数据资产管理及接口管理技术趋势及策略探讨

马锦贤
中国电信股份有限公司新疆分公司，新疆 乌鲁木齐 830026

[摘要]网络信息技术创新日新月异，数字化、网络化、智能化融合发展，对我国建设网络强国、智慧社会、数字中国发挥着至关重要的作用。目前世界各国都把推进经济数字化作为创新高质量发展驱动力，在技术研发，数据流通及共享，做出前瞻性布局。数字经济发展历程中数据已成为关键要素，数字技术已新理念、新业态、新模式融入经济、社会、文化、生态文明建设得各领域和各关键环节，数据价值也由最初的数据资源发展成为数据资产，进一步发展为数据资本。国家已将数据安全放在重要位置，并对数据资产的识别、接口安全管理等安全技术能力的建设和使用提出了新要求，为有效保障数据在安全环境下运行，保障国家战略落地实施及内部业务数据使用效率，结合企业自身业务、数据安全现状，提升数据安全技术管理能力和接口管理，促进数据合理、合法、合规使用，推进数字化经济高质量创新发展。

[关键词]数据安全；数据资产；系统接口安全
DOI：10.33142/sca.v5i7.7879 中图分类号：F123.7 文献标识码：A

Discussion on the Trend and Strategy of Data Asset Management and Interface Management Technology

MA Jinxian
Xinjiang Branch of China Telecom Co., Ltd., Urumqi, Xinjiang, 830026, China

Abstract: Network information technology innovation is changing with each passing day. The integrated development of digitalization, networking and intelligence plays a vital role in building China into a powerful network country, a smart society and a digital China. At present, countries all over the world regard the promotion of economic digitization as the driving force of innovative and high-quality development, and make forward-looking layout in technology research and development, data circulation and sharing. Data has become a key element in the development of digital economy. Digital technology has integrated new concepts, new formats and new models into all fields and key links of economic, social, cultural and ecological civilization construction. Data value has also developed from initial data resources into data assets and further developed into data capital. The country has put data security at an important position, and put forward new requirements for the construction and use of data asset identification, interface security management and other security technology capabilities. In order to effectively ensure the operation of data in a safe environment, ensure the implementation of national strategy and the efficiency of internal business data use, combine the enterprise's own business and data security status, improve the data security technology management capabilities and interface management, and promote data rationality, legality use in compliance and promote high-quality innovative development of digital economy.

Keywords: data security; data assets; system interface safety

1 网络数据安全风险危害驱动需要

当前数字经济已上升到国家战略，数字经济飞速发展，数据价值显性化，催生了数据黑色产业，黑客、部分内部员工非法获取个人隐私信息，个人隐私数据被黑客和部分内部员工在互联网被公开出售、通过暗网数据进行买卖，再到通信互联网诈骗、企业对目标客户群体精准“杀熟”、虚拟资产盗取等数据黑色产业及滥用乱象丛生，整体网络安全威胁呈现全天候、常态化、多样性的特征。企业内部及业务数据包含大量个人通讯信息、个人身份信息、敏感信息等多种敏感数据，一旦泄露会造成个人及社会非常大影响，面对无时无刻，内部外部的网络安全风险，构建全面、可持续、可管、可控数据安全防护体系已迫在眉睫。

2 网络数据安全合规管理要求需要

随着国家对网络安全、数据安全越发重视，相继颁布及更新了针对数据相关安全方面的法律法规，不同发展阶段安全要求内容不同，建立完善的技术支撑体系、管理体系、运维服务体系是国家、行业相关要求的落地执行。《网络安全法》对网络数据以及个人信息的使用、防护和管理提出了明确要求，要求网络运营者采取数据分类、重要数据备份和加密等措施，防止网络数据被窃取或者被篡改；要求网络运营者合法收集公民个人信息，加强对公民个人信息的保护，采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。加强对重要数据和个人信息的保护，已是法律所赋予的责任和义务。《数据安全法》中从多个维度对数据安全进行明确要求。一是确立数据分级分类管理以及风险评估，检测预警和应急处置等数据安全管理各项基本制度；二是确开展数据活动的组织、个人的数据安全保护义务，落实数据安全保护

