

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) 安全保护策略：重要信息系统的安全策略与脆弱性分析、安全管理新方法研究、风险管理策略、大数据安全保护策略等。

(二) 安全风险评估：信息安全风险评估模型、信息安全保障工程评估模型、威胁风险评估、威胁情报技术需求、安全监测预警机制等。

(三) 安全等级保护：等级保护等保体系建设；下一代互联网（IPv6）云环境、物联网、大数据、云计算、云环境下的新技术、新环境下的等级保护支撑性技术，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：信任体系模型与构建技术、可信计算技术、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、工控安全

、工控安全保护技术、工业互联网安全：工业互联网安全监测的数据采集、工控安全保护技术、工业互联网安全信任体系构建、工控安全等级保护技术、安全风险评估技术、安全事件关联分析技术、安全溯源可恢复技术等。

(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: 态势感知预警技术、安全监测技术、安全事件检测与响应、溯源取证、应急处置技术等。信息安全取证技术、应急响应技术、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, 等级保护支撑性技术和具体实践等。

(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) 国外网络安全策略研究: 国外网络安全战略、策略、理念等对我国网络安全的影响, 国外网络安全新技术研究, 国外信息安全新标准研究。

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。

超过 10 页 (5000 字)。

(三) 稿件以 Email 的方式发送到会议征稿邮箱 cspec@cspec.gov.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: 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708