第 3 章 数据安全防护参考架构

本章学习目标

- 掌握数据全生命周期各阶段含义。
- 了解数据全生命周期安全体系。
- 熟悉各阶段的防护需求和安全技术。

本章编者结合数据安全产业经验，提出了数据全生命周期安全防护参考框架，再根据各个阶段的特点介绍其防护需求和实现技术。

3.1 数据全生命周期安全

数据作为一种资产，具备资产的通用属性，有完整的生命周期，在数据的整个生命周期各个环节均存在数据安全风险。数据生命周期安全则是从数据生命周期的观点出发，确保数据在生命周期的每个活动阶段的行为和特征符合预期和数据本质。因此，数据生命周期为建设数据安全提供了一种方法论。

数据全生命周期安全是一种综合性的安全理念和实践，旨在保障数据在其从采集、存储、使用、加工、传输、提供、公开到销毁的整个生命周期中的安全性。这种安全策略涵盖了从数据的生成点到最终销毁的全过程，以确保数据在各个阶段都受到适当的保护和控制，防范数据泄露、篡改、滥用和未经授权的访问。

本书根据当前各权威标准、法规，提出了新的数据生命周期，并在此基础上提出了数据全生命周期安全体系，如图 3.1 所示。该体系大致可以分为 5 部分，分别是数据安全治理、数据安全分级防护、数据安全防护技术、数据分级分类和数据安全标准规范。

1. 数据安全治理

数据安全治理包含数据安全规划、数据安全建设、数据安全运营和数据安全评估优化 4 项内容。数据安全规划阶段主要确定组织数据安全治理工作的总体定位和愿景，根据组织整体发展战略内容，结合实际情况进行现状分析，制定数据安全规划，并对规划进行充分论证。数据安全建设阶段主要对数据安全规划进行落地实施，建成与组织相适应的数据安全治理能力，包括组织架构建设、制度体系完善、技术工具建立和人员能力培养等。数据安全运营阶段通过不断适配业务环境和风险管理需求，持续优化安全策略措施，强化整个数据安全治理体系的有效运转。数据安全评估优化阶段主要是通过内部评估与第三方评估相结合的方式，对组织的数据安全治理能力进行评估分析，总结不足并动态纠偏，实现数据安全治理的持续优化及闭环工作机制的建立。关于这 4 项内容的详细介绍，请参考第 12 章。

2. 数据安全分级防护

数据安全分级防护是基于数据生命周期各个阶段的精细化安全策略。从数据采集开始，到数据存储、使用、加工、传输、提供、公开、销毁等各个环节，都面临着不同的安全挑战和风险。为了确保数据在这些阶段都得到适当的保护，数据安全分级防护提出了针对性的安全防护策

图 3.1　数据全生命周期安全体系

略。关于每个阶段所提出的策略，在本章的后续均会进行详细的介绍。

3. 数据安全防护技术

数据安全防护技术涵盖了数据加密、数据脱敏、数据访问控制、数据水印、数据容灾备份、数据安全销毁、隐私计算、数据审计、数据安全治理共 9 部分。数据加密是保障数据传输和存储安全的重要手段，通过使用加密算法和密钥管理技术，确保数据在传输和存储过程中不会被未授权访问或篡改。此外，通过对敏感数据进行脱敏处理，即在保留数据格式的同时去除或替换其中的敏感信息，可以平衡数据安全和业务需求之间的关系。数据访问控制是数据安全基础服务的重要组成部分。通过对用户身份进行验证和授权，确保只有合法用户能够访问和操作数据，有助于防止未经授权的访问和操作，保障数据的安全性和完整性。数据水印是一种用于追踪和保护数据的技术手段，通过在数据中添加特定的标记信息，可以追溯数据的来源。数据容灾备份可以拆分为数据容灾和数据备份。其中，数据容灾是为了在遭遇灾害时能保证信息系统能正常运行，数据备份是为了应对灾难来临时造成的数据丢失问题。数据安全销毁要求针对数据的内容进行清除和净化，以确保攻击者无法通过存储介质中的数据内容进行恶意恢复。隐私计算是指通过在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算，可以保障数据以“可用不可见”的方式进行安全流通。数据审计是通过对数据进行采集、转换、清理、验证和分析，帮助审计人员掌握总体情况，发现审计线索，搜集审计证据，从而进一步形

成审计结论，实现审计目标。数据安全治理以人与数据为中心，通过平衡业务需求与风险，制定数据安全策略，对数据分级分类，对数据的全生命周期进行管理，从技术到产品、从策略到管理，提供完整的产品与服务支撑。

4. 数据分类分级

数据分类分级对于数据基础制度建设具有重要意义，不仅是完善数据产权、规范数据交易的前提条件，也是维护数据安全的必要手段。国家和地方制定出台系列法律政策和标准规范，如《网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例（征求意见稿）》《工业数据分类分级指南（试行）》等，为数据分类分级提供上位法和操作指导。

5. 数据安全标准规范

在对数据进行安全防护的同时，也需要遵守相应的数据安全标准规范。当前，已有许多政府或企业等官方机构出台了数据安全的标准规范，例如 2019 年 8 月 30 日，国家市场监督管理总局和中国国家标准化管理委员会发布的国家标准 GB/T 37973—2019《信息安全技术 大数据安全管理指南》；2023 年，中关村网络安全与信息化产业联盟和数据安全治理专业委员会编著的《数据安全治理白皮书 5.0》。众多标准规范出台，不仅意味着数据安全的重要性与日俱增，更指明了数据安全的发展正朝着更加合理规范的方向稳步前进。

总体而言，数据全生命周期安全体系的作用是建立一个全面、系统的数据安全框架，保障数据在其整个生命周期中受到有效的保护，从而维护组织的声誉、确保业务的正常运作，并遵守法规和合规性要求。

此外，数据全生命周期安全体系具有多重意义，对个人、组织和社会都具有重要影响，主要体现在以下几方面。

（1）保护隐私和个人信息安全。

在今天的数字化时代，个人信息安全至关重要。通过数据全生命周期安全体系，可以确保个人信息在数据的创建、传输、存储和处理过程中得到有效保护，防止个人隐私泄露和身份盗窃等问题。

（2）维护商业机密和竞争优势。

对于企业和组织而言，数据往往是最宝贵的资产之一。数据全生命周期安全确保了商业机密和敏感信息在整个生命周期中受到保护，避免了竞争对手和恶意行为者获取关键信息，从而维护了企业的竞争优势和商业利益。

（3）确保数据的准确性和完整性。

数据在整个生命周期中可能会经历多次处理、传输和存储，这些过程中可能会出现数据损坏、篡改或丢失的风险。数据全生命周期安全通过技术手段和管理措施，确保数据的准确性和完整性，提高了数据的可信度和可用性。

（4）遵守法规和合规性要求。

许多国家和地区都制定了严格的数据安全保护法规和合规性要求，要求组织在处理数据时必须保证数据的安全和隐私。数据全生命周期安全帮助组织确保其数据处理活动符合法规和合规性要求，避免了可能的法律责任和罚款。

（5）增强信任和声誉。

组织通过有效保护数据的安全和隐私，可以增强用户、客户和合作伙伴对其的信任度，提升企业的声誉和品牌形象。信任是企业长期发展的基石，良好的数据安全措施有助于建立和维护信任关系。

（6）降低安全风险和成本。

数据泄露、数据丢失和数据被篡改等安全事件可能导致严重的商业损失和声誉损害。通过实施全生命周期安全措施，可以降低数据面临的安全风险，减少潜在的损失和成本。

3.2　数据采集安全

3.2.1　安全要求概述

数据采集安全是指根据组织对数据采集的安全要求，建立数据采集安全管理措施和安全防护措施，规范数据采集相关的流程，从而保证数据采集的合法、合规、正当和诚信。数据采集过程涉及包括个人信息和商业数据在内的海量数据，当前对个人隐私和商业秘密的保护提出了很高要求，为了防止个人信息和商业数据滥用，采集过程需要获得信息主体的授权，其间需要遵守国家相关法律、行政法规的规定和用户的约定。另外，还要在满足法律法规的前提下，在数据应用和数据安全保护之间寻找一个适度平衡。

