



## 关于征集《网络安全技术和产业动态》专报编制组成员的通知

CCIA 秘[2022]061 号

各会员单位：

中国网络安全产业联盟（CCIA）自 2020 年组织成立《网络安全技术和产业动态》专报编制组以来，每月定期将专报报送相关主管部门及业界专家，得到了充分肯定和好评。为进一步做好专报编制工作，CCIA 现面向会员单位继续征集专报编制组成员，有关事项通知如下。

### 一、工作内容

编写《网络安全技术和产业动态》专报，参与专报编制组工作会议，包括：

1. 梳理全球网络安全技术动态、组织跟踪国内外网络安全核心技术、关键技术、前沿技术的技术发展情况、技术发展难点、产业落地实施情况，并提出相关意见建议等。
2. 梳理国外网络安全技术领先的先进企业、创新机构及重要的网络安全用户，分析国外网络安全战略发展等。

### 二、参加方式

1. 各单位推荐 1-2 名相关专家报名参加，保证专报编制

工作时间。

2. 填写《网络安全技术和产业动态》专报编制组成员申请表（见附件1）和2023年专报新专题（见附件2）。

3. 申请表电子版（盖章PDF版和WORD版）和新专题电子版（WORD版）发送至CCIA秘书处邮箱。

4. 申请表纸质版邮寄至CCIA秘书处。

5. 截止日期：2022年12月1日。

### 三、联系方式

联系人：周梦妍

联系方式：010-64102639

邮 箱：cciahyz@china-cia.org.cn

地 址：北京市东城区安定门东大街1号 中国网络安全产业联盟秘书处

附件：

1. 《网络安全技术和产业动态》编制组成员申请表
2. 2023年专报新专题征集参考样式
3. 总第1-28期《网络安全技术和产业动态》专报专题名称及编制单位

中国网络安全产业联盟秘书处

2022年11月10日



附件 1:

### 《网络安全技术和产业动态》编制组成员申请表

单位名称			
主要业务领域			
姓名		手机	
职务		电子邮箱	
单位地址			
个人工作经历、 专业特长等			
有何发明、著 作、学术论文， 发表时间、发表 刊物名称			
参加何种学术 组织、担任何种 职务			
单位意见	负责人: (签名、盖公章)  年 月 日		

附件 2:

## 2023 年专报新专题征集参考样式

### 【样式一】

选题：威胁框架

提出单位：安天科技

申报日期：2021 年 1 月 4 日

提出理由：技术和产业现状 2 个方面：

- 技术方面：一方面恶意代码的种类、数量急剧增加，新技术和新应用带来攻击面的增大，使得传统依靠特征来识别和防范恶意代码的技术受到越来越多的挑战；

威胁框架则提出了一种全新的视角，从实战出发，重新诠释和定义恶意代码的“特征”，与传统特征不同的是，这些“特征”普通恶意代码难以绕过和规避（除非特别新型的），因此能大大提高了防范的有效性、并提高攻击方的成本。

- 产业现状：威胁框架的概念是 MITRE 组织 2015 年提出的，它在传统杀伤链模型的基础上，经过数次修改和完善，目前已经是 8.0 版（2020 年 11 月发布）。正在得到国际主流网络安全厂商的支持和应用。

### 【样式二】

选题：机密计算技术发展研究及政策建议

提出单位：北京天融信网络安全技术有限公司

申报日期：2021 年 1 月 19 日

提出理由：技术和产业现状 2 个方面：

在全球范围内，隐私作为一项基本人权正在逐步进步的法律法规中体现。数据保护的精确目标是确保公共部门和私营部门都公平地处理包括但不限于收集、使用、存储个人数据。

数据在计算中以三种状态存在：传输、存储和使用中。跨网络传输的数据状态是“传输中”，以某种类型保存在存储介质中的数据状态，正在处理的数据状态是“使用中”。

机密计算就是处理使用中的数据。机密计算就是保护选定的代码和数据不被泄露和修改。机密计算通过基于硬件的可信执行环境实现了执行环境的隔离。本质上讲，机密计算的安全性与硬件本身的安全性强相关。