责任；三是坚持安全与发展并重，锁定支持促进数据安全与发展的措施。工业和信息化部对数据安全技术能力的建设和使用提出了明确要求，要求企业应具备对数据资产的识别、接口安全管理等技术能力。

3 业务发展需要

随着内部信息化不断发展及外部合规要求，近年来企业在安全方面已取得了一定进展，整体还存在数据安全管控不够细、数据安全范围不够广、数据防护手段不够多等问题，随着新兴信息技术与通信服务的深度融合，网络安全风险日益加剧，安全防护难度骤增，网络数据安全防护体系亟需进一步加强。一方面，以事业发展为契机，以国家法律法规为底线，以国家、行业标准为依据，完善网络数据安全防护体系，补齐安全防护短板，拉平安全防护能力；另一方面，在安全技术创新层面有更积极作为，做好大数据管理、便民惠民服务、个人隐私保护等工作。

4 数据资产管理及接口安全管理

完善数据资产管理能力，通过数据集中采集、直连方式对数据资产进行自动发现、采集，可智能识别发现 IT 系统中的数据存管设备与服务，对数据管理服务、数据资产的来源、结构化数据进行识别分析，对采集与分析过程产生结果数据进行存储，方便快速为其他服务提供支撑，存储的信息包括不限于数据的元信息、分类分级信息、属主信息、采集过程信息、分析结果等。对数据的访问按照配置策略进行权限控制，并支持存储数据的定期备份和故障容错机制，提高资产信息的安全保障能力。

4.1 数据态势分析

通过对访问者、被保护对象、行为方式、操作内容等操作生成统计报表，添加及修改报表的数量、格式、内容等，以满足网络信息安全审计需求。具备丰富的报表内容，包含访问量统计、数据访问来源、访问途径、访问对象、操作行为、操作对象、操作条件、操作结果、操作频率、攻击行为等。并对全场景用户行为分析，通过用户使用的客户端，数据库服务器，数据库类型，操作行为，详细操作命令和返回数据情况，完整的展现某用户对数据的访问详情。将涉及重要数据得关键操作每一个操作流都支持继续下钻分析，从全局到详细，一层层分析用户的实际访问行为。

可以对数据库账号高频请求统计分析，展示高频请求类型 TOP10、高频请求标签 TOP10、高频请求数据等级 TOP5、高频请求数据类别 TOP10、高频请求表 TOP10、高频请求列 TOP10 用户统计等维度，并可按时间进行筛选。

实现对不同维度、不同层次、不同角度、不同关系结构的数据流量安全监测结果的交互可视化。支持多种视图展示流量监测结果：数据安全风险监测、数据访问行为监测、数据分布情况监测。展示类型包括但不限于雷达图、关联关系图、攻击路径图、热度图、地理信息图等，可以按需进行交互操作。

通过大数据分析技术等手段对安全态势采集的数据进行整体分析，利用机器学习自动建立安全基线，识别低于安全基线的系统运行异常、数据交互异常、访问操作异常等风险，及时发现系统异常现象，识别各种攻击威胁行为，从而帮助信息安全部门了解业务系统面临的风险，安全态势分析内容需要包含：

具备安全基线分析能力，通过机器学习对安全态势采集的日志进行自动分析处理与数据挖掘，采用分类、聚类、回归、深度学习等算法，从安全态势采集的日志数据中识别出潜在的安全威胁，并提取关键特征建立安全基线模型。

具备异常流量分析能力，通过对网络流量日志、业务系统日志、用户行为日志等数据进行分析，利用数学建模、机器学习、关联挖掘等技术，建立业务、用户行为画像，围绕业务、用户等内容实现异常流量分析。

