大数据时代数据安全防护通用最佳实践

中国信通院-阿里巴巴集团安全创新中心

2017 年 10 月

版权声明

目录

一、概述

当前，随着信息技术产业革命浪潮，特别是大数据技术创新应用，全球社会正式进入“数据驱动”的时代。大数据技术赋予了人类前所未有的对海量数据的处理和分析能力，促使数据成为国家基础战略资源和创新生产要素，战略价值和资产价值急速攀升。

对国家而言，对数据的掌握和利用已成为重塑国家竞争优势、完善国家公共治理体系的关键。大数据时代，国家竞争力部分体现为一国拥有数据的规模、质量以及运用治理数据的能力。世界各国普遍高度重视数据资源战略价值，出台国家战略，落实配套措施，系统提升国家数据掌控能力。另一方面，数据驱动国家治理体系发生根本性改变，从“主观主义” 的模糊治理方式，向“数据引领”的精准治理方式转变，利用大数据等新兴信息技术实现科学决策、智慧治理，打破“信息孤岛”，实现部门间、政府和民众间信息共享，形成新型社会众包式、自治式等治理新模式。

对企业而言，数据驱动的创新应用成为企业全生产链条升级发展的全新范式。数据是数字经济时代社会生产的新主导要素，也是新工业革命的核心内容，以数据为驱动的智能制造企业，通过数据实时采集、智能分析和动态反

馈，实现从原材料采购、生产加工、物流运输等全生产链条的智能决策，提升资源配置和劳动生产效率。同时，数据改变了传统业务发展形态，企业利用数据快速感知市场需求，构建以数据为驱动的产品布局、市场定位等企业业务发展综合决策新模式，催生大量新产品、新业态，激发市场活力的同时，助力企业提升市场竞争力。

然而，我们要看到，大数据技术引发的数据利用新需求、新模式、新业态与保护数据安全之间存在天然冲突，形成了数据利用与保护国家数据资源、数据利用与保护商业秘密、数据利用与保护个人隐私三个主要矛盾。解决这三个矛盾问题，不仅需要国家在顶层设计层面完善数据安全管理体系，加强数据安全法律法规建设，强化数据安全政府监管，还需要数据控制者，即掌握数据资源的企业或机构提升自身数据安全防护能力，切实保障数据机密性、完整性、可用性的同时，保护国家数据资源、企业商业秘密、公民个人信息免遭泄漏、窃取及毁损。

阿里巴巴—信通院创新中心在阿里巴巴数据运营和安全防护实际工作经验基础之上，总结提出了数据安全防护通用最佳实践：分析总结了大数据时代下数据安全防护面临的新挑战和新需求，提出了数据安全防护总体目标和框架，并系统阐述了数据安全防护管理措施和技术措施实践方法，最后根据阿里巴巴及合作伙伴实际业务运营工作，

给出了数据安全防护体系建设的典型案例。

二、大数据时代下数据安全面临的挑战

大数据时代下，数据的产生、流通和应用更加普遍化和密集化。从国家层面而言，数据安全是保障国家安全，维护国家网络空间主权，强化相关国际事务话语权的工作重点；从企业层面来看，数据安全关系到商业秘密的规范化管理和合理保护与支配，是企业长久发展不可回避的新阶段任务；对于个人而言，数据安全与个人生活息息相关，直接关系到每位公民的合法权益。大数据时代背景下，新的技术、新的需求和新的应用场景都给数据安全防护带来全新的挑战。

（一）新技术带来的挑战

分布式计算存储架构、数据深度挖掘及可视化等大数据技术能够大大提升数据资源大规模存储和高性能分析处理能力。然而，分布式的系统部署、开放的网络环境、众多的用户访问，使得数据安全保护面临更大挑战。一是底层复杂开放的分布式存储和计算架构导致系统安全边界模糊，基于边界防护的传统安全措施有效性降低。二是大数据技术引发的全新变革在软件、硬件、协议等多方面引入

的未知漏洞，极有可能存在大量安全威胁和隐患。三是分布式节点之间、大数据相关组件之间的通信安全成为新的安全薄弱环节，数据传输面临遭监听、窃取或篡改的威胁。四是分布式数据资源池可能汇集众多用户数据，数据量大和数据种类多为用户数据隔离带来困难。

面对新技术带来的挑战，网络与数据安全技术需要同步演进，打破传统基于安全边界的防护策略，实现更细粒度的访问控制，具备更高性能的加密和密钥管理能力，进而保证数据自身安全。

（二）新需求带来的挑战

大数据时代下，新需求主要体现在对数据资源的占有和利用，由此形成了广泛收集数据和共享开放数据两种具体表现形式。一方面，当前移动智能终端、传感器、智能联网设备时刻采集物理世界的信息，并转化为电子数据，虚拟世界正在成为现实世界的完整映射。另一方面，由于数据的资产价值和经济价值不断攀升，政府部门、企业间数据开放和共享需求随之增加，通过汇聚多方数据进行处理、挖掘分析得出的有用信息是单一数据集无法获得的，所创造的价值也是单一数据集无法比拟的。

同时也要看到，数据广泛、多源收集对数据安全本身及个人信息保护带来了新的挑战。一是数据收集中数据来

源和真实性验证变得格外重要，直接影响后期数据分析结果和智能决策的准确性。然而，采集终端性能限制、技术不足、信息量有限、来源种类繁杂等多种原因，使得数据来源和真实性验证面临多重挑战。二是当前企业可以利用各类智能终端设备、智能联网设备全天候收集人们生活方面的信息，但是在收集个人信息过程中存在过度收集、未履行告知义务、采取签订一揽子协议方式征得用户同意等现象，侵害个人合法权益。

