

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 1 期（总第 27 期）

2024 年 1 月 31 日

本期目录

国家标准研制.....	1
1. 7 项网络安全国家标准计划下达.....	1
2. 2 项国家标准征求意见稿专家审查.....	1
3. 4 项国家标准公开征求意见.....	2
4. 5 项国家标准送审稿专家审查.....	2
国际标准化推进.....	3
1. 完成 3 项国际标准文件投票和评议工作.....	3
其他.....	3
1. 2023 年网络安全标准线上知识竞赛获奖名单公布.....	3
附件 1: 2024 年 1 月在研标准项目推进工作一览表.....	4
附件 2: 3 项国际标准文件投票和评议工作一览表.....	7

▽ 国家标准研制

1.7 项网络安全国家标准计划下达

2023年12月28日，国家标准化管理委员会下达的推荐性国家标准计划中，由网安标委归口的标准项目共计7项，包括《信息安全技术 信息系统灾难恢复规范》《信息安全技术 公钥基础设施 时间戳规范》《信息安全技术 公钥基础设施 证书管理协议》等。2024年1月29日，秘书处向工作组、项目牵头承担单位印发《关于下达7项网络安全推荐性国家标准计划的通知》，请项目所属工作组制定项目推进计划，督促项目牵头承担单位按计划抓紧落实，在计划执行中要加强协调，广泛征求意见，确保标准质量和水平，按要求完成国家标准制修订任务。

2.2 项国家标准征求意见稿专家审查

1月25日，秘书处组织《信息安全技术 数据安全和个人信息保护社会责任指南》《信息安全技术 云计算服务安全能力评估方法》2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。2项标准均通过审查。详见附件1。

3.4 项国家标准公开征求意见

1月4日，《信息安全技术 网络安全产品互联互通 告警信息格式》《信息安全技术 网络安全产品互联互通 资产信息格式》《信息安全技术 信息安全管理体系 要求》《信息安全技术 信息安全风险管理指导》4项国家标准征求意见稿面向社会公开征求意见，同时秘书处书面发函征求副主任委员单位意见，征求意见期限为60天。详见附件1。

4.5 项国家标准送审稿专家审查

1月18日，秘书处组织《信息安全技术 杂凑函数 第1部分：总则》《信息安全技术 杂凑函数 第2部分：采用分组密码的杂凑函数》《信息安全技术 杂凑函数 第3部分：专门设计的杂凑函数》《信息安全技术 消息鉴别码 第2部分：采用专用杂凑函数的机制》《信息安全技术 实体鉴别 第2部分：采用可鉴别加密技术的机制》5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。5项标准均通过审查。详见附件1。



国际化推进

1. 完成 3 项国际标准文件投票和评议工作

2024 年 1 月，秘书处共组织完成 ISO/IEC 27035-4《信息技术 信息安全事件管理 第 4 部分：协同》、ISO/IEC 20008-3《信息技术 安全技术 匿名数字签名 第 3 部分：使用多公钥的机制》、ISO/IEC 27011《信息安全 网络安全和隐私保护 基于 ISO/IEC 27002 的电信组织信息安全控制》3 项国际标准文件投票和评议工作，详见附件 2。



其他

1. 2023 年网络安全标准线上知识竞赛获奖名单公布

2024 年 1 月 4 日，秘书处公布 2023 年网络安全标准线上知识竞赛获奖名单，此次知识竞赛于 2023 年 12 月 5 日至 12 月 24 日期间举办，受到社会各方的广泛关注和积极参与，来自各单位共 5000 余人参与了此次知识竞赛，对促使各相关方了解和掌握网络安全国家标准知识起到了积极的推动作用。

附件 1：2024 年 1 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	《信息安全技术 数据安全和个人信息保护社会责任指南》	该标准为组织理解数据安全和个人信息保护社会责任以及实施相关活动提供指南；适用于处理数据的组织，还适用于评价数据处理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。	已形成征求意见稿，并通过专家审查会评审。
2	20231926-T-469	《信息安全技术 云计算服务安全能力评估方法》	该标准给出了依据 GB/T 31168-2023 开展评估的原则、实施过程以及针对各项具体安全要求进行评估的方法；适用于第三方评估机构对云服务商提供云计算服务时具备的安全能力进行评估。	已形成征求意见稿，并通过专家审查会评审。
3	暂无	《信息安全技术 网络安全产品互联互通告警信息格式》	该标准规定了网络安全产品互联互通时告警信息的描述格式；适用于网络安全产品互联互通的设计、开发、应用和测试。	已形成征求意见稿，并于 2024 年 1 月 4 日至 2024 年 3 月 3 日公开征求意见。
4	暂无	《信息安全技术 网络安全产品互联互通资产信息格式》	该标准规定了网络安全产品互联互通资产信息的描述格式；适用于网络安全产品的设计、开发、应用和测试。	已形成征求意见稿，并于 2024 年 1 月 4 日至 2024 年 3 月 3 日公开征求意见。

