面向云网安全的新型防护技术专题导读

专题策划人

解冲锋，中国电信集团高级技术专家，博士，教授级高工，欧洲ETSI IPE工作组副主席、中国互联网协会学术委员会副主任委员、北京市IPv6重点实验室主任；曾在美国加利福尼亚大学洛杉矶分校做政府公派访问学者一年；长期从事网络架构、IPv6下一代互联网、物联网、网络安全、云网融合等方面的研究；在IETF合作发布RFC 5项，拥有授权发明专利50余项。

杨义先，北京邮电大学教授、“长江学者”特聘教授、国家杰出青年基金获得者、国家教学名师、国家教学团队带头人、全国百篇优秀博士学位论文指导教师、国家精品课程负责人；长期从事网络与信息安全方面的科研和教学工作；创立了网络空间安全的统一理论并编写了《安全通论》《博弈系统论》《黑客心理学》等书籍。

近年来，云网融合逐渐打破云和网相对独立和隔离的局面，融合人工智能（AI）、算力、大数据、安全、绿色等多种要素，从而为各行各业数字化转型提供强大的基础设施支撑。云网融合在基础架构、底层设施和资源调度等方面使得云和网趋于一体化，成为中国信息基础设施的核心特征。与此同时，随着国际形势的变化和安全攻防技术的演进，信息基础设施面临的安全形势也日趋复杂和严峻，云网攻击呈现出自动化强、复杂性高、隐匿性深、破坏性大等新的阶段性特性。数据泄露、勒索软件、高级持续性威胁（APT）攻击、路由劫持等安全事件频发，企业用户对安全防护的多样化需求正在与日俱增。信息基础设施快速发展与安全防御能力不足的矛盾日益突出。如何利用新技术、新手段应对云网面临的安全威胁，是业界非常关注的问题。

本专题中的多篇论文论述了云网场景下的安全风险挑战，并对各种新型防护技术展开讨论。《面向云网融合的网络安全互操作》分析了云网时代的主要安全挑战，认为网络安全互操作是云网融合安全发展的重要路径，从标准规范、能力验证、行业示范等方面指出云网安全互操作的重点发展方向；针对5G网络中云、终端、协同机制中的安全缺陷威胁，《基于超级SIM的5G端云安全体系架构与关键技术》论述了“云、端、卡”协同运作的完整安全体系，对端云安全体系关键技术的发展提出新思路；《云网融合下的安全能力池关键技术与应用》提出了云网安全一体化的安全能力池技术方案，实现了网络安全防护能力的快速扩展、灵活定制和可编排，从而满足用户对安全防护能力多层次可定制的需求；《未来网络内生安全通信技术》基于网络可信身份的轻量化密钥验证机制，提出了网络可信通信技术，该技术具备近源协同防护、无状态随路验证等特征，为未来网络安全可信保障提供参考；《云平台DNS安全体系研究》在介绍域名系统（DNS）技术和业态演进过程的基础上，梳理了云平台DNS的安全风险和特征，提出了云平台DNS安全体系框架，并介绍了所在企业的安全实践；《构建可扩展的RPKI依赖方系统部署机制》梳理了影响互联网码号资源公钥基础设施（RPKI）依赖方系统运行效能的4对矛盾，探讨了RPKI依赖方系统部署机制以及对应的运行机制；《大型企业SASE解决方案及应用实践》在分析安全访问服务边缘（SASE）架构基础上，设计了企业一体化安全运营系统Q-SASE及其技术方案，分享了其为大型企业客户提升安全防护方面的实践。《关于发展中国安全浏览器的建议》通过对全球安全浏览器发展趋势的洞察和重要性分析，论述了中国在安全浏览器领域所面临的机会与挑战，提出中国发展安全浏览器的对策建议。

本专题的作者来自各知名高校、企业与科研机构，文章聚焦于云网安全面临的新挑战及当前主要的防护技术。作者们从行业需求分析、系统设计、理论分析、性能评估、实际运营等方面，介绍了云网安全最新的研究成果和经验。希望本期的内容能为读者提供有益的借鉴与启示，并在此对所有作者的大力支持表示由衷的感谢！

解冲锋　杨义先

2023年1月18日

DOI：10.12142/ZTETJ.202301002
收稿日期：2023-01-19