另外，数据开放共享也对国家数据资源和企业商业秘密的安全构成一定威胁。一是目前对于政府数据开放的分级分类标准、开放渠道安全、开放过程安全缺乏统一规范和指导，可能会出现该开放的数据没开放，不该开放的数据开放等问题和风险。二是出于保护商业秘密的考虑，企业各方在提供数据资源进行多方数据计算时，不希望其他人看到自己的数据，因此如何实现数据“可用不可见”，保护数据机密性的同时又能够完成计算，是当前亟待解决的数据应用安全性问题。

（三）新的应用场景带来的挑战

大数据背景下，数据应用浪潮逐渐从互联网、金融、电信等热点行业领域向融合业务、物联网、传统制造等行业和领域拓展渗透。数字化生活、智慧城市、工业大数据

等新技术、新业务、新领域创造出纷繁多样的数据应用场景。

多样的数据应用场景增加了数据安全保护具体情境的复杂性，对数据安全防护工作提出了新挑战和新需求。一是如何在多样化的应用场景之下，采取全新的应对模式，灵活而有效地保护数据处理过程中每一环节的客观安全，确保大数据技术在多渠道流通、多领域融合的复杂过程中的机密性、完整性、可用性，是大数据安全防护体系在新的应用场景下面临的全新挑战。二是频繁的数据共享和交换促使数据流动路径变得交错复杂，数据从产生到销毁不再是单向、单路径的简单流动模式，也不再仅限于组织内部流转，而会从一个数据控制者流向另一个控制者。在此过程中，实现异构网络环境下跨越数据控制者或安全域的全路径数据追踪溯源变得更加困难，特别是数据溯源中数据标记的可信性、数据标记与数据内容之间捆绑的安全性等问题更加突出。

三、数据安全防护目标和防护体系

（一）防护目标

对于不同安全责任主体，数据安全防护工作的目标和侧重点也有所差异。对国家而言，需要从保障国家安全的

高度建设完善数据安全保障体系；对企业或组织而言，需要从保护商业秘密、业务正常运行、客户合法权益等方面开展数据安全防护工作。

国家层面的数据安全防护目标可以根据数据属性类型和重要敏感程度划分为三个层次：基础层是数据自身安全，保障目标是维护网络数据的完整性、保密性和可用性，防止网络数据泄漏或者被窃取、篡改。第二层是个人信息保护，保障目标是在保障数据自身安全的同时，保障信息主体对个人信息的控制权利，维护公民个人合法权益。最上层是国家层面的数据安全，保障目标是在保障数据自身安全的同时，强化国家对重要数据的掌控能力，防止国家重要数据遭恶意使用，对国家安全造成威胁。

企业或组织层面的数据安全防护目标可以划分为两个层次：一是保护数据本身安全，即为保护商业秘密和业务正常运行而必须保障数据机密性、完整性、可用性；二是满足国家相关法律法规提出的合规性要求，包括对个人信息和国家重要数据的保护要求。

国家层面和企业层面的数据安全防护目标虽然有所差异，但不是割裂的。企业或组织作为数据控制者，首先需要强化自身数据安全防护能力，实现企业层面数据安全防护目标，在此基础上，才能进一步实现国家层面的数据安全防护目标。从本报告的定位出发，下面重点就如何实现

企业或组织层面的数据安全防护目标进行论述。

（二）防护体系

企业或组织层面的数据安全防护体系由数据安全组织管理、制度规程、技术手段“三架马车”构成，形成数据安全防护的闭环管理链条，以实现数据安全防护总体目标，防范批量数据泄漏以及敏感信息非授权访问等风险。其中，

数据安全组织管理是落实数据安全实践工作的首要环节。企业通过成立专门的数据安全管理团队，自上而下地建立起从各个领导层面至基层员工的管理组织架构，保证数据安全管理方针、策略、制度的统一制定和有效实施。着眼全局，把握细节，以完整而规范的管理组织体系架构保证数据流通每个环节的安全管理工作。

数据安全制度规程是数据安全实践工作的制度保障。在数据安全防护实践中，数据安全制度规程提供具体的方式方法，以规范化的流程指导数据安全管理工作的具体落实，避免了实际业务流程中“无规可依”的场景，是数据安全管理工作实际操作中的办事规程和行动准则。

数据安全技术手段是数据安全实践工作的保障条件。作为数据安全管理的辅助手段，数据安全技术手段提供了数据收集、使用具体场景中的安全工具，为落实数据安全

制度规程、实现数据安全防护的总体目标提供了技术支持，保证纸面上的管理制度要求在实际工作中切实得到执行。

图 1　企业或组织的数据安全防护体系

此外，数据安全防护建设的总体思路是以“数据为中心”建设安全防护体系，聚焦数据，聚焦数据生态。明确数据的来源、形态、应用场景，有针对性地建立防护措施；理清数据生态体系的参与主体，生产数据、加工数据、消费数据的具体承担者，构建覆盖全面的安全防护体系。

