

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安全等级保护工作，推进网络安全等级保护技术研究和交流，公安部决定召开第七届全国网络安全等级保护技术大会。

会议的主要任务是：深入学习贯彻中央领导关于网络安全工作的重要指示精神，全面落实《中华人民共和国网络安全法》的要求，总结推广网络安全等级保护工作成果，交流网络安全等级保护技术研究成果，部署下一阶段网络安全等级保护工作。

会议的主要任务是：深入学习贯彻中央领导关于网络安全工作的重要指示精神，全面落实《中华人民共和国网络安全法》的要求，总结推广网络安全等级保护工作成果，交流网络安全等级保护技术研究成果，部署下一阶段网络安全等级保护工作。

会议的主要任务是：深入学习贯彻中央领导关于网络安全工作的重要指示精神，全面落实《中华人民共和国网络安全法》的要求，总结推广网络安全等级保护工作成果，交流网络安全等级保护技术研究成果，部署下一阶段网络安全等级保护工作。

会议的主要任务是：深入学习贯彻中央领导关于网络安全工作的重要指示精神，全面落实《中华人民共和国网络安全法》的要求，总结推广网络安全等级保护工作成果，交流网络安全等级保护技术研究成果，部署下一阶段网络安全等级保护工作。

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



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》

明确规定国家要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，

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、安全基础验证技术、漏洞检测技术、渗透测试技术、攻击面建模分析技术、操作安全分析技术等。

（五）网络安全等级保护的安全监督技术：用于实施安全监督的安全监测系统，包括审计分析技术、异常检测安全监督技术、安全事件分析技术、安全事件溯源技术等。

（六）网络安全等级保护的安全防护技术：入侵检测、入侵

表现、可追溯问题。

（六）网络安全等级保护关键技术：态势感知技术、安全检测技术、通报预警技术、安全事件检测（溯源）响应技术、应急处置技术、灾难备份技术、恢复和恢复技术、风险评估技术、入侵检测技术等。

（七）网络安全等级保护预警机制效果：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。如和现状未发生网络安全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、论文发表截止日期：2018 年 7 月 30 日。

三、联系方式

联系地址：北京市怀柔区北口镇中环路 221 号中国计算机技术研究所

邮编：100085

联系人：张婧、陈静

联系电话：010-89045829 18612679929

010-89045829 13816717312