形成数据态势分析能力，建立业务系统敏感数据分类分级标准，自动发现敏感数据分布情况，根据数据的流转、交互、使用等过程进行分析，数据态势分析维度需要包含数据流转分析、数据交换分析、数据趋势分析、数据敏感程度分析、数据流量分析等多种类型。

具备权限态势分析能力，通过对业务系统业务人员、运维人员的权限进行分析，主要梳理人员的权限变化和分析人员的权限异常，权限态势分析应从用户、对象维度进行分析。具备用户维度能力，监控业务系统、数据库中的用户的启用状态、权限划分、角色归属等基本信息；具备对象维度分析，对业务系统、数据库中的程序或对象进行分析，特别是含了敏感数据的程序或对象，监测其访问权限划分情况，一旦程序或对象权限发生了较大变更。

具备敏感数据分析能力，按照业务系统数据分类分级标准，自动发现敏感数据，同时支持基于关键字的信息审计，实现敏感数据的深度检测识别，对机密信息外发、敏感数据批量获取等行为进行记录分析。具备流量统计分析能力，通过对业务系统流量、协议进行统计分析，基于 IP 地址、攻击事件、应用协议等条件产生详细的流量报表，数据安全管理员通过协议、流量的排名了解当前网络带宽的使用状况以及数据交互流量情况，并形成数据安全态势地图为运维管理工作提供决策依据。

4.2 数据资产管理

数据资产采集可智能发现 IT 系统中的数据存管设备与服务，对数据管理服务、数据资产的来源、结构化数据进行识别分析，减少人工参与，提高资产管理效率。通过按时间定制任务的方式发现在网数据资产，周期性扫描及时发现新增资产，如采集过程中断，可提供异常恢复机制，确保发现的连续性。通过数据源直连方式对数据资产进行自动发现、采集，对不能自动发现的资产可通过接口、手动录入、批量导入等方式添加。

数据分类是数据保护工作中的一个关键部分，是建立统一、准确、完善的数据架构的基础，是实现集中化、专

业化、标准化数据管理的基础。行业机构按照统一的数据分类方法，依据自身业务特点对产生、采集、加工、使用或管理的数据进行分类，可以全面清晰地厘清数据资产，对数据资产实现规范化管理，并有利于数据的维护和扩充。数据分类为数据分级管理奠定基础。

数据分级是以数据分类为基础，采用规范、明确的方法区分数据的重要性和敏感度差异，并确定数据级别。数据分级有助于行业机构根据数据不同级别，确定数据在其生命周期的各个环节应采取的数据安全防护策略和管控措施，进而提高机构的数据管理和安全防护水平，确保数据的完整性、保密性和可用性。评估系统帮助实现数据分类分级管理，厘清数据资产、确定数据重要性和敏感度。通过分类分级可以有针对性地采取适当、合理的管理措施和安全防护措施，形成一套科学、规范的数据资产管理与保护机制，从而在保证数据安全的基础上促进数据开放共享。评估可结合人工对敏感数据进行分类和等级划分，便于用户根据不同需要对数据资产进行重点防护。

完成数据分类分级并建立数据资产字典，绘制数据资产图谱，对敏感数据进行定义，提供全网敏感数据进行自动扫描发现能力，对扫描的敏感数据进行索引标记。并对敏感数据进行分级分类标识，建立敏感数据资产分布视图，实现敏感数据的可发现，可展示、可稽核，全面掌控业务数据核心资产。

4.3 接口安全管理系统

4.3.1 接口信息采集

接口信息采集方式可以通过并联采集(镜像或分光)、串联采集、或者软件代理等方式获取。对所关联的接口通过网络流量画像进行识别，包括但不限于企业内部接口、内部日志接口、对外开放数据接口、对外开放业务接口等。

