

主管：中华人民共和国公安部

主办：公安部第三研究所

中国计算机学会计算机安全专业委员会

ISSN1671-1122

CN31-1859/TN

增刊备案号：311859201602

中国科技核心期刊

信息网络安全

NETINFO SECURITY

为配合“第五届全国信息安全等级保护技术大会”
的召开和“全国电子数据取证鉴定技术优秀论文征集”
活动的举行，杂志社以增刊形式印发一期《论文集》，
专题刊登了评选出的部分论文。

ISSN 1671-1122



9 771671 112163

2016增刊

□ 信息安全等级保护技术大会优秀论文

- 1 CTCS-3 级列车控制系统信息安全防护策略浅析 王绍杰, 柯皓仁, 卢凯
- 5 基于等级保护的国有大型保险企业信息安全体系建设实务 赵军, 姬海波, 王达波, 于晓雪
- 9 浅谈后量子密码体制在信息安全等级保护中的应用 徐松艳, 刘明洁, 李鑫
- 13 工业控制系统信息安全事件分析及对安全防护的启示 高志新
- 19 《信息系统安全等级保护定级指南》修订要点解析 李明, 曲洁
- 22 试析中小网站入云安全防护可行性 陈益, 白鸥, 石锐
- 26 基于岗位的访问控制模型的研究 鲁金松, 牧涛, 刘琼
- 30 甘蔗制糖工业控制系统网络安全防护研究 钟剑
- 34 基于等级保护和风险评估的重大工程网络安全验收工作模型研究 张振峰, 张伟, 王李乐
- 37 基于 SDN 技术实现等级保护网络安全要求研究 于东升
- 41 大数据应用之企业信息安全管理 汪萌, 梁雨锋
- 45 信息安全等级保护测评中信息技术服务外包常见问题分析及对策探讨 夏侯振宇
- 48 基于 sinkhole 的僵尸网络检测技术的研究和实现 刘莹, 王勇, 孙强, 王小亮
- 57 基于安全域的云计算安全防护策略研究 廖飞, 陈捷
- 61 基于 AGA-LVQ 神经网络的网站安全漏洞预测模型研究 刘文志, 李海涛, 朱江
- 68 一种利用手机动态隐藏加密磁盘分区的数据安全保护策略 何为, 高鲁程, 伍洁
- 72 浅析云计算环境下等级保护访问控制测评技术研究 徐丽娟, 赵颖坤, 张德馨, 唐刚
- 77 新型安全威胁下的互联网金融纵深防护策略研究 郭桂生
- 81 智能电网安全漏洞报告与预警平台研究 方玉昕, 陈亮, 王劲松, 丁月民
- 85 典型 APT 攻击事件案例分析 李术夫, 李薛, 王超

□ 信息安全等级保护技术大会入选论文

- 89 有色金属行业典型工业控制系统通信协议安全性分析 梁雨锋, 汪萌, 赵军凯, 孟雅辉
- 96 浅谈新形势下金融保险企业纵深防御信息安全体系的构建 李秀宾
- 100 浅析我国网络信息安全保险体系的建立与发展 陈伟, 吴刚, 祁志敏
- 104 以制定行业等级保护实施细则为抓手推进卫生计生行业等保工作落实 王晖, 郑攀
- 107 工业控制系统信息安全等级保护测评方案研究 卢凯, 赵云飞, 柯皓仁
- 112 基于移动目标的物理访问控制研究与实现 李小川, 朱光剑, 胥滔, 郭亮
- 117 基于虚拟化技术的网络攻防仿真平台的设计与实现 黎水林, 陈广勇
- 121 浅谈如何实现电力信息安全有效管理 熊璐
- 125 论大中型保险机构的信息安全应急响应机制和体系建设 刘思远
- 129 国外入侵检测系统现状的研究 杨光

132 基于模糊概率的信息系统威胁态势感知方法	田建伟, 田峥, 黎曦, 薛海伟
137 物联网安全架构初探	王博识
141 工业控制系统信息安全多层防御体系模型探析	刘磊, 陆渝, 张志伟, 滕征岑
146 重要数据恢复平台建设研究	张志, 陈欣欣, 李世强
149 重点单位信息安全等级保护建设方案研究	赵文, 申罕骥, 丁铸
154 虚拟环境下等级保护测评研究	姜高聪
158 安全域划分在企业中的实际应用研究	郭睿, 陈涛
164 大型企业网络安全通报机制及支撑平台建设实践	靖小伟, 杨志贤, 滕征岑, 于普漪
170 电力企业信息安全保障体系规划设计探索与研究	王勇, 孙强, 王小亮, 李冬
174 云计算环境虚拟化的安全检测研究与实践	章恒, 禄凯
179 大数据安全测评框架和技术研究	黄钟, 陈肖, 文书豪
183 移动互联网终端入侵检测技术设计与实现	何倩, 涂静
188 Android 应用的安全框架与现状	陈彦文
194 证券期货行业互联网金融信息安全风险浅析	倪惠康, 李宏达
198 基于模糊测试的 Web 应用漏洞检测优化方法	程诚, 吴京朋, 周彦晖
203 APT 检测及防御	张璐
208 省级政务云中心安全体系策略与实践	张学谦
211 基于威胁情报的恶意软件识别	周松松, 马勇
217 基于大数据的 Web 应用安全研究	佟南, 汪浩
222 浅谈提升电力行业网络与信息安全水平策略	常英贤, 石鑫磊, 胡恒瑞, 周团峰
226 敏感数据保护和强制访问控制实现研究	王惠, 李蒙, 冉晋雪

□ 电子数据取证鉴定技术优秀论文

229 手机取证模型的优化与完善	张永
232 基于 APT 攻击的蜜罐技术的研究	王传极
237 基于 Nitro 攻击的 APT 木马取证研究	崔宇寅
241 基于 PS4 游戏主机的隐匿信息研究	高峰
244 基于 shellcode 静态虚拟执行的文档类漏洞恶意代码取证技术研究	管林玉
248 游戏主机取证初探	蔡立明
253 电子数据取证与鉴定实验室质量管理的关键控制点分析	黄道丽, 雷云婷, 金波
259 电子数据取证标准的研究与展望	郭弘, 夏荣
265 闪存芯片数据恢复和案例分析	沙晶, 钱伟