KSSJ/AQ12-2023

智能化矿山数据融合共享

数据安全规范

Intelligent mine data fusion and sharing

Specifications for data security

国家矿山安全监察局

2023 年 6 月

目 次

前　言

本文件参照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件起草单位： 山东能源集团有限公司、北京神州绿盟科技有限公司、中国华电集团有限公司、应急管理部信息研究院、国家能源投资集团有限责任公司、陕西煤业化工集团有限责任公司、中国中煤能源集团有限公司、云鼎科技股份有限公司、华电煤业集团有限公司、陕煤集团神木张家峁矿业有限公司、华电煤业集团数智技术有限公司、国能数智科技开发（北京）有限公司、中煤信息技术（北京）有限公司、国能神东煤炭集团有限责任公司、新华三技术有限公司、西安电子科技大学杭州研究院、山东云天安全技术有限公司、北京北矿智能科技有限公司、宁波和利时信息安全研究院有限公司、兴唐通信科技有限公司、晋能控股集团有限公司、奇安信科技集团股份有限公司、华为技术有限公司、中安智讯（北京）信息科技有限公司、云南磷化集团有限公司、精英数智科技股份有限公司、北京踏歌智行科技有限公司、青岛慧拓智能机器有限公司、山西阳光三极科技股份有限公司、北京长亭科技有限公司。

本文件技术指导：王立才、王致兵、王鹏、杨荣明、赵宇波、马世志、王瑞、徐加利、王秀林、胡而已、刘波、王卜堂、田臣、蔡峰、丁震、樊九林、王喜升、冯志华。

本文件主要起草人：施岭、杨林、张睿、赵文豪、宋雨轩、张冬阳、韩培强、杨博、赵金娥、王磊、关有利、张艳军、徐金陵、黄金、陈帅领、潘涛、邓文革、郑耀涛、王许培、杨国梁、王陈书略、黄韶杰、贺海涛、王波、王鹏、蕖帅、孙建国、李峰、朱天云、周亚清、刘旭、刘派、穆雷霆、李泽、赵闪、张雁渤、赵崇福、周道渊、王潇、杨欧、王孟来、杨建光、朱晓宁、侯宇辉、余贵珍、刘润森、艾云峰、陈龙、李晓方、宋永宝、高川。

智能化矿山数据融合共享 数据安全规范

1 范围

本文件规定了智能化矿山数据的基本安全要求、安全风险评估要求、安全管理要求、安全技术要求以及安全运营要求。

本文件适用于数据控制者安全开展智能化矿山建设相关业务。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件。不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22240-2020 《信息安全技术 网络安全等级保护定级指南》

GB/T 25069-2022 《信息安全技术 术语》

GB/T 29246-2017 《信息技术 安全技术 信息安全管理体系 概述和词汇》

GB/T 35273-2020 《信息安全技术 个人信息安全规范》

GB/T 37988-2019 《信息安全技术 数据安全能力成熟度模型》

GB/T 38667-2020 《信息技术 大数据 数据分类指南》

《网络安全标准实践指南——网络数据分类分级指引》

3 术语和定义

下列术语和定义适用于本文件。

3.1 数据安全 data security

通过管理和技术措施，确保数据有效保护和合规使用的状态。

[GB/T 37988-2019，定义3.1]

3.2 保密性 confidentiality

信息对未授权的个人、实体或过程不可用或不泄露的性质。

[GB/T 25069-2022，定义3.41]

3.3 **完整性** integrity

准确和完备的特性。

[GB/T 29246-2017，定义2.40]

3.4 **可用性** availability

可由经授权实体按需访问和使用的性质。

[GB/T 25069-2022，定义3.345]

3.5 **敏感性** sensitivity

信息拥有者赋予信息，以标明其保护需求重要程度的一种度量。

[GB/T 25069-2022，定义3.422]

3.6 **安全级别** security level

有关敏感信息访问的级别划分，以此级别加之安全范畴更精细地控制对数据的访问。

3.7 **数据处理活动** data processing activity

基于矿山数据从产生到销毁的过程，包括数据采集、数据生产、数据传输、数据存储、数据交换、数据应用、数据展示、数据销毁。

3.8 **数据采集** data acquisition

提供标准通信协议、通信接口，从矿山数据源获得原始数据，处理并转换为满足数据共享与利用需求的活动。

3.9 **数据生产** data production

原始数据或数据材料通过加工、清洗、包装、质量控制、合规性审核等手段成为新数据或数据产品的过程。

3.10 **数据传输** data transmission

数据在组织机构内部从一个实体通过网络流动到另一个实体的过程。

3.11 **数据存储** data storage

非动态数据以任何数字格式进行物理存储的阶段。根据数据热度不同，对存储量、时效性、读写查询性能等差异性要求选择合适的存储技术。

3.12 **数据交换** data exchange

数据经由组织机构内部与外部组织机构及个人在交互过程中提供数据的过程。

3.13 **数据展示** data presentation

通过可视化的手段帮助用户快速的定位和浏览数据，达到高效协同工作的目的。

3.14 **数据销毁** data destruction

对数据及数据的存储介质通过相应的操作手段，使数据彻底灭失且无法通过任何手段恢复的过程。

4 数据安全基本原则

为防范和抵御数据安全风险，矿山企业在开展智能化矿山建设过程中应遵循以下数据安全基本原则。

4.1 合法正当原则

应确保智能化矿山数据全生命周期各环节数据活动的合法性和正当性。

4.2 目的明确原则

应制定智能化矿山数据安全防护策略，明确智能化矿山数据生命周期各环节的安全防护目标和要求。

4.3 全程可控原则

应采取与智能化矿山数据安全级别相匹配的安全管控机制和技术措施，确保智能化矿山数据在数据处理活动各环节的保密性、完整性和可用性，避免数据在

数据处理活动内被未授权访问。

4.4 动态控制原则

智能化矿山数据的安全控制策略和安全防护措施不应是一次性和静态的，应可基于业务需求、安全环境属性、系统用户行为等因素进行实时和动态调整。

4.5 权责一致原则

应明确本单位数据安全防护工作相关部门及其职责，有关部门及人员应积极落实相关措施，履行数据安全防护职责。

5 数据处理活动安全要求

5.1 数据采集安全要求

5.1.1 设备安全防护

5.1.1.1 传感器数据

传感器数据具体采集安全要求如下：

a) 应选用支持标准Modbus、Profibus、Profinet等协议的传感器，智能传感器设备自身应设置登录密码。
b) 智能传感器数据通信时，应绑定IP/MAC地址。
c) 传感器应每年至少进行一次信号采集的精度检测，确保信号的准确和稳定。
d) 对于业务重要数据点的检测，应采用多点测量、多次测量的方式保证数据测量准确和安全使用。

5.1.1.2 控制器数据

控制器数据具体采集安全要求如下：

a) 应采用控制器冗余的方式加强数据采集的可用性及可靠性，对于重要的数据宜采用冗余I/O卡的方式保证数据的安全真实可用。
b) 控制器自身应具备主动防御能力，动态实时监测控制器内的运行进程，可以阻断非法的外部连接。

c) 控制器自身的运行状态及工作负荷等重要数据，宜支持记录、导出功能。

d) 控制设备应有唯一性标识，防止未经授权的修改。

e) 宜选用国产自主研发的控制器，减少控制器自身系统漏洞被利用的风险。

5.1.1.3 监控系统数据

监控系统数据具体采集安全要求如下：

a) 应对控制器与监控系统之间的数据通信进行安全防护，保证通信数据的真实性、稳定性、防窃取等。

b) 对监控系统的访问和控制应具有身份鉴别的措施。

c) 应对监控系统数据采集服务器进行主机加固。

5.1.2 业务系统安全

对于系统出现重要报警、故障、破坏、失灵将直接影响到人员生命安全或业务安全的关键系统，对其数据采集过程应重点防护，具体数据采集安全要求如下：

a) 应对关键系统及控制数据定期备份，缩短维护时间，提高维护效率。

b) 减少非必要的数据采集点。

c) 对系统的实时数据、历史数据应定期监测，确保系统的运行正常。

d) 应减少关键控制系统与外界或其他业务系统的交互。必要时采取单向传输、数据加密的方式实现互联互通。

e) 无线通信的发送端与接收端之间应采用身份认证、数据加密等方式传输，保证通信安全。

f) 应确保数据采集的高时效性，实时刷新数据最新状态。

g) 宜选择国产自主研发的数采控制器及控制系统，降低威胁侵入及数据泄露风险。

对于系统出现重要报警、故障、破坏、失灵将直接影响到安全生产的关键系统，对其数据采集过程应主要防护，具体数据采集安全要求如下：

a) 应保证数据在设定的周期下规律采集。

b) 应采用通信加密的方式降低控制系统的非法干扰。

c) 宜选择国产自主研发的数采控制器及控制系统，降低威胁侵入及数据泄

露风险。

d) 宜采用相同、少量不同的工控协议进行通信，便于观察与发现网络中异常流量行为。

用于辅助企业生产业务直接关联的控制系统，对其数据采集过程应采取防护措施，具体数据采集安全要求如下：

a) 宜选择国产自主研发的数采控制器及控制系统，降低威胁侵入及数据泄露风险。

b) 宜采用通信加密或私有协议的方式降低控制系统的非法干扰。

5.1.3 数据接入

数据接入具体安全要求如下：

a) 应明确数据的发送方、发送途径、发送方式及发送数据的类型。

b) 应严禁未知身份的发送源访问系统的数据接口。

c) 新增需要接入的数据源应报备和登记，并与现有接收方式保持一致。

d) 应严格评估数据发起端和接收端设备的物理安全和网络安全。

5.1.4 个人数据采集

个人数据采集具体安全要求如下：

a) 涉及个人数据的设备采集端和处理端应加强访问控制权限及身份鉴别，应加强数据防泄漏、数据防篡改能力。

b) 对个人真实的数据信息应采取加密或脱敏的方式后传递应用。

5.1.5 音视频数据采集

音视频数据采集具体安全要求如下：

a) 应确定对音视频检测点的实时性、清晰度需求，以避免流量过大影响带宽。

b) 应确保安全监控系统的数据与图像监视系统的数据分开采集。

5.1.6 数采对象确认

数采对象确认过程的具体安全要求如下：

a) 应确定数据采集的需求范围，秉持“最小够用”原则，避免资源浪费及错误信息采集等情况。
b) 应采用明确的、合法的数据采集方式进行采集。新增的数据采集需求，原则上与现有采集方式一致。
c) 应明确数据的用途及使用人。数据的使用人应对数据范围、用途负直接责任。
d) 应明确视频数据的数据源、数据量、数据格式、传输方式等基本属性。
e) 应明确个人数据的采集方式、传输方式、加密形式等。

