电信和互联网行业数据安全
标准体系建设指南

2020 年 12 月

目录

前 言

随着信息技术和人类生产生活交汇融合，全球数据呈现爆发增长、海量聚集的特点，大数据产业正值活跃发展期，技术演进和应用创新并行加速推进，数据资源已成为国家基础战略性资源和社会生产的创新要素。当前，我国电信和互联网行业高速发展，汇聚大量数据，在释放数字经济发展潜力、促进数字经济加快成长的同时，面临严峻的安全风险。这要求我们深刻认识电信和互联网行业数据安全的重要性和紧迫性，坚持安全和发展并重，积极应对复杂严峻的安全风险与挑战，加速构建数据安全保障体系。

“安全发展、标准先行”，标准化工作是保障数据安全的重要基础。为落实《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》等法律法规要求，指导电信和互联网行业数据安全标准化工作，工业和信息化部组织制定了《电信和互联网行业数据安全标准体系建设指南》。

一、总体要求

以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大和十九届二中、三中、四中、五中全会精神，深入落实《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》等法律法规要求，以保障电信和互联网行业数据安全为主线，着力增加标准有效供给，不断完善技术标准体系，持续推动标准的制定、实施和国际化，支撑和引领数字经济高质量发展。

（一）基本原则。

统筹规划，全面布局。结合电信和互联网行业技术、产业发展现状及特点，发挥好行业主管部门在顶层设计、组织协调和政策制定等方面的重要作用，坚持政府引导和市场驱动相结合，建立健全电信和互联网行业数据安全标准体系。

基础先立，急用先行。从数据安全管理工作的重点和难点出发，确定重点领域，加快基础共性、关键技术、安全管理类标准的研究制定。综合考虑相关领域的数据安全现状及面临的风险和挑战，加快推进急需标准项目的研究制定。

多方参与，协同合作。充分凝聚电信运营企业、互联网企业、设备提供商、安全企业、科研院所、高校等产学研用各方力量，统筹推进标准的研究制定和实施应用。支持相关单位积极参与国际标准化活动，加强国际交流与合作。

（二）建设目标。

到2021年，研制数据安全行业标准20项以上，初步建立电信和互联网行业数据安全标准体系，有效落实数据安全管理要求，基本满足行业数据安全保护需要，推动标准在重点领域中的应用。

到2023年，研制数据安全行业标准50项以上，健全完善电信和互联网行业数据安全标准体系，标准的技术水平、应用效果和国际化程度显著提高，有力支撑行业数据安全保护能力提升。

二、主要内容

（一）标准体系框架。

电信和互联网行业数据安全标准体系包括基础共性、关键技术、安全管理和重点领域等标准。其中，基础共性标准包括术语定义、数据安全框架、数据分类分级等，为各类标准提供基础支撑。关键技术标准从数据采集、传输、存储、处理、交换、销毁等全生命周期维度，对数据安全关键技术进行规范。安全管理标准包括数据安全规范、数据安全评估、监测预警与处置、应急响应与灾难备份、安全能力认证等。重点领域标准主要是结合相关领域的实际情况和具体要求，指导行业有效开展重点领域数据安全保护工作。电信和互联网行业数据安全标准体系框架如图1所示。