在数据采集环节，风险威胁涵盖保密性威胁、完整性威胁，以及超范围采集用户信息等。保密性威胁指攻击者对信息流向、流量、通信频度和长度等参数的分析，窃取敏感的、有价值的信息；完整性威胁指攻击者实施数据伪造、刻意篡改、数据与元数据的错位，或者在源数据端注入破坏完整性的恶意代码。

下面将根据图 3.2 中的内容展开叙述。

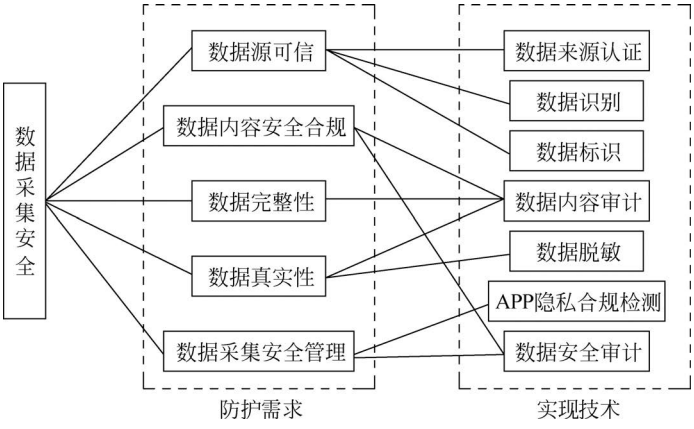

图 3.2　数据采集阶段需求——技术映射图

3.2.3　防护需求与技术

1. 数据源可信

随着数据量的增加，数据可靠性和质量变得越来越重要。可信数据是指可信任、可靠、准确的数据。在大数据领域，可信数据的重要性更是凸显。可信数据可以帮助企业更好地做出决策，提高业务效率，降低风险。

数据采集安全首要考虑的应当是数据源的安全问题。对数据采集来源进行管理的目的是确保采集数据的数据源是安全可信的，确保采集对象是可靠的。采集数据源的安全可通过数据源可信验证技术来实现，包括可信管理、身份鉴定、用户授权等。

数据来源认证是数据采集安全过程中的重要步骤，可分为数据源鉴别和数据源记录两部

分。数据源鉴别是指对收集的数据源进行身份识别，以防止组织机构采集到其他非法或不被认可的数据源产生的数据，防止采集到错误的或失真的数据；数据源记录是指对需要提供数据采集服务的数据源进行标识与记录，保证可以在必要时对数据源进行追踪和溯源。

2. 数据内容安全合规

亿万数据要素市场的有效运转，离不开数据安全合规这一基础和前提。2023 年 12 月 31 日，国家数据局等 17 个部门联合发布《“数据要素×”三年行动计划（2024—2026 年）》，对加强数据安全保障提出了系统要求。随着制度体系逐步建立健全，落实数据安全法规制度、网络安全等级保护、关键信息基础设施安全保护等制度，根据数据分类分级保护的要求，加强个人信息和重要数据的保护，成为当前数据安全合规治理的重点。

1）个人信息保护

个人信息保护是数据内容安全合规的一大关键。事实上，从我国数据合规的立法与执法案例不难窥见，其中关于个人信息的全面保护一直以来都是企业数据合规中的最关键目的和立法的制度核心。我国关于个人信息的立法保护最早可以追溯到 2004 年 1 月 1 日生效的《居民身份证法》，规定公安机关对因制作、发放、查验、扣押居民身份证而知悉的公民的个人信息，应当予以保密。而各行业的意识全面提升和技术手段跟进，是从 2017 年《网络安全法》的实施开始，从“网络信息安全”的角度明确规定了网络运营者的多项个人信息保护义务。同年，《民法总则》颁布，规定任何组织和个人不得非法收集、使用、加工、传输、提供或公开他人个人信息，从民事基本法层面确立了公民就个人信息享有权益。2020 年通过的《中华人民共和国民法典》在此基础上更进一步，以专章对“隐私权和个人信息保护”做出规定。2021 年，《个人信息保护法》出台实施，细化、完善个人信息保护应遵循的原则和个人信息处理规则，明确个人信息处理活动中的权利义务边界，健全个人信息保护工作体制机制。

《网络安全法》对收集用户信息规定了明示原则，并要求对收集的用户信息严格保密并建立健全用户信息保护制度。《数据安全法》从宏观方面对保护数据安全做出了规定，如开展数据处理活动不得危害国家安全、公共利益，不得损害个人、组织的合法权益；收集数据应当采取合法、正当的方式；应建立健全全流程数据安全管理制度，采取相应的技术措施和其他必要措施保障数据安全；开展数据处理活动应当加强风险监测；重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估等。

2）重要数据保护

2022 年 9 月 14 日发布的国家标准《信息安全技术 网络数据分类分级要求》征求意见稿给出了重要数据的定义：特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。为了加强重要数据的保护，《数据安全法》在国家数据安全制度构建方面，除了规定建立数据分类分级保护制度，数据安全风险评估、报告、信息共享、监测预警机制，数据安全应急处置机制等基本制度外，还针对重要数据规定了重要数据目录制定、数据安全审查和数据出口管制等制度。

（1）重要数据目录的制定。

制定重要数据目录一般应当考虑以下因素。

第一，数据的类型。有关国家安全、国计民生、公共利益行业或领域的数据，因其关系重大，通常应作为重要数据进行保护。其中，关系国家安全、国民经济命脉、重要民生、重大公共利益的数据，还应作为国家核心数据进行严格保护。

第二，数据的数量。数据数量往往会影响其所蕴含的社会、经济价值；数量越大，所蕴含

的社会、经济信息价值越大，发生泄露、披露或滥用时，危害国家安全和损害社会公共利益的风险越大。因此，大规模的数据应当纳入重要数据范畴。

第三，可能的危害后果。数据的重要性还可以从危害后果角度进行评估。假定数据遭到了篡改、破坏、泄露或者非法获取、非法利用，根据其对国家安全、公共利益或者个人、组织合法权益造成的危害程度，如经济损失、负面影响、持续时间等，通常可以分为三类：危害较小，危害较大，危害巨大。可能造成较大危害或巨大危害的数据，就可以纳入重要数据范围。

(2) 重要数据的安全审查制度。

数据安全审查源于《国家安全法》上的国家安全审查制度。《国家安全法》规定，国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务，涉及国家安全事项的建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险。

(3) 重要数据的出口管制制度。

根据《数据安全法》第25条规定，国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。上述有关管制物项的数据，通常也属于重要数据。与维护国家安全和利益相关的管制物项数据自然属于重要数据范畴，而与履行国家义务相关的管制物项数据，因为对该项数据的不当泄露或出口，会直接影响我国对国际义务的履行，事关我国国家信誉和国际形象，直接或间接损害国家利益，因而也应纳入重要数据范畴。

3) 数据跨境传输

当前各界对数据跨境界定仍存在差异，尚未形成统一认知。通常将其理解为“数据从一法域被转移至另一法域的行为”或“跨越国界对存储在计算机中的机器可读数据进行处理”。以“境外实体接触”为标准，数据跨境主要包括以下三类。

