

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) 安全保障策略：需要关注系统的资产威胁与脆弱性分析、安全管理规范与政策、应急响应策略、大数据安全保护策略等。

(二) 安全策略与机制：包括安全策略的制定、实施与安全策略工作的评价机制、策略制定机制、策略制定流程与策略、策略监测预警机制等。

(三) 安全策略与机制：包括安全策略的制定、实施与安全策略工作的评价机制、策略制定机制、策略制定流程与策略、策略监测预警机制等。

(四) 安全策略与机制：包括安全策略的制定、实施与安全策略工作的评价机制、策略制定机制、策略制定流程与策略、策略监测预警机制等。

(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技术、安全事件分析技术、安全态势分析技术等。

(五) 等级保护的支撑技术：用户身份鉴别与认证技术、安全策略与机制、策略制定机制、策略制定流程与策略、策略监测预警机制等。

(六) 等级保护的支撑技术：用户身份鉴别与认证技术、安全策略与机制、策略制定机制、策略制定流程与策略、策略监测预警机制等。

(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) 应急处置预案演练技术: 攻击仿真、演练设计、演练实施、演练总结、演练改进、演练报告、演练记录、演练评估、演练考核、演练验收、演练复盘和总结报告、演练报告书、应急演练评估报告。

(八) 其他技术: 信息安全风险评估技术、信息安全等级保护技术、信息安全应急响应技术、信息安全事件调查技术、信息安全事件处理技术、信息安全事件报告技术、信息安全事件处置技术、信息安全事件处置报告、信息安全事件处置记录、信息安全事件处置评估、信息安全事件处置考核、信息安全事件处置验收、信息安全事件处置复盘和总结报告、信息安全事件处置报告书、信息安全事件处置评估报告。

(九) 其他技术: 信息安全风险评估技术、信息安全等级保护技术、信息安全应急响应技术、信息安全事件调查技术、信息安全事件处理技术、信息安全事件报告技术、信息安全事件处置技术、信息安全事件处置报告、信息安全事件处置记录、信息安全事件处置评估、信息安全事件处置考核、信息安全事件处置验收、信息安全事件处置复盘和总结报告、信息安全事件处置报告书、信息安全事件处置评估报告。

九、国外最新安全事件应急响应技术。

三、投稿要求

(一) 来稿者应属于本领域的科研成果，数据真实，可靠，未公开发表过，与国内外学术界没有重复发表，是首次公开发表，为国内外学术界所关注和重视。

(二) 稿件须按微软 Word 格式的电子稿件，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 Gille@comp.org.cn。

(四) 论文版权属于会议组委会且本稿件的所有权，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58号新洲商务大厦708

三

邮编: 100048

联系人: 王宇 刘静

联系电话: 010-87100000 010-87100000