5.2 数据生产安全要求

5.2.1 数据生产通用要求

矿山企业应针对生产核心数据、重要数据、一般数据采取专项安全防护，数据生产通用安全要求具体如下：

a) 保证数据机密性。生产系统核心数据、重要数据在传输、存储过程中应采取身份鉴别、数据库数据存储加密、多级密钥管理、安全备份等措施实现数据的机密性。
b) 保证数据完整性。应使用消息校验码（MAC）或数字签名等措施实现数据完整性。
c) 保证数据真实性。应使用对称加密、动态口令、数字签名等措施实现数据真实性。

5.2.2 数据生产专用要求

数据生产专用安全要求具体如下：

a) 矿山企业生产运行数据应根据重要数据安全防护措施进行防护，确保矿山生产运行数据的保密性、完整性、安全性要求。
b) 矿山企业分析统计数据应根据一般数据安全防护措施进行防护。
c) 矿山核心数据应进行数据生产备案，明确生产数据的目的和用途，明确数据生产的渠道及方法，保障数据生产渠道的合法性和正当性，向生产数据的上报归口管理部门进行备案，严禁与外部数据资源库进行互联互

通。

5.3 数据传输安全要求

5.3.1 数据传输模式

数据传输安全应能支持“请求-响应”、“订阅-发布”两类会话模型，支持基于不同会话模式提供对应的安全传输保护。两类会话模式示意图参考附录B。

5.3.2 “请求-响应”安全传输

“请求-响应”式会话的安全传输模型示意图如图B.3，具体数据传输安全要求如下：

a) “请求-响应”式会话的安全传输应支持在设备间网络传输能力的基础上构建设备级的安全传输通道。

b) “请求-响应”式会话安全应满足以下安全属性要求：

1) 传输通道两端应通过通道完成双向设备连接认证，建立互信关系。

2) 应对会话数据加密和签名后进行安全传输，保证机密性和完整性。

3) 数据传输使用的密钥宜通过协商方式确定，密钥应通过安全通道更新。

4) 客户端设备和服务端设备之间宜建立一个或多个安全传输通道，不同的会话宜复用同一个安全传输通道。

c) “请求-响应”式会话安全应满足以下安全传输通道能力要求：

1) 初始化安全通道应建立一个设备间的传输通道，完成设备间连接认证，并完成可信的安全传输通道的初始化。

2) 创建安全会话应在已初始化的安全传输通道上基于服务的安全传输策略确定会话数据安全传输模式，并完成会话的客户端身份等信息传递。

3) 关闭安全会话应清除会话的客户端身份、权限等信息。

5.3.3 “订阅-发布”安全传输

“订阅-发布”式会话的安全传输模型示意图如图B.4，具体数据传输安全要

求如下：

a) “订阅-发布”式会话的安全传输宜采用合法参与方之间“共享密钥的组播加密方案”的方式提供会话过程中传输数据的安全保护。

b) “订阅-发布”式会话安全应满足以下要求：

1) 由可信方生成会话加密和签名的密钥，应通过“请求-响应”式会话安全传递给发布端和订阅端。发布端和订阅端的身份合法性则应由可信方分别对双方进行认证来实现，确保仅特定设备可以获得消息的密钥。

2) 发布端宜使用密钥保护数据后进行广播，订阅端收到数据后可使用密钥进行解密、完整性验证，实现数据的安全传输。

5.4 数据存储安全要求

5.4.1 存储介质安全要求

数据存储介质具体安全要求如下：

a) 应建立存储介质管理要求和管理制度，以满足数据介质可靠性、可用性等安全目标。

b) 各类存储介质应根据使用情况进行安全管理，非移动存储介质要保存在受控制的区域，通过物理或者逻辑手段建立存储区域对存储介质进行保护，并将存储介质做唯一标识。

c) 应对信息系统存储介质性能进行监控，包括存储介质的剩余使用量，错误或者损坏的告警，对超过安全阈值的存储媒体介质进行预警。

d) 应严格限制移动存储介质的使用，针对生产、办公环境中计算机、服务器、工业主机等，控制其通过不必要的USB、光驱、无线等接口进行数据存储操作。仅保留工作需要的接口，并通过技术手段进行数据存储管控。

5.4.2 数据存储区域

根据数据分类分级的结果，将应用系统的存储服务器部署在对应的保护区域，重点数据保护区域应重点保护，不同的存储区域可通过物理或者逻辑隔离手段实

现。

5.4.3 数据存储加解密要求

数据存储加解密具体安全要求如下：

a) 应将数据加解密技术应用到数据存储数据库应用系统中，同时做好访问权限的控制。

b) 数据存储加解密可包括但不限于鉴别数据、重要业务数据和个人敏感数据。

c) 加密算法宜采用国密算法。

5.4.4 数据备份恢复要求

数据备份与恢复具体安全要求如下：

a) 应建立数据备份与恢复的策略和管理制度，以满足数据服务可靠性、可用性等安全目标。

b) 重要信息系统应具备数据本地/异地备份的能力以支持数据快速恢复；重要信息系统应采取冗余部署机制，保证信息系统的高可用性。

c) 指定数据备份恢复计划，宜定期开展重要信息系统数据备份恢复的演练、测试，及时发现问题，不断优化数据存储备份过程中的问题。

5.4.5 数据存储安全规则

数据存储安全规则具体如下：

a) 数据（流式数据、数据库、文件等类型的数据）在数据库存储后，应重点防范数据库内部出现DBA越权访问、数据拖库、存储介质被盗等极端情况而导致的数据泄密事故。

b) 为解决数据存储阶段的风险问题，应基于数据进行数据加密存储、数据备份和存储介质管控。

c) 应基于敏感数据识别规则，通过扫描数据库和文件存储服务器获取敏感数据分布情况。

d) 应对存储数据扫描结果进行敏感数据类型、敏感数据级别的标签管理。

e) 宜从数据源、数据表、数据字段、文件等多个维度统计敏感数据量。

f) 应依据数据分类分级的标准规范，对核心数据在存储时进行加密处理。

g) 加密后的数据应以密文的形式存储，保证在存储介质丢失或数据库文件被非法复制情况下的数据安全。

5.5 数据交换安全要求

5.5.1 数据访问安全

数据访问具体安全要求如下：

a) 应根据矿山数据安全级别，制定数据访问控制过程中的相关安全措施，同时对数据的访问请求进行监控，对异常请求进行告警。

b) 应对数据库的使用进行审计，及时发现异常查询、操作数据的情况，保障矿山数据在被访问过程中的保密性和完整性。

c) 3级数据访问应建立访问权限申请和审核批准机制，并通过访问控制组件或访问控制代理技术对访问的终端设备、系统进行控制，以及对实际操作和申请操作进行验证，保证实际操作与申请及审批操作的一致性。

d) 2级及以上的数据访问应进行身份认证，对访问者进行实名认证，将数据访问权限与实际访问者的身份或角色进行关联，防止数据的非授权访问。

e) 2级及以上的数据访问过程应留存相关操作日志，操作日志应至少包含明确的主体、客体、操作时间、具体操作类型、操作结果等。

f) 3级数据访问应实现多因素认证或二次授权，并应结合业务需要对数据采取脱敏和控制访问数据行数的技术措施。

5.5.2 数据导入导出安全

数据导入导出操作具体安全要求如下：

a) 数据的导入导出操作应明确安全责任人，设立专岗、专员，配备安全、完善的身份验证措施对导出操作人员进行实名认证。

b) 数据的导入导出操作应依据分类分级要求建立安全策略，健全授权审批流程，建立导入导出介质管理。

c) 数据的导入导出应有详细操作记录，包括操作人、操作时间、操作结果、

数据类型及安全级别等，留存时间不少于6个月。

d) 对数据导入导出的终端、用户或服务组件执行有效的访问控制，保证其身份的真实性和合法性。

e) 在导入导出完成后，应对数据导入导出通道中缓存的数据进行清除，以保证在导入导出过程中涉及的数据不会被恶意恢复。

f) 2级及以上数据的导出操作应有明确的权限申请和审核批准机制。

g) 2级及以上数据导出操作前应使用多因素认证或二次授权机制，并将操作执行的网络地址限制在有限的范围内。

h) 2级及以上的数据导出应使用加密、脱敏、访问控制等技术手段，保障数据在导入导出过程中的保密性、完整性和可用性。

i) 3级数据原则上不应导出，确需导出的，除上述要求外还应配套数据跟踪溯源机制。

5.5.3 数据共享安全

数据共享过程具体安全要求如下：

a) 应区分不同组织机构间不同的数据共享场景，结合矿山数据安全分级，对不同的数据共享场景建立相应的数据共享安全策略，明确数据共享范围的内容和数据共享的有效控制机制。

b) 应建立共享数据格式规范，如提供机器可读的格式规范，确保高效获取共享数据。

c) 应建立组织统一的数据共享交换系统，建立安全共享交换区域，综合采用数据脱敏、安全多方计算/联邦学习、同态加密、数据加密、安全通道等措施，确保矿山数据在对外共享场景中的安全合规。

d) 应对数据共享过程及共享数据进行监控审计，确保共享的数据未超出数据共享使用授权范围，并形成审计日志，日志留存时间不少于6个月。

e) 利用自动化工具如代码、脚本、接口、算法模型、软件开发工具包等进行数据共享时，应通过身份认证、数据加密、反爬虫机制、攻击防护和流量监控等手段，有效防范网络监听、接口滥用等网络攻击，并定期检查和评估自动化工具的安全性和可靠性。

f) 2级以上的数据内部共享时，应进行数据脱敏处理。若无法进行脱敏处理，应对数据进行加密、选用安全可靠的传输协议或在安全可控的环境中进行共享。

g) 2级以上的数据外部共享时，应对数据进行加密处理，并采用数据标记、签名、数字水印等技术，降低数据被泄露、误用、滥用的风险。

h) 按照国家及行业主管部门有关要求，在向行业主管和监管部门等有关机构履行数据报送义务时，应采取有效措施确保数据接收方的身份真实性，以及数据的保密性、真实性与完整性。