第一类：数据跨越国界的传输、转移行为。

第二类：尽管数据尚未跨越国界，但能够被境外的主体进行访问。

第三类：数据跨越国界采集，直接从位于另一法域的数据主体处采集数据至处理方所在地。

随着《数据安全法》《个人信息保护法》的最终颁布施行，《数据安全出境评估办法》(征求意见稿)、《网络数据安全管理条例》(征求意见稿)、《网络安全审查办法》(征求意见稿)对于执行细节制定工作的稳步推进，我国已建立了数据出境的基本合规框架，为数字经济的发展奠定了最坚实的基础。该框架一方面采纳了国际通行的数据跨境流动原则及制度，将我国的数据出境合规规则积极地融入全球数据跨境流动的规则体系中去；同时，其展现的创新性安全审查审批制度、安全与发展的平衡之道，也为全球的数据跨境流动体系做出了“中国贡献”。

针对数据内容安全合规问题，通常使用数据识别、数据标识、数据内容审计、数据脱敏、App隐私合规检测和数据安全审计等技术，以确保采集的数据符合各项法规制度和要求。数据识别技术通过对数据进行分类和识别，帮助确定哪些数据是敏感数据，从而为数据保护和合规性检测提供基础。数据标识通过对数据进行标签化，明确标识其敏感性等级和使用权限，确保合规要求得到遵守。数据内容审计通过实时监控和记录数据操作行为，及时发现数据访问和处理过程中的异常情况，保证操作的合法性和合规性。数据脱敏技术可以在保留数据的可用性同时，降低数据泄露风险。App隐私合规检测通过分析应用程序的数据收集、存储、使用和共享行为，避免数据滥用和泄露。数据安全审计技术能对数据处理和访问全过程进行全程监控和审计，确保每个环节符合合规性要求，并提供合规性报告，从而减少法律和安全风险。

3. 数据完整性

数据完整性是信息安全的三个基本要点之一，是指在传输、存储信息或数据的过程中，确

保信息或数据不被未授权地篡改或在篡改后能够被迅速发现。许多行业和法规对数据的完整性提出了具体要求，如金融行业的合规性要求、医疗行业的个人隐私保护要求等。保证数据的完整性有助于组织和企业遵守相关的合规性要求，避免面临法律责任和处罚。数据完整性的一个主要目标是防止数据在传输或存储过程中被未经授权地篡改。通过数据完整性保护机制，如加密、数字签名等技术，可以检测到数据是否被篡改，并在发现篡改时及时做出响应，保证数据的完整性。利用数据识别技术，可以准确识别和分类不同类型的数据，从而为数据完整性的保护提供基础。此外，还可以通过数据内容审计技术，进一步检验数据采集过程中的内容完整性和合规性。

4. 数据真实性

由于数据采集来源的多样性和数量庞大，以及当前生成式人工智能技术的兴起，确保采集到的数据真实可信变得异常困难。此外，在涉及个人隐私的数据采集过程中，保护数据所有者的隐私也是一个至关重要的任务。因此，为了确保数据真实性和保护隐私，需要运用相应的技术手段提供保障。

首先，数据识别可以识别数据的来源和类型，有助于验证数据的真实性，确保数据没有经过伪造或篡改。然后，数据标识通过为每类数据分配唯一标识符或标签，提供数据的追溯能力，可以验证数据的原始性和完整性。最后，通过建立真实数据规则库及采用数据内容审计技术，检验数据的真实性。通过这种方式可以创建一个基于真实数据的规则库，然后利用数据内容审计技术来验证采集到的数据是否符合这些规则，从而确保数据的可信度和真实性。

5. 数据采集安全管理

数据采集安全管理，在 GB/T 37988—2019《信息安全技术 数据安全能力成熟度模型》中描述定义为在采集外部客户、合作伙伴等相关方数据的过程中，组织应明确采集数据的目的和用途，确保满足数据源的真实性、有效性和最少够用等原则要求，并明确数据采集渠道、规范数据格式以及相关的流程和方式，从而保证数据采集的合规性、正当性、一致性。

在数据采集安全管理环节，通常采用 App 隐私合规检测和数据安全审计等技术。App 隐私合规检测是一种评估和确保移动应用程序(App)在处理用户个人信息时遵守相关法律法规的过程。这个过程包括对 App 的隐私政策文本的合规性(形式合规)和代码层面的合规性(实质合规)进行检查。检测的目标是从个人信息收集、权限使用场景、超范围采集、隐私政策、三方 SDK 等多个维度帮助企业和开发者提前识别 App 隐私合规相关风险，规避监管通报、应用下架等重大风险。对于数据安全审计，陕西省地方标准 DB 61/T 1636—2022《数据安全审计规范》给出的定义是，对被审计对象的数据在数据安全运营、数据安全风险、数据安全事件中的合规性和安全性进行审查、监督与持续改进。数据安全审计涉及的技术包括数据加密技术、访问控制技术、身份认证技术、审计追踪技术等，利用这些技术能够有效规避数据采集过程中的风险。

通过上述严格的数据采集安全管理措施，可以有效预防数据泄露、篡改、损坏等风险，保护个人隐私和机密信息不受未经授权的访问和利用。同时，数据采集安全管理也有助于提升数据质量和可信度，为数据分析、决策和创新提供可靠的基础。

3.3 数据存储安全

3.3.1 安全要求概述

数据存储安全是指根据组织内部数据存储安全要求，提供有效的技术和管理手段，防止对

存储介质的不当使用而可能引发的数据泄露风险，并规范数据存储的冗余管理流程，保障数据可用性，实现数据存储安全。数字经济时代，信息技术已经渗透到生活的方方面面，人工智能、大数据、5G 等新技术发展使得数据量呈指数级增长，数据激增带来存储计算需求的飞速增长，为数据存储安全带来了新需求、新挑战和新机遇。

在数据存储环节，风险威胁来自外部因素、内部因素、数据库系统安全等。外部因素包括黑客脱库、数据库后门、挖矿木马、数据库勒索、恶意篡改等；内部因素包括内部人员窃取、不同利益方对数据的超权限使用、弱口令配置、离线暴力破解、错误配置等；数据库系统安全包括数据库软件漏洞和应用程序逻辑漏洞，如 SQL 注入、提权、缓冲区溢出，存储设备丢失等其他情况。

本节将通过先介绍数据存储合规、数据存储安全、存储完整性和数据时效性来讲述数据存储安全的防护需求，然后简单介绍数据加密、数据容灾备份、数据脱敏、访问控制和数据安全审计等技术，如图 3.3 所示。

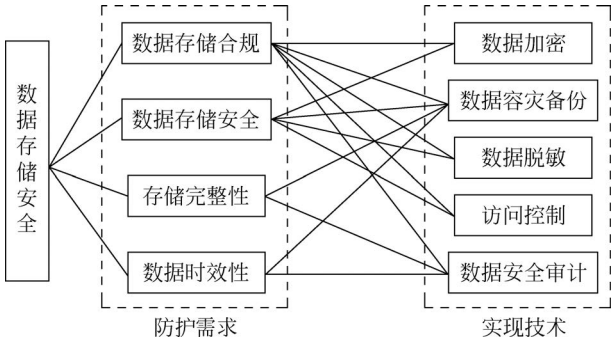

图 3.3　数据存储安全需求-技术映射图

3.3.2　防护需求与技术

1. 数据存储合规

1）存储期限

不同的法律法规及文件针对存储时间有着不同的规定，这些规定往往基于不同的行业标准、数据类型和法律要求。理解和遵守相关法律法规以及内部政策对于确定数据存储时间非常重要。应根据自身业务需求、法律要求和最佳实践制定合适的数据管理策略，确保数据存储合规性。这里总结了部分数据存储时间的明文规定，如表 3.1 所示。

表 3.1　数据存储时间规定

依 据 法 条	具 体 规 定
《网络安全法》第 21 条	网络运营者应当履行以下安全保护义务：制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任，采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；采取监测、记录网络运行状态网络安全事件的技术措施，并按照规定留存相关的网络日志不少于 6 个月
《个人信息保护法》第 19 条	除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间