RISC-V 架构中 keynote 提供一个可信执行环境。基于 RISC-V 的 KeyNote 是机密计算是一个有前途技术方向。

## 附件 3:

### 总第 1-28 期《网络安全技术和产业动态》专报专题名称 及编制单位

总期号	专题名称	编制单位
总第 1 期	人工智能助力网络安全防御技术的新发展	中国电子科技网络信息安全有限公司、中电科网络空间安全研究院
总第 2 期	国外优秀网络安全厂商情况分析	杭州安恒信息技术股份有限公司
总第 3 期	零信任安全技术发展研究及政策建议	绿盟科技集团股份有限公司
总第 4 期	安全编排与自动化响应技术发展研究及政策建议	天融信科技集团股份有限公司
总第 5 期	应用系统自动化攻击防护技术发展研究及政策建议	瑞数信息技术(上海)有限公司、恒安嘉新(北京)科技股份公司、北京北信源软件股份有限公司
总第 6 期	分层网络威慑战略发展研究及建议	安天科技集团股份有限公司、北京立思辰计算机技术有限公司
总第 7 期	同态加密技术发展研究及政策建议	格尔软件股份有限公司、启明星辰集团北京网御星云信息技术有限公司、深圳市联软科技股份有限公司
总第 8 期	数字孪生在网络安全领域应用的研究及建议	杭州立思辰安科科技有限公司、北京天融信网络安全技术有限公司
总第 9 期	美国国防部数据战略发展研究及政策建议	北京网御星云信息技术有限公司、北京安天网络安全技术有限公司、格尔软件股份有限公司
总第 10 期	安全访问服务边缘(SASE)技术发展研究及政策建议	杭州安恒信息技术股份有限公司
总第 11 期	ATT&CK 威胁框架发展研究及政策建议	安天科技集团股份有限公司
总第 12 期	端点检测与响应(EDR)技术发展研究及政策建议	北京北信源软件股份有限公司
总第 13 期	网络欺骗技术发展研究及政策建议	深圳市联软科技股份有限公司、格尔软件股份有限公司
总第 14 期	联邦学习技术发展研究及政策建议	绿盟科技集团股份有限公司

总期号	专题名称	编制单位
总第 15 期	关于美国 2020 改善数字身份法律提案的思考及政策建议	北京数字认证股份有限公司
总第 16 期	机密计算发展研究及产业政策建议	北京天融信网络安全技术有限公司
总第 17 期	容器安全技术发展研究及政策建议	北京启明星辰信息安全技术有限公司
总第 18 期	网络安全靶场平台发展研究及建议	博智安全科技股份有限公司
总第 19 期	新版 ATT&CK 威胁框架技术演进及产业落地实践	安天科技集团股份有限公司
总第 20 期	软件定义边界 (SDP) 安全访问技术发展研究及政策建议	恒安嘉新 (北京) 科技股份公司、北京天融信网络安全技术有限公司
总第 21 期	威胁狩猎发展研究及政策建议	北京升鑫网络科技有限公司
总第 22 期	软件供应链安全发展研究及政策建议	绿盟科技集团股份有限公司
总第 23 期	元宇宙发展研究及政策建议	北京大学
总第 24 期	应用程序接口 (API) 防护技术发展研究及对策建议	瑞数信息技术 (上海) 有限公司
总第 25 期	智能物联网安全技术发展研究及政策建议	北京安御道合科技有限公司
总第 26 期	中美关键信息基础设施保护政策比较与建议	深信服科技股份有限公司
总第 27 期	零信任体系下身份和访问管理 (IAM) 的应用研究及建议	北京天融信网络安全技术有限公司
总第 28 期	隐私计算技术发展研究及政策建议	深圳市腾讯计算机有限公司