5.5.4 数据接口安全

数据接口具体安全要求如下：

a) 应明确对外提供业务的信息系统的服务内容，根据服务内容确定数据访问接口的范围。根据最小授权原则，对外业务系统仅提供必要的服务以及必要的数据访问API接口。

b) 应与矿山数据共享接口调用方签署合作协议，在合作协议中明确对数据的使用目的、供应方式、保密约定等。

c) 应定期对企业的对外数据接口进行清查，对不符合要求的数据接口应立即关停。

d) 应采用技术工具实现对数据服务接口调用的身份鉴别和访问控制。

e) 应具备对接口不安全输入参数进行限制或过滤的能力，为接口提供异常处理能力。

f) 应对服务接口访问提供审计能力，并能够为大数据安全审计提供可配置的数据服务接口。

g) 应对跨安全域间的服务接口调用采用安全通道、加密传输、时间戳等安全机制。

h) 系统应支持自定义sql查询，支持第三方厂家灵活的查询需求。

i) 对实时性要求较高的数据，应支持数据主动推送能力。

j) 系统数据交换应支持接口鉴权，根据不同数据权限对用户鉴权，保证数据安全。

k) 接口应支持运行时监控，对异常情况进行及时报警。

5.6 数据应用安全要求

数据应用是智能化矿山数据产生价值的出口，前期所有的数据动作应为后期的价值输出做准备。数据应用安全具体要求如下：

a) 操作合规审计
   1) 应收集并存储数据应用中的各类操作信息；
   2) 应审计数据应用的操作流程、操作权限、操作范围、操作结果等信息，记录信息可用于追踪溯源；
   3) 对不合规操作，应给予审计告警；
   4) 应提供关键字分析、关联分析和统计分析功能。
b) 内容合规审计
   1) 应进行关键字、数据格式、数据状态、归属权等的审计；
   2) 应进行数据的真实性、一致性、完整性审计；
   3) 应进行数据使用范围审计，检查是否包含用户隐私、敏感数据、重要标识等内容。
c) 应用数据输出接口管理
   1) 应提供数据输出接口类型、加密方式、传输周期的管理；
   2) 管理内容可包括接口使用用途、认证方式、日常管理等。
d) 应用数据脱敏
   1) 应在业务系统中对应用的数据进行脱敏处理，包括动态脱敏和静态脱敏；
   2) 应明确应用数据脱敏的目的、方式、算法；
   3) 对于实时应用的数据宜采取动态脱敏技术；
   4) 对于测试、开发场景中的数据宜采用静态脱敏技术。
e) 审计操作留痕
   1) 对应用数据所有审计行为宜留有记录并独立存储；
   2) 应禁止在任何情况下开放对审计结果的修改与删除权限。

5.7 数据展示安全要求

数据展示前需对数据进行保密性与完整性验证，针对涉及敏感、个人隐私的数据，确有展示必要的需在展示前进行脱敏处理，确保用户关键信息不被泄露。

数据展示过程中需进行完整性验证，防止数据篡改导致信息、事件等内容误判，降低生产管理效率甚至引发生产事故，数据展示过程具体安全要求如下：

a) 应加强数据展示前合规性与必要性检查，禁止公开展示涉及国家、行业、公司秘密的数据。对于确有必要展示的数据，严格控制受众范围与阅览权限。

b) 应针对重要业务数据、关键信息、基础设施数据、个人信息，经合规性检查后确有必要进行展示的，需经过脱敏处理后再进行展示，并于最终展示前经过责任方确认或通过审批。

c) 数据展示过程中，针对能够影响决策、生产参数设定等关键展示内容，根据所采取的技术架构，应配备防篡改控制措施，防止数据非授权篡改导致错误决策及引发安全事故。

d) 数据展示过程中，展示内容应满足数据分类分级规范要求，对于安全要求或业务价值高的数据，应配备防截屏、拍照、录像的安全控制措施，防止数据因集中化展示导致泄露，对组织收入、声誉、知识产权等带来负面影响。

5.8 数据销毁安全要求

数据销毁过程具体安全要求如下：

a) 应加强对涉外数据、敏感数据销毁等过程的监督控制。

b) 应关注数据销毁阶段所涉及的数据销毁安全管理、介质销毁安全管理等内容。

c) 在数据销毁过程中，应确保数据销毁动作执行之前有备案记录且经过审批。在技术手段上采用可靠的销毁技术，避免因销毁不彻底数据被恢复导致的数据泄漏风险。

d) 存储高密级数据的硬盘，应采用硬销毁（物理销毁、化学销毁），保障

硬盘数据不可被恢复。

e) 应对用户访问归档数据的权限进行控制，确保归档数据安全。

f) 应在中国境内对数据进行清除或销毁。

g) 数据整体迁移过程中，应杜绝数据残留。

h) 重要文档数据宜设置阅读次数、阅读时限及过期自动销毁等保护。

i) 数据销毁前宜采用归档方式将数据暂时留存，归档数据不可被直接访问。

6 数据安全风险评估要求

6.1 安全评估要求

数据安全评估相关要求如下：

a) 应建立数据安全评估相关制度规范，定期开展数据安全评估，评估的内容包括但不限于数据管理能力、数据安全能力、数据安全防护能力等，分析数据被未经授权的访问、控制、处理或数据被泄露、窃取、篡改、滥用等风险，并形成相应的数据安全评估报告。

b) 应在新业务上线、数据迁移、数据出境、数据开放共享等重大操作行为涉及第三方管理的情况下启动数据安全评估工作，分析可能存在的风险、造成的问题和影响等，并形成相应的数据安全评估报告。

c) 应及时整改数据安全评估中发现的风险隐患和问题。

6.2 风险评估要素要求

数据风险评估要素相关要求如下：

a) 风险评估基本要素应围绕业务、资产、威胁、脆弱性、安全措施和风险展开。

b) 在对基本要素的评估过程中，应充分考虑战略、安全需求、安全事件、残余风险、业务重要性和资产价值等与基本要素相关的各类属性。

c) 数据安全风险分析应包含数据资产、应用场景、威胁、脆弱性、安全措施和风险六个基本要素。

d) 数据资产应根据数据受到损害后的影响对象和影响程度进行内容识别。

e) 应用场景应根据场景中涉及到的数据资产、数据处理行为、参与主体、

数据处理环境进行内容识别。

f) 威胁的识别内容应包含动机、能力、频率和可能性等。

g) 脆弱性的识别内容应包含业务和资产弱点的严重程度。

6.3 风险分析的主要内容要求

数据风险分析的主要内容要求如下：

a) 应对数据资产进行识别，并对数据资产的重要程度进行分析与赋值。

b) 应对数据资产涉及的数据应用场景进行识别及描述。

c) 应识别数据应用场景中的威胁，对威胁频率进行赋值，并根据威胁动机、威胁能力对威胁频率进行修正。

d) 应对脆弱性进行识别，并对与具体安全措施关联分析后的脆弱性、可利用性和严重程度进行赋值。

e) 应根据威胁及威胁利用脆弱性的难易程度判断安全事件发生的可能性。

f) 应根据脆弱性的严重程度及安全事件所作用的数据资产的价值计算安全事件的损失。

g) 应根据安全事件发生的可能性以及安全事件出现后的损失，计算安全事件一旦发生对组织的影响，即风险值。

6.4 风险评估流程要求

6.4.1 风险评估准备要求

数据风险评估准备的相关安全要求如下：

a) 确定被评估对象。应进行充分的系统调研，为风险评估依据和方法的选择、评估内容的实施奠定基础。调研内容至少应包括：

1) 数据安全管理组织架构、职责和人员配备情况；

2) 数据安全管理相关制度、流程；

3) 待评估业务及相关流程，具体管理和支撑部门及其相关人员；

4) 待评估业务相关信息系统的网络拓扑结构和安全域划分；

5) 待评估IT系统的安全控制访问策略；

6) 其他。

b) 前期的系统调研可采取问卷调查、现场面谈相结合的方式进行。

c) 应根据评估的工作形式（自评估或检查评估）确定评估依据（法律、规范、要求），使之能够与组织环境和安全要求相适应。

6.4.2 数据资产识别要求

数据资产识别的相关安全要求如下：

a) 应在确定评估范围的基础上，针对评估范围内的业务，识别业务涉及的数据资产。

b) 应输出数据资产清单，包括数据类型、数据所在位置等内容。

c) 若已有数据资产清单，应判断清单是否真实、完整。

d) 在尚未建立数据资产清单的情况下，可通过如下方法开展数据调研：识别业务逻辑、业务功能、业务流程步骤等内容；识别各业务功能、流程相关信息系统；调查信息系统收集、存储、使用的业务数据；识别业务数据类型、数据所在位置、数据量、保存方式（信息系统、终端、文档服务器）等内容。

e) 应根据影响对象与影响程度两个要素识别数据重要程度并给与赋值，见表A.1。

f) 应将重要程度较高的数据资产作为评估的重点，可根据实际需求选择是否评估重要程度较低的数据资产。

6.4.3 数据应用场景识别要求

数据应用场景识别的相关安全要求如下：

a) 针对待评估的数据对象，应识别其涉及的应用场景，包括该数据对象所涉及的数据处理行为、数据处理环境、参与主体。

b) 数据处理行为宜从数据处理活动的各个阶段进行识别。

c) 数据处理环境可包括内外部系统、接口等IT支撑措施，如业务系统、移动APP、数据库服务器、文件服务器、云平台、办公终端、堡垒机等，也可包括数据处理行为所在的办公场地，如监控操作室、办公区、组织外部的公开场所等。