续表

依据法条	具体规定
GB/T 35273—2020《信息安全技术个人信息安全规范》第 6.1a)	个人信息存储期限应为实现个人信息主体授权使用的目的所必需的最短时间，法律法规另有规定或者个人信息主体另行授权同意的除外。超出上述个人信息存储期限后，应对个人信息进行删除或匿名化处理
《数据安全管理办法（征求意见稿）》第 20 条	网络运营者保存个人信息不应超出收集使用规则中的存储期限，用户注销账号后应当及时删除其个人信息，经过处理无法关联到特定个人且不能复原（以下称匿名化处理）的除外
《网络游戏管理暂行办法》第 19 条	网络游戏运营企业发行网络游戏虚拟货币的，应当遵守以下规定：（三）保存网络游戏用户的购买记录。保存期限自用户最后一次接受服务之日起，不得少于 180 日
《网络游戏管理暂行办法》第 20 条	网络虚拟货币交易服务企业应当遵守以下规定：（四）接到利害关系人、政府部门、司法机关通知后，应当协助核实交易行为的合法性。经核实属于违法交易的，应当立即采取措施终止交易服务并保存有关记录。（五）保存用户间的交易记录和账务记录等信息不得少于 180 日
《互联网直播服务管理规定》第 16 条	互联网直播服务提供者应当记录互联网直播服务使用者发布内容和日志信息，保存 60 日

2）存储范围

《网络安全法》第 41 条规定：网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

由此可见，网络运营者想要搜集、存储个人信息，应当遵循“必要性原则”。

《个人信息保护法》第 6 条也指出，处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息，存储数据的范围应当为实现目的的最小范围。

为了实现数据存储合规，从技术层面上来说可以分为存储内容、访问控制、存储安全管理三个部分。首先，针对存储内容本身的安全，通常用到的技术包括数据加密、数据容灾备份和数据脱敏。数据加密能确保被存储数据的完整性和机密性，数据容灾备份可以应对数据丢失的情况，数据脱敏能够保护数据的隐私。其次，访问控制技术在数据存储安全中的作用主要体现在保护数据隐私、防止数据泄露和篡改、遵守合规性要求，以及管理数据权限等方面，是确保数据存储安全和合规性的重要手段之一。最后，存储安全管理需要用到数据安全审计技术，来发现安全漏洞、监控数据访问、合规性验证、事后追溯和调查。对于上述技术，读者可以翻阅教材第 2 部分——数据安全原理与技术，进行更加深入的学习。

2. 数据存储安全

数据存储安全可以确保个人和敏感信息的保密性，例如，使用数据加密和数据脱敏技术对数据的完整性和隐私提供保障。对于个人、企业和组织来说，数据是宝贵的资产，其中可能包含有关客户、员工、合作伙伴以及业务运营的敏感信息。通过采取合适的安全措施，如访问控制可以防止未经授权的访问和数据泄露，保护个人隐私和敏感信息的安全。数据存储安全措施还可以确保数据的完整性和可用性。例如，数据丢失或损坏可能由多种原因引起，如硬件故

障、自然灾害、人为错误等。而通过定期备份数据、实施冗余存储和恢复策略，可以最大限度地减少数据丢失风险，并保证数据在需要时能够及时恢复。

3. 存储完整性

存储完整性指的是数据在存储过程中保持完整、不被篡改或损坏的状态。这种完整性的保证对于数据的可信度、可靠性和可用性至关重要。数据在存储过程中如果遭到意外损坏或篡改，可能导致数据不可用或不完整，进而影响到数据的使用和分析。通过确保存储完整性，可以最大程度地减少数据损坏或篡改的风险，确保数据的可靠性和可用性，保障业务的正常运行，此种情况通常会使用数据容灾备份技术来实现。而数据安全审计可以通过分析审计日志，发现数据存储系统中存在的潜在安全风险和漏洞。例如，检测到频繁的登录失败或异常的数据访问行为可能暗示着未经授权的访问尝试，需要及时进行调查和处理，以防止数据泄露或篡改等安全事件发生。

4. 数据时效性

数据时效性是指数据在不同的时间具有很大的性质上的差异，这个差异性定义为数据时效性，时效性影响着数据质量，随着时间的推移，数据质量会快速地下降。

数据的时效性对数据确权、入表、交易等方面都有很大影响。一是在数据确权方面，由于原始数据贬值最快，因此，原始数据所有者对数据的权益最小，甚至可以忽略不计；二是在数据定价和入表方面，由于数据贬值速度快，当企业将数据产品以无形资产或存货科目计入企业资产时，应该计提相应的大比例的无形资产减值准备或存货减值准备；三是在数据交易方面，对数据卖方来说，数据交易的前期沟通时间越长，其拥有数据的价值就越低，而对于数据买方来说，交易的数据对象如果没有及时交付，其价值就会大打折扣。因此，对数据时效性的把控是一个重要任务。

通常，在突发情况下导致的数据丢失会破坏已存储数据的时效性，此时需要使用数据容灾备份技术进行及时补救。例如，在日常工作时需要制定备份计划，备份数据到磁带、硬盘等存储介质中，并存放在安全的地方，以便需要时进行数据恢复。此外，数据安全审计在数据时效性方面的作用主要是确保数据的处理、传输和存储过程中能够及时准确地反映数据的最新状态，从而保障数据的时效性和可用性。

3.4　数据使用安全

3.4.1　安全要求概述

数据使用指通过数据分析和数据可视化等技术从数据中提取信息，提炼出有用知识和价值的系列操作。数据使用的主要操作包括但不限于数据查询、数据读取、数据索引、批处理、交互式处理、流处理、数据统计分析、数据预测分析、数据关联分析、数据可视化、生成分析报告等。

在数据使用环节，风险威胁来自于外部因素、内部因素、系统安全等。外部因素包括账户劫持、APT 攻击、身份伪装、认证失效、密钥丢失、漏洞攻击、木马注入等；内部因素包括内部人员、DBA 违规操作窃取、滥用、泄露数据等，如非授权访问敏感数据、非工作时间、工作场所访问核心业务表、高危指令操作；系统安全包括不严格的权限访问、多源异构数据集成中隐私泄露等。针对上述威胁需要采取众多防护技术予以保障。下面将根据图 3.4 对本节内容展开介绍。

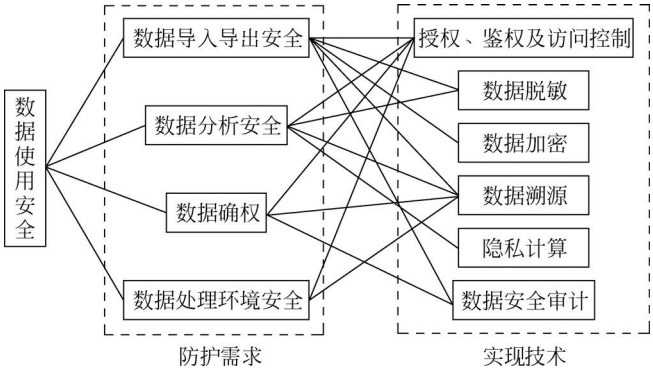

图 3.4　数据使用安全需求-技术映射图

3.4.2　防护需求与技术

1. 数据导入导出安全

数据导入导出是数据交换过程中的重要步骤，因为在数据交换的过程中存在着大量数据导入导出的场景及需求，而在此过程中，由于导入导出的数据量一般来说都是比较大的，因此数据导入导出过程更容易成为攻击者瞄准的目标。数据导入导出过程面临着十分严峻的数据泄露、数据篡改等安全风险，所以进行数据导入导出安全管理的建设十分有必要。通过数据导入导出过程中对数据的安全性进行管理，防止数据导入导出过程中可能对数据自身的可用性和完整性构成的危害，降低可能存在的数据泄露风险。