序号	国标计划号	项目名称	标准范围	项目进展
5	20231925-T-469	《信息安全技术 信息安全管理体系 要求》	该标准规定了在组织环境下建立、实现、维护和持续改进信息安全管理体系的要求，以及根据组织需求所剪裁的信息安全风险评估和处置的要求；适用于各种类型、规模或性质的组织。	已形成征求意见稿，并于 2024 年 1 月 4 日至 2024 年 3 月 3 日公开征求意见。
6	20231924-T-469	《信息安全技术 信息安全风险管理指导》	该标准提供了信息安全风险管理指导，以帮助组织满足 GB/T 22080—xxxx 有关应对信息安全风险活动的要求；实施信息安全风险管理活动，特别是信息安全风险评估和处置。该标准适用于所有组织，无论其类型、规模或领域。	已形成征求意见稿，并于 2024 年 1 月 4 日至 2024 年 3 月 3 日公开征求意见。
7	20230242-T-469	《信息安全技术 杂凑函数 第 1 部分：总则》	该标准规定了杂凑函数的要求和通用模型，描述了杂凑运算的四个步骤，并给出了通用模型的使用方法，包含 GB/T 18238(所有部分)所共用的定义、符号和要求。	已形成送审稿，并通过专家审查会评审。
8	20230243-T-469	《信息安全技术 杂凑函数 第 2 部分：采用分组密码的杂凑函数》	该标准规定了三种采用 (n 位) 分组密码的杂凑函数。第一种杂凑函数提供长度不大于 n 位的杂凑值，第二种杂凑函数提供 2n 位的杂凑值，第三种杂凑函数提供 3n 位的杂凑值。	已形成送审稿，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
9	20230244-T-469	《信息安全技术 杂凑函数 第3部分：专门设计的杂凑函数》	该标准规定了专门设计的杂凑函数，描述了要求和模型。	已形成送审稿，并通过专家审查会评审。
10	20230252-T-469	《信息安全技术 消息鉴别码 第2部分：采用专用杂凑函数的机制》	该标准规定了采用专用杂凑函数的消息鉴别码（MAC）的用户使用要求，提供了4种采用专用杂凑函数的消息鉴别码算法；适用于安全体系结构、过程及应用的安全服务。	已形成送审稿，并通过专家审查会评审。
11	20230240-T-469	《信息安全技术 实体鉴别 第2部分：采用可鉴别加密技术的机制》	该标准规定了两类采用遵循GB/T 36624的鉴别式加密实现实体鉴别的机制；适用于指导基于鉴别式加密实现的实体鉴别系统、产品或服务的设计、开发和测试等。	已形成送审稿，并通过专家审查会评审。



附件 2：3 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 27035-4	Information technology — Information security incident management — Part 4: Coordination	信息技术 信息安全事件管理 第 4 部分：协同	DIS	该项目由中国提出。ISO/IEC 27035-4 提供协同信息安全事件管理指南，用于指导多个组织之间协同处理信息安全事件。本文件阐述了协同工作对一个组织的内部事件管理的影响，并为单个组织适应协同事件管理过程提供指南。
2.	ISO/IEC 20008-3	Information technology — Security techniques — Anonymous digital signatures — Part 3: Mechanisms using multiple public keys	信息技术 安全技术 匿名数字签名 第 3 部分：使用多公钥的机制	DIS	该项目由 SC27/WG2 提出修订。ISO/IEC 20008-3 规定了使用多公钥的匿名数字签名机制，包括机制的通用描述以及具体的匿名数字签名机制。

序号	标准编号	英文名称	中文名称	阶段	标准内容
3.	ISO/IEC 27011	Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations	信息安全 网络安全和隐私保护 基于 ISO/IEC 27002 的电信组织信息安全控制	FDIS	该项目由 SC27/WG1 提出修订。ISO/IEC 27011 在 ISO/IEC 27002 的基础上, 针对电信组织特有的信息安全风险, 提出了信息安全控制及其实 施指南。