

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》等法律法规，深入贯彻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、信息产业和信息化标准研究所牵头组织编写《网络安全等级保护实施指南》一书，已于2017年9月召开《网络安全等级保护实施指南》编写工作组第一次会议，明确了编写任务分工和工作计划，明确了编写、审核、出版等环节的工作职责。目前，编写工作正在有序推进中。为进一步提升编写工作水平，我局拟邀请网络安全等级保护领域专家、学者、企业技术人员等，围绕《网络安全等级保护实施指南》相关内容，撰写第七届全国网络安全等级保护技术大会论文。现将有关事项函告如下：

一、会议名称：第七届全国网络安全等级保护技术大会

二、会议时间：2018年10月27-29日

三、会议地点：北京

四、会议主题：网络安全等级保护实施指南解读与案例分析

五、论文征集范围：网络安全等级保护实施指南解读、案例分析、实践经验、技术创新等。

六、论文征集截止时间：2018年9月30日

七、论文征集方式：通过邮件或现场提交。

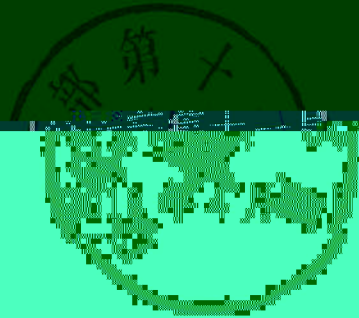
八、论文征集邮箱：[email address]

九、论文征集联系人：[name]

十、其他事项：[other information]

息安全信息通报工作开展情况，积极报送安全成果（详见附件），
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



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) 普及性技术(包括传统信息安全、网络信息安全)

为落实国家《信息安全等级保护管理办法》、《网络安全等级保护制度》进入“0A时代”、《办法》、《制度》网络信息安全等级保护制度

网络安全等级保护，如何落实国家《信息安全等级保护管理办法》、《网络安全等级保护制度》进入“0A时代”、《办法》、《制度》网络信息安全等级保护制度

(五) 网络信息安全等级保护安全技术：信任体系模型与物理技术、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、安全基线验证技术、漏洞检测技术、渗透测试技术、弱口令识别技术、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。综合利用大数据技术、云计算技术进行设备关联分析、日志存储与分析，解决网络攻击取证困难、可追溯问题。

(六) 网络安全态势感知技术。通过应用大数据、云计算技术，融合海量数据，融合感知与态势感知系统，建立态势感知系统，实现态势感知、态势分析、态势评估、态势决策、态势预警等技术。

(七) 网络安全态势感知和预警技术。网络安全态势感知和预警技术是网络安全态势感知和预警技术的重要组成部分，是实现网络安全态势感知和预警技术的关键技术。在网络安全态势感知和预警技术平台建设方面，应注重以下几个方面：

一是，网络安全态势感知和预警技术平台建设，应注重数据集成和共享。网络安全态势感知和预警技术平台建设，应注重数据集成和共享。二是，网络安全态势感知和预警技术平台建设，应注重态势感知和预警技术的集成。三是，网络安全态势感知和预警技术平台建设，应注重态势感知和预警技术的集成。

(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，国外的网络安全新技术研究，国外的网络安全工

新稿征集启事

一、征稿范围

(一) 来稿内容应属于作者的原创成果，未经发表，可

以是作者本人或所在单位的最新研究成果，具有学术价值、理论

意义或应用价值，且尚未公开发表过，或虽公开发表过，但属

国内首次公开发表，或属国内首次公开发表，或属国内首次

公开发表，或属国内首次公开发表，或属国内首次公开发表。

二、稿件要求

1. 稿件格式

2. 稿件内容

3. 稿件出版

(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西路9号(中关村)德胜