数据导入导出安全的技术工具应从两方面来设计：一方面是数据导入安全，其作用是防止导入恶意数据，造成数据被篡改或破坏；另一方面是数据导出安全，其作用是防止导出未授权的数据，造成敏感信息泄露。完整的数据导入导出安全工具应该同时包含两方面。其次，由于导入导出作业的数据量一般都比较大，因此数据导入导出安全的技术工具还需要具备对导入导出的数据进行可用性和完整性校验的功能。

数据导入导出安全的全流程必须包含以下几个技术。

（1）授权、鉴权及访问控制。

只有通过身份认证的用户才可以使用数据导入导出管理平台/工具，进行后续的数据导入导出作业，身份认证应为多因素认证。不同的身份访问数据导入导出管理平台/工具，会获得不同的数据导入导出权限，权限分配应遵循“最小够用”原则。

（2）数据脱敏。

导入数据时进行脱敏处理可以防止内部人员造成的数据泄露，导出数据时对某些敏感数据进行脱敏可以保护数据所有者的隐私。

（3）数据加密。

在数据导入或导出阶段对数据进行加密，可以在数据传输过程中确保数据的完整性不被破坏。

（4）数据溯源。

将数据溯源技术应用于数据导入导出阶段，可以确保数据在传输过程中出现被篡改、伪造或发生泄漏等情况时，能够追本溯源，以明确责任承担方。

（5）数据安全审计。

在执行数据导入操作时，在进行最终的导入之前，需要对数据的格式、安全性和完整性等

进行审计，只有通过审计的数据，才允许执行最终的导入动作；在执行数据导出操作时，需要对导出的数据先进行完整性校验，校验通过后才能结束导出作业。

上述几种技术的详细内容读者可查阅本教材第2部分数据安全原理与技术的相应章节。

2．数据分析安全

通过在数据分析过程中采取适当的安全控制措施，可以防止数据挖掘、分析过程中有价值信息和个人隐私泄露的安全风险。在当前信息爆炸的时代，数据面临着越来越多的威胁。黑客、病毒、恶意软件等安全风险无时不在，数据泄露和信息窃取的事件也屡见不鲜。数据安全分析的重要性体现在以下几方面。

（1）及早发现潜在的安全威胁，避免数据遭受损失。

（2）提高数据安全性和保密性，保护个人隐私和商业机密。

（3）加强对数据的监控和管理，防止未授权的访问和篡改。

（4）遵守相关法律法规，避免因数据泄露而面临的法律风险和商誉损失。

通常在数据分析中，为了提供安全保障，会采用访问控制、数据脱敏、数据溯源、隐私计算等技术。通过权限管理和身份验证，限制用户对数据的访问，确保只有授权用户可以访问敏感数据，并根据其权限级别控制其对数据的操作。在分析之前对数据进行脱敏处理，可以减少敏感信息的泄露风险。此外，使用数据溯源确保对数据的修改、操作都可以被追溯和审计。隐私计算则通过加密技术或安全多方计算等方法，确保在数据分析过程中保护用户隐私，防止敏感数据暴露。

3．数据确权

所谓数据确权，是通过对数据处理者等赋权，使其对数据享有相应的法律控制手段，从而在一定程度或范围内针对数据具有排除他人侵害的效力。数据确权有利于激励数据生产，有利于促进数据流通，有利于解决“数据孤岛”困境。在数据使用阶段，需要通过数据确权，明确数据处理者的权限。一方面，可以限制数据处理者使用数据的权利，防止数据滥用；另一方面，可以进一步保护数据内容，防止数据遭受篡改、窃取等恶意攻击。

在数据确权中，需要用到授权、鉴权、访问控制、数据溯源和数据安全审计技术。在数据确权中，授权定义了哪些用户或实体有权访问特定的数据资源，鉴权用于验证用户或实体是否具有访问特定数据资源的权限，有效的访问控制机制可以防止未经授权的访问和潜在的数据泄露风险，从而保护数据的安全性和隐私性。数据溯源在数据确权中通过记录数据的操作和传输历史，保证数据的可信度、完整性和安全性，同时为解决数据纠纷和责任追究提供了有力的支持。数据安全审计可以验证数据使用是否符合相关法规和政策要求，确保数据处理者的操作符合法律规范。

4．数据处理环境安全

数据处理环境安全是指如何有效地防止数据损坏，丢失或泄密等问题，例如，数据在录入、处理、统计或打印的过程中，由于硬件故障、断电、死机、人为的误操作、程序缺陷、病毒等造成的数据库损坏或数据丢失问题，以及某些敏感或保密的数据可能会被不具备资格的人员操作或读取，从而造成数据泄密的问题。

为了保证数据处理环境的安全，需要使用访问控制和数据溯源技术。

1）网络访问控制措施

网络访问控制措施通常包含网络隔离，部署堡垒机和远程运维管理等，具体如下。

（1）网络隔离。

数据处理平台对生产数据网络与非生产数据网络进行安全隔离，由于从非生产数据网络

不能直接访问生产数据网络中的任何服务器和网络设备，因此从非生产数据网络中不能对生产数据网络发起攻击。

（2）部署堡垒机。

为了平衡效率和安全性，在运维入口部署堡垒机，只允许办公网的运维人员快速通过堡垒机进入数据处理平台进行运维管理。运维人员登录堡垒机时，需要使用域账号密码加动态口令的方式进行双因素认证，堡垒机通常会使用高强度加密算法，以保障运维通道数据传输的机密性和完整性。

（3）远程运维管理。

可以为不在公司的员工提供远程运维通道，运维人员需要预先向数据处理环境安全管控部门申请 VPN 接入公司办公网之后访问堡垒机的权限。VPN 在接入公司办公网络的接入区时，需要使用域账号密码加动态口令的方式进行双因素认证，再从办公网接入区访问堡垒机，VPN 通常会使用高强度加密算法，以保障运维通道数据传输的机密性和完整性。

2）数据溯源

制定数据处理溯源策略和溯源机制，溯源数据存储和使用的管理制度，并制定溯源数据的表达方式和格式规范，从而实现溯源数据的规范化组织、存储和管理。

3.5 数据加工安全

3.5.1 安全要求概述

数据加工是指对原始数据进行清洗、转换、整合等操作，以便于进行后续的数据分析和挖掘。数据加工的主要目标是将原始数据转换为有价值的信息，以满足企业或个人的需求。数据加工包括但不限于数据清洗、数据转换、数据整合、数据质量检查等。

在数据加工环节，泄露风险主要是由分类分级不当、数据脱敏质量较低、恶意篡改/误操作等情况所导致。接下来将围绕图 3.5 展开叙述。

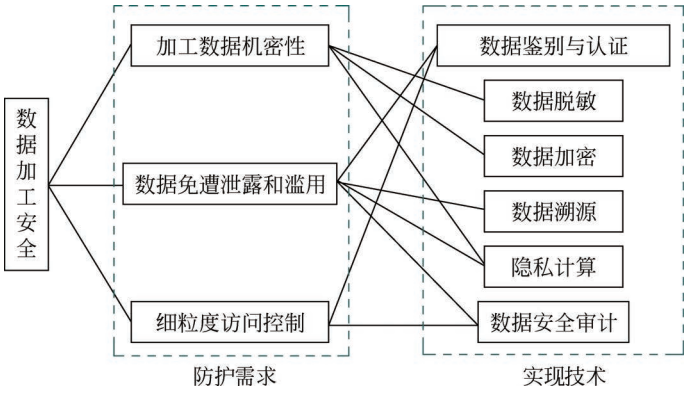

图 3.5　数据加工安全需求-技术映射图

3.5.2 防护需求与技术

1. 加工数据机密性

在数据加工过程中，保护数据的机密性是至关重要的。这要求采取严格的防护措施，确保

敏感信息在清洗、整合、转换和分析等各个环节不被未授权访问或泄露。为此，需实施如数据加密、数据脱敏、隐私计算等策略，以保障数据在加工过程中的安全性，防止机密数据遭受非法获取或滥用，从而维护数据所有者的隐私权益。同时，还需关注加工环境的物理安全和网络安全，确保整个数据加工过程符合相关法律法规的要求，降低数据泄露风险。

