基于典型数据应用场景的数据安全能力建设

向柳[1]，张皎[1]，周姿彤[2]，董欣[1]
1. 奇安信网神信息技术（北京）股份有限公司，北京 100044
2. 信息工程大学，河南 郑州 450001
DOI: 10.61369/TACS.2025140049

摘　　要： 数据安全治理是一项复杂度高、综合性强的信息化系统工程。本文以业务流程关键环节为核心聚焦典型数据应用场景（开发测试运维场景、办公数据应用场景、数据共享交换场景和数据开放交易场景）下的数据安全风险，在数据安全治理方法论 DGPC 和最佳实践 DSG 指导下，重点阐述了在特权访问安全管理、数据库安全防护、数据泄漏防护、监测与风险分析和隐私计算五个方面开展数据安全能力建设，有助于企业和组织深化、完善数据安全体系建设。

关 键 词： 典型数据应用场景；数据安全；能力建设

Data Security Capability Building Based on Typical Data Application Scenarios

Xiang Liu[1], Zhang Jiao[1], Zhou Zitong[2], Dong Xin[1]
1. QiAnXin WangShen Information Technology (Beijing) Co., Ltd. Beijing 100044
2. Information Engineering University, Zhengzhou, Henan 450001

Abstract: Data security governance is an information system engineering with high complexity and strong comprehensiveness. This paper focuses on typical data application scenarios (development, testing, operation and maintenance scenarios, office data application scenarios, data sharing and exchange scenarios, and data open trading scenarios) centered around key business process links. Guided by the data security governance methodology DGPC and best practices DSG, it emphasizes the development of data security capabilities in five aspects: privileged access security management, database security protection, data leakage prevention, monitoring and risk analysis, and privacy computation. This is helpful for enterprises and organizations to deepen and improve their data security system construction.

Keywords: typical data application scenarios; data security; capacity building

引言

在近年来的国民经济发展中，土地、劳动力、资本和技术作为传统生产要素对政企数字化转型和传统产业智能化发展依旧提供稳定的基础动力。然而，随着 IT 技术的不断升级迭代以及业务与信息化技术深度融合的需求，数据作为一种新型生产要素[1]，在培育数字经济新产业、新业态和新模式中起到重要作用。国家相关部门及行业机构正在积极推动农业、工业、交通、教育、安防、城市管理、公共资源交易等领域的数据开发利用场景规范化和数据采集标准化。充分发挥数据这一新型要素对其他要素效率的倍增作用，培育发展数据要素市场，使大数据成为推动经济高质量发展的新动能。

一、数据面临的安全挑战

随着数据量飞速发展，据权威机构统计，2035年全球总数据量将超过2万亿 TB。大量数据在使用、流通、交易等环节存在安全风险，数据安全面临着监管要求、流动过程风险和业务过程风险三方面的挑战。第一，《数据安全法》和《个人信息保护法》为代表的一系列法律法规的颁布，为监管提供了数据安全合规和数据安全保护的依据，用户需要解决业务正常运转过程中满足监管对数据安全的要求；第二，数据流动过程面临更多数据来源、应用调用、外部合作和跨域流动带来的风险；第三，数据业务运转过程面临数据权限、用户权益、数据存储和业务质量等方面存在的风险。

二、数据安全治理方法论

面对数据全生命周期存在的风险和数据安全面临的挑战，国际上知名的数据安全治理方法论和最佳实践为微软的 DGPC[2]（Data Governance for Privacy ,Confidentiality

and Conmpliance）和 Gartner 的 DSG[3]（Data Security Governance），强调了技术工具、组织人员及策略流程为核心的数据安全治理机制的重要性。

DGPC 提供了人员、流程和技术三个能力维度的治理方法。其中，人员方面，需建立由组织内部人员组成的 DGPC 团队，明确定义其角色和职责，提供足够的资源来执行他们所需的职责，以及对总体数据治理目标给予明确指导。流程方面，必须满足的各种要求涉及的各种权威文件（法律、法规、标准以及公司政策和战略文件），并理解这些法定要求、组织策略和战略目标是如何相互交叉并影响的。确定在特定数据流程中数据安全、隐私和合规面临的威胁，分析相关风险并确定适当的控制目标和控制活动。技术方面，通过一种分析特定数据流的方法，以识别信息安全管理系统或控制框架存在残留的、特定的风险。以数据生命周期为第一维度，以安全架构、身份认证与访问控制、信息保护、审计为第二维度，组成了二维的数据安全防护矩阵。

DSG 提供了数据安全治理框架。从平衡业务与数据安全风险开始进行规划，开展对数据的梳理和管理数据的全生命周期。针对业务运转过程，定义数据安全策略和部署数据安全产品，最后为所有产品编排统一的安全策略，完成数据安全的集中管理。

