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

2025 年第 1 期（总第 39 期）　　2025 年 1 月 31 日

本 期 目 录

国家标准研制

1. 10 项国家标准送审稿全体委员审查

1 月 16 日，秘书处组织《网络安全技术 公钥基础设施 PKI 组件最小互操作规范》《网络安全技术 公钥基础设施 时间戳规范》《数据安全技术 个人信息保护合规审计要求》《数据安全技术 个人信息转移技术要求》《网络安全技术 生成式人工智能服务安全基本要求》《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》等 10 项国家标准送审稿全体委员审查。与会委员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。10 项标准均通过审查。

2. 5 项国家标准送审稿全体委员投票

1 月 24 日，秘书处面向委员会全体委员组织开展《网络安全技术 公钥基础设施 PKI 组件最小互操作规范》《网络安全技术 公钥基础设施 时间戳规范》《网络安全技术 公钥基础设施 证书管理协议》《数据安全技术 数据安全和个人信息保护社会责任指南》《网络安全技术 人工智能计算平台安全框架》等 5 项国家标准送审稿投票表决工作，并于 1 月 28 日 24 时前完成投票。

3.1 项网络安全国家标准获批发布

根据2025年1月24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（2025年第2号），全国网络安全标准化技术委员会归口的1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	实施日期
1	GB/T 45230-2025	数据安全技术 机密计算通用框架	2025-08-01

国际标准化推进

1. 征集2025年网络安全国际标准提案

1月24日，为推进我国网络安全国际标准化工作，丰富国际标准化技术成果储备，鼓励更多网络安全技术和应用领域优秀实践经验以及科研项目标准成果向国际输出，推动我国网络安全标准“走出去”，网安标委秘书处面向社会各界广泛征集网络安全国际标准需求。征集截止日期为2月21日。

2. 完成12项国际标准文件投票和评议工作

2025年1月，秘书处组织完成ISO/IEC 19790《信息安全 网络安全和隐私保护 密码模块安全要求》、ISO/IEC 24759《信息安全 网络安全和隐私保护 密码模块检测要求》、

ISO/IEC 5181.2《信息安全 网络安全和隐私保护 数据来源》等 12 项国际标准文件投票和评议工作。

重要会议和活动

1. 全国网络安全标准化技术委员会 WG1 和工作组组长联席会议在北京召开

2025 年 1 月 22 日，全国网络安全标准化技术委员会（简称网安标委）WG1 和工作组组长联席会议在北京召开。WG1 专家组成员，各工作组组长、副组长，中央网信办网络安全协调局副局长罗锋盈，中国电子技术标准化研究院院长杨旭东、副院长范科峰等 40 余人参加了会议。会议由 WG1 组长顾建国主持。

会议讨论了《网安标委 2024 年工作总结和 2025 年工作要点（讨论稿）》，审议了《网络安全国家标准体系（2024 版）（审议稿）》，与会专家提出了许多建设性意见和建议。会议评选形成了“2024 年度网安标委标准化工作先进个人提名名单”。后续，秘书处将按照会议意见对相关文件进行修改完善后进行下一步工作程序。

其他

1.《人工智能安全标准体系（V1.0）》（征求意见稿）公开征求意见

为积极响应《全球人工智能治理倡议》，支撑落实《人工智能安全治理框架》，充分发挥标准对人工智能技术应用和产业发展的规范引领作用，持续完善人工智能安全标准体系建设，秘书处组织编制了《人工智能安全标准体系（V1.0）》（征求意见稿），并于1月26日至2月21日面向社会公开征求意见。

2. 1项网络安全标准实践指南发布

1月26日，秘书处组织编制的《网络安全标准实践指南——人脸识别支付场景个人信息安全保护要求》发布。该实践指南给出了人脸识别支付场景数据收集、存储、传输、导出、删除等环节的安全要求，可为人脸识别支付服务提供方、人脸验证服务方、场所管理方、设备运营方处理个人信息提供参考。

3. 2项网络安全标准实践指南公开征求意见

为支撑《人工智能生成合成内容标识办法》和强制性国家标准《网络安全技术 人工智能生成合成内容标识方法》，

为生成合成服务提供者和内容传播服务提供者提供编码规则，指导其开展人工智能生成合成内容的文件元数据隐式标识工作，秘书处组织编制了《网络安全标准实践指南——人工智能生成合成内容标识 服务提供者编码规则（征求意见稿）》，并于1月22日至2月5日面向社会公开征求意见。

