# 全国网络安全标准化技术委员会秘书处

# 网络安全标准化工作月报

2024 年第 3 期（总第 29 期）　　2024 年 3 月 31 日

## 本 期 目 录

## 国家标准研制

### 1. 6 项国家标准征求意见稿专家审查

3 月 15 日，秘书处组织《网络安全技术 生成式人工智能预训练和优化训练数据安全规范》《网络安全技术 生成式人工智能数据标注安全规范》《网络安全技术 数据安全保护要求》《网络安全技术 个人信息保护合规审计要求》《网络安全技术 数字水印技术实现指南》《网络安全技术 个人信息转移技术要求》等 6 项网络安全国家标准征求意见稿专家审查。与会专家围绕标准主要技术内容、意见处理情况进行了审查，并提出修改意见。6 项标准均通过审查。详见附件 1。

### 2. 3 项国家标准送审稿专家审查

3 月 14 日，秘书处组织《网络安全技术 机密计算通用框架》《网络安全技术 人工智能计算平台安全框架》《网络安全技术 公钥基础设施 在线证书状态协议》3 项国家标准送审稿专家审查。与会专家围绕标准主要技术内容、意见处理情况进行了审查，并提出修改意见。其中，2 项标准通过审查。详见附件 1。

## 3.5项网络安全国家标准获批发布

根据2024年3月15日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2024年第1号），网安标委归口的5项国家标准正式发布。具体清单如下:

| 序号 | 标准编号 | 标准名称 | 代替标准号 | 实施日期 |
|---|---|---|---|---|
| 1 | GB/T 43697-2024 | 数据安全技术 数据分类分级规则 | | 2024-10-01 |
| 2 | GB/T 17903.1-2024 | 信息技术 安全技术 抗抵赖 第1部分：概述 | GB/T 17903.1-2008 | 2024-10-01 |
| 3 | GB/T 17903.3-2024 | 信息技术 安全技术 抗抵赖 第3部分：采用非对称技术的机制 | GB/T 17903.3-2008 | 2024-10-01 |
| 4 | GB/T 15843.4-2024 | 信息技术 安全技术 实体鉴别 第4部分：采用密码校验函数的机制 | GB/T 15843.4-2008 | 2024-10-01 |
| 5 | GB/T 31497-2024 | 信息技术 安全技术 信息安全管理 监视、测量、分析和评价 | GB/T 31497-2015 | 2024-10-01 |

## 国际标准化推进

### 1. 完成 8 项国际标准文件投票和评议工作

2024 年 3 月，秘书处共组织完成 ISO/IEC 29151《信息技术 安全技术 个人身份信息保护实践指南》、ISO/IEC 27028《信息安全 网络安全和隐私保护 ISO/IEC 27002 属性指南》、ISO/IEC 27090《网络安全 人工智能 应对人工智能系统中的安全威胁和故障的指南》等 8 项国际标准文件投票和评议工作，详见附件 2。

### 2. 召开 2024 年上半年 SC27 中国代表团行前会议

3 月 22 日，召开“2024 年上半年 SC27 中国代表团行前会议”，会议明确了此次参会重点任务安排、外事纪律要求等，会上各提案负责人汇报了参会任务和目标，并对推进可能遇到的问题提出应对措施。

## 重要会议和活动

### 1. 网安标委第一次主任办公会在京召开

3 月 20 日，网安标委第一次主任办公会在京召开。会议审议通过了网安标委工作组调整方案、网安标委第一次全体会议方案、网安标委 2023 年工作总结和 2024 年工作要点，网安标委章程、标准制修订工作程序、技术文件制定工作程序等 3 个制度文件，5 项网络安全国家标准报批稿、53 项网络安全国家标准复审结论建议，以及 2023 年度网安标委标准化工作先进个人提名名单。

会议指出，组建网安标委是贯彻落实大网络安全工作格局的具体举措。会议强调：一是要发挥好委员会平台作用，加强对网络安全国家标准的统筹协调，求同存异形成合力，针对网络安全产品互联互通等重点标准，组织相关部门、工作组、测评机构、企业等深入研究，形成体系化的标准成果。二是要加强网络安全国际标准化研究，提升技术驾驭能力，在保证安全的前提下大胆主动进行国际交流合作，积极吸收国外标准先进经验。三是秘书处要更好发挥作用，打通“政、产、学、研、用”技术交流通道，深入了解网络安全工作的关切点、标准需求点，为网络安全管理部门提供意见建议。

**2. 表彰 2023 年度网安标委标准化工作先进个人**

3 月 28 日，为表彰在 2023 年国家网络安全标准化工作中做出突出贡献的个人，报经主任委员同意，决定授予王姣等 12 名同志为“2023 年度全国网络安全标准化技术委员会标准化工作先进个人”。