2. 数据免遭泄露和滥用

在数据加工过程中，面临着诸多潜在的安全威胁，包括数据泄露、不当访问、数据滥用等风险。同时，敏感信息可能因网络攻击、内部人员失误等原因泄露给未经授权的第三方。因此，需要使用数据鉴别与认证、数据溯源、隐私计算、数据安全审计等措施来降低数据泄露的风险。

数据鉴别通过验证数据的来源和完整性，建立数据的信任基础；而数据认证则利用技术手段如数字签名、加密算法和哈希函数，进一步保障数据在加工过程中的安全性和机密性。数据溯源能够在数据加工过程出现数据泄露和滥用的情况下，通过数据流转路径及时溯源，找到威胁来源。隐私计算能在保护数据本身不被泄露的前提下，实现数据的分析计算，有利于保护数据在加工阶段的隐私。数据安全审计通过对数据加工过程进行全面审计，确保数据加工活动符合安全规范，有效预防数据泄露和滥用。

3. 细粒度访问控制

在数据加工过程中，由于数据会经过多个不同权限用户的处理，如数据录入员、数据分析师、数据科学家以及管理层等，每个角色对数据的访问和操作需求各不相同。因此，仅依靠传统的粗粒度访问控制已无法满足复杂的数据安全需求。为了确保数据的安全性和完整性，需要使用更加细粒度的访问控制策略来进行权限管控。这包括对用户进行角色划分，为不同角色设定不同的数据访问和操作权限，以及实现动态的权限管理，根据业务需求和用户行为实时调整权限设置。通过实施细粒度的访问控制，可以有效地防止数据泄露、误操作等风险，保障数据加工过程的顺利进行。

细粒度访问控制是基于对单个数据资源的多个条件和/或多个权限来授予或拒绝对关键资产（如资源和数据）的访问的能力。在细粒度访问控制中，对于每个数据资源，都可以定义精细的访问控制规则，以确保数据的安全性和保密性。细粒度访问控制通常用于对数据安全要求非常高的系统，如金融、医疗等领域。在此基础上，使用数据鉴别与认证和数据安全审计等技术能够进一步构建一个更加安全、可靠的数据加工环境，为数据安全提供有力保障。

3.6　数据传输安全

3.6.1　安全要求概述

2022年7月，工业和信息化部网络安全产业发展中心编写的《数据传输安全白皮书》给出了数据传输安全的定义，即指通过采取必要措施，确保数据在传输阶段，处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。随着新一代信息技术的迭代发展和数字经济的快速推进，各类数据海量汇聚，数据安全问题日益凸显，成为关系国家安全和经济社会发展，关系广大人民群众切身利益的重大问题。数据传输安全作为数据全生命周期安全的关键环节，对于保障数据整体安全有着重要的意义。

在数据传输环节，会遇到网络攻击、传输泄露等风险。网络攻击包括DDoS攻击、APT攻击、通信流量劫持、中间人攻击、DNS欺骗和IP欺骗、泛洪攻击威胁等；传输泄露包括电磁泄漏或搭线窃听、传输协议漏洞、未授权身份人员登录系统、无线网安全薄弱等。

从国家层面看，保障数据传输安全是保护数据安全，维护国家安全，保障数字经济健康发展，推动构筑国家竞争新优势的重要部分。从企业层面看，保障数据传输安全对于保护企业数据安全，维护企业经济利益、竞争力以及持续经营能力有着重要意义。从个人层面看，保障数据传输安全对于保护个人信息安全，维护个人合法权益和人身安全有着重要作用。接下来将围绕图 3.6 展开叙述。

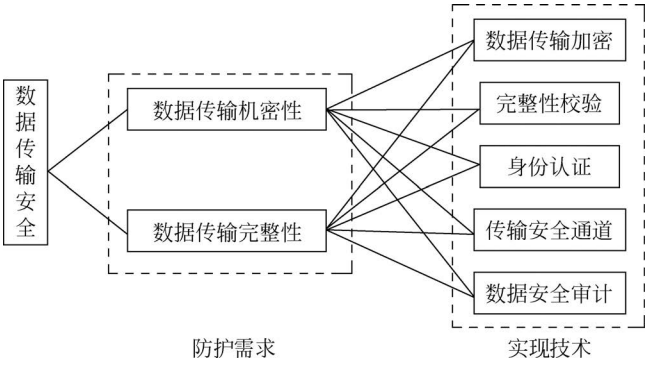

图 3.6　数据传输安全需求-技术映射图

3.6.2　防护需求与技术

1. 数据传输机密性

数据传输活动的“主体”涉及发送方、接收方以及传输路径上的多个中间节点等多个实体。这些实体共同构成了数据传输的安全责任主体。在数据处理过程中，确保主体的真实性是首要的安全需求，这意味着所有参与方的身份必须是真实可信的，以防止任何未经授权的访问或干预。对于传输的数据本身，除了真实性之外，还包括两个核心的安全需求：机密性和完整性。机密性指的是数据在传输过程中必须得到保护，防止被未授权的第三方访问。这意味着必须采用加密技术来确保数据在传输过程中的保密性，防止数据泄露给潜在的窃听者。此外，数据的完整性要求保证数据在传输过程中不被篡改或损坏，确保接收方接收到的数据与发送方发送的数据完全一致。

2. 数据传输完整性

在数据传输过程中，存在多种威胁可能导致数据的泄露或篡改。首先，数据泄露是数据传输中最常见的安全问题之一。攻击者可能会通过网络窃取数据，或者从内部获取敏感数据，从而导致数据泄露，给数据所有者带来损失。其次，中间人攻击是另一种常见的威胁形式，攻击者会植入恶意节点来拦截传输的数据，并可能篡改数据或者偷窃敏感信息。此外，恶意软件也可能通过感染传输过程中的设备来窃取数据或者篡改数据内容。面对上述威胁，保护数据传输的完整性至关重要。

对于数据传输的机密性和完整性，在进行安全防护时并没有特别明显的区分，往往是两者同时进行保护。常用的技术如下。

（1）数据传输加密。

采用加密技术可以确保数据在传输过程中的机密性，而数字签名等技术则可以验证数据的完整性，防止数据在传输过程中被篡改。

（2）完整性校验。

完整性校验技术可以帮助用户确保数据的完整性。其核心思想是对数据进行哈希算法等运

算，生成唯一的摘要信息并记录下来，可帮助用户在数据传输或存储过程中检测出是否被篡改。

（3）身份认证。

常见的身份认证方式包括口令认证技术、双因素身份认证技术、数字证书的身份认证技术、基于生物特征的身份认证技术、Kerberos 身份认证机制、协同签名技术、标识认证技术等。

（4）传输安全通道。

传输通道可分为代理服务器到终端、代理服务器到互联网和代理服务器到代理服务器。安全防护保障由基于 SSL 协议、IPSec 协议或其他协议的传输加密技术提供。

（5）数据安全审计。

数据安全审计可以监控数据传输的始末，包括数据从源到目的地的传输路径、传输速度、传输量等信息，确保数据在传输过程中没有被篡改、窃取或丢失。

3.7　数据提供安全

3.7.1　安全要求概述

目前信息系统主要采取物理隔离、访问控制、数据加密、行为审计等安全措施，解决电子数据在存储、传输中的安全问题，但是随着信息化的发展，尤其是智能手机的普及，电子屏幕和纸质文档已然成为重要的安全管控缺口，通过拍摄、扫描、复印等造成的数据泄露威胁日益严峻，成为数据安全管控的重灾区，迫切需要有效的管控措施。