4.3.2 接口安全管理

具备面向流量的 HTTP 接口监管，支持对 HTTP 接口的自动发现能力，支持通过接口使用情况、活跃度等维度发现接口的异常行为并告警的能力，可对接口管理分析。实现接口清单、接口使用情况、接口活跃度、接口敏感级别等统计与可视化展示的能力。面向流量的接口敏感数据监管，支持结合数据敏感级划分规则库，提供对敏感数据传输情况的监测能力，支持对敏感数据检测结果的告警能力。网络数据的流转与组成分析与监管，支持对网络数据流向、流量等关键信息的数据流转分析与监管能力，支持数据流转可视化，支持数据跨域、数据跨境等网络流量流转异常检测与告警，支持分区域、分主题的网络上下行流量、在线人数以及协议构成等流量构成分析与监管。面向网络流量的数据安全风险监测，支持对接口暴露风险、账号盗用风险等网络侧数据安全风险的检测与告警能力。基于网络流量分析技术以及协议解析技术，可以自动发现及梳理应用及接口资产清单、管理应用及接口资产基础信息、提供应用及接口资产的敏感标签管理以及提供敏感数据资产的使用和分布情况，清单、接口使用情况、接口活跃度、接口敏感级别等统计与可视化展示的能力。应用接口自动发现、敏感数据识别、应用账号发现、协助全面掌握敏感数据使用状况，及时防控敏感数据行为风险支持按照策略进行结果集审计，可以指定敏感表审计结果集，支持通过返回行数和内容大小控制返回结果集大小。

敏感数据行为监测、数据流向监测、应用监测、接口监测、账户监测、访问 IP 监测功能，针对敏感数据行为全程留痕、多维度可查、可分析、可追溯。

4.3.3 对外开放管理

不同场景下数据资产对外开放不同管理能力，通过对数据资产分类分级结果及接口流量抽样分析，监测出数据对外开放情况，发现数据异常流转及违规开放安全事件，并通过数据分析提取特征，补充数据安全风险监测策略库和数据流转行为规则库。合作中的持续监控功能。根据合作前审查结果，结合接口流量，形成行为规则库，对数据对外开放情况进行监测，发现数据异常流转与违规开放等数据安全事件。

5 结语

数字经济的核心是数字技术和数据，维护网络信息和数据安全已是国家战略，需要全社会积极参与，只有在这个基础上，提升网络信息安全防护技术能力，构建全民网络信息安全防护意识，方能高效防范网络入侵和威胁。通过并联采集（镜像或分光）、串联采集、或者软件代理等方式，将所关联的接口通过网络流量画像进行识别，实现接口清单、接口使用情况、接口活跃度、接口敏感级别等统计与可视化展示的能力，将数据资产分类分级并建立数据资产字典，绘制数据资产图谱，对敏感数据进行定义，提供全网敏感数据进行自动扫描发现能力，对扫描的敏感数据进行索引标记，并对敏感数据进行分级分类标识，建立敏感数据资产分布视图，实现敏感数据的可发现，可展示、可稽核，全面掌控业务数据核心资产，自动发现敏感数据分布情况，根据数据的流转、交互、使用等过程进行分析，数据态势分析维度需要包含数据流转分析、数据交换分析、数据趋势分析、数据敏感程度分析、数据流量分析等多种类型，实现数据资产的管理能力，管理好数据资产，加快构建新发展格局，才能为数字经济高质量发展助力，更好地建设和谐美丽的现代化强国。

[参考文献]

[1]刘芳芳.计算机网络信息安全及防护策略[J].数字通信世界,2017(10):234.
[2]侯明,李书领.大数据时代计算机网络信息安全及防护策略[J].信息记录材料,2021(10):40-41.
[3]努尔古丽·吐尔逊.大数据时代计算机网络信息安全及防护策略[J].无线互联科技,2021(18):19-20.

作者简介：马锦贤（1980.5-），毕业于新疆大学，通信工程专业，研究方向：网络信息安全。