## 其他

**1. 1 项网安标委技术文件发布**

3 月 1 日，委员会技术文件 TC260-003《生成式人工智能服务安全基本要求》发布。该文件规定了生成式人工智能服务在安全方面的基本要求，包括语料安全、模型安全、安全措施等，并给出了安全评估要求，适用于服务提供者开展安全评估、提高安全水平，也可为相关主管部门评判生成式人工智能服务安全水平提供参考。

**2. 2 项网络安全标准实践指南发布**

3 月 7 日，秘书处组织编制的《网络安全标准实践指南——车外画面局部轮廓化处理效果验证》发布。该实践指南给出了验证车外画面进行人脸、车牌局部轮廓化处理效果的

流程、方法及验证指标，可为汽车数据处理者及有关机构验证车外画面局部轮廓化处理效果提供参考。

3 月 25 日，秘书处组织编制的《网络安全标准实践指南——网络安全产品互联互通 资产信息格式》发布。该实践指南给出了网络安全产品互联互通时资产信息的描述格式，可用于指导网络安全产品互联互通功能的设计、开发、应用和测试。

## ◁ 附件 1：2024 年 3 月在研标准项目推进工作一览表

| 序号 | 国标计划号 | 项目名称 | 标准范围 | 项目进展 |
|---|---|---|---|---|
| 1 | 暂无 | 《网络安全技术 个人信息转移技术要求》 | 该标准规定了个人信息主体请求转移其个人信息的适用和行使的条件、可请求转移的个人信息范围，以及个人信息处理者在处理个人信息主体转移个人信息的请求时应遵守的安全原则、流程和技术要求；适用于个人信息处理者响应个人信息主体转移信息请求的全流程。 | 已形成征求意见稿，并通过专家审查会评审。 |
| 2 | 暂无 | 《网络安全技术 生成式人工智能预训练和优化训练数据安全规范》 | 该标准规定了生成式人工智能预训练和优化训练数据的基本安全要求、预训练数据处理活动的安全要求、优化训练数据处理活动的安全要求，以及检测方法；适用于面向我国境内公众提供生成式人工智能服务的组织或个人提高预训练及优化训练数据处理活动的安全水平。 | 已形成征求意见稿，并通过专家审查会评审。 |
| 3 | 暂无 | 《网络安全技术 生成式人工智能数据标注安全规范》 | 该标准给出了生成式人工智能数据标注任务前期准备、标注任务执行、标注结果输出、标注过程活动控制的安全要求以及标注安全测试方法；适用于数据标注方开展生成式人工智能数据标注活动。 | 已形成征求意见稿，并通过专家审查会评审。 |
| 4 | 暂无 | 《网络安全技术 数据安全保护要求》 | 该标准提出了数据安全保护框架，规定了数据安全保护的原则、目标和要求；适用于指导数据处理者开展数据分类分级保护工作。 | 已形成征求意见稿，并通过专家审查会评审。 |

| 序号 | 国标计划号 | 项目名称 | 标准范围 | 项目进展 |
| --- | --- | --- | --- | --- |
| 5 | 暂无 | 《网络安全技术 个人信息保护合规审计要求》 | 该标准给出了个人信息保护合规审计的原则、内容要求以及总体要求；适用于个人信息处理者内部机构或委托专业机构开展的个人信息保护合规审计工作。 | 已形成征求意见稿，并通过专家审查会评审。 |
| 6 | 暂无 | 《网络安全技术 数字水印技术实现指南》 | 该标准提出了数字水印技术的实现框架、实现目标、实现流程、水印算法选择、水印服务封装形式选择等方面的建议，并给出了常见数字水印算法、典型安全场景等相关信息；适用于数字水印技术的设计、开发、应用和测试。 | 已形成征求意见稿，并通过专家审查会评审。 |
| 7 | 20230246-T-469 | 《网络安全技术 机密计算通用框架》 | 该标准给出了机密计算通用框架，描述了框架的核心组件和基础功能，提供了机密计算服务的实现机制；适用于为机密计算相关方设计、开发、使用和部署机密计算相关产品或解决方案时提供参考。 | 已形成送审稿，并通过专家审查会评审。 |
| 8 | 20230249-T-469 | 《网络安全技术 人工智能计算平台安全框架》 | 该标准规定了人工智能计算平台安全框架的安全功能、安全机制及安全模块；适用于设计、实现与应用人工智能计算平台安全功能。 | 已形成送审稿。 |

| 序号 | 国标计划号 | 项目名称 | 标准范围 | 项目进展 |
| --- | --- | --- | --- | --- |
| 9 | 20230239-T-469 | 《网络安全技术 公钥基础设施 在线证书状态协议》 | 该标准规定了一种无需请求证书撤销列表即可查询数字证书状态的机制，规定了在线证书状态协议的协议内容、语法规范等；适用于公钥基础设施的建设以及应用在线证书状态协议的依赖方等。 | 已形成送审稿，并通过专家审查会评审。 |