6.4.4 威胁识别要求

数据威胁识别的相关安全要求如下：

a) 威胁来源的识别应以组织职能和发展战略为核心。

b) 威胁来源可分为人为因素和环境因素。

c) 威胁作用形式宜包含对业务或信息系统直接或间接的攻击，也包含偶发的或蓄意的事件。

d) 判断威胁出现的频率是威胁赋值的重要内容，应根据有关的统计数据进行判断，评估环境中不同威胁出现的频率：

   1) 以往安全事件报告中出现过的威胁及其频率统计；

   2) 实际环境中通过检测工具以及各种日志发现的威胁及其频率统计；

   3) 实际环境中的监测数据发现的威胁及其频率统计；

   4) 近一两年来国际组织发布的对于整个社会或特定行业的威胁及其频率统计以及发布的威胁预警；

e) 威胁发生的可能性可结合威胁发生的动机、能力对威胁发生的频率进行修正，从而得出最终的威胁值。

f) 针对威胁识别与赋值可参考表A.2和表A.3。

6.4.5 脆弱性识别要求

数据脆弱性识别的相关安全要求如下：

a) 脆弱性识别采用的方法可包括：问卷调查、工具检测、人工核查、文档查阅、渗透性测试等。

b) 脆弱性可从技术和管理两个方面进行审视，可参考表A.4。

c) 可根据对资产的损害程度、技术实现的难易程度、弱点的流行程度，采用等级方式对已识别的脆弱性的严重程度进行赋值。

d) 数据资产的脆弱性赋值应参考技术管理和组织管理脆弱性的严重程度。

e) 脆弱性可利用性和严重程度赋值可参考表A.5。

6.4.6 已有安全措施识别要求

数据已有安全措施识别的相关安全要求如下：

a) 应对已采取的安全措施的有效性进行确认。

b) 安全措施的确认应评估其有效性，即是否真正降低了系统的脆弱性，抵御了威胁。

c) 对有效的安全措施应继续保持以避免不必要的工作和费用，防止安全措施的重复实施。

d) 对确认为不适当的安全措施应核实是否应被取消或对其进行修正，或用更合适的安全措施替代。

6.4.7 风险分析要求

数据风险分析的相关安全要求如下：

a) 风险分析应综合安全事件所作用的数据资产价值及脆弱性的严重程度，判断安全事件造成的损失对组织的影响。

b) 应根据威胁出现频率及弱点的状况，计算威胁利用脆弱性导致数据安全事件发生的可能性。

c) 在具体评估中，应综合攻击者技术能力（专业技术程度、攻击设备等）、脆弱性被利用的难易程度（可访问时间、设计和操作知识公开程度等）、数据资产吸引力等因素来判断数据安全事件发生的可能性。

d) 在计算某个数据安全事件的损失时，应将对组织的影响考虑在内。部分数据安全事件损失的判断还应参照安全事件发生可能性的结果，对发生可能性极小的安全事件可以不计算其损失。

e) 为实现对风险的控制与管理，可对风险评估的结果进行等级化处理。可将风险划分为五级，等级越高风险越高。每个等级代表了相应风险的严重程度。风险等级划分方法可参考表A.6。

6.4.8 风险评估文档记录要求

数据风险评估文档记录的相关安全要求如下：

a) 应确保文档发布前是得到批准的。

b) 应确保文档的更改和现行修订状态是可识别的（有版本控制措施）。

c) 应确保文档的分发得到适当的控制，并确保在使用时可获得有关版本的

适用文档。

d) 宜防止作废文档的非预期使用，因任何目的需保留作废文档时，应对文档进行适当标识。

e) 对于风险评估过程中形成的相关文档，可规定其标识、存储、保护、检索、保存期限以及处置所需的控制。

6.5 数据安全审计要求

6.5.1 自评估

数据自评估相关安全要求如下：

a) 自评估应在本文件的指导下，结合数据特定的安全要求进行实施。

b) 周期性进行的自评估可在评估流程上适当简化，重点针对自上次评估后系统发生变化引入的新威胁，以及系统脆弱性的完整识别，以便于两次评估结果进行对比。

c) 系统发生重大变更时，应依据本文件进行完整的评估。

d) 自评估可由发起方实施或委托风险评估服务技术支持方实施。

e) 为保证风险评估的实施，系统相关方应相互配合，防止给其他方的使用带来困难或引入新的风险。

6.5.2 检查评估

数据检查评估相关安全要求如下：

a) 检查评估宜依据本文件的要求，实施完整的风险评估过程。

b) 检查评估可在自评估实施的基础上，对关键环节或重点内容实施抽样评估，包括但不限于以下内容：

1) 自评估队伍及技术人员审计；

2) 自评估方法的检查；

3) 自评估过程控制与文档记录检查；

4) 自评估数据资产列表审计；

5) 自评估数据应用场景列表审计；

6) 自评估威胁列表审计；

7) 自评估脆弱性列表审计；

8) 现有安全措施有效性检查；

9) 自评估结果审计与采取相应措施的跟踪检查；

10) 自评估技术技能限制未完成项目的检查评估；

11) 上级关注或要求的关键环节和重点内容的检查评估；

12) 数据安全事件应对措施的检查。

c) 检查评估可委托数据安全风险评估服务技术支持方实施，但评估结果仅对检查评估的发起单位负责。

7 数据安全管理要求

7.1 管理制度与流程要求

数据管理制度与流程的具体安全要求如下：

a) 宜制定数据安全工作流程以及各类数据安全审批流程。

b) 宜制定涵盖数据处理活动各环节的管理制度，包括但不限于数据采集安全管理制度、数据传输安全管理制度、数据使用安全管理制度、数据共享安全管理制度。

c) 宜制定数据安全工作流程，明确数据安全总体策略、数据安全制度和规程、数据系统和应用安全实施细则、数据安全制度规程分发机制、数据安全制度及规程的评审、发布流程、数据安全战略规划。

d) 宜制定数据安全审批流程，明确申请、审批、总结、报备、留存等流程环节。

7.2 组织人员管理要求

应明确数据安全责任部门与责任人并进行权责角色划分，具体安全要求如下：

a) 角色可包含：数据所有者、业务系统负责人、数据安全官、数据管理员、开发人员、信息安全员、合规员、系统运维人员、测试人员等。

b) 数据安全官主导数据安全管理体系正常运行，其它岗位按照职能落实本角色对应数据安全工作的相应职责。

c) 数据采集阶段：数据所有者、合规员同步审查数据采集规范要求；开发

与测试人员负责数据采集接口及系统的研发与测试；矿山业务系统负责人负责数据合理分级、数据采集安全管理、数据源鉴别及记录、数据质量管理。

d) 数据传输阶段：信息安全员负责设计安全传输策略；系统运维人员负责传输信道的可用性维护，确保数据加密传输、网络可用性安全管理。

e) 数据存储阶段：数据管理员协同矿山业务系统负责人、信息安全员负责设计安全存储策略；系统运维人员负责存储系统可用性维护；合规员负责审查存储周期与存储介质合规要求，确保存储介质安全、逻辑存储安全、数据备份和恢复。

f) 数据处理阶段：数据所有者负责授权数据处理权限；数据安全官负责确保数据处理过程可控；信息安全员负责处理计算过程中安全策略配置；合规员负责审查数据处理计算合规要求，确保敏感数据脱敏、数据分析安全、数据正当使用、数据处理环境安全。

g) 数据交换阶段：数据所有者负责授权数据交换范围；开发与测试人员负责数据交换接口的功能开发与测试；信息安全员负责交换安全策略的设计；合规员负责审查交换与共享合规要求，确保数据导入导出安全、数据共享安全、数据发布安全、数据接口安全。

h) 数据销毁阶段：数据管理员、信息安全员或销毁专员负责数据销毁；合规员负责同步审查数据保存周期合规要求，确保数据销毁安全、介质销毁安全、介质销毁处理安全。

7.3 数据供应链管理要求

应针对供应链上下游供应商及客户提出数据安全相关要求，具体如下：

a) 组织建设方面相关要求：宜组建专职负责数据供应链安全的团队或个人。主要工作内容包括建设岗位职责、数据供应链多方协调、推动供应链管理规范的落地执行与完善等。

b) 制度流程建设方面相关要求：

1) 宜建设合作方管理协议（以合作生命周期为基础，从企业、个人等多个维度强化安全责任、安全义务、违约责任、保密协议，明确数据链

中数据的使用目的、供应方式等内容）；

2) 宜建设数据供应链安全管理规范，定义数据供应链安全目标、原则和范围，明确数据供应链的责任部门和人员、数据供应链上下游的责任和义务以及组织内部的审核原则；

3) 宜建立持续性评估机制，定期对供应链相关企业进行安全评估，并将评估结果应用于供应商选择、供应商审核等供应商管理过程中。

c) 技术建设方面相关要求：

1) 宜建设数据供应链资源库，用于管理数据供应链目录和相关数据源数据字典，便于及时查看并更新组织上下游数据链路的整体情况，并用于事后追踪分析数据供应链上下游合规情况；