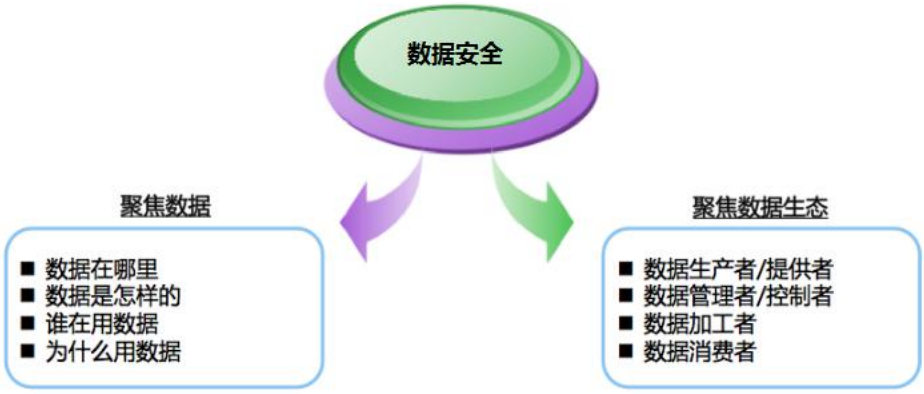

图 2 数据安全防护体系建设总体思路

四、数据安全防护管理措施实践方法

本章从组织内部的数据安全管理架构及机构设置、岗位设置、管理制度及规程等方面总结数据安全防护管理措施的实践方法。

（一）组织架构设置

为保证数据安全管理方针、策略、制度的统一制定和有效施行，组织内部应建立贯穿企业最高领导层到普通员工的数据安全管理组织架构，如图 3 给出的示例。组织架构可以自上而下分为策略层、管理层、控制层和执行层。

图 3 数据安全管理组织架构

策略层负责制定组织内部数据安全管理的总体目标、方针、策略等，从全局角度把控数据安全风险，就重大数据安全事件或案例进行决策。策略层实际呈现形式可以是数据安全小组或数据安全委员会，建议由主管数据安全工作的副总裁或同级别领导担任组长，小组成员至少包括网络安全管理、数据安全管理、财务、法务、人力资源及相关业务部门的经理或负责人。

管理层负责按照策略层确定的管理目标、方针、策略制定组织内部数据安全管理制度规范并执行，负责数据安全防护技术措施的规划建设和落地，指导协助相关业务部门建立数据安全管理的组织体系并执行管理制度规范。**建议成立或指定数据安全管理部门，**负责上述管理层工作职责。同时，建议成立由数据安全管理部门、相关业务部门负责人组成的虚拟数据安全管理团队，负责落实相关业务

部门的数据安全管理责任，执行数据安全管理制度规范。

控制层在部门层面负责实施数据安全管理规范、策略等。建议相关业务部门明确**数据安全责任人（一般由部门经理或负责人担任）、数据安全管理员**，负责数据访问权限审批、异常行为告警处置等数据安全日常运营工作。

执行层由普通员工组成，需要按照数据安全管理制度规范开展日常工作。

（二）机构及岗位设置

为有效执行数据安全管理制度规范、策略，组织内部需要成立或指定数据安全管理部门，明确部门职责及部门内部每个数据安全管理岗位的职责。根据组织的业务发展规模、增长速度，设置并及时调整数据安全管理部门规模和人员数量。除数据安全管理部门外，还需要在相关业务部门设置专职或兼职数据安全管理岗位，负责在业务部门内部执行数据安全管理制度规范及策略，同时做好与数据安全管理部门的沟通与协作。

（三）人员管理

人员管理除建立完善的人力资源管理体系和制度外，从数据安全管理角度还需要考虑专业技能、奖惩机制、教育培训等方面工作。在人员入职时，需考察人员专业能力

与数据安全管理岗位要求是否匹配。在人员在岗期间，需建立工作业绩考核机制及相应的奖惩机制。同时，建立数据安全教育培训机制，针对数据安全管理人员，建议至少每季度举办一次专业培训；针对所有全职员工、外包服务人员、合作伙伴的员工、实习生等，建议在入职前、在职、转岗、待离职、离职等关键节点，组织安全意识教育和数据安全管理制度宣传培训。

（四）管理制度及规程

管理制度不仅是落实在纸面上的规定，更是要落实在组织内部的实际工作中，在各个业务环节、工作流程中切实按照管理制度的规定要求开展工作，才是在真正意义上实现安全管理。为此，对管理制度的编制也提出了一定要求：一是要明确相关工作的责任部门和责任人，即明确每项工作由谁来负责；二是规定要求清晰易懂，明确应该做什么，不允许做什么，例外情况是什么；三是要明确奖惩措施。

就数据安全管理制度体系而言，范围要覆盖数据全生命周期，包括数据产生／采集、传输、存储、使用、共享、销毁等环节；体例上，可以根据组织规模和实际情况，形成数据安全总体要求、实施细则、数据共享安全管理、个人信息保护等多个管理文件，或在一个文件中涵盖

全部内容；内容上，可以在如下几方面进行重点规范。

1、数据分级分类管理

对掌握的数据资源进行数据分级分类，是实现数据有效管理和利用，保障数据安全的基础。管理制度在数据分级分类管理方面要明确如下内容：一是数据类型，可以根据数据属性、来源、内容进行分类，例如按照数据来源分为业务数据、企业数据、用户数据。二是数据安全等级和等级划分标准，一般可以根据数据重要性、敏感程度将数据分为三级或者四级，对每级数据制定差异化的保护措施。三是明确数据的安全责任部门和责任人，对于存量数据，一般是生产或主要使用该数据类型的部门承担；对于新产生的数据，一般规定由生产该数据类型的部门负责数据定级及后续的安全管理。

2、账号权限管理及审批规程

数据安全管理的账号权限管理及审批主要关注的是组织内部不同账号类型对生产数据库进行操作的权限管理及授权审批规则。账号权限管理同样是保障数据安全的基础制度，完善的授权规则能够有效防范内部人员恶意窃取、泄漏数据的风险。制定账号权限管理及审批制度需注意以下几点：一是对账号类型进行精细分类，对每个账号类型