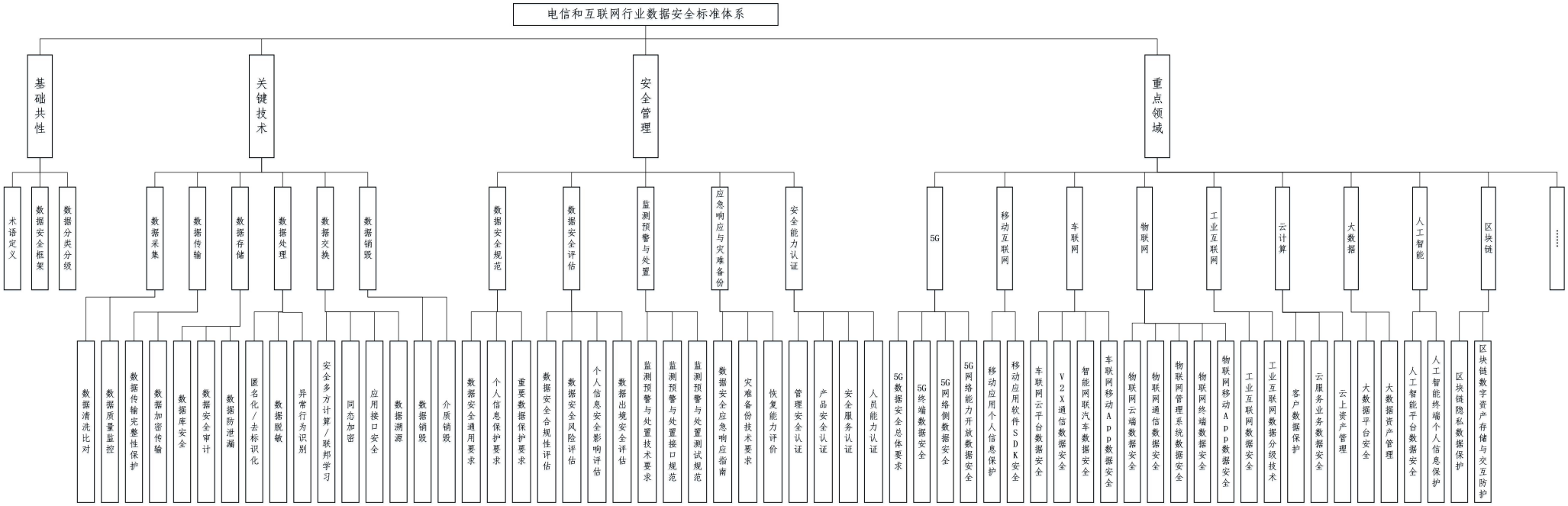

图 1 电信和互联网行业数据安全标准体系框架

（二）重点领域。

1.基础共性标准

基础共性标准是数据安全保护的基础性、通用性、指导性标准，包括术语定义、数据安全框架、数据分类分级等标准。基础共性标准子体系如图 2 所示。

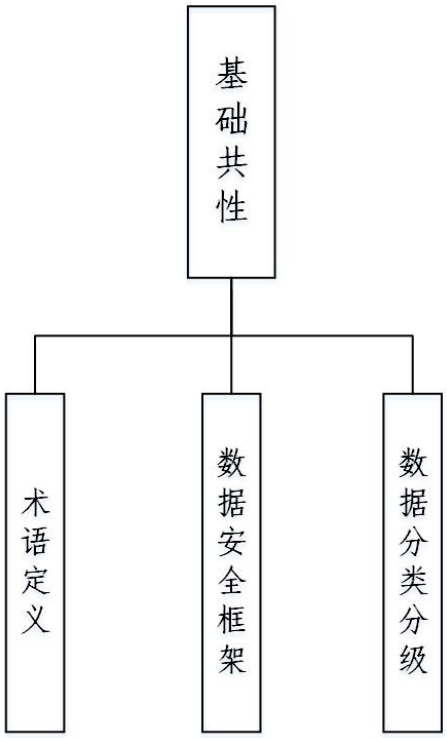

图 2 基础共性标准子体系

1.1 术语定义

术语定义用于规范数据安全相关概念，为其他部分标准的制定提供支撑，包括技术、规范、应用领域的相关术语、概念定义、相近概念之间的关系等。

1.2 数据安全框架

数据安全框架标准包括数据安全体系框架以及各部分参考框架，以明确和界定数据安全的角色、职责、边界、各

部分的层级关系和内在联系。

1.3 数据分类分级

数据分类分级标准用于指导数据分类分级，给出数据分类分级的基本原则、维度、方法、示例等，为数据安全分类、分级保护提供依据，为数据安全规范、数据安全评估等方面的标准制定提供支撑。