2) 宜通过技术工具量化组织整体的数据供应链情况，对组织上下游的数据供应需求、对象和方式进行分类整理，能够及时发现并跟进数据供应链管理过程中的潜在风险，对数据供应链上下游的数据服务提供者和数据使用者的行为进行合规性审核和分析。

d) 人员能力建设方面相关要求：宜了解组织上下游数据供应链的整体情况，熟悉供应链安全方面的法规和标准，并具备推进供应链管理方案执行的能力。

7.4 合规性管理要求

应建立数据安全的合规性管理要求，具体安全要求如下：

a) 宜对合规制度进行评估，每项制度的建立需进行实际评估后才能够正式投入使用。

b) 宜对合规制度进行审计，建立合规制度并在进行合规管理时需要审计部门的审计评价。

c) 宜建立流程支持的合规管理。宜建立相应流程并将各个合规管理的节点纳入到整个流程中，使得合规管理工作顺利开展。

d) 宜慎重选择合规管理人员、合规流程、合规制度，保障合规管理工作的有序进行，特别在选择承担合规管理工作的人员方面需更加慎重。

e) 宜进行规制和支持的合规管理。应受到国家法律、法规和政策规制，或

不被国家法律、法规和政策否定的。

8 数据安全技术要求

8.1 数据安全监测

8.1.1 数据监测要求

数据监测具体安全要求如下：

a) 应对通信线路、主机、网络设备和应用软件的运行状况、流量、用户行为等进行监测和报警，形成记录并妥善保存。

b) 应根据监测指令对信用信息平台的双向数据流进行监测，对发现的不良信息进行记录，形成监测日志，重大问题应及时上报有关部门。

c) 应根据过滤指令对信用信息平台的双向数据流进行过滤，对发现的不良信息进行过滤处置并进行记录，形成过滤日志，重大问题及时上报有关部门。

d) 应定期对监测和报警记录进行分析、评审，发现可疑行为应形成分析报告并采取必要的应对措施。

e) 应对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行统一管理。

f) 应对系统数据的使用进行预测，以确保充足的处理速度和存储容量。

g) 应对通过平台面向公众发布的信息内容进行实时安全监控，并进行日志留存。

h) 应对用户进行审计，全程记录使用行为。

i) 应定期对运行日志和审计数据进行分析，以便及时发现异常行为。

j) 应具备对分布式拒绝服务攻击的监测与过滤能力。

8.1.2 安全审计要求

数据安全审计具体要求如下：

a) 应建立数据安全审计相关制度，明确审计目的、审计对象、审计操作规程、审计频度、审计内容、审计结果规范等。

b) 应明确数据安全审计工作涉及部门和人员的权限、责任以及相关权限的授予规程。

c) 应明确数据安全审计的内容，包括但不限于企业内部权限控制、企业数据流动跟踪情况、数据安全事件、数据安全防护措施有效性等。

d) 应在数据安全审计过程中准确记录对数据的操作时间、操作地点、操作人、操作方式、操作数据内容等信息，以及审计发现的相关安全事件。

e) 应记录并形成数据安全审计报告，并及时整改审计发现的问题。

f) 应实时检测用户对数据库进行的SQL注入和缓冲区溢出攻击，并报警或阻止攻击行为，同时详细审计攻击操作发生的时间、来源IP、登录数据库的用户名、攻击代码等详细信息。

g) 应对以下事件生成审计日志：

1) 管理员和用户鉴别；

2) 管理员和用户的操作行为；

3) 网络访问控制，包括平台、主机和数据库的远程连接、远程操作、远程数据传输。

h) 审计日志可包括事件类型、事件时间、事件主体、事件客体、用户IP、事件成功/失败、事件详细信息等字段。

i) 平台内应设置统一的时钟源并确保平台各信息设备的时间与时钟源同步，从而保证安全审计记录中事件时间的准确性。

j) 审计日志宜提供查询功能，可按以下条件之一或组合进行查询：事件类型、事件时间、触发事件用户、事件主体等。

k) 应保护审计日志不被未授权访问、修改和破坏。

l) 审计日志存储设备应采取相应措施，保证审计日志不丢失。

m) 宜提供对审计日志的统计、查询、分析、生成审计报表、导出和清空等功能。

8.1.3 定位溯源要求

数据定位溯源具体安全要求如下：

a) 应具备数据定位溯源技术能力，准确定位存在信息安全问题的应用或服

务的源头，并保存相关记录及时上报有关部门。

b) 应启用数据溯源机制，对非溯源数据进行警示。

c) 应具备出现问题后可以立即启用溯源的技术手段，确保溯源及时有效。

8.1.4 日志留存要求

日志留存的具体安全要求如下：

a) 应对数据采集、生产、传输、存储、交换、展示、销毁等环节实施日志留存管理。

b) 应根据监测指令和过滤指令对信用信息平台的数据流进行监测，形成监测日志和过滤日志。

c) 日志记录信息可包括执行时间、操作账号、处理方式、授权情况、登录信息等，并确保日志记录完整、准确。

d) 监测日志和过滤日志记录宜至少包括：源/目的IP、物理地址、源/目的端口、不良信息、采集时间以及触发监测动作的监测指令标识等。

e) 日志的留存时间应满足国家相关法律法规要求，日志留存应不少于六个月，对超过六个月的日志通过存储介质进行备份。

f) 宜提供日志查询功能，可依据时间、IP地址、URL等进行独立查询或条件组合查询。

g) 日志留存的信息存储应与其他业务系统有效隔离。

h) 应对日志操作进行权限控制，配备日志审计员，加强对日志访问和处理的管理。

i) 应记录系统管理员的操作日志，日志记录可包括：操作用户、操作时间、操作用户IP地址、操作用户物理地址、操作内容等，并定期对操作日志进行审计。

j) 应对平台中的用户信息、日志信息等负有保密义务，不得出售、篡改、伪造、删除、泄露或违法使用用户信息及日志信息。

8.1.5 数据分析要求

数据分析过程具体安全要求如下：

a) 敏感数据发现应通过多种方式配置敏感数据识别算法。内置敏感数据特征库，可对姓名、地址、电话、身份证、统一信用代码、银行卡号、日期、Email等多种敏感信息自动识别。

b) SQL风险分析宜扁平化，避免生成、二次解析和遍历复杂的抽象语法树。宜将解析和风险计算整合到同一个过程中，避免多遍处理导致的性能损失。宜使用缓存技术、缓存解释结果、授权检验和风险计算结果。

c) 用户行为分析应对用户相关行为数据进行全方面采集，针对数据自动化处理、关联分析、索引归类，管理者和审计人员可搜索任何行为操作，可定点查看相关操作日志，全面掌控用户的使用行为，确保合规安全地利用矿山数据资源。

d) 数据风险关联分析应运用可视化关联分析技术对数据风险进行综合分析，可通过图形化界面、流畅交互操作等形式提高数据分析的工作效率，减少遗漏线索，提升风险分析质量。

e) 数据风险智能化宜针对流量日志、原始告警、安全事件、资产脆弱性、资产与风险、异常用户与实体进行全面查询、统计、分析与展示，可动态拖拽统计分析与聚合字段，可通过不同图标范例（直方图、折线图、饼图、区域图等）、明细、聚合表格以及统计值进行可视化展示与分析。

f) 数据安全可视化宜包括关联关系可视化分析、网络行为透视可视化分析、流量弦图可视化分析、事件河流可视化分析、行为热度可视化分析、攻击链可视化分析等多种可视化分析方法。

8.2 数据安全防护

8.2.1 数据防护强度要求

数据防护强度具体安全要求如下：

a) 认证方式应采用密码+动态验证码的认证方式，提供数据访问的有效控制，密码应包含数字、大小写字母、特殊符号，密码长度应不低于12位，密码应定期修改。

b) 数据访问应采用授权及身份认证的方式，其中第三方证书应由权威可信

机构颁发，提供数据访问者鉴别。应采用安全的访问通道，保障对数据的安全访问，如通过web访问数据时，应提供VPN安全隧道。

c) 权限管理应采用基于用户组或角色的方法，进行用户组、角色的统一创建、管理、权限分配，保障主体访问数据的权限边界。

d) 数据隔离应对平台不同类型的数据进行逻辑隔离，不同隔离域应具有不同访问操作权限。

e) 数据传输应采用安全措施保证数据传输安全。数据传输中数字摘要应符合国家密码算法相关规定，保障数据的完整性。应能够对简单的完整性错误进行检测和恢复。

f) 数据销毁可采用消磁、高级清零或多次复写等方式，在用户要求删除数据或设备弃置、转售前将其所有数据彻底删除并无法复原。

g) 数据监控应提供数据的基本监控手段，如通过数据监控可获取数据的历史访问活动等。

h) 可采用区块链技术保障敏感数据的防篡改，并可利用区块链技术实现对数据的追踪溯源。

8.2.2 数据库安全防护要求

数据库安全防护具体要求如下：

a) 应提供数据库自动发现能力，通过对数据库网络流量的采集和数据解析，利用不同类型数据库的私有通信协议特征，实现对不同类型数据库的自动识别，同时可从协议内容获取更加精确的数据库参数，如数据库版本号、协议版本号、通信端口等信息。