能够获得的最高权限进行明确规定。对于内部全职员工，根据工作职责设置不同账号类型，对外包服务人员、合作伙伴的员工、实习生等外部人员单独设置账号类型。二是定期对账号进行复核，及时回收权限。账号管理要与人员管理紧密结合，在员工入职、转岗、离职等关键节点同步管理账号及权限；定期对所有账号的权限分配情况进行复核，对于不再有合理需求的账号权限及时关闭。三是明确账号权限审批流程，规定初审、复审等审批环节以及每个审批环节的责任人。可以由每个部门内部的数据安全管理员承担初审工作，部门负责人进行复审。权限审批应当依据最小化原则，同时确认所申请权限与工作实际需求匹配，超出合理需求的申请不予授权。四是对于测试账号等高危账号类型，明确管理责任人，在系统开发测试完毕后立即清除。

3、第三方数据共享安全管理

为保障数据全生命周期安全，组织向第三方提供或共享数据的过程需要建立相应的安全管理制度，除了法律合规方面的要求外，数据共享安全管理制度要包含如下内容：一是开展数据共享活动前，对数据接受方的背景、资质进行审查；当满足国家关于个人信息和重要数据出境安全评估相关判定条件时，还应按照相关法律法规和国家标

准开展安全评估。二是检验数据接受方的数据安全保护能力，可以通过要求数据接受方出具相关资质、权威检测报告等形式进行验证，目的是保障数据共享后的安全水平不降低。三是签订安全协议或在合同中设置安全条款，明确双方安全责任，明确数据接受方是否有权向他人再次提供数据。

4、外包服务数据安全管理

外包服务人员及其使用设备应当纳入组织内部整体网络安全管理体系中，至少在人员管理、设备管理、网络接入管理等方面明确管理要求和限制措施。除上述对外包服务人员加强账号权限管理外，还需注意以下几点：一是不对外包服务人员的账户开放批量数据提取或下载权限，如确需此类权限，应单独制定更为严格的审批流程，至少通过数据安全管理部门审批，并对授权设置有效期或及时回收。二是在外包服务人员撤场后，及时撤销相关账户。三是对外包服务人员使用的设备接入内网，应建立单独审批流程。

5、日志管理和安全审计

对各类账号访问、操作行为进行日志记录并定期审计，是发现违规行为的必要手段，也是安全事件事后调查

的必要手段。关于日志管理和安全审计，管理制度应当明确：一是日志记录的信息，至少包括时间、账号 ID、操作对象、操作类型等字段信息。二是日志记录保存的时间。三是安全审计的周期，可以按照数据等级差异化制定审计周期，例如高安全等级的数据，每季度审计一次；较高安全等级的数据，每半年审计一次等。

6、数据备份与恢复

数据备份是关系到系统灾难恢复、业务连续性的重要工作。关于数据备份与恢复，管理制度应当明确：一是数据备份的策略，根据数据重要性、业务系统对数据的依赖程度，明确热备或冷备，本地备份或异地备份等策略。二是数据备份的频率，可以与备份策略结合采取差异化的备份频率，如每天增量热备，每月全量冷备等。三是恢复性测试的频率和范围，可以制定多个组合策略，如每月对部分备份数据进行恢复性测试，每年对全量备份数据进行测试等。

最后，还需特别说明的是，上述内容不是数据安全管理制度应当规范的全部内容，数据传输安全、存储安全、数据脱敏、数据防泄漏等措施，在管理制度中同样应当明确规则，但是因为这些措施与技术手段及工具结合紧密，为避免重复，将在下一章进行重点介绍。

五、数据安全防护技术措施实践方法

本章结合第四章数据安全防护管理措施，从数据产生/采集、传输、存储、使用、共享、销毁等数据生命周期关键环节梳理总结数据安全防护需要具备的技术手段和工具，包括但不限于身份认证、访问控制、安全审计、异常行为监测预警、数据加密、数据脱敏、数据防泄漏等数据安全技术。

（一）数据产生/采集环节的安全技术措施

从数据安全角度考虑，在数据产生/采集环节需要实现的技术能力主要是元数据安全管理、数据类型和安全等级打标，相应功能需要内嵌入后台运维管理系统，或与其无缝对接，从而实现安全责任制、数据分级分类管理等管理制度在实际业务流程中的落地实施。

1、元数据安全管理

以结构化数据为例，元数据安全管理需要实现的功能包括数据表级的所属部门、开发人、安全责任人的设置和查询，表字段的资产等级、安全等级查询，表与上下游表的血缘关系查询，表访问操作权限申请入口。图4是一个元数据安全管理功能示例，在后台系统界面上显示了一个数据表基本情况，包括每个字段的类型、具体描述、数据

类型、安全等级等，同时显示这个数据表的开发人、负责人、安全接口人、所属部门等信息，并且可以通过这个界面申请对该表访问操作权限。

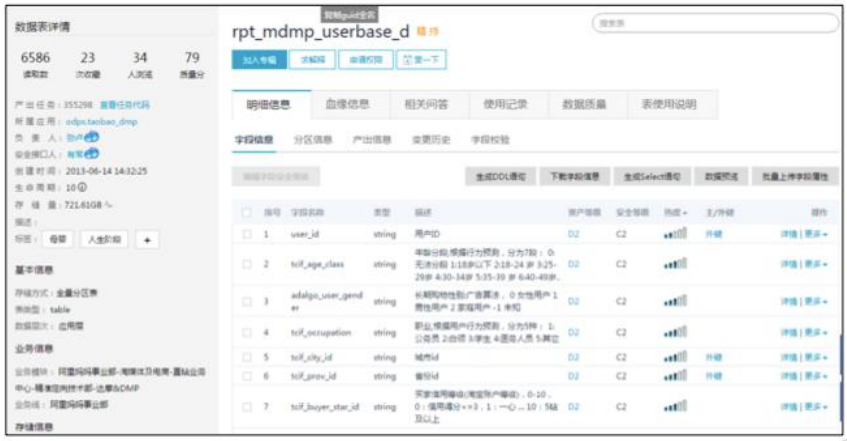

图 4 元数据安全管理系统示例

2、数据类型、安全等级打标

自动化的数据类型、安全等级打标工具帮助组织内部实现数据分级分类管理，特别是在组织内部拥有大量数据的情况下，能够保证管理效率。打标工具根据数据分级分类管理制度中定义的数据类型、安全等级进行标识化，通过预设判定规则实现数据表字段级别的自动化识别和打标。图 5 和图 6 是一个打标工具的功能示例。图 5 显示了一个数据表每个字段的数据类型和安全等级，在这个示例中，“C”表示该字段的数据类型，“C”后面的数字表示该字段的安全等级。图 6 显示的是一个预设规则的列表，每一条规则包括了适用范围、匹配项目、匹配方式，以及

匹配成功后应标识的数据类型和安全等级。

序号	字段名称	类型	热度	是否业务主键	是否外键	资产等级	安全等级	描述
1	member_id	bigint			Y	D1	C2	会员id
2	password	string					C4	会员密码---已作废
3	nick	string			Y	D1	C2	会员名
4	fullname	string					C3	全名
5	shop_name	string				D2	C2	商铺名称
6	address	string					C3	地址
7	city	string				D1	C2	注册填写城市
8	province	string				D1	C2	注册填写省
9	country	string					C2	注册填写国家
10	zip	string					C2	邮政编码
11	phone	string					C3	电话号码

图 5 数据类型、安全等级标识示例

图 6 数据类型、安全等级打标规则示例

（二）数据传输存储环节的安全技术措施

数据传输和存储环节主要通过密码技术保障数据机密性、完整性。在数据传输环节，可以通过 HTTPS、VPN 等技术建立不同安全域间的加密传输链路，也可以直接对数据进行加密，以密文形式传输，保障数据传输过程安全。在数据存储环节，可以采取数据加密、硬盘加密等多种技术

方式保障数据存储安全。

（三）数据使用环节的安全技术措施

数据使用环节安全防护的目标是保障数据在授权范围内被访问、处理，防止数据遭窃取、泄漏、损毁。为实现这一目标，除了防火墙、入侵检测、防病毒、防 DDoS、漏洞检测等网络安全防护技术措施外，数据使用环节还需实现的安全技术能力包括：

1、账号权限管理

建立统一账号权限管理系统，对各类业务系统、数据库等账号实现统一管理，是保障数据在授权范围内被使用的有效方式，也是落实账号权限管理及审批制度必需的技术支撑手段。账号权限管理系统具体实现功能与组织自身需求有关，除基本的创建或删除账号、权限管理和审批功能外，建议实现的功能还包括：一是权限控制的颗粒度尽可能小，最好做到对数据表列级的访问和操作权限控制。二是对权限的授予设置有效期，到期自动回收权限。三是记录账号管理操作日志、权限审批日志，并实现自动化审计；日志和审计功能也可以由独立的系统完成。

2、数据安全域

数据安全域的概念是运用虚拟化技术搭建一个能够访

问、操作数据的安全环境，组织内部的用户在不需要将原始数据提取或下载到本地的情况下，即可以完成必要的查看和数据分析。原始数据不离开数据安全域，能够有效防范内部人员盗取数据的风险。图 7 是数据安全域的拓扑结构示例，数据安全域由一个虚拟机集群组成，与数据库服务器通过网关连接，组织内部用户安装相应的终端软件，可以通过中转机实现对原始数据的访问和操作。

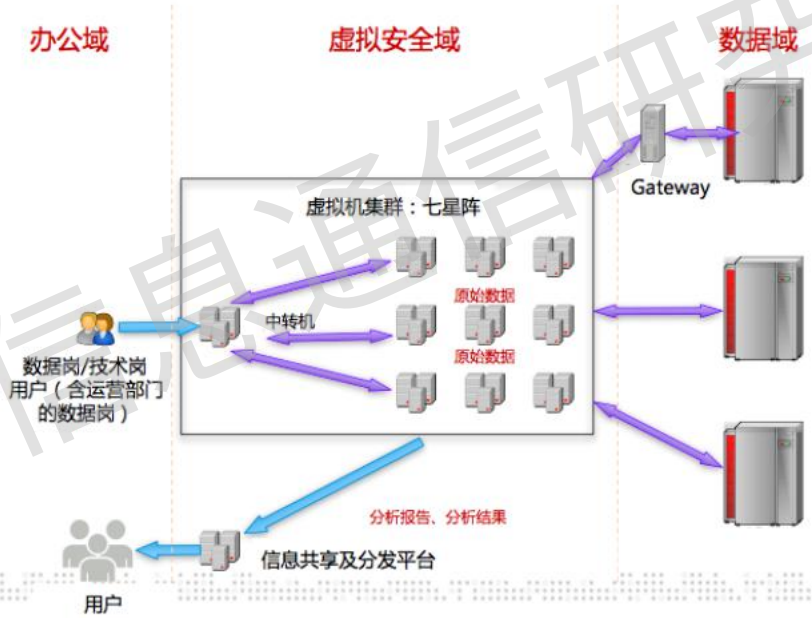

图 7 数据安全域拓扑结构示例

3、数据脱敏

从保护敏感数据机密性的角度出发，在进行数据展示时，需要对敏感数据进行模糊化处理。特别是对手机号码、身份证件号码等个人敏感信息，模糊化展示也是保护

个人信息安全所必须采取的措施。业务系统或后台管理系统在展示数据时需要具备数据脱敏功能，或嵌入专门的数据脱敏工具。图 8 是一个数据脱敏工具的示例，展示了预先设置的脱敏策略，可以实现对数值和文本类型的数据脱敏，支持多种脱敏方式，包括不可逆加密、区间随机、掩码替换等。

图 8 数据脱敏规则示例

4、日志管理和审计

日志管理和审计方面的技术能力要求主要是对账号管理操作日志、权限审批日志、数据访问操作日志等进行记录和审计，以辅助相关管理制度的落地执行。技术实现上，可以根据组织内容实际情况，建设统一的日志管理和审计系统，或由相关系统各自实现功能，如账号管理和权

限审批系统,实现账号管理操作日志、权限审批日志记录和审计功能。

5、异常行为实时监控与终端数据防泄漏

相对于日志记录和安全审计等“事后”追查性质的安全技术措施，异常行为实时监控是实现“事前”、“事中”环节监测预警和实时处置的必要技术措施。异常行为监控系统应当能够对数据的非授权访问、数据文件的敏感操作等危险行为进行实时监测。同时，终端数据防泄漏工具能够在本地监控办公终端设备操作行为，是组织内部异常行为监控体系的主要组成部分，可以有效防范内部人员窃取、泄漏数据的风险，同时有助于安全事件发生后的溯源取证。图 9 是终端数据防泄漏工具可实现功能的示意图。终端数据防泄漏工具通过监测终端设备的网络流量、运行的软件、USB 接口等，实时发现发送、上传、拷贝、转移数据文件等行为，扫描文件是否包含禁止提供或披露的数据，进而实时告警或阻断。

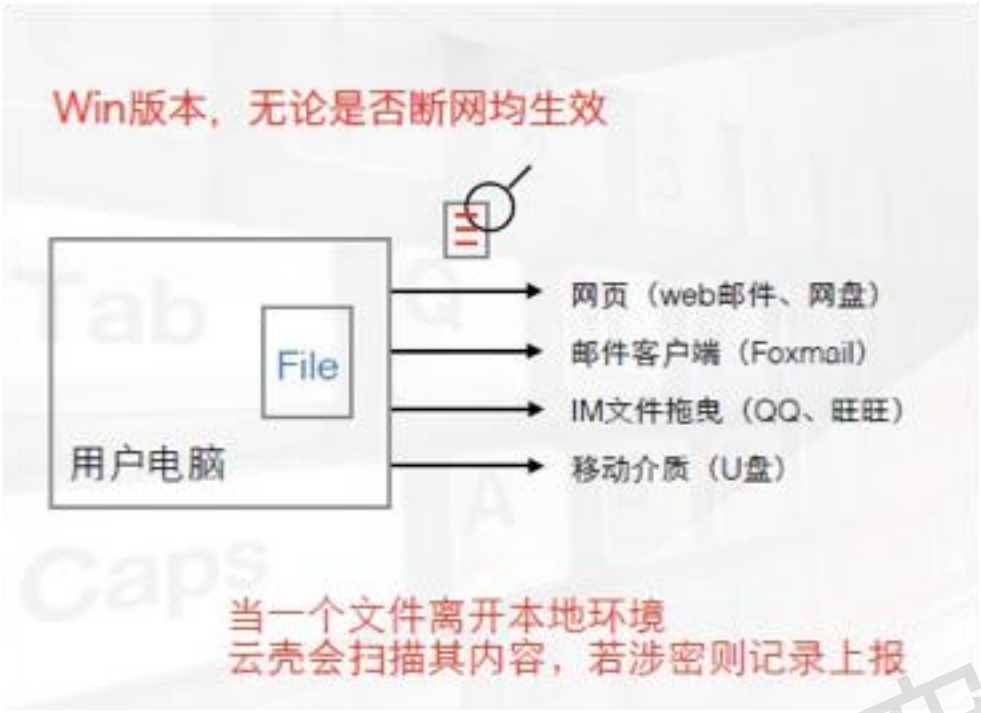

图 9 终端数据防泄漏工具功能示意图

（四）数据共享环节的安全技术措施

数据共享环节涉及向第三方提供数据、对外披露数据等不同业务场景，在执行数据共享安全相关管理制度规定的同时，可以建设统一数据分发平台，与数据安全域技术结合，作为数据离开数据安全域的唯一出口，进而在满足业务需求的同时，有效管理数据共享行为，防范数据遭窃取、泄漏等安全风险。统一数据分发平台需要整合所有数据共享业务场景，例如基于原始数据的处理分析结果向第三方共享、数据分析报告下载到办公终端设备等情形，对每一类数据共享场景实现差异化的线上审批流程。

（五）数据销毁环节的安全技术措施

在数据销毁环节，安全目标是保证磁盘中存储数据的永久删除、不可恢复，可以通过软件或物理方式实现。数据销毁软件主要采用多次填充垃圾信息等原理，此外，硬盘消磁机、硬盘粉碎机、硬盘折弯机等硬件设备也可以通过物理方式彻底毁坏硬盘。

六、数据安全防护典型案例

（一）案例一：钉钉移动智能办公平台

钉钉智能移动办公平台在数据安全方面依照上述数据安全防护方法展开了相关工作，全面推行集团安全策略要求，通过技术创新和大数据运营，持续改进各项安全控制措施，探索研究前沿技术，有效地对平台运营过程中数据安全进行防护，提升数据安全威胁防范能力，其实践情况大致如下。

1、数据安全防护管理措施

该公司建立的信息安全管理体系覆盖了产品研发、业务运营、安全保障、营销推广等全生命周期，实现信息安全管理的每一位“责任人”，按照明确的“规范”、遵守标准的“流程”，安全流程基本实现线上化，过程数据指

标化，运营度量平台化，基本覆盖各项安全控制措施，有效保障了业务安全、稳定、合规。

（1）完善数据安全管理组织架构

该公司安全组织团队建立了规范的信息安全管理组织架构。策略层由 CRO 和在其领导下的安全管理委员会组成，下分安全产品团队和安全运营团队，从全局角度把控数据安全风险，就重大数据安全事件或案例进行决策。在管理层面，安全产品团队承担主要职责，以策略层确定的管理目标、方针和策略为指导，落实相关业务部门的数据安全管理责任。在控制层面，安全运营团队由集团安全部及各产品线相关人员组成，快速响应业务系统潜在的各类网络运行风险，并在不断对抗中，推动优化各项安全措施。执行层由普通员工组成，从聘用、入职、日常工作、调岗离职各个环节严格遵照全局安全策略要求，保证数据安全管理制度规范的日常应用。

（2）明确数据安全管理机构和岗位设置

该公司安全团队成立了专门的数据安全管理部门，即安全产品团队和安全运营团队，明确部门职责及部门内部每个数据安全管理岗位的职责，有效地执行数据安全管理制度规范、策略。除数据安全管理部门外，为了快速响应业务，该公司事业部建立了灵活的 Scrum 小组，按需与集团安全部进行无缝对接，快速复用集团全链路的动态防御

体系，保障业务安全稳定运行。

（3）强化数据安全人员管理

该公司安全团队在用工招聘录用时，进行技术能力和品行性格、职业道德的全方位考察。员工入职之前必须签署保密协议，关键岗位人员视接触信息的敏感程度还需单独签署专项保密协议，参加《商业行为准则》的培训，明确“公平公正、安全可靠”的服务承诺。同时，集团会开展《数据权限安全》、《员工行为纪律》、《安全红线》等相关培训，明确组织对于安全管理的要求和规定，了解个人在日常工作中承担的义务以及违反相关安全管理要求时面临的惩戒措施。日常工作中，员工定期接受组织的的强制安全意识培训和考试。员工调岗离职时，HR 和部门主管共同确定岗位应回收的信息资产、关闭应用权限，对于关键岗位员工视情况签署竞业协议并开展离职审计；对于违反安全管理要求的员工，依据员工纪律条款和约定进行处理。

（4）固化数据安全管理制度规程

在组织内部的实际工作中，针对数据安全管理制度体系，该公司安全管理团队全面落实了明确的管理制度规程。

- **数据分级分类管理**

该公司制定数据安全策略规范，按照数据类型、敏感

程度、数据价值等相关属性明确数据分类分级标准，在数据产生时，统一对数据进行分类分级打标，确保业务流转过程中，所有数据按照策略规范要求实施分类管控、分级授权。

- **账号权限管理及审批规程**

在服务端应用层面，必须统一接入权限管理系统，访问主体必须根据权限、角色和风险级别按需申请，并详细说明访问内容、访问理由、访问时长等相关信息，获得的访问权限定期复核，离职转岗后权限自动关闭。

- **第三方数据共享安全管理**

在对外数据开放共享方面，该公司严格遵循《网络安全法》要求，以用户隐私信息保护为首要前提，制定对外数据披露细则，明确要求所有对外数据输出必须遵循保护用户隐私、必要性和最小化、合规性的要求，保障数全生命周期安全。

- **日志管理和安全审计**

该公司在数据库操作层面，对增删改查的操作命令全程监控，实现操作日志集中存储，操作流量实时分析，一旦发现高危 sql 语句、批量违规操作、危险时段异常操作等违背安全管理要求的行为，及时告警并可实时在线拦截。

2、数据安全防护技术措施

该公司以数据安全为愿景，结合数据安全防护管理措施，在数据生命周期各阶段如数据产生、数据存储、数据使用、数据传输、数据共享、数据销毁等都嵌入了安全控制措施，保障用户数据的机密性、完整性、可用性。

（1）数据产生／采集环节实现数据分类分级

在实际应用中，该公司在数据产生/采集环节对数据安全等级进行分类管控，分级授权，应用元数据安全管理将相应的功能需要内嵌入后台运维管理系统，从而在实际业务过程中落实安全责任制、数据分级分类管理等管理制度。

（2）数据传输存储环节实现加密统一管理

在客户端，用户聊天信息（包括消息文本、图片、音视频和其他文件）采用高强度的对称密钥算法 AES-256-GCM 实施整库加密保护，并根据用户可信设备信息生成唯一的密钥，保护存储在客户端的敏感数据不被攻击者非法获取，同时企业可按需设置用户聊天信息自动销毁，确保本地数据的机密性。

在服务端，每个应用采用独立密钥，通过高强度对称密钥算法 AES-256-GCM 加密数据，且每个企业密钥各不相同，由硬件加密系统统一管理，保证了服务端数据存储的安全性。

（3）数据使用环节实现实时监测并记录

为了在数据使用环节实现安全防护的目标，保障数据在授权范围内被访问、处理，防止数据遭窃取、泄漏、损毁，在前端应用层面、服务端应用层面、数据库操作层面分别实施了相应的安全策略，保证数据使用环节的安全性和可靠性。在前端应用层面，涉敏页面全部数字水印处理，敏感信息已默认打点隐藏；在服务端应用层面，统一接入权限管理系统，获得的访问权限定期复核，离职转岗后权限自动关闭；在数据库操作层面，增删改查的操作命令全程监控，操作日志集中存储，操作流量实时分析，一旦发现高危 sql 语句、批量违规操作、危险时段异常操作等违背安全管理要求的行为，及时告警并可实时在线拦截。

同时，该公司建立了统一账号权限管理系统，对各类业务系统、数据库等账号实现统一管理，保障数据在授权范围内被使用，并记录账号管理操作日志、权限审批日志。

此外，该公司在每个数据中心内部立统一标准化的网络拓扑结构，并划分不同安全区域，依据每个区域承载业务的重要程度，又划分多个安全级别。不同级别区域之间部署严格的访问控制和路由策略，同时通过流量分光镜像和 flow 采样，实现流量 DPI/DFI 分析和监控，有效识别异

常行为。

在安全运营与应急响应阶段，安全工程师通过 SOC 安全运营平台实现安全事件分析、处置、跟踪和复盘，保障应用安全稳定运行。

（4）数据共享环节实现合理开放与披露

在数据共享环节，该公司严格遵循《网络安全法》要求，以用户个人信息保护为首要前提，制定对外数据披露细则，明确要求所有对外数据输出必须保护用户隐私。涉及用户个人信息，未经用户授权，不得收集、分析或向任何第三方输出，严格限制数据输出的范围、数量及知情者。

（5）数据销毁环节实现彻底性清除

该公司使用的信息处理设施，存储介质出数据中心前遵照 DoD 5220.22-M、NIST 800-88 标准进行数据清除、磁盘消磁以及物理销毁，避免数据泄漏风险。

（二）案例二：南方某供电公司最佳案例

该供电公司主要从事特大城市电网投资、建设与运营，负责管辖区域内的电力供应与服务。

该公司在数据安全方面同样依照本最佳实践提供的方法，对数据安全过程实施了正式的控制和管理，在组织层面具有清晰的数据安全岗位和职责定义。该公司与安全过

程配套的流程制度已经基本具备，并且能够通过固定的流程和技术工具、平台，保证安全过程的数据安全风险得到有效控制，其数据安全防护的实践大致如下。

1、数据安全防护管理措施

（1）构建统领全局的数据安全组织架构

从组织建设层面来看，该公司信息部和信息中心承担数据安全管理工作，对公司整体的数据使用情况负责，承担策略层和管理层的角色。同时成立了专门负责数据库管理的团队，负责处理数据库安装工单，执行数据库状态巡检，维护数据库账号等工作，实现控制层的职责。执行层由普通员工组成，在实际业务的各个环节遵照全局安全策略要求，保证数据安全管理制度规范的日常落实。

（2）明确数据安全管理机构和岗位分类职责

该公司以信息部和信息中心为主要数据安全管理部门，承担数据安全管理工作，对公司整体的数据使用情况负责。同时，针对为了加强数据质量管理和数据安全保护，该公司成立了专门负责数据库管理的团队，负责处理数据库安装工单，执行数据库状态巡检，维护数据库账号等工作。

（3）以宣传培训强化数据安全人员管理

对于人员管理，该公司会进行数据安全相关的培训、宣传，以网络培训系统做协助支持。从人力资源管理角度，将数据安全融入到员工入职、调岗和离职的标准流程中。

（4）细化管理制度流程的具体规则

该公司重视制度与规范的建设，颁发了《公司信息安全等级保护管理办法》、《信息安全防护管理办法》、《管理信息系统网络与信息安全应急预案》等多个管理办法。内部事务审批处理流程管理严格，一般申请遵循先提交工单、接单后操作、结单闭环等基本原则。审批流程的设置综合了相关业务部门和信息部门的意见，力求流程的合理与精简。但是数据分类分级、数据使用监控审计等为薄弱环节，有待完善。

2、数据安全防护技术措施

该公司结合数据安全防护管理措施，该公司建设了统一的安全管理平台解决方案，从数据产生／采集、传输、存储、使用、共享、销毁等数据生命周期关键环节梳理总结数据安全防护需要具备的技术手段和工具，有效保证了数据安全防护全周期安全防护。

（1）数据产生／采集环节实现数据真实性验证

在数据产生阶段，各大业务系统会收集用户档案、用

电信息、设备台账、设备运行信息等多种数据。其中，用户档案是数据量最为庞大的一类数据。庞大的用户隐私数据给数据安全保护带来了极大的挑战。为了保证数据采集的有效性和合规性，要求用户提供身份证明、房产证明等保证数据的真实有效。数据收集遵循“最小够用”原则，避免过多采集。

（2）数据传输存储环节采取堡垒机防护

在数据存储阶段，数据库管理员（DBA）接受和处理数据库安装工单、数据库状态巡检、数据库账号管理、数据库扩容以及数据导出等工作。数据库安装部署时，DBA 会检查数据库安全基线，例如账号密码有效期、账号锁定策略、禁用默认端口等。在网络方面，数据库服务器都安装有防火墙，只能在生产网段内访问数据库，且需要登陆堡垒机，从技术层面保证数据的储存安全。在数据传输阶段，公司的业务系统间传输数据使用企业信息集成平台，监控数据传输丢失情况，为数据传输安全提供保障。

（3）数据使用环节安全加强数据脱敏和终端管理

在数据使用阶段，数据导出时需要在相关系统中下单申请，审批通过后，由 DBA 执行数据导出。如果涉及敏感或隐私数据，数据提供方会提供脱敏字段列表和脱敏脚本，DBA 将按要求脱敏数据。一般脱敏方式包括数据替换、打乱顺序和使用随机数等。终端安全管理措施较为完善，

员工需要使用公司配发的电脑进行办公，且必须安装指定防病毒软件、文档加密软件等，可以实现U盘的管控，保障办公电脑数据安全。

（4）数据销毁环节实现无用数据及时处理

该公司的数据销毁环节中，比较典型的处理办法是系统退运后，将不使用的数据转移到低端和廉价存储设备上保存。