为规范App和第三方SDK展示和触发摇一摇开屏广告的行为、保障用户个人权益，秘书处组织编制了《网络安全标准实践指南——摇一摇广告个人权益规范指引（征求意见稿）》，并于1月22日至2月5日面向社会公开征求意见。

附件 1：2025 年 1 月在研标准项目推进工作一览表

序号	国标计划号	标准名称	标准范围	项目进展
1	20231921-T-469	网络安全技术 公钥基础设施 时间戳规范	该标准描述了时间戳系统组成、时间戳的内容和申请颁发流程，规定了时间戳安全要求，给出了对应的测试评价方法；适用于时间戳系统及其应用的设计、开发与测试。	2025 年 1 月 24 日至 1 月 28 日，秘书处组织全体委员对送审稿进行投票表决。
2	20231916-T-469	网络安全技术 公钥基础设施PKI组件最小互操作规范	该标准规定了公钥基础设施组件最小互操作的基本功能要求和数据格式要求，给出了测试评价方法；适用于电子签名、电子签章、身份管理等活动中PKI的设计、开发、测试及其应用。	2025 年 1 月 24 日至 1 月 28 日，秘书处组织全体委员对送审稿进行投票表决。
3	20231923-T-469	网络安全技术 公钥基础设施 证书管理协议	该标准提出了公钥基础设施（PKI）中证书管理协议的结构和内容，规定了证书产生和管理所需要的协议消息格式，可为公钥基础设施的设计、开发、运行提供参考。	2025 年 1 月 24 日至 1 月 28 日，秘书处组织全体委员对送审稿进行投票表决。
4	20240401-T-469	数据安全技术 数据安全和个人信息保护社会责任指南	该标准为组织实施数据安全和个人信息保护社会责任相关活动提供指南；适用于处理数据和个人信息的组织，还适用于评价组织履行数据安全和个人信息保护社会责任程度的第三方机构。	2025 年 1 月 24 日至 1 月 28 日，秘书处组织全体委员对送审稿进行投票表决。
5	20230249-T-469	网络安全技术 人工智能计算平台安全框架	该标准给出了人工智能计算平台的安全框架，包括安全功能、安全管理和角色安全职责；适用于指导人工智能计算平台的安全设计、建设和运维管理。	2025 年 1 月 24 日至 1 月 28 日，秘书处组织全体委员对送审稿进行投票表决。

序号	国标计划号	标准名称	标准范围	项目进展
6	20240896-T-469	数据安全技术 个人信息保护合规审计要求	该标准提出了个人信息保护合规审计原则，规定了个人信息保护合规审计的实施要求、内容和方法；适用于个人信息处理者开展个人信息保护合规审计工作。	已形成送审稿，并通过全体委员审查会评审。
7	20242027-T-469	数据安全技术 个人信息转移技术要求	该标准规定了基于个人信息主体请求转移以电子方式记录的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流程和要求；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。	已形成送审稿，并通过全体委员审查会评审。
8	20241752-T-469	网络安全技术 生成式人工智能服务安全基本要求	该标准规定了生成式人工智能服务在训练数据安全、模型安全、安全措施等方面的要求，并给出了安全评估参考方法；适用于服务提供者开展生成式人工智能服务相关活动。	已形成送审稿，并通过全体委员审查会评审。
9	20242095-T-469	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及其处理活动的安全要求，描述了对应的评价方法；适用于指导生成式人工智能服务提供者开展预训练和优化训练数据处理活动以及开展与训练预训练和优化训练数据安全自评价。	已形成送审稿，并通过全体委员审查会评审。
10	20242097-T-469	网络安全技术 生成式人工智能数据标注安全规范	该标准规定了生成式人工智能训练的数据标注工具安全要求、数据标注规则安全要求、标注人员要求、数据标注核验要求和数据标注安全评价方法；适用于生成式人工智能数据标注方开展训练数据标注活动。	已形成送审稿，并通过全体委员审查会评审。