b) 应提供对异常数据库访问行为采取阻断控制的能力，包括：“中断会话”和“拦截语句”两种方式。

c) 应提供SQL语句黑白名单的能力，通过SQL语法分析构建动态模型，形成SQL白名单和SQL黑名单，对符合SQL白名单的语句放行，对符合SQL黑名单的特征语句阻断。

d) 应提供“许可模型”实现白名单访问控制。“许可模型”中定义许可规则，在许可规则中定义的访问行为均应放行；不在许可规则中定义的所

有访问行为均应禁止。应提供“禁止模型”实现黑名单访问控制。“禁止模型”中定义禁止规则，在禁止规则中定义的访问行为均应禁止；不在禁止规则中定义的所有访问行为均应放行。

e) 应提供数据库操作行为审计能力，包含操作风险审计和会话事件审计。在此基础上实现通过多维的访问分析、语句分析和会话分析进行问题追踪。通过制定数据库审计策略，建立数据库操作的风险特征与审计行为的映射规则，审计引擎根据制定的审计规则对捕获的SQL语句进行专业的SQL语法分析,并根据SQL行为特征和关键特征，实现高效精准的审计分析。

f) 宜提供数据库SQL注入判断规则，可启用、停用和调整优先级。

g) 宜提供基于CVE上公开的数据库安全漏洞攻击检测判断规则库，可启用、停用和调整风险优先级。

h) 宜提供关联应用层的访问和数据库层的访问操作，可追溯到应用层最初访问的数据及请求信息，实现精确关联匹配。

8.2.3 敏感数据分类分级扫描要求

对传统数据环境和大数据环境中存储的数据做扫描发现，扫描出数据资产存储位置、数据大小、数据属性、数据属主/属组、数据描述等信息，结合元数据、数据内容、上下文等进行数据识别，具体安全要求如下：

a) 应提供矿山行业分类分级规则模板，可自动识别出敏感数据并进行分类分级标识，打标率可达到80%以上。

b) 应具备自定义规则配置能力，可根据自身业务特性自定义数据分类分级规则和模板。

c) 可对静态存储在传统关系型数据库和分布式数据库中的结构化数据、半结构化数据、非结构化数据进行主动扫描。

d) 可对扫描出的数据资产进行识别、分类、分级、存储位置记录，以数据库、数据表、数据字段、簇/列的维度，对数据资产进行统计分析，梳理数据资产分布全景图。

e) 可具备对流量实时监控、异常告警和敏感数据分类分级的审计能力，审

计分类分级数据访问者、访问接口、访问时间、访问内容、访问大小、数据分类分级等信息。对发现异常请求数据的行为进行告警，审计敏感数据的交换、共享、操作情况，为溯源和行为分析提供数据及数据流转地图。

8.2.4 数据脱敏要求

8.2.4.1 脱敏功能要求

数据脱敏应包含规则管理、数据发现、访问统计、风险审计等能力，支持多种矿山行业数据源，基于可视化的规则和内置任务进行功能实现，需要提供的能力如下：

a) 敏感数据的自动发现；
b) 多种类型的数据脱敏方式；
c) 敏感数据访问权限控制；
d) 子集脱敏；
e) 增量脱敏；
f) 脱敏水印；
g) 脱敏审批；
h) 脱敏风险评估；
i) 敏感信息的维护。

8.2.4.2 脱敏方式与要求

数据脱敏方式与相应安全要求如下：

a) 可基于脱敏算法对数据进行变形、掩盖、打乱、加密等，实现对敏感信息的脱敏，防止信息泄漏，满足数据防护策略的规定。
b) 应包括可恢复脱敏和不可恢复脱敏两类。可恢复类是指脱敏后的数据可以通过一定的方式恢复成原来的敏感数据，如加密；不可恢复类是指脱敏后的数据通过任何方式均不能恢复成原来的敏感数据，如掩盖、Hash等。可以根据实际场景进行选择。
c) 脱敏方式应支持掩盖、哈希、替换等方法，并针对不同的识别规则内置

推荐脱敏方式，通过多种内置或自定义脱敏算法实现敏感信息的脱敏，并且对通过表关联、撞库等方式进行敏感数据获取的行为进行预防，最大程度保障数据安全，防止信息泄漏。

d) 应提供数据不落地动态脱敏，通过对外暴露API接口的方式提供敏感数据的查询服务。通过准确的解析SQL语句匹配脱敏条件，对数据进行拦截脱敏。

e) 可对用户、schema、特定表等子集进行脱敏。

f) 可基于时间和主键两种方式的增量脱敏。

g) 可采用公私钥的形式对脱敏后的数据添加水印，数据泄露后根据密钥追溯数据泄露源头。

h) 数据从数据源抽取后应直接在内存中进行脱敏，不增加原始数据在脱敏产品本地硬盘中泄密的风险。

i) 进行静态脱敏时应发起审批申请，审批通过后方可执行脱敏。

j) 对已脱敏的数据进行重识别的风险评估，应经过评估后给出风险值以及需要再脱敏的字段。

8.2.4.3 访问权限控制

数据访问权限控制具体安全要求如下：

a) 应针对不同用户对访问权限控制的需求提供用户授权配置，可实现针对不同用户访问不同级别的敏感数据。

b) 应对数据源授权和系统用户授权两种模式进行脱敏授权匹配。

c) 数据源授权：数据脱敏组件只针对授权的数据源进行识别、脱敏、监控，可方便用户有针对性的进行灵活配置使用。

d) 系统用户授权：针对不同用户需要访问不同级别敏感数据的需求，提供用户授权配置，实现不同用户访问不同级别的敏感数据，达到权限控制的目的。

8.2.4.4 敏感数据展示

展示通过数据识别规则识别到的敏感字段信息，包括敏感字段所属的表、数

据源信息、敏感字段对应的识别规则等，具体安全要求如下：

a) 可对识别不准确的数据进行手动修正。

b) 可对不需要脱敏的字段进行剔除。

c) 可提供可视化的相关统计信息，包括敏感字段统计、访问统计、风险统计等，方便对系统中的数据进行多维度分析。

8.2.5 数据泄露防护要求

8.2.5.1 网络数据泄露防护

网络数据泄露防护具体安全要求如下：

a) 应基于网络出口点扫描所有通过网络途径离开安全体系的数据，以查看是否含有敏感信息。宜根据配置策略进行审计或阻止其发送。

b) 应以被动方式检查网络通信，并针对所有网络协议及内容类型，在信息离开网络之前检测其是否包含敏感数据信息，从而界定和量化数据丢失的风险。

8.2.5.2 终端数据泄露防护

终端数据泄露防护具体安全要求如下：

a) 应基于前期数据梳理结果制定数据安全防护策略。

b) 应对文件进行强制加密处理，从文件创建开始即可自动加密保护。提供主动加密能力，可根据自身需求，选择性对文档进行加密处理。通过对核心数据进行数据处理过程的保护，确保核心数据只可在企业安全域内正常、透明使用，通过任意方式将数据非法带离内部环境将无法正常使用。核心数据在加密前后对于数据合法使用者应无任何差异，不增加用户负担、不改变任何工作流程及使用习惯。文件的保存加密、打开解密完全由后台加解密驱动内核自动完成，对用户而言完全透明、无感知。

c) 应根据文件的重要程度，按照组织架构对文件进行授权管理，只允许合法授权用户根据分配权限受控使用，非授权用户即使获取数据也无法进行查阅。

d) 合法用户打开加密文件时，应对合法程序的剪切板行为进行监控，受控

程序之间可以进行内容的复制、粘贴、剪切等操作，但受控程序的内容不允许粘贴至非受控程序中。

e) 合法用户打开加密文件后，应根据副本及格式另存为的操作目的，完全识别另存为行为，自动完成数据强制加密存储，确保核心数据存储安全。

f) 合法用户打开加密文件后，应实时监控用户的截屏及录屏行为，用户发起截屏请求时（如键盘PrintScreen、QQ截屏以及其他截屏工具等），系统会自动拦截截屏请求，实现屏幕黑屏保护；用户未打开任意加密文件时，系统不对用户截屏行为进行任何控制。

g) 根据文档密级等级，应在用户使用文档时进行截屏控制。可设置指定密级及以上的文档，打开时不允许用户截取文档内容。

h) 应对用户的打印行为进行灵活控制，可实现“开/关式”打印控制，控制用户允许或禁止打印加密文件。通过打印水印的控制手段保障核心数据的打印安全及可追溯。

i) 应针对回家办公场景的终端数据泄露进行防护。将终端内的加密文件拷贝至专用的回家办公移动存储介质，并且只有具备回家办公功能的移动存储介质连接外部电脑后能够打开内部加密文件，进行文档的相关编辑工作。

j) 应利用核心数据加密及授权封装的方式，保障数据在外部环境的存储及使用安全。保障手段包含文件加密保护、安全身份校验、文件使用权限控制、文件内容安全控制。

k) 宜通过拦截操作系统或应用软件等对硬盘数据读写请求的磁盘加密终端数据泄露防护能力，实现对磁盘数据的实时加密和解密操作。

l) 应依据数据敏感内容识别，监控需要下载或写入本地磁盘的数据，并监控和阻止组织核心机密数据传输到组织外部USB设备或云盘等。

8.2.5.3 邮件数据泄露防护

应利用内容识别技术对敏感邮件进行指定处理，包括剥离敏感附件、邮件内容敏感信息脱敏/替换、阻止发送、邮件隔离审批、邮件告警、放行审计等措施。

8.2.6 数据保密强度

数据保密强度具体安全要求如下：

a) 平台数据存储应符合国家密码算法相关规定，密钥长度应不低于128位；对涉及个人隐私的重要数据，如个人身份信息等，密钥长度应不低于256位。

b) 应对信用信息平台中涉及个人隐私的重要数据进行敏感标记，避免相关敏感数据的泄露。

c) 应对信用信息平台中敏感标记的数据按照脱敏规则进行数据脱敏处理，实现敏感隐私数据的可靠保护。

d) 应明确数据隐私保护的范围和要求。

e) 应采用存储设备保护技术，保障承载数据设备的安全，并应确保未授权的恶意用户无法读取设备内容。

8.2.7 数据备份强度

数据备份强度具体安全要求如下：

a) 应提供本地数据备份与恢复功能，保障数据被破坏时可实时恢复。数据应每天增量备份，完全数据备份应至少每周一次，备份介质应场外存放。

b) 容灾应采用异地备份方式。异地灾备应确保备份中心与主中心之间具有足够的安全距离，应从地震、海啸等自然灾害影响范围考虑两中心间的安全距离，同时应明确双中心系统的切换时间，以便快速恢复。