在数据提供环节，风险威胁来自不合规的提供和共享；缺乏数据复制的使用管控和终端审计、行为抵赖、数据发送错误、非授权隐私泄露/修改、第三方过失而造成数据泄露；恶意程序入侵、病毒侵扰、网络宽带被盗用等情况。下面将根据图 3.7 对本节内容展开介绍。

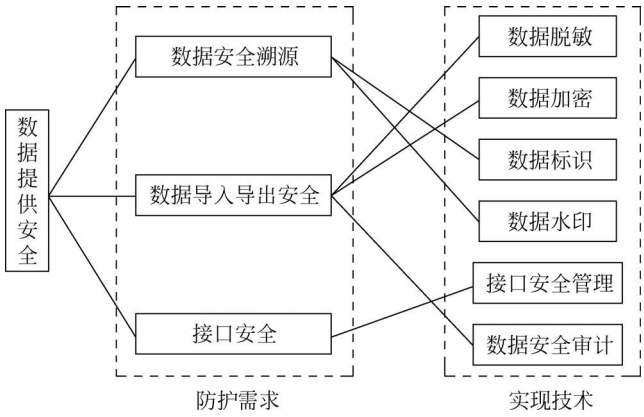

图 3.7　数据提供安全需求-技术映射图

3.7.2　防护需求与技术

1. 数据安全溯源

数据提供安全作为数据安全的关键一环，亟待解决电子屏幕和纸质文档被拍照泄露后，存在管控难、溯源难和管理抓手缺失等难题。通过先进的数据标识和数据水印技术可精准定位泄露源头，对责任人形成巨大震慑作用的同时，进一步减少违规拍摄、复印等行为的发生，最大化地有效降低数据泄露风险。

数据标识技术是一种基于密码技术的高安全、高可信和高可用的数据属性标注与识别技术。它以规范化的数据格式描述数据属性，采用密码技术对描述信息进行安全保护，能够确保信息完整有效和真实可信。数据水印是将特定的数字信号嵌入数字产品中保护数字产品版权、完整性、防复制或去向追踪的技术。一方面，数据水印能够标识共享数据的接收方信息，数据共享后，如果发生数据泄露，能够从泄露数据中提取出数字水印信息进行追踪溯源，及时发现泄露者。另一方面，数据水印技术也能够标识数据发布方信息，数据发布后，如果需要对数据版权进行确认，能够从数据中提取出水印信息以进行版权确认。

2. 数据导入导出安全

数据导入导出广泛存在于数据交换过程中，通过数据导入导出，数据被批量化流转，加速数据应用价值的体现。如果没有安全保障措施，非法人员可能通过非法技术手段导出非授权数据，导入恶意数据等，带来数据篡改和数据泄露的重大事故。由于一般数据导入导出的数据量都很大，因此相关安全风险和安全危害也会被成倍放大。所以，需要采取有效的技术措施控制数据导入导出的安全风险。

使用数据脱敏技术能保护导入导出阶段的数据隐私，使用数据加密技术能保护数据在此过程中的机密性和完整性，使用数据安全审计技术能够对导入导出全过程进行监管记录，及时防范各种威胁和风险。

3. 接口安全

近年来，随着 API 等数据接口的应用范围急剧增长，由于对其安全保障措施和监测预警机制不足，导致大规模数据泄露等安全事件频出。例如，2023 年 12 月，据央视新闻报道，一求职招聘类 App 短信验证码接口遭遇了 1300 多万次的攻击，黑客获取到大量个人信息和公司账号数据在境外出售。

因此，开展数据接口安全风险监测是避免数据遭受泄露、篡改、滥用等的重要举措。2023 年，国家标准《信息安全技术 数据接口安全风险监测方法》在全国信息安全标准化技术委员会立项制定，该标准描述了数据接口要素关系，分析了数据接口自身脆弱性、接口不合理承载数据的脆弱性、接口调用行为威胁、接口提供活动威胁等风险源，为开展数据接口安全风险监测工作提出了方法。

从技术层面上看，对接口安全进行管理通常包含接口鉴权和接口访问控制两种技术。接口鉴权时需要对接口调用方实行用户鉴权，对访问 API 的权限进行限制，如果鉴权通过则允许用户调用 API，在这个过程中一般需要使用数据加密和数据签名等方法。通过接口访问控制，可以细粒度地管理不同用户或客户端对接口的访问权限。通过合理配置访问控制列表，可以限制非法流量的流入，减少不必要的请求，从而提高网络性能和接口的响应速度。

3.8 数据公开安全

3.8.1 安全要求概述

在一般数据全生命周期安全保护中，要求公开前须对其数据进行分析研判，判断是否可公开、是否需脱敏等。例如，应在数据公开前对数据公开的必要性、范围、规模、方式等进行分析研判，研判结果为可以公开的，应根据数据特点、应用场景等采取合适方法对数据进行必要的脱敏处理，确保数据公开安全。在数据公开时，需要注意数据导入/导出安全和接口安全。

在数据公开环节，风险主要是很多数据在未经过严格保密审查、未进行泄密隐患风险评

估，或者未意识到数据情报价值或涉及公民隐私的情况下随意发布的情况。下面将依照图 3.8 展开介绍。

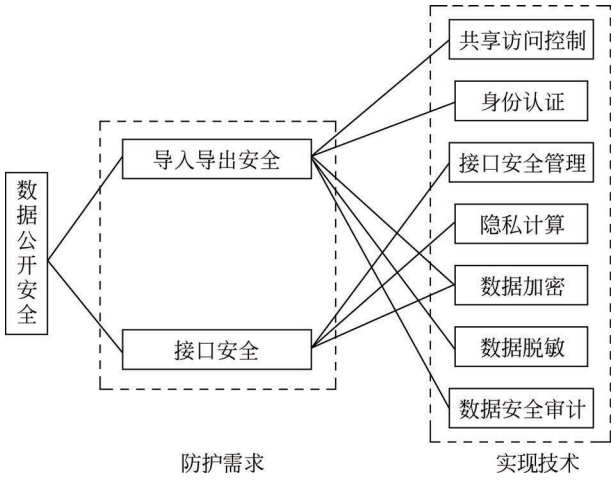

图 3.8　数据公开安全需求-技术映射图

3.8.2　防护需求与技术

1. 导入导出安全

在数据公开阶段，特别是在数据导入导出过程中，面临着多种安全威胁，这些威胁包括数据泄露、中间人攻击、敏感信息未加密传输、数据篡改以及 API 安全漏洞等。为了确保数据安全，需要实施以下防护措施：采用共享访问控制策略，确保只有经过授权的用户或系统才能访问特定的数据或资源；采用多因素认证（MFA）机制，如密码、生物识别和智能卡等技术，以增强用户身份的验证强度，防止未授权访问；在数据传输过程中应用强加密算法，如 AES（高级加密标准）和 TLS（传输层安全性），以保护数据不被未授权的第三方读取；在必要时对敏感数据进行脱敏处理，例如，使用数据掩码、伪匿名化或数据伪装技术，确保在数据导入导出过程中个人隐私和敏感信息不会被泄露；建立全面的数据安全审计系统，记录和监控所有数据访问和修改活动，以便在发生安全事件时能够快速检测、响应和追溯。

2. 接口安全

在数据公开阶段，用来获取数据最常见的方式之一是使用数据接口，所以数据接口也成为攻击者重点关注的对象，因为一旦数据接口出现问题，就会导致数据在通过数据接口时发生数据泄露等风险，所以为了规范数据接口调用行为，对数据接口进行安全管理十分有必要。