## 附件 2：8 项国际标准文件投票和评议工作一览表

| 序号 | 标准编号 | 英文名称 | 中文名称 | 阶段 | 标准内容 |
|---|---|---|---|---|---|
| 1. | ISO/IEC 29151 | Information technology Security techniques— Code of practice for personally identifiable information protection | 信息技术 安全技术 个人身份信息保护实践指南 | CD | 该项目由 SC27/WG5 提出修订。ISO/IEC 29151 补充了针对 PII 保护的新控制，建立了控制目标、控制措施和实施控制措施的指南，以满足与 PII 相关的风险和影响评估的要求。 |
| 2. | ISO/IEC 27028 | Information security—cyber security and privacy protection— Guidance on ISO/IEC 27002 attributes | 信息安全 网络安全和隐私保护 ISO/IEC 27002 属性指南 | CD | 该项目由 SC27/WG1 提出。ISO/IEC 27028 在 ISO/IEC 27002 的基础上，进一步提供了其他类型的控制属性，为相关方根据自身需要开发和使用信息控制的属性提供了指导。 |

| 序号 | 标准编号 | 英文名称 | 中文名称 | 阶段 | 标准内容 |
|---|---|---|---|---|---|
| 3. | ISO/IEC 27090 | Cybersecurity— Artificial Intelligence— Guidance for addressing security threats and failures in artificial intelligence systems | 网络安全 人工智能 应对人工智能系统中的安全威胁和故障的指南 | CD | 该项目由英国提出。ISO/IEC 27090 为组织解决特定人工智能（AI）系统安全提供指导，以帮助组织更好地了解特定于 AI 系统的安全威胁及负面后果，并就如何检测和缓解此类威胁提出建议。 |
| 4. | ISO/IEC TS 27564 | Privacy protection— Guidance on the use of models for privacy engineering | 隐私保护 隐私工程模型使用指南 | PWI | 该项目由 SC27/WG5 提出。ISO/IEC TS 27564 为如何在隐私工程中使用建模提供指导，描述了可使用的模型类别，以及隐私工程、其他建模参考和标准三者之间关系 |
| 5. | ISO/IEC 27701 | Information security cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance | 信息安全 网络安全和隐私保护 隐私信息管理系统 要求和指南 | CD | 该项目由 SC27/WG5 提出修订。ISO/IEC 27701 规定了建立、实施、维护和持续改进隐私信息管理系统（PIMS）的要求，适用于 PII 控制者和 PII 处理者，使组织能够确保自身的 PIMS 与其他管理体系标准相关要求保持一致。 |

| 序号 | 标准编号 | 英文名称 | 中文名称 | 阶段 | 标准内容 |
|---|---|---|---|---|---|
| 6. | ISO/IEC 19896-2 | Information security cybersecurity and privacy protection—Requirements for the competence of IT security conformance assessment body personnel—Part 2: Knowledge and skills requirements for ISO/IEC 19790 testers and validators | 信息安全 网络安全和隐私保护 对IT安全一致性评估机构人员能力的要求 第2部分：ISO/IEC 19790测试人员和验证人员的知识和技能要求 | CD | 该项目由SC27/WG3提出修订。ISO/IEC 19896-2定义了与测试人员相关的术语、概念，基本知识和技能要求，可以为依据ISO/IEC 19790开展密码模块测试和结果验证的机构选择及评定人员技术等级提供支持。 |
| 7. | ISO/IEC 19896-1 | Information security cybersecurity and privacy protection—Requirements for the competence of IT security conformance assessment body personnel—Part 1: Introduction, concepts and general requirements | 信息安全 网络安全和隐私保护 对IT安全一致性评估机构人员能力的要求 第1部分：简介、概念和一般要求 | CD | 该项目由SC27/WG3提出修订。ISO/IEC 19896-1定义了与IT安全符合性测试、评估、认证及验证人员能力相关的术语、概念和最小要求，可以为测试机构、评估机构及认证机构选择、培训及评定人员技术等级提供支持。 |

| 序号 | 标准编号 | 英文名称 | 中文名称 | 阶段 | 标准内容 |
|---|---|---|---|---|---|
| 8. | ISO/IEC 19792 | Information security cybersecurity and privacy protection—General principles of security evaluation of biometric systems | 信息安全 网络安全和隐私保护 生物识别系统安全评估的一般原则 | CD | 该项目由 SC27/WG3 提出修订。ISO/IEC 19792 对生物认证系统安全评估的一般术语、概念、系统结构进行了描述，还描述了十余种生物认证系统特定的安全威胁，在此基础上对伪造攻击检测（PAD）技术的评估，以及生物特征数据隐私保护的一般方法进行了规范。 |