三、典型数据应用场景下的数据安全能力建设

基于 DGPC 的技术能力要求和 DSG 的数据安全治理流程，本文重点研讨典型数据应用场景下的数据安全能力建设，分为以下四种场景：在开发测试运维场景下，涉及人员及终端具备高操作权限，容易产生数据泄露或破坏；在办公数据应用场景下，业务终端可利用工作便利获取敏感数据，容易产生数据泄露；在数据共享交换场景下，数据交互频繁，极易产生数据违规分发情况；在数据开放交易场景下，既要保护隐私，又要兼顾数据价值挖掘，以支撑数据开放交易。四种典型数据应用场景如下图所示：

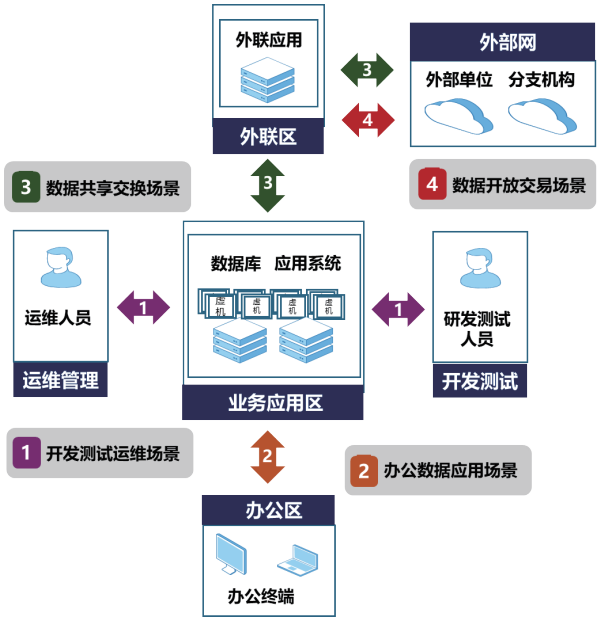

图 1 典型数据应用场景

（一）风险分析

在典型数据应用场景下，用户存在以下数据安全痛点和问题：

（1）特权账号管理混乱：数据依赖的资源环境中，存在大量的僵尸账号、幽灵账号，长期未改密账号等风险账号。特权账号被利用造成数据破坏或泄露。

（2）敏感数据泄露问题：敏感数据分布及流动状况不清，难以监测使用状况，容易造成数据泄露。

（3）敏感数据越权访问问题：不同角色的人员应具备不同的数据权限，缺少细粒度的权限管控，易造成敏感数据的泄露。

（4）威胁操作问题：运维\开发人员具备高操作权限，误操作、滥用操作容易造成数据破坏或泄露。

（5）安全合规问题：缺少针对数据库操作、运维操作的审计能力，不满足等保2.0[4] 等法律配套标准要求。

（6）隐私保护与数据挖掘的矛盾问题：脱敏后数据难以进行有效的价值挖掘，直接交换数据容易产生数据泄露，因此在隐私保护与数据挖掘之间的矛盾难以平衡。

（二）能力建设

数据安全能力依托于数据安全技术的合理运用。数据安全技术主要分为数据资产管理类、数据资产防护类、数据处理行为防控类和数据开发利用类[5]。面对典型数据应用场景下的数据安全风险，为保障业务正常运行和数据全生命周期的安全，数据安全能力主要包括特权访问安全管理（运用数据资产管理类技术）、数据库安全防护（运用数据资产防护类技术）、数据泄漏防护（运用数据资产防护类技术）、监测与风险分析（数据处理行为防控类技术）和隐私计算（数据开发利用类技术）。

特权访问安全管理能力包括账号发现分析、账号纳管改密、运维访问控制和运维操作审计；数据库安全防护能力包括数据库访问控制、数据库攻击防护和数据库安全审计；数据泄漏防护能力包括网络数据防泄漏、邮件数据防泄漏、终端数据防泄漏和数据脱敏；监测与风险分析能力包括数据分布监测、数据流动监测、泄露风险监测和用户行为分析；隐私计算能力包括数据安全分离。

针对四种典型数据应用场景将以上能力融合后，形成特定数据应用场景下的数据安全能力建设方案。详细内容如下：

（1）开发测试运维场景

开发测试运维场景的数据安全能力建设主要从以下几个方面进行考虑：

统一运维管理：通过集中化运维管控、运维过程实时监管、运维访问合规性控制、运维过程图形化审计等功能，构建一套完善的事前预防、事中监控、事后审计安全管理体系。

集中账号管控：提供特权账号的发现分析、安全存储、自动改密等功能，帮助系统化、流程化和规范化特权帐号管理的工作，降低特权账号管理不善带来的安全风险。

消除应用“硬编码[6]”：消除应用系统中的明文存储的账号密码，同时应用系统动态获取账号密码，改密不影响应用系统使用，保证应用系统的连续性。

敏感数据脱敏应用：提供数据库和文件的脱敏能力，满足从生产环境导出数据以供业务数据分析者在开发测试环境使用的需求。

数据库安全防护：对开发测试运维场景下的数据维护和数据分析提供访问控制与审计能力，防止对数据库的恶意破坏和数据窃取，保证数据的安全。

高权限终端数据防泄漏：有效防控开发测试运维等高权限人员通过终端对核心数据的泄露。

因此，本场景采用以下技术措施：运维访问控制、数据库访问控制、终端数据防泄漏、账号发现分析、账号纳管改密、运维身份认证、运维访问控制、运维操作审计、数据库审计和数据脱敏。

