

附件：

第二届全国信息安全等级保护技术大会

征文需求

一、征文范围

(一) 安全防护策略：重要信息系统的安全威胁与脆弱性分析、安全等级保护实施研究、业界典型案例、大型单位安全防护策略等。

(二) 安全防护机制：信息安全管理评估、信息安全保障工作的运行机制、攻防对抗攻防、攻防对抗技术体系、攻防对抗预警体系等。

(三) 安全防护新技术和新机制等最新研究成果：下一代互联网（IPv6）、云计算、物联网、空网融合；新媒体、虚拟化等新技术，新环境下的等级保护或风险评估技术，等级保护技术体系在新环境下的应用方法等。

(四) 等级保护安全技术新技术：信任体系模型与物理技术、可信计算技术、密码技术、区块链技术与可信技术、主动防御技术、漏洞检测技术、网络安全态势感知与预警、条件安全技术等。

(五) 等级保护落地安全监测体系：网络安全态势感知与监测的

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。

(六) 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。

(七) 应急与事件处置技术：入侵感知预警技术、安全事件溯源取证技术、恶意代码清除技术、入侵检测技术等。

(八) 工控系统安全保护技术：工控系统的安全威胁分析、等级保护增强性技术和具体应用等。

(九) 信息安全产品研究：产品检测策略、技术、国内外信息安全产品性能比较，产品的安全性检测，国外新产品研究等。

(十) 国产化安全合格认证：国产化安全合格认证。

2.1.1 投稿须知及评审程序

二、投稿须知

(一) 本稿内容应属于作者的科研成果，数据真实、可靠，未经公开发表，且未被他人或单位公开报道，未曾公开发表论文摘要及全文不涉及保密内容。

(二) 稿件须按 Word 格式提交电子稿件，稿件一般不超过 10 页（3000 字）。

(三) 稿件以 Email 的方式发送到会议征稿邮箱 qjhb@compuser.com。

(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: 2013年5月15日

三、联系方式

通讯地址: 北京市海淀区阜成路59号新洲商务大厦703

010-88148756-8020

010-88148756-8020 13911629181

010-88148756-8020 13911629181