已经发布了《云计算中信息安

全的优势、风险和建议》、《政府云的安全和弹性》、《ENISA云计算信息保证框架》、《政府云的安全性与复原力》。2012年出台《云计算合同安全服务水平监测指南》，提供了一套持续检测云计算服务商服务级别协议运行情况的操作体系。

中国有多个机构从事云计算标准研究制定。信标委于2011年9月完成《云计算安全及标准研究报告V1.0》，目前正在研究《政府部门云计算安全》和《基于云计算的因特网数据中心安全指南》等标准，SOA标准工作组开展了智慧城市、云计算技术和相关产品的标准研究工作，提出了我国智慧城市基础参考模型和智慧城市标准体系，出版了《云计算标准化研究报告》，推动了31项相关标准项目研制[7]。

2012年，信标委成立云计算工作组和非结构化数据管理工作组，重点对美国政府云安全管理思路、云计算安全审查机构职能和流程、云安全国际标准等进行研究，正积极开展我国云计算标准体系框架研究和十二项云计算国家标准的编制，提出了《政府部门云计算服务安全指南》和《政府部门云计算服务安全能力要求》。《政府部门云计算服务安全指南》为政府部门使用云计算服务提供管理指导，《政府部门云计算服务安全能力要求》为政府部门使用云计算服务的信息系统进行了技术规范，对服务提供商的云计算服务提出了安全保障要求。

3.2 工业控制系统信息安全标准研制现状

工业控制系统（ICS）是国家重要基础设施（如电力、交通、能源、通信、水利、金融等）的中枢神经。2010年10月伊朗核电站遭受“震网”（Stuxnet）病毒的破坏，为工业生产控制系统安全敲响了警钟，也引起了各国对国家基础设施及工业控制系统安全的关注。ISO、NIST、IEC和国际自动化协会（ISA）均对工业控制系统的信息安全标准化开展了一系列研究。

2011年ISO下属的SC27开始关注智能电网的信息安全标准化工作。IEC/TC65（工业过程测量、控制和自动化）的网络和系统信息安全工作组WG10与ISA 99委员会成立联合工作组，共同制定IEC 62443《工业过程测量、控制和自动化 网络与系统信息安全》系列标准。

NIST依据2002年《联邦信息安全管理法》等编制了SP 800-82《工业控制系统（ICS）安全指南》，该指南适用于电力、水利、石化、交通、化工、制药等行业的ICS系统。出台的SP 800-53《联邦信息系统推荐安全控制》对工业信息系统具有指导意义[8]。

目前中国芯片、操作系统等软硬件产品，以及通用协议和标准90%以上依赖进口，对基础网络、重要信息系统和工业控制系统信息安全带来严峻挑战[9]。2011年9月，工业和信息化部发布《关于加强工业控制系统信息安全管理的通知》（工信部协[2011]451号），明确了工业控制系统信息安全管理的组织领导、技术保障、规章制度等方面的要求。2011年底，工业和信息化部对全国重要工业控制系统信息安全进行全面调查，在2012年启动了重点企业、重点领域的检查。2012年6月28日国务院《关于大力推进信息化发展和切实保障信息安全的若干意见（国发〔2012〕23号）》明确要求保障工业控制系统安全。

我国的信标委（TC260）、全国电力系统管理及其信息交换标准化技术委员会（TC82）、全国工业过程测量和控制标准化技术委员会（TC124）和全国电力监管标准化技术委员会（TC 296）也开展了一系列研究。TC260提出了工控系统信息安全标准体系，正在研制《信息安全技术SCADA系统安全控制指南》和《信息安全技术安全可控信息系统（电力系统）安全指标体系》。TC82已经发布《电力系统管理及其信息交换数据和通信安全》部分标准。TC296正在研制《电力二次系统安全防护标准》、《电力信息系统安全检查规范》、《电力行业信息安全水平评价指标》等标准。

4 结语

本文围绕信息安全标准研制进展，分析了国内外信息安全标准的概况，研究了云计算信息安全标准和工业控制系统信息安全标准的研制进展，从而为大数据、社交网络等新技术新应用的信息安全标准的制定提供借鉴。

参考文献

[1] IETF互动百科[EB/OL]. [2013-12-16]. http://www.baike.com/wiki/IETF.

[2] 上官晓丽,杨建军. 2012年信息安全国际标准化趋势和我国提案进展[J].标准化研究,2013(1):48-52.

[3] 全国信息安全标准化技术委员会[EB/OL]. [2013-12-16]. http://www.tc260.org.cn.

[4] 颜斌.云计算安全相关标准研究现状初探[J].信息安全与通信保密,2012(11):66-68.

[5] 王惠莅,杨晨,杨建军.云计算安全和标准研究[J].信息技术与标准化,2012(5):18-21.

[6] 王惠莅,杨晨,杨建军.美国NIST云计算安全标准跟踪及研究[J].信息技术与标准化,2012(6):49-52.

[7] 蔡永顺,雷葆华.云计算标准化现状概览[J].电信网技术,2012(2):22-26.

[8] 杨建军,唐一鸿.工业控制系统信息安全标准化[J].信息技术与标准化,2012(3):20-23.

[9] 李鸿培,忽朝俭,于旸,等.工业控制系统的安全性研究[J].中国计算机学会通讯, 2013,9(9):37-42.

作者简介

李留英（1972-），女，博士，南京政治学院上海校区军事信息管理系教授，硕士生导师，研究方向：信息安全、信息化。E-mail: lly003@vip.sina.com

Progress in the Research of Information Security Standards

Li Liuying / Department of Military Information Management, Shanghai Branch of Nanjing Political College, Shanghai, 200433

Abstract: Information security standards has become a frontier and focus of the international cyberspace competition, international organizations and governments of around the world are stepping up research on related issues. This paper focuses on the information security standards, analyses the development status of national and international information security standards, research progress in the development of information security standards in cloud computing and industrial control systems, in order to provide a reference for national information security standards.

Keywords: Standard, Information security, Cloud computing security, Industry control system security

（收稿日期：2014-01-08）