中华人民共和国公安部

公信安〔2018〕843号

关于组织撰写第七届全国网络安全等级保护技术大会论文的函

为贯彻落实中央领导关于网络安全工作的重要指示精神以及《中华人民共和国网络安全法》的相关要求，深化国家网络安全等级保护制度和信息通报预警工作，推进网络安全等级保护技术交流和工作开展，由我局指导，信息产业信息安全测评中心承办的第七届全国网络安全等级保护技术大会（ICSP'2018）将于2018年9月召开（具体时间另行通知）。本届会议拟邀请中央网信办、国家保密局、国家密码管理局等部门担任指导单位。届时，公安机关、网络安全职能部门、网络安全领域的院士专家学者、行业用户和网络安全企业等将围绕新时代网络安全等级保护技术动态、关键信息基础设施安全保护策略和机制、新技术新应用安全风险和管控、网络安全产品、漏洞隐患监测分析、渗透测试、攻防等，就最新研究成果、技术路线、解决方案、最佳实践等进行研讨和交流。作为会议的一项重要成果，将出版大会论文集，其中，经专家评选的部分优秀论文，将推荐至国家核心期刊发表。请你单位结合网络安全等级保护工作和网络与信

息安全信息通报工作开展情况，根据征文要求（见附件），组织力量撰写论文，积极投稿。

附件：第七届全国网络安全等级保护技术大会征文要求

公安部第十一局

2018年4月4日

附件：

第七届全国网络安全等级保护技术大会
征文要求

一、 征文范围

（一）新形势下安全保护策略和机制：《网络安全法》明确规定国家实施网络安全等级保护制度。网络安全等级保护制度进入2.0时代，如何深入落实网络安全等级保护制度，在网络安全防护策略、机制、技术、产品等方面加强创新，主动适应等级保护制度的新要求；如何加强关键信息基础设施保护与国家网络安全等级保护制度的有效衔接；如何建立网络安全效能评估、网络安全保障工作评价机制、应急响应机制、应急响应技术体系、安全监测和通报预警机制等。

（二）新技术应用的等级保护管理和技术：下一代互联网（IPv6）、云计算、物联网、移动互联网、大数据、工业控制系统的网络安全等级保护建设和管理内容。如何确定定级对象、如何确定安全保护级别、如何开展安全建设、如何开展等级测评，如何构建网络安全保护管理和技术体系。新技术新应用的等级保护基本要求、安全设计技术要求、等级测评要求等安全标准研究与验证实践经验。

（三）网络安全等级保护安全建设技术：信任体系模型与构建技术、可信计算技术、人工智能技术、密码技术、灾难恢复与备份技术、主动防御技术、漏洞检测技术、网络攻

击分析与防范、软件安全技术等。如何利用虚拟机、沙箱技术、黑白名单技术和产品联动技术加强对重要信息系统的保护。

（四）网络安全等级保护测评技术：标准符合性检验技术、安全基准验证技术、无损检测技术、渗透测试技术、逆向工程剖析技术、源代码安全分析技术等。

（五）网络安全等级保护的安全监管技术：用于支撑安全监测的数据采集、挖掘与分析技术，用于支撑安全监管的敏感数据保护技术、安全态势评估技术、安全事件关联分析技术、安全绩效评估技术等。如何利用大数据技术、审计措施进行设备关联分析、日志存储与分析，解决网络攻击的可发现、可追溯问题。

（六）应急与事件处置技术：态势感知技术、安全监测技术、通报预警技术、安全事件检测（识别）响应技术、应急处置技术、灾难备份技术、恢复和跟踪技术、风险评估技术、入侵检测技术等。

（七）网络安全通报预警机制建设：网络安全信息通报预警机制建设的主要内容，态势感知与通报预警技术平台建设，如何利用大数据技术支持态势感知与通报预警工作。

（八）网络安全产品研究：产品检测策略、技术，国内外网络安全产品性能比较，产品的安全性检测，国外新技术、新产品研究等。

（九）国外网络安全基础研究：国外网络安全战略、策略、管理等研究，国外网络安全新技术研究，国外网络安全新标准研究。

二、投稿要求

（一）来稿内容应属于作者的科研成果，数据真实、可靠，未公开发表过，引用他人成果已注明出处，署名无争议，论文摘要及全文不涉及保密内容。

（二）会议只接受以 Word 排版的电子稿件，稿件一般不超过 10 页（5000 字）。

（三）稿件以 Email 的方式发送到会议征稿邮箱 zhangj@itstec.org.cn。

（四）凡投稿文章被录用且未作特殊声明者，视为已同意授权出版。

（五）论文提交截止日期：2018 年 7 月 30 日。

三、联系方式

通讯地址：北京市海淀区北四环中路 211 号华北计算技术研究所

邮编：100083

联系人：张洁、陈愚

联系电话：010-89055525　18612673329

010-89055529　13810717212