（2）办公数据应用场景

办公数据应用场景的数据安全能力建设主要从以下几个方面进行考虑[7]：

数据防泄漏：结合办公场景对用户行为分析，制定合适的敏感文件控制策略，通过管理 + 技术的方式解决用户数据防泄漏的难题，防止办公人员对核心数据的外发泄露。

数据库安全审计：通过用户、业务系统、数据库三层信息的关联审计，准确描述何人、何时、何地、以何种方式进行违规操作，并提供溯源与定责依据[8]。

因此，本场景采用以下技术措施：终端数据防泄漏、网络数据防泄漏、邮件数据防泄漏、用户行为分析和数据库操作审计。

（3）数据共享交换场景

数据共享交换场景的数据安全能力建设主要从以下几个方面进行考虑：

数据资产分布地图：提供一个敏感数据资产分布情况的全面、直观的管理视角，实现敏感数据、应用、账户、API 接口的全感知全展现。

数据流动可视化：通过网络流量的还原分析，构建数据流动视图，实时解析和监测数据轨迹。

数据安全风险态势：实时监测数据泄露风险，及时定位及时预警，支撑数据安全常态化运营。

数据泄露溯源：提供主体溯源和线索溯源能力，支撑数据安全事件的事后定责。

敏感数据脱敏应用：提供数据库和文件的脱敏能力，满足敏感数据对外共享的隐私安全。

因此，本场景采用以下技术措施：敏感数据分布监测、数据流动监测、泄露风险分析、数据脱敏、泄露风险监测和敏感数据分布监测[9]。

（4）数据开放交易场景

数据开放交易场景的数据安全能力建设主要从以下几个方面进行考虑：

安全前提下的数据价值挖掘：合法合规安全地对外开放数据，既保证数据安全，又能充分发挥数据的最大价值，助推企业数据业务的快速发展。

原始数据不流出：秉承“数据不动程序动”、“数据可用不可见”的安全理念，实现了数据所有权和使用权分离[10]，确保原始数据不流出。完美保留数据价值，支撑数据安全的开放交易。

因此，本场景采用以下技术措施：隐私计算（数据沙箱、隐私求交、联邦学习）。

四、结语

面对不断叠加演进的安全威胁，数据安全建设是长期而复杂的过程，需要在建设过程中持续聚焦业务流程中数据应用存在的安全风险，针对不同的数据应用场景，厘清安全、数据、业务流程之间的深层次联系，构建清晰的数据流转视图。通过采用合理的数据安全技术，明确重点环节，按照有序推进、分步建设的实施路线，分场景分阶段落地并完善数据安全能力建设，确保安全能力深入融合到业务流程中，实现安全能力的自生长。

参考文献

[1] 杨慧珍 . 数据要素交易中数据安全风险的协同治理研究 [D]. 山东 : 山东财经大学 ,2025.

[2] 中关村网络安全与信息化产业联盟 , 数据安全治理专业委员会 . 数据安全治理白皮书5.0[EB/OL].(2024-11-06).https://www.hljbigdata.org/data/upload/2024-11-06/672b2c61a3168.pdf.

[3]Joerg Fritsch,Mike Wonham.How to successfully design and implement a data-centric security architecture[EB/OL].(2019-07-22).https://www.gartner.com/en/documents/3953491.

[4]GB/T 22239-2019,《信息安全技术 网络安全等级保护基本要求》[S].

[5] 关伟东 , 汪露露 . 数据安全技术现状及发展趋势研究 [J]. 信息通信技术 ,2025(1):48-51.

[6] 黄晨量 . 对象关系映射的硬编码方式的设计与实现 [J]. 上海示范大学 ,2005(7).

[7] 张晶姝 . 终端数据防泄漏系统在企业中的应用实践 [J]. 数字技术与应用 ,2018,36(05):191-192.

[8] 周建宁 , 季君 , 吴陈龙 , 等 . 多维度数据库安全审计设计和实现 [J]. 中国公共安全 (学术版),2019,(04):111-115.

[9] 孟祥猛 . 信息网络建设中的安全问题分析 [J]. 电脑编程技巧与维护 ,2019,(05):171-173.

[10] 刘业政 , 宗兰芳 , 周芦娟 , 等 . 数据要素流通交易的可信指标及测度方法 [J]. 管理评论 ,2024,36(12):26-36.