2.关键技术标准

关键技术标准从数据采集、传输、存储、处理、交换、销毁等全生命周期环节出发，对数据安全的关键技术进行规范。关键技术标准子体系如图 3 所示。

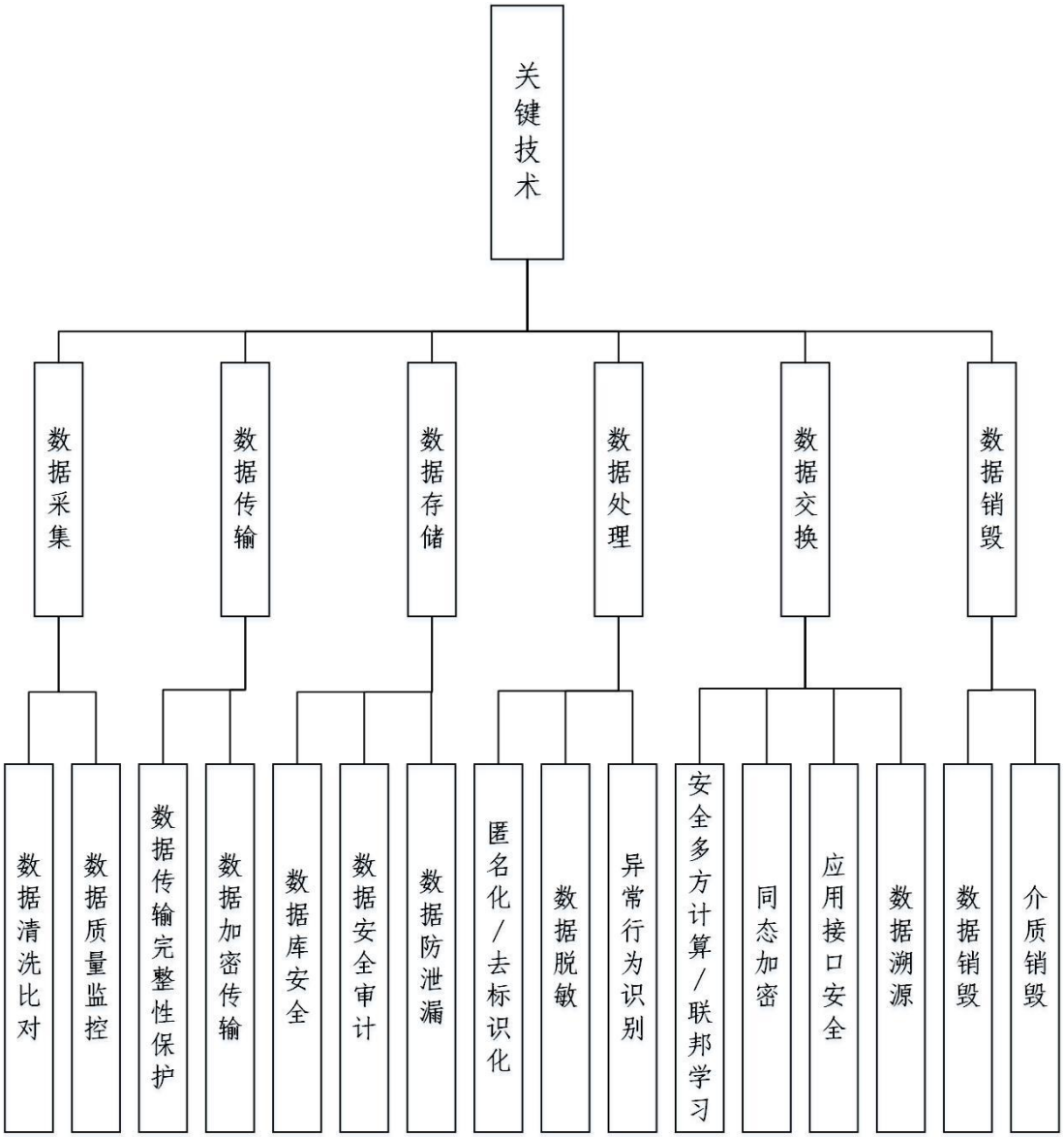

图 3 关键技术标准子体系

2.1 数据采集

数据采集标准用于规范数据采集格式、数据标签、数据审查校验等方面相关技术要求，有效提升数据质量，主要包括数据清洗比对、数据质量监控等标准。

2.2 数据传输

数据传输标准用于规范数据传输过程中可以标准化的功能架构、安全协议及其他安全相关技术要求，主要包括数

据传输完整性保护、数据加密传输等标准。

2.3 数据存储

数据存储标准用于规范存储平台安全机制、数据安全存储方法、安全审计、安全防护技术等相关技术要求，主要包括数据库安全、数据安全审计、数据防泄漏等标准。

2.4 数据处理

数据处理标准用于规范敏感数据、个人信息的保护机制及相关技术要求，明确敏感数据保护的场景、规则、技术方法，主要包括匿名化/去标识化、数据脱敏、异常行为识别等标准。

2.5 数据交换

数据交换标准用于规范数据安全交换模型、角色权责定义、安全管控技术框架，并明确数据溯源模型、过程和方法，支撑包括数据交易在内的各类场景下的数据安全共享、审计和监管，主要包括安全多方计算/联邦学习、同态加密、应用接口安全、数据溯源等标准。