数据接口安全阶段的技术检测，需要使用技术工具对数据接口的调用进行接口鉴权和接口访问控制，以确保所有人对数据接口的访问与调用都是合法的、符合标准的；对数据接口传输的内容应用隐私计算技术，允许数据使用者在保护隐私的同时，充分利用数据的价值；使用加密和脱敏技术能够进一步确保接口调用时的数据完整性、机密性和隐私安全。

3.9　数据销毁安全

3.9.1　安全要求概述

数据销毁安全是指通过制定数据销毁机制，实现有效的数据销毁管控，防止因对存储介质

中的数据进行恢复而导致的数据泄露风险。为了满足合规要求及组织机构本身的业务发展需求，组织机构需要对数据进行销毁处理。

在数据销毁环节，风险主要来自数据销毁的不彻底性。数据销毁处理要求针对数据的内容进行清除和净化，以确保攻击者无法通过存储介质中的数据内容进行恶意恢复，而造成严重的敏感信息泄露问题。

下面将围绕安全销毁防护需求和其中用到的数据安全销毁技术和介质安全销毁技术进行讲解，如图 3.9 所示。

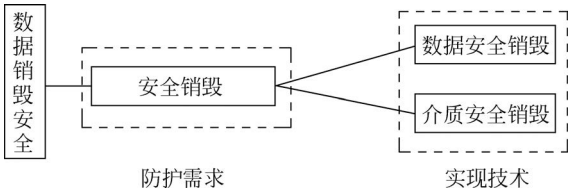

图 3.9　数据销毁安全需求-技术映射图

3.9.2　防护需求与技术

在文义解释层面，《个人信息保护法》所规定的“删除权”通常被理解为从信息处理者的数据库中删除已经“过期”或自然人不愿再留存的个人信息，即达到了数据销毁的效果；但是在技术方案层面，“删除”和“销毁”并不是两个完全等同的概念。数据销毁与数据删除具有典型的技术语境属性。数据销毁通常被视为数据安全业务流程的最后环节，直接目的是避免第三人通过数据复原、存储介质窃取等方式重新复原业已销毁的数据；而数据删除并不是数据安全业务流程的必备环节，而是数据处理者根据法定义务、业务需求等多种因素选择不再对外公开特定数据。

数据销毁安全是指在监管业务和服务涉及的系统及设备中清除数据时，通过建立针对数据的删除、销毁、净化机制，防止数据被恢复而采取的一系列防控措施。不及时、不彻底的销毁将给内部人员和黑客提供可乘之机，可能产生数据泄露、个人信息被重新识别、数据二次转售等恶性影响，特别是当数据存储在云端时，云服务商可能拒绝按照用户的删除指令销毁数据，而是恶意保留数据，从而使数据面临被泄露的风险。

因此，为了减小数据销毁可能产生的安全威胁，数据销毁应满足以下原则。

（1）合法合规原则：在法律法规规定的范围内，开展数据销毁处理活动。

（2）保密性原则：应对销毁过程中所接触的数据进行保密，不得随意向外泄露。数据销毁设备在执行销毁作业时，除作业必需的基本数据，如设备序列号、型号和存储结构等信息外，严格禁止读取和传送任何数据信息。

（3）安全可靠性原则：应通过安全可靠的方式对存储介质中的数据或存储介质进行销毁，实现对数据及其蕴含信息的有效清除，以防范通过对存储介质中的内容进行恢复而导致的数据或信息泄露风险。

（4）就高不就低原则：应依据存储介质载有的最高级别数据确定存储介质的销毁方式，并对应执行销毁措施。

从技术层面上看，可以分为数据安全销毁技术和介质安全销毁技术。

（1）数据安全销毁技术。一般包含本地数据销毁技术和网络数据销毁技术。本地数据销毁可使用数据覆写，即将非敏感数据写入以前存有敏感数据的存储位置，以达到清除数据的目

的。网络数据销毁技术又分为基于密钥销毁的数据不可用销毁方式和基于时间过期机制的数据自销毁方式。基于密钥销毁的数据不可用销毁方式不会销毁数据本身，它销毁的是加密数据的密钥，进而实现数据不可访问的目的。基于时间过期机制的数据自销毁方式是云存储环境下的另外一种安全的数据销毁方式，其思想也是通过数据不可用来实现数据销毁的目的。

（2）介质安全销毁技术。对存储介质如闪存盘、磁盘、磁带、光盘等进行物理销毁，确保数据无法复原。目前主要是通过物理、化学的方式直接销毁存储介质。物理销毁可分为消磁、捣碎、焚毁等方法。化学销毁方法主要是滴盐酸法。

小结

数据安全防护架构是一个全面而系统的保障体系，旨在确保数据在其整个生命周期中得到有效的保护。本章涵盖了数据安全的各个关键方面，包括数据处理的各个阶段。通过综合考虑数据安全的各个方面，建立完善的安全防护体系，以确保数据在整个生命周期中的机密性、完整性和可用性，从而有效应对各种潜在的安全威胁与风险。通过本章的学习，可以帮助读者构建数据安全防护架构的相关体系，使读者对数据安全的各阶段有一个初步的了解，以便后续的进一步学习。

习题

在线测试

一、单项选择题

1. 数据全生命周期安全体系共包括5部分，（　　）不属于该体系。

A. 数据安全治理　　B. 数据安全分级防护

C. 数据安全防护技术　　D. 数据加密安全

2. 数据使用环节的外部风险威胁不包括（　　）。

A. 账户劫持　　B. APT攻击

C. DBA违规操作窃取　　D. 密钥丢失

3. 在数据处理环境安全中，网络访问控制措施不包括（　　）。

A. 网络隔离　　B. 堡垒机　　C. 数据溯源　　D. 远程运维

4. 防泄露技术不包括（　　）。

A. 数据鉴别与认证　　B. 隐私计算

C. 数据存储技术　　D. 数据安全审计

5. 在数据传输环节可能遇到的网络攻击不包括（　　）。

A. DDoS攻击　　B. APT攻击　　C. 搭线窃听　　D. 通信流量劫持

6. 身份认证访问控制是指通过身份认证技术限制用户对数据或资源的访问。常见的身份认证方式不包括（　　）。

A. 口令认证技术　　B. 双因素身份认证技术

C. 数据加密技术　　D. 数字证书的身份认证技术

7. 数据存储安全的防护需求不包括（　　）。

A. 数据存储合规　　B. 数据源可信　　C. 存储完整性　　D. 数据时效性

8. 网络访问控制措施通常不包含（　　）。

A. 单因素认证　　B. 网络隔离　　C. 部署堡垒机　　D. 远程运维管理

9. 数据销毁应满足的原则不包括(　　)。

A. 合法合规原则　　B. 就高不就低原则

C. 主体参与原则　　D. 安全可靠性原则

10. 存储介质的物理销毁方法不包括(　　)。

A. 焚毁法　　B. 腐蚀法　　C. 消磁法　　D. 剪碎法

二、判断题

1. 数据生命周期只包括数据采集、数据传输、数据存储、数据处理、数据交换以及数据销毁。(　　)

2. 数据作为一种资产,具备资产的通用属性,有完整的生命周期,在数据的整个生命周期各个环节均存在数据安全风险。(　　)

3. 一般来说,仅应用加密技术就能够有效确保数据存储安全。(　　)

4. 在数据销毁环节,风险主要来自数据销毁的不彻底性。(　　)

5. 可信数据是指可信任、可靠、准确的数据。(　　)

三、简答题

1. 建立完善的数据全生命周期安全体系有何具体作用？试简要描述。

2. 列举在数据传输安全中所使用的技术,要求不少于 3 个。

3. 简述数据销毁安全所用到的销毁技术。