附件 2：12 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 19790	Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules	信息安全 网络安全和隐私保护 密码模块安全要求	FDIS	ISO/IEC 19790 规定了用于保护计算机和通信系统敏感信息的安全系统中所使用的密码模块的安全要求，为加密模块定义了四个安全级别，涵盖了 11 个安全功能要求领域。
2.	ISO/IEC 24759	Information security, cybersecurity and privacy protection — Test requirements for cryptographic modules	信息安全 网络安全和隐私保护 密码模块检测要求	FDIS	ISO/IEC 24759 规定了测试实验室用于测试加密模块是否符合 ISO/IEC 19790 要求的方法，以及供应商可以提供给测试实验室的一些信息上的要求。
3.	ISO/IEC 5181.2	Information security, cybersecurity and privacy protection — Data provenance	信息安全 网络安全和隐私保护 数据来源	CD	ISO/IEC 5181.2 给出了数据溯源的方法论、指南和技术。
4.	ISO/IEC 19896-2	Information security, cybersecurity and privacy protection — Part 2: Knowledge and skills requirements for ISO/IEC 19790 testers	信息安全 网络安全和隐私保护 IT 安全符合性评估人员能力要求 第 2 部分：ISO/IEC 19790 测试和验证人员的知识和技能要求	DIS	ISO/IEC 19896-2 提出了依据 ISO/IEC 19790 和 ISO/IEC 24759 开展符合性测试的测试者和验证者所需满足的最基本的知识和技能要求。

序号	标准编号	英文名称	中文名称	阶段	标准内容
5.	ISO/IEC 27706	Requirements for bodies providing audit and certification of privacy information management systems	隐私信息管理系统审计认证机构要求	FDIS	ISO/IEC 27706 规定了按照 ISO/IEC 27701 标准，对隐私信息管理系统（PIMS）提供审计认证的机构相关要求。
6.	ISO/IEC 28033-3	Information Security — Fully homomorphic encryption — Part 3: Mechanisms for arithmetic on approximate numbers	信息安全 全同态加密 第 3 部分：近似数字的算法机制	FDIS	ISO/IEC 28033-3 把加密噪声视为近似计算的一部分，用消息和噪声替代原消息，描述了格密码分解步骤、编码解码、密钥生成、加解密算法、同态加、乘、旋转和共轭算法。
7.	ISO/IEC 28033-4	Information Security — Fully homomorphic encryption — Part 4: Mechanisms for arithmetic based on look-up table evaluation	信息安全 全同态加密 第 4 部分：基于查找表评估的算法机制	CD	ISO/IEC 28033-4 规范了基于查找表评估的同态加密机制，并针对不同安全级别给出了参数选择的具体指导。
8.	ISO/IEC 24760-2	IT Security and Privacy — A framework for identity management — Part 2: Reference architecture and requirements	信息技术安全和隐私 身份管理框架 第 2 部分：参考架构和要求	FDIS	ISO/IEC 24760-2 适用于与身份相关的信息的任何信息系统处理或储存。

序号	标准编号	英文名称	中文名称	阶段	标准内容
9.	ISO/IEC 24760-3	IT Security and Privacy — A framework for identity management — Part 3: Practicecontrols	信息技术安全和隐私 身份管理框架 第 3 部分：惯例	FDIS	ISO/IEC 24760-3 适用于处理或存储与身份有关信息的信息系统；区分了“身份”和“身份标识符”等概念，可用于评估身份管理系统的隐私性和保护身份相关属性。
10.	ISO/IEC 20009-4: 2017/Amd 1	Information technology — Security techniques — Anonymous entity authentication — Part 4: Mechanisms based on weak secrets Amendment 1	信息技术 安全技术 匿名实体鉴别 第 4 部分：基于弱秘密的机制 补篇 1	CD	ISO/IEC 20009-4:2017/Amd1 旨在将我国自主研发的匿名实体鉴别 ZYHW 机制以补篇形式纳入 ISO/IEC 20009-4:2017，以实现高效的匿名实体鉴别。
11.	ISO/IEC 28033-1	Information Security — Fully homomorphic encryption — Part 1: General	信息安全 全同态加密 第 1 部分：总则	CD	ISO/IEC 28033-1 定义了全同态加密的一般概念和原理，包括基础定义、符号和格式，描述了其安全模型、具体安全性的难度假设、消息空间、明文空间、密文空间和密钥空间。
12.	ISO/IEC 11770-8	Information security — Key management — Part 8: Password-based key derivation	信息安全 密钥管理 第 8 部分: 基于口令的密钥派生	CD	ISO/IEC 11770-8 定义了一种密钥派生函数，即旨在以人类可记忆的口令作为输入的密钥派生函数，适用于需要从口令派生加密密钥的环境。