2.6 数据销毁

数据销毁标准用于规范数据销毁和介质销毁的安全机制和技术要求，确保存储数据永久删除、不可恢复，主要包括数据销毁、介质销毁等标准。

3.安全管理标准

安全管理标准从数据安全框架的管理视角出发，指导行

业落实法律法规以及行业主管部门的管理要求，包括数据安全规范、数据安全评估、监测预警与处置、应急响应与灾难备份、安全能力认证等。安全管理标准子体系如图 4 所示。

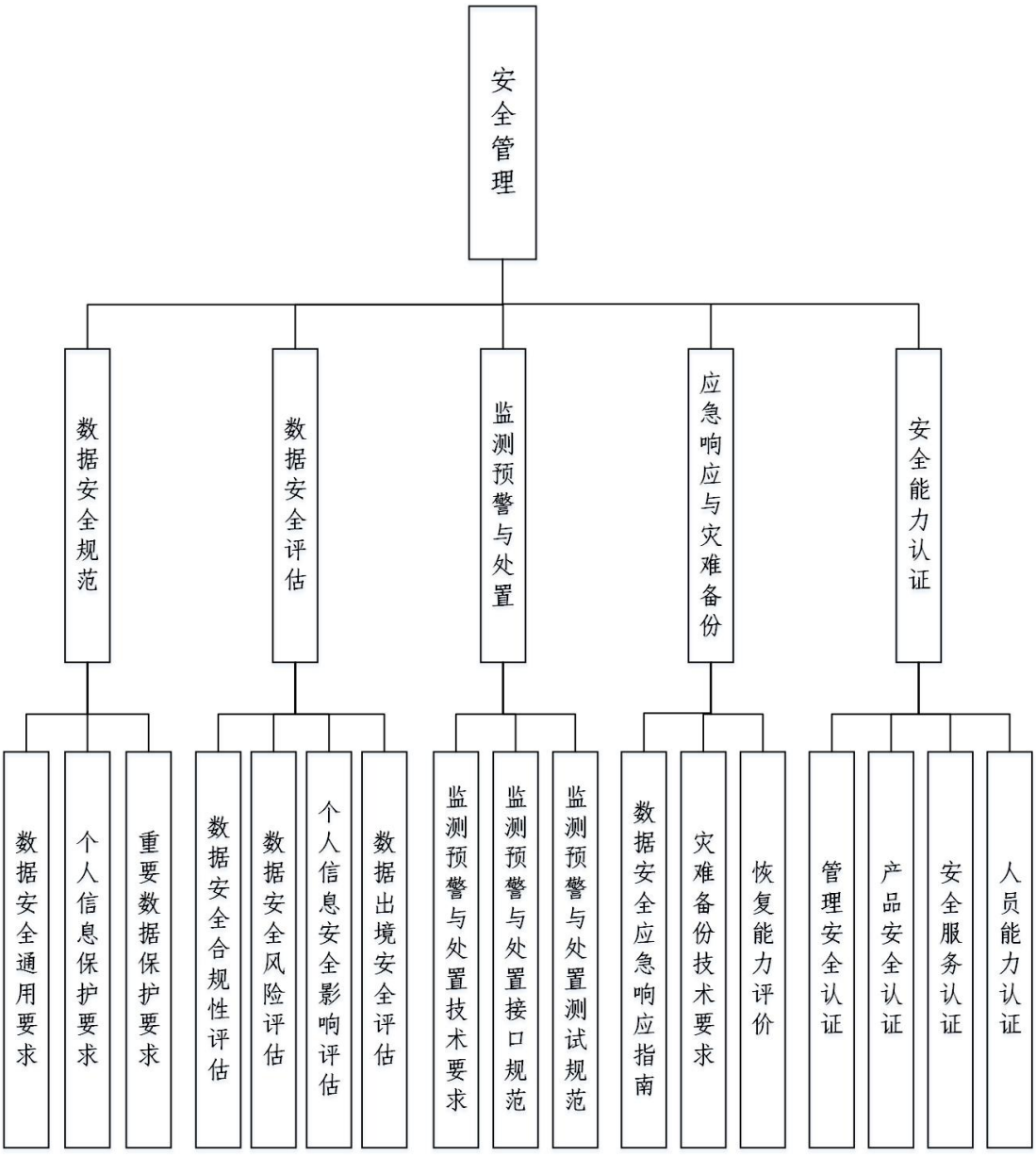

图 4 安全管理标准子体系

3.1 数据安全规范

数据安全规范标准用于落实细化相关法律法规对数据安全保护的要求，对行业开展数据安全管理提供指导和规

范，主要包括数据安全通用要求、个人信息保护要求、重要数据保护要求等标准。

3.2 数据安全评估

数据安全评估标准用于指导行业落实数据安全评估的要求，明确评估的基本概念、要素关系、分析原理、评估方法、实施流程、实施要点和工作形式等要素，指导行业规范开展数据安全评估工作，主要包括数据安全合规性评估、数据安全风险评估、个人信息安全影响评估、数据出境安全评估等标准。

3.3 监测预警与处置

监测预警与处置标准明确数据安全监测预警与处置系统及其技术要求，结合数据的敏感度、量级、流向以及账号权限等进行综合分析，实时动态追踪数据安全风险，主要包括监测预警与处置方面的技术要求、接口规范、测试规范等标准。

3.4 应急响应与灾难备份

应急响应与灾难备份标准用于规范数据安全事件的应急响应管理、处置措施，规范灾难备份及恢复工作的目标和原则、技术要求以及实施方法，主要包括数据安全应急响应指南、灾难备份技术要求、恢复能力评价等标准。

3.5 安全能力认证

安全能力认证标准用于规范组织及人员数据安全保障

能力、产品与服务数据安全保护水平、数据安全服务能力等相关认证要求，用于指导网络运营者与安全服务机构提升自身的安全能力、服务能力，主要包括管理安全认证、产品安全认证、安全服务认证、人员能力认证等标准。

4.重点领域标准

在基础共性标准、关键技术标准、安全管理标准的基础上，结合新一代信息通信技术发展情况，主要在5G、移动互联网、车联网、物联网、工业互联网、云计算、大数据、人工智能、区块链等重点领域进行布局，并结合行业发展情况，逐步覆盖其他重点领域。结合重点领域自身发展情况和数据安全保护需求，制定相关数据安全标准。重点领域安全标准子体系如图5所示。

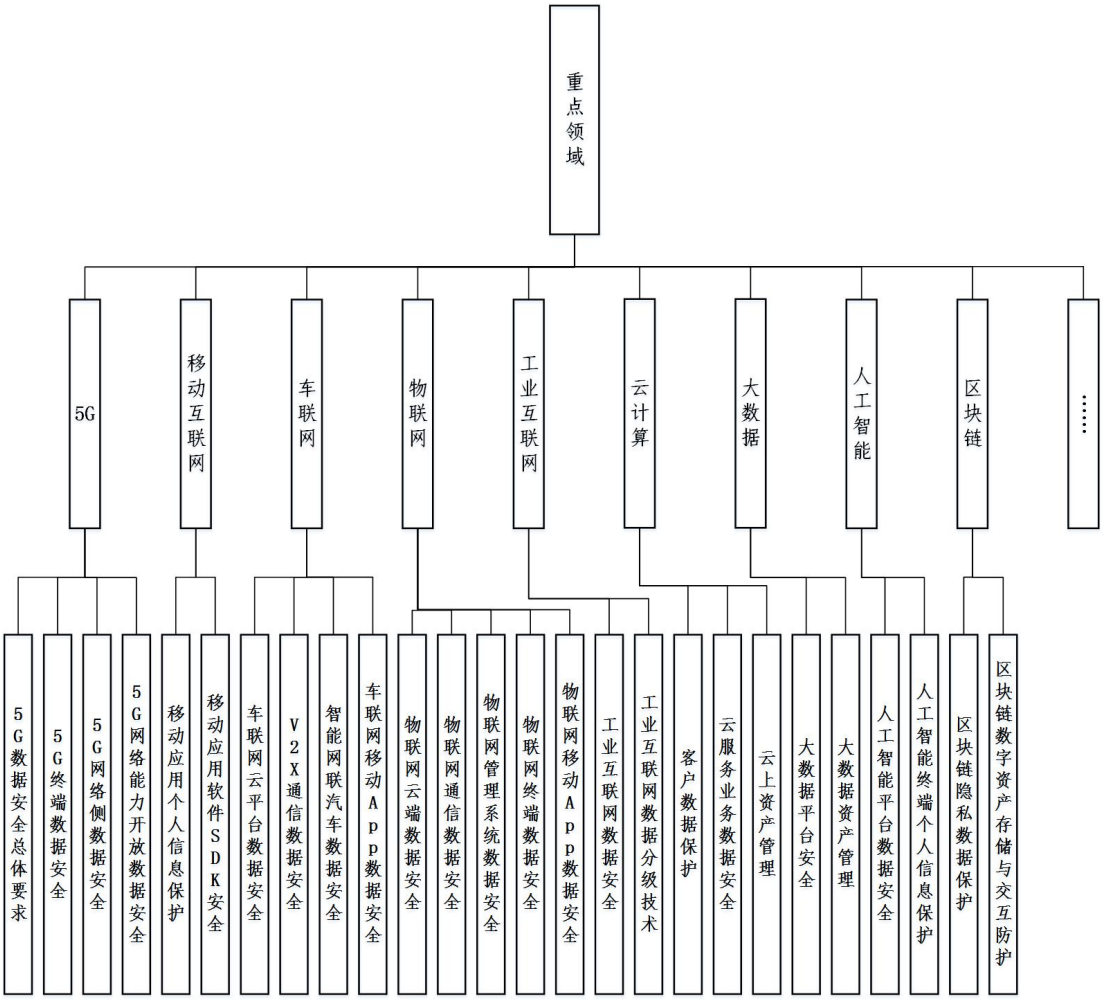

图 5 重点领域标准子体系

4.1 5G

5G 安全机制在满足通用安全要求基础上，为不同业务场景提供差异化安全服务，适应多种网络接入方式及新型网络架构，保护用户个人隐私，并支持提供开放的安全能力。5G 领域的数据安全标准主要包括 5G 数据安全总体要求、5G 终端数据安全、5G 网络侧数据安全、5G 网络能力开放数据安全等。

4.2 移动互联网

传统的移动互联网安全主要包括终端安全、网络安全和

应用安全等方面。随着开放生态体系下移动操作系统的普遍应用和数据的大规模流动，移动互联网的数据安全风险进一步凸显。移动互联网领域的数据安全标准主要包括移动应用个人信息保护、移动应用软件 SDK 安全等。

4.3 车联网

车联网安全覆盖车内、车与车、车与路、车与人、车与服务平台的全方位连接和数据交互过程，数据安全和隐私保护贯穿于车联网的各个环节。车联网领域的数据安全标准主要包括车联网云平台数据安全、V2X 通信数据安全、智能网联汽车数据安全、车联网移动 App 数据安全等。

4.4 物联网

物联网安全涵盖物联网的感知层、传输层、应用层，涉及服务端安全、终端安全和通信网络安全等方面，数据安全贯穿于其中的各个环节。物联网领域的数据安全标准主要包括物联网云端数据安全、物联网通信数据安全、物联网管理系统数据安全、物联网终端数据安全、物联网移动 App 数据安全等。

4.5 工业互联网

工业互联网安全重点关注控制系统、设备、网络、数据、平台、应用程序安全和安全管理等。工业互联网领域的数据安全标准主要包括工业互联网数据安全保护、工业互联网数据分级技术等。

4.6 云计算

云计算安全以云主机安全为核心，涵盖网络安全、数据安全、应用安全、安全管理、业务安全等方面。云计算领域的数据安全标准主要包括客户数据保护、云服务业务数据安全、云上资产管理等。

4.7 大数据

大数据安全覆盖数据全生命周期管理各环节，涵盖对大数据平台运行安全功能保障及以数据为对象进行资产管理等。大数据领域的数据安全标准主要包括大数据平台安全、大数据资产管理等。

4.8 人工智能

人工智能安全覆盖个人信息安全、算法安全、数据安全、网络安全等。人工智能领域的数据安全标准主要包括人工智能平台数据安全、人工智能终端个人信息保护等。

4.9 区块链

区块链安全包括应用服务的安全性、系统设计的安全性（包含智能合约、共识机制）、基础组件的安全性（包含网络通信、数据安全、密码技术）三个维度。区块链领域的数据安全标准主要包括区块链隐私数据保护、区块链数字资产存储与交互保护等。

三、组织实施

一是持续完善标准体系。保持体系的开放性，随着经济

社会数字化转型持续推进、数据安全认知与实践水平的不断提高，结合数据安全相关法律法规的新要求，适时修订完善标准体系。

二是加快急需标准研制。组织中国通信标准化协会等单位，加快推进重点和基础公益类行业标准研制，注重数据安全标准化工作与数据安全保护最新研究成果、行业最佳实践的有机结合。

三是推动标准应用实施。鼓励行业协会、标准化技术组织等开展面向生产者、使用者、公共利益方的标准宣传和培训，引导企业在研发、生产、管理等环节对标达标，推动标准的落地实施。

四是加强国际交流合作。鼓励企事业单位积极参与国际电信联盟（ITU）、国际标准化组织（ISO）、国际电工技术委员会（IEC）等国际标准化活动，推动相关国际标准的制定。