c) 应采用冗余技术设计网络拓扑结构，应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统高可用性。

d) 若信用信息平台部署在虚拟机上，承载数据的虚拟机系统应具备高可用性，当虚拟机出现异常时，可通过自动迁移技术在其他宿主系统上运行。

e) 应定期检查和测试备份介质的有效性，确保可用性。

8.2.8 系统与设备安全管理

系统与设备安全管理相关要求如下：

a) 系统设备（服务器、交换机等）接入前，宜由安全管理机构对设备的涉

密情况、基本配置情况、用途、安装软件、使用端口和服务、MAC地址等登记备案并进行安全审核，合格后方可入网与处理信息。

b) 系统设备应根据业务需求和安全级别设置用户访问控制策略，用户权限应执行分类分级、权限最小化、权限执行一致性等原则。

c) 系统设备的用户口令应按照安全管理规定进行设置，并定期修改。

d) 应定期进行漏洞扫描，及时修补发现的系统安全漏洞。

e) 应采用边界防护、入侵防范、身份鉴别、安全审计等措施，加强承载工业互联网数据的系统与设备安全，并对系统与设备定期开展安全检测与运维管理。

9 数据安全运营要求

9.1 预警处置

应建立数据安全监测预警机制，发现数据安全缺陷、漏洞等风险时，宜立即采取补救措施。

加强数据安全风险、威胁监测预警、数据安全事件应急处置工作，结合矿山业务属性确定数据安全事件发生后的影响程度。

根据不同类别数据遭篡改、破坏、泄露或非法利用后，可能对生产、经济效益等带来的潜在影响，将安全事件级别分为一级、二级、三级3个级别。

a) 潜在影响符合下列条件之一的事件为三级事件：

1) 易引发特别重大生产安全事故或突发环境事件，或造成直接经济损失特别巨大；

2) 对国民经济、行业发展、公众利益、社会秩序乃至国家安全造成严重影响。

b) 潜在影响符合下列条件之一的事件为二级事件：

1) 易引发较大或重大生产安全事故或突发环境事件，给企业造成较大负面影响，或直接经济损失较大；

2) 引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或影响持续时间长，或可导致大量供应商、客户资源被非法获

取或大量个人信息泄露；

3) 恢复正常生产运行或消除负面影响所需付出的代价较大。

c) 潜在影响符合下列条件之一的事件为一级事件：

1) 对生产控制系统及设备、互联网平台等的正常生产运行影响较小；

2) 给企业造成负面影响较小，或直接经济损失较小；

3) 受影响的用户和企业数量较少、生产生活区域范围较小、持续时间较短；

4) 恢复正常生产运行或消除负面影响所需付出的代价较小。

d) 应在网络安全相关应急预案中明确数据安全事件的应急措施，并在相关应急演练中有针对性的开展数据安全应急演练。

e) 应在发生数据安全事件时，及时按照应急管理制度和应急预案采取应急措施。

f) 应在发生重大数据安全事件时，立即启动应急响应机制并进行处置。

g) 数据安全事件应急处置方法：

1) 紧急措施：当发现数据安全事件时，应报告数据安全事件应急响应领导小组，由应急响应领导小组组织协调人员进行检查，及时防止数据安全事件影响范围扩大；

2) 抑制处理：由应急响应日常运行部门组织协调人员排查系统及数据库、应用系统等相关日志，及时下线或切断相关业务系统外联网络并保留证据，必要时由公安机关介入。

3) 根除：应急响应领导小组组织协调相关部门、厂商工作人员对业务系统和相关日志进行检查，分析事件原因并进行总结。

h) 应建立信用数据应急处置机制，形成相应的应急处置技术能力并编制应急处理方案，以便及时处理存在信息安全问题的数据、应用或服务。

i) 在紧急情况下，应能够停止全部或部分服务并保存相关记录，及时上报有关部门。

9.2 问题通报

问题通报具体安全要求如下：

a) 加强数据安全审查工作。若发现数据被恶意更改，应立即停止服务同时检查分析被更改的原因，在被更改的原因找到并排除之前不得重新开放数据服务。

b) 网络管理部门实行节假日值班制度，开通值班电话，保证与上级主管部门和当地公安机关的热线联系。若发现异常应立即向应急小组及有关部门、上级领导报告。

c) 加强安全事件的快速反应。运行维护小组具体负责网络安全和数据安全工作，对突发的信息网络安全事件应做到以下内容：

1) 及时发现、及时报告，发现后及时向应急小组及上一级领导报告；

2) 保护现场，立即进行网络隔离，防止影响扩大；

3) 及时取证，分析、查找原因；

4) 消除有害信息，防止进一步传播，将事件的影响降到最低；

5) 在处置有害信息的过程中，任何单位和个人不得保留、贮存、散布、传播所发现的有害信息。

9.3 策略优化

策略优化具体安全要求如下：

a) 所有业务数据处理活动和信息系统的建立、使用和管理应符合信息安全策略的要求。

b) 应定期检查业务数据处理活动和信息系统安全管理是否符合信息安全策略的要求。

c) 信息系统的各级管理者有责任审查所负责系统内的安全机制是否符合信息系统安全策略。

d) 应定期对信息系统进行技术符合性检查，检查内容包括：

1) 检查各信息系统是否完全执行了所要求的安全策略标准。任何安全策略符合性检查都必须由具有专业资格的人员在有效的监督下完成；

2) 应由独立的第三方安全服务机构进行专业安全测试，包括配置核查、渗透性测试等。

e) 应对符合性检查所发现的不符合项的信息安全策略，形成书面改进意见。

f) 应对不符合项的安全策略优化改进意见进行落实和实施，并对实施后的结果进行跟踪。

g) 应建立有效的网络防病毒工作机制，及时做好防病毒软件的网络升级，保证病毒库的及时更新。

9.4 人员培训

人员培训具体安全要求如下：

a) 应建立数据安全教育培训制度，针对数据安全管理相关岗位，制定相应培训计划并对培训计划定期审核和更新。

b) 应定期开展数据安全培训，培训人员范围应覆盖企业数据安全岗位全体人员。培训结束后，宜对培训效果进行评定、记录和归档。

c) 数据安全培训内容应覆盖数据安全制度要求和实操规范等内容，如数据安全法律法规、标准制度、管理方法、合规性评估、技术防护、应急演练和相关知识技能等。

附 录 A

（规范性附录）

表 A.1　数据重要程度赋值表

赋值	标识	定义
5	很高	数据安全性遭到破坏后，对国家安全造成影响，或对公众权益造成严重影响。
4	高	数据安全性遭到破坏后，对公众权益造成一般影响，或对个人隐私或企业合法权益造成严重影响，但不影响国家安全。
3	中等	数据的安全性遭到破坏后，对公众权益造成轻微影响，或对个人隐私或企业合法权益造成一般影响，但不影响国家安全。
2	低	数据的安全性遭到破坏后，对个人隐私或对企业合法权益造成轻微影响，但不影响国家安全、公众权益。
1	很低	数据的安全性遭到破坏后，可能对个人隐私或企业合法权益不造成影响，或仅造成微弱影响但不影响国家安全、公众权益。

表 A.2　威胁来源列表

来源		描述
环境因素		断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震、意外事故等环境危害或自然灾害，以及软件、硬件、数据、通讯线路等方面的故障，或者依赖的第三方平台或者信息系统等方面的故障。
人为因素	恶意人员	不满或有预谋的内部人员对数据进行恶意破坏。采用自主或内外勾结的方式盗窃数据或进行篡改，获取利益。 外部人员利用数据安全的脆弱性，对数据的保密性、完整性和可用性进行破坏，以获取利益或炫耀能力。

	非恶意人员	内部人员由于缺乏责任心，或者由于不关心或不专注，或者没有遵循规章制度和操作流程而导致故障或数据损坏。内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致数据安全受到损害。

表 A.3　威胁可能性赋值表

等级	标识	定义
5	很高	威胁发生的可能性很高（或≥1 次/周），在大多数情况下几乎不可避免或者可以证实经常发生过
4	高	威胁发生的可能性较高（或≥1 次/月），在大多数情况下很有可能会发生或者可以证实多次发生过
3	中等	威胁发生的可能性中等（或>1 次/半年），在某种情况下可能会发生或被证实曾经发生过
2	低	威胁发生的可能性较小，一般不太可能发生，或没有被证实发生过
1	很低	威胁几乎不可能发生，仅可能在非常罕见和例外的情况下发生

表 A.4　脆弱性识别内容表

类型	识别对象	识别内容
技术脆弱性	物理环境	从机房场地、机房防火、机房供配电、机房防静电、机房接地与防雷、电磁防护、通信线路的保护、机房区域防护、机房设备管理等方面进行识别
	网络结构	从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络设备安全配置等方面进行识别
	系统软件	从补丁安装、物理保护、用户账号、口令策略、资源共享、事件审计、访问控制、新系统配置、注册表加固、网络安全、系统管理等方面进行识别

类型	识别对象	识别内容
	数据库	从用户信息、时间记录、地址信息、影响对象、使用工具、操作行为、行为结果发现结构化、半结构化以及非结构化数据库的信息
	应用中间件	从协议安全、交易完整性、数据完整性等方面进行识别
	应用系统	从审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面进行识别
管理脆弱性	技术管理	从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别
	组织管理	从安全策略、组织安全、资产分类与控制、人员安全、符合性等方面进行识别

表 A.5　脆弱性可利用性和严重程度赋值表

等级	标识	定义
5	很高	脆弱性可利用性很高，如果被威胁利用，将对业务和资产造成完全损害
4	高	脆弱性可利用性高、或很高，如果被威胁利用，将对业务和资产造成重大损害
3	中等	脆弱性可利用性较高、高或很高，如果被威胁利用，将对业务和资产造成一般损害
2	低	脆弱性可利用性一般、较高、高或很高，如果被威胁利用，将对业务和资产造成较小损害
1	很低	脆弱性可利用性低、一般、较高、高或很高，如果被威胁利用，将对业务和资产造成的损害可以忽略

表 A.6　资产风险等级划分表

等 级	标 识	描 述

5	很高	一旦发生将对业务或组织产生非常严重而深远的影响，对组织信誉严重破坏，严重影响业务或组织的正常运行，产生非常严重的经济损失或社会影响。
4	高	一旦发生将对业务、其他业务或组织产生较大的影响，在一定范围内给业务或组织的经营、组织信誉造成损害，产生较大的经济损失或社会影响。
3	中等	一旦发生将对业务或组织运行、组织信誉造成一定的影响，但对经济或社会的影响不大，不影响其他业务或对其他业务影响程度不大。
2	低	一旦发生造成的影响程较低，一般仅限于业务、组织内部或数据资产本身，通过一定手段很快能解决。
1	很低	一旦发生造成的影响低微。

附 录 B

（资料性附录）

跨组数据传输-两类会话模式

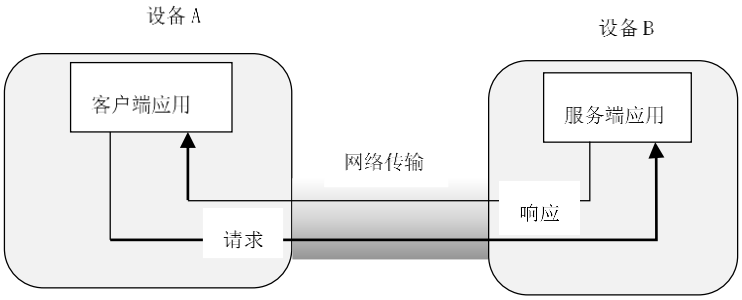

图 B.1 “请求-响应”会话模式示意

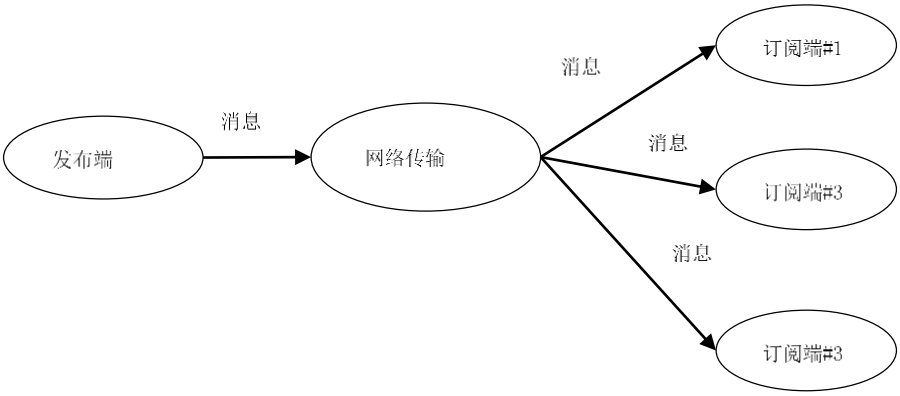

图 B.2 “订阅-发布”会话模式示意

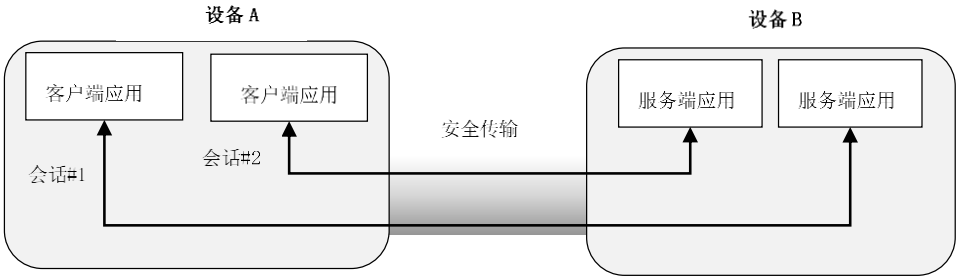

图 B.3 “请求-响应”模式的安全传输模型

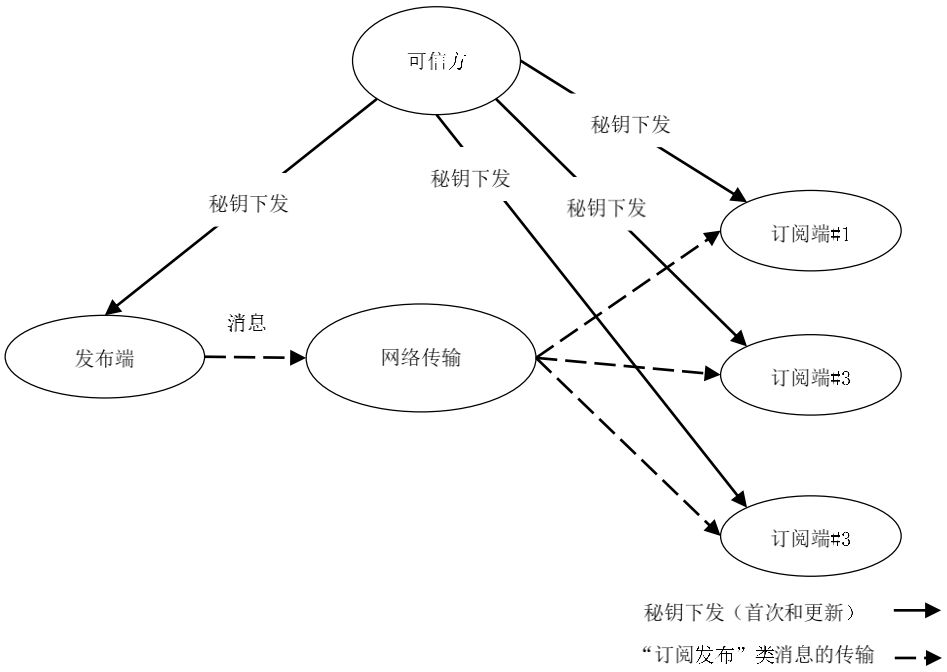

图 B.4 “订阅-发布”类消息的安全传输模型

参 考 文 献

[1] GB/T 15843.2-2017 信息技术 安全技术 实体鉴别 第 2 部分：采用对称加密算法的机制

[2] GB/T 15843.3-2017 信息技术 安全技术 实体鉴别 第 3 部分：采用数字签名技术的机制

[3] GB/T 15843.4-2017 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

[4] GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求

[5] GB/T 30976.1-2014 工业控制系统信息安全 第 1 部分：评估规范

[6] GB/T 30976.2-2014 工业控制系统信息安全 第 2 部分：验收规范

[7] GB/T 35273-2020 信息安全技术 个人信息安全规范

[8] GB/T 35274-2017 信息安全技术 大数据服务安全能力要求

[9] GB/T 36073-2018 数据管理能力成熟度评估模型

[10] GB/T 36323-2018 信息安全技术 工业控制系统安全管理基本要求

[11] GB/T 36625.3-2021 智慧城市数据融合 第 3 部分:数据采集规范

[12] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

[13] GB/T 39477-2022 信息安全技术 政务信息共享 数据安全技术要求

[14] GB/T 40050-2021 信息安全技术 网络关键设备安全技术要求 通用要求

[15] ISO/IEC 9798-3 信息安全技术 实体认证 第 3 部分：使用数字签名技术的机制（IT Security techniques-Entity authentication Part3:Mechanisms using digital signature techniques）

[16] ISO/IEC 9798-4 信息安全技术-实体认证 第 4 部分：使用密码检查功能的机制（IT Security techniques-Entity authentication Part4:Mechanisms using a cryptographic check function）

[17] RFC 1994 PPP 挑战握手认证协议（PPP Challenge Handshake Authentication Protocol (CHAP)）

[18] RFC 2246 传输层安全协议版本 1.0（The TLS Protocol Version 1.0）

[19] RFC 4279 用于传输层安全的预共享秘钥密码套件（Pre-Shared Key

Ciphersuites for Transport Layer Security (TLS)）

[20] RFC 5019 轻量级在线证书状态协议配置文件（The Lightweight Online Certificate Status Protocol (OCSP) Profile）

[21] RFC 5246 传输层安全协议版本 1.2（The Transport Layer Security (TLS) Protocol Version 1.2）

[22] RFC 5280 互联网 X.509 公钥基础设施证书和证书吊销列表配置文件 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[23] RFC 5869 基于 HMAC 的密钥提取和扩展导出函数（HMAC-based Extract-and-Expand Key Derivation Function (HKDF)）

[24] RFC 7914 基于 scrypt 密码的密钥派生函数（The scrypt Password-Based Key Derivation Function(PBKDF)）

[25] RFC 9068 OAuth 2.0 访问令牌的 JSON Web 令牌配置文件（JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens）