CAICT 中国信通院　奇安信 新一代网络安全领导者

数据安全风险分析及应对策略研究

（2022 年）

中国信息通信研究院云计算与大数据研究所
奇安信科技集团股份有限公司

2022 年 1 月

版权声明

前　言

数据作为一种新兴生产要素，已成为经济社会发展的核心驱动力，与此同时日益严峻的数据安全风险为数字化转型的持续深化带来严重威胁。为保障数字经济的健康有序发展，提高数据安全风险防控能力，国家、行业、地方相继出台多项数据安全法律法规，并接连开展相应的审查整治行动。总体来说，国内数据安全已进入合规合法的强监管新阶段。面对日益严格的合规要求及数字化场景下的新型安全威胁，本报告梳理了当前数据安全面临的几个突出问题：

一是 APP 对用户信息的过度采集。大量非必要的个人信息聚集，不仅滋生数据滥用等安全风险，也带来合规问题。

二是账号弱口令的使用普遍。低成本的攻击门槛，容易导致特权账号被盗取，带来内部管理难题的同时引入数据安全风险。

三是数据权限分配、使用不透明。当数据权限管理成为“黑盒”，越权访问、数据滥用等问题将无法管控。

四是 API 接口成为新型攻击手段。API 作为应用与数据服务的通信接口，应用场景广泛，已成为攻击者窃取数据的重点攻击对象。

五是数据安全的持续状态难以保持。一方面，应用数字化改造及数据消费场景较为复杂；另一方面，管理要求和技术落地存在一定脱节，导致持续的数据安全状态难以保障。

针对以上问题，本报告结合实战化攻防演习的实践经验，提出数据安全体系建设的行动思路和关键举措，旨在为组织开展数据安全体系化建设提供参考和建议。

目 录

图 目 录

一、数字化时代数据安全发展现状

数字化时代，数据已成为数字经济发展的核心生产要素。2020 年全球 47 个国家数字经济增加值规模达到 32.6 万亿美元，我国数字经济规模位居世界第二接近 5.4 万亿美元[1]。在此背景下，数据安全已成为事关国家安全与经济社会发展的重大问题。

（一）数据安全进入法治化的强监管时代

法律制度是数据安全的重要保障。当前我国数据安全法律法规建设取得突飞猛进的进展。**国家层面**，2021 年 9 月 1 日《数据安全法》施行，首次从法律层面明确数据安全保护义务，为开展数据处理活动的组织和个人提供了行为指引，填补了我国数据安全保护立法的空白。2021 年 11 月 1 日《个人信息保护法》施行，立足于数据产业发展实践和个人信息保护的迫切需求，更全面地保障了个人权利，及时回应了国家、社会、个人对个人信息保护的关切。**行业监管层面**，2021 年 9 月 30 日工业和信息化部发布《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》并公开征求意见，旨在加快推动工业和信息化领域数据安全管理工作制度化、规范化，提升工业、电信行业数据安全保护能力，防范数据安全风险。2022 年 1 月 4 日，国家互联网信息办公室颁布《网络安全审查办法》修订版，将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查。**地方政府层面**，积极落实国家政策和上位法精神，陆续出台相关地方法律法规。2021 年 6 月 29 日《深圳经济特区数据条例》

[1] 数据来源：中国信息通信研究院《全球数字经济新图景（2020 年）——大变局下的可持续发展新动能》

出台，率先就数据保护和利用开展地方立法，规范数据要素市场化行为，推动数据的有序流动和数据产业的健康发展。2021 年 9 月 30 日《上海数据条例（草案）》公开征求意见，征求意见稿在《数据安全法》等上位法的框架下，结合上海实际，建立了全面的数据安全治理体系。

（二）数据安全事件频发安全威胁日益严峻

根据风险基础安全（Risk Based Security）[2]的数据显示，2020 年全球数据泄漏达到 360 亿条，创历史新高。对比传统的网络安全威胁，数据安全威胁更加多样化，不再局限于利用安全漏洞、恶意流量、病毒木马等攻击手段，数据安全问题集中爆发在特权账号弱口令、数据权限滥用、API 接口攻击等方面。

弱口令成数据泄漏爆发点。由于弱口令账号的低攻击成本和高命中效果，通过盗取弱口令账号以横向渗透获得特权账号，进而破坏或泄露重要数据资源的攻击行为，给数据安全管理带来很大挑战。根据 Verizon 发布的《2021 年数据泄露调查报告》[3]分析，61%的数据泄露与凭证数据泄漏有关。

API 成热门攻击入口。由于应用架构的快速演变，API 成为业务应用与数据服务之间的主要通信方式，这导致利用 API 接口成为新型攻击手段。2021 年 4 月，Facebook 5 亿用户数据在暗网公开售卖，起因为 2019 年某在线业务的 API 遭到误用，导致数据泄露，影响约 5.3 亿用户。

[2] 安全内参：历史新高！2020 年数据泄露数量突破 360 亿条 https://www.secrss.com/articles/26712
[3] Verizon 2021 年 5 月发布 https://www.verizon.com/

权限滥用仍是数据安全事件的重要触发点。不规范的数据权限管理以及缺失的技术防护手段，极易发生由于权限滥用而引起的数据资源被破坏、篡改、删除等安全事件。2020 年 2 月，港股某上市公司员工通过 VPN 登入服务器，对线上生产环境进行恶意删库，造成旗下数百万用户业务中断，直接赔付人民币 1.5 亿元[4]。

隐私泄露成为数据安全的重要威胁。由于个人隐私泄露导致的数据诈骗、大数据杀熟以及个人生物特征信息滥用等问题，已经严重危害了个人信息主体的合法权益。据市场调研公司 Canalys 统计，2020 年全球个人信息泄露事件超出过去 15 年总和，成为影响个人权益、组织发展甚至国家安全的重要因素[5]。

（三）技术架构演进伴生数据使用场景改变

2021 年 3 月 14 日，《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》全文发布，就数字经济、数字社会、数字政府、数字生态建设做了重要部署。传统信息技术开始向以数据和业务为核心的新一代信息技术转变。**组织内**普遍通过采用大数据、云计算等新技术，帮助组织提升决策水平，构建新型业务模式，实现产业升级；**组织间**则大幅增加信息化交互，合作关系也更加密切，通过业务协同、数据共享实现流程优化、合作共赢已经成为共识。由此可见，**数据应用场景和参与主体的日益多样化，使得数据伴随业务及应用在不同载体间流动和留存，贯穿于信息化和业务系统的各层面、各环节**。因此，在复杂应用环境下，保证重要数据、核心数

[4] https://www.163.com/tech/article/F6MSOQN4000999LD.html
[5] 安全内参：2020 年全球个人信息泄漏超过去 15 年总和 www.secrss.com/articles/30202

据以及用户个人隐私数据等敏感数据不发生外泄，是数据安全的首要目标。

二、数字化时代下的数据安全痛点

《数据安全法》作为数据领域的纲领性和基础性法律，以准确定义数据、数据处理、数据安全为出发点，明确了数据安全的目的，**即确保数据处于有效保护和合法利用的状态，使其具备保障持续安全状态的能力**。

（一）个人信息合规合法使用的监管应对难度增加

过度收集的个人信息，一旦结合大数据分析能力，能够使匿名化处理的数据被还原，导致数据脱敏技术“失灵”，直接威胁用户的隐私安全。近年来，全球范围内的数据安全执法案例基本围绕个人信息的过度收集、滥用等主题。**国外**，Facebook 因违规向数据分析公司提供 5000 万个人信息，被美国联邦贸易委员会（FTC）处以 50 亿美元的罚金，是历史上最大的隐私违规罚款[6]。**国内**，《APP 违法违规收集使用个人信息监测分析报告》[7]显示，2021 年 5 月以来，被通报的 12 类 351 款 APP 中，有 257 款由于存在“违反必要原则，收集与其提供的服务无关的个人信息”问题，被公开通报并责令限期整改，对未在规定时限内整改的依法采取了相关处罚措施。

面对不断加大的个人信息保护监管力度，如何建立符合组织现状及发展需求的个人信息保护管理体系，确保个人信息在安全合法使用的同时充分发挥对组织发展的积极推动作用，已成为各行业发展面临

[6] 安全内参：Facebook 认罚 50 亿创记录 https://www.secrss.com/articles/18981
[7] http://www.cac.gov.cn/2021-12/09/c_1640647038708751.htm

的重大议题。

（二）账号、权限、API 成数据保护脆弱环节

1.特权账号隐藏严重安全风险

账号凭证泄漏是导致数据泄露的主要因素。账号作为主体访问客体的重要凭证，在通过安全验证后可以直接访问数据库、数据仓库等载体的数据资源，因此保障账号安全是组织数据安全工作的重要目标之一。但由于系统和应用程序的不断增加，账号尤其是高数据访问权限账号的共享及弱口令设置等问题日益突出。IBM Security 发布的《2021 年数据泄露成本报告》[8]指出，数据泄漏事件中最常见的初始化攻击路径就是直接窃取凭证，如图 1 所示。

来源：IBM Security《Cost of a Data Breach Report 2021》

图 1 最常见的初始化攻击路径

特权账号是最直接、最快速的攻击入口。基于近年来的数据安全事件以及攻防演练的实践分析，特权账号作为访问资源、配置策略的最直接入口，其安全问题一直是困扰各组织的痛点。从攻击者视角进行切入，与其穿透层层的组织内网防护设施窃取数据，不如窃取账号，通过内网横向移动，最终攻破特权账号，再利用特权账号权限执行删

[8] https://www.ibm.com/cn-zh/security/data-breach

库、删表等高危操作，达到破坏或窃取敏感数据的目的。

2.IT 环境演变导致权限问题成数据安全严峻威胁

边界弱化、场景演变，导致数据资源暴露面增加。随着新一代信息技术的快速演进，业务系统面临着包括手机、台式机、平板电脑等多种类型的终端设备接入，网络安全边界范围由数据中心向云端、终端等各个环节不断延伸。疫情时代，员工使用自有设备进行远程办公逐渐成为常态，访问需求的复杂性扩大了内部资源的暴露面。此外，各种设备（如：BYOD、合作伙伴设备）及各类人员的接入也带来了更多不可控因素，增加了数据风险暴露面。

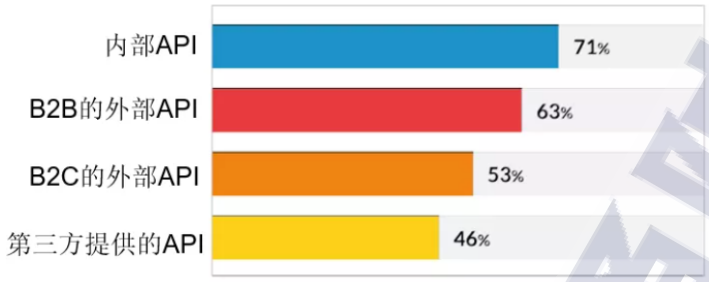
数据资源面临更频繁访问，数据权限滥用问题不容忽视。组织间的合作共享导致数据资源的访问量和访问人员大幅增加，多样化的访问接入，容易引发数据权限管理不清、使用情况不明等安全问题，最终造成业务和数据资源违规访问，酿成数据安全事件。历年的“净网行动”曾发现多起由于权限盗用导致的敏感数据泄露事件。

3.API 防护缺失成数据安全最大风险敞口

API 作为数据连接利器，其安全风险重视程度有待提高。如图 2 所示，Imvision 发布的《Enterprise API Security Survey》[9]报告展示了不同场景下的 API 使用情况，其中内部 API 的使用程度最高达到 71%。作为最重要的数据传输方式之一，API 也成为攻击者窃取数据的重点攻击对象。然而，组织对外暴露了哪些 API、对谁开放、API 通信中携带了哪些敏感数据、对方如何使用这些数据等问题却并未得到应有

[9] https://www.imvision.ai/2021-api-security-survey/

的重视。



来源：Imvision：《Enterprise API Security Survey》报告

图 2 不同场景下 API 使用情况

API 格式的多样性、复杂性增大安全挑战。如图 3 所示，随着业务场景的动态发展，API 的协议和格式也发生快速变化，API 在广泛应用的同时，也引入了大量数据安全挑战。2019 年 12 月，OWASP 组织发布了 API Security Top 10 的安全风险[10]，其中失效的对象级别授权、失效的用户身份验证、失效的功能级授权等成为 API 面临的重要安全问题。因此，亟需进化 API 安全思维和安全架构，以适应不断变化的新型安全风险。

来源：奇安信科技集团股份有限公司

图 3 API 业务发展历程

[10] OWASP:2019 年 10 大 API 风险 https://owasp.org/www-project-api-security/

（三）数据安全状态持续保障成落地难点

数据资产梳理不全面导致安全保障不彻底。随着数据处理技术的不断成熟，数据量呈 PB 级迅速增长，业务的持续扩大与数据应用的不断裂变，海量、多元和非结构化成为数据发展新常态。各组织通常在数据治理阶段并未全面考虑相关的安全特性，数据本身又因为特征多、分布散，关联关系复杂等特性，造成大量低质量、关系模糊的数据存储在分散的数据载体中。这给组织的数据资产梳理造成了困难，而建立在数据资产梳理基础之上的持续安全保障更是难以实施。

数据快速流转增加数据安全持续保障难度。数据流转过程中的安全属性面临多种变化，**一是安全域的变化**，数据在多个业务和应用场景下的流动交互，必然会出现跨越不同安全域的使用现象。**二是数据载体的变化**，流转过程加速了数据的大量汇聚、加工、使用，必然导致数据在不同载体中的使用和留存。**三是数据主体的变化**，数据交互过程的主体角色变化，导致数据权责不明。以上安全属性的变化导致组织难以清晰的梳理数据与访问主体、传输链路、承载环境、安全策略等的关系，进而在数据安全建设时只能以“离散”的补丁方式解决风险问题，而导致全局化、体系化联防联控沦为纸上谈兵。如何开展数据流转过程中的安全防护工作，已成为数据价值释放的重大挑战。

三、解决数据安全痛点问题行动思路

为解决以上数据安全痛点问题，本报告从战略规划、机构管理、精准管控、安全运营等方面提出数据安全建设行动思路。

（一）明确数据安全总体战略

数据作为重要资产，组织必须深刻认识到数据安全工作的重要性和复杂性。因此，在启动数据安全工作前，必须制定相应的战略规划，明确总体目标和具体任务。需要综合考量组织在合规管控、安全管理、业务发展等方面的总体目标，制定符合组织经营发展与风险管控需求的数据安全总体战略。

（二）建立数据安全管理机构

管理机构建设是数据安全工作开展的首要环节，通过自上而下建立从各个领导层面至基层执行层面的管理组织架构，明确各方数据安全职责，有助于强化业务、应用、数据所有者以及全体员工的安全责任与意识，推动数据安全战略的有效执行与充分协同。**一是决策层**，负责组织数据安全整体目标及发展规划等的制定。**二是管理层**，负责梳理和明确数据安全工作的重点方向与环节，制定与组织整体目标相适应的数据安全管理策略，形成规范化管理体系等。**三是执行层**，负责按照既定的数据安全管理策略、管理要求，在不同的业务流程中进行落地及运营维护。**四是监督层**，负责对管理层、执行层的工作进行定期审核监督，并将发现的问题及时反馈给决策层，对薄弱环节予以加强[11]。

（三）落实安全策略精准管控

数据安全与业务场景紧密相关，为防范数据安全风险，必须深入业务逻辑，制定可落地的精准管控策略。**一是治理先行，构建安全底**

[11] 中国信息通信研究院云计算与大数据研究所：《数据安全治理实践指南（1.0）》

座。通过发现、识别数据资产，进行资产盘点，开展数据分类分级，基于数据分类分级结果、重要数据的流转及使用情况，构建数据脉络，为后续场景化的数据安全能力落地提供坚实支撑。**二是“数据生命周期”与“数据流转”相结合，设计安全策略**。基于数据全生命周期视角，梳理数据安全策略架构；基于数据流转视角，识别具体业务场景，将数据、动作和特定人员或组织进行关联，有针对性的设计安全防护措施。**三是有序建设，分步落实数据安全能力**。围绕威胁路径，梳理数据安全关键能力，明确数据安全能力建设的优先级、依赖关系、所需资源，确保可执行性，实现数据安全痛点问题的精准管控。

（四）持续保障数据安全运营

持续运营保障的目的**一是看清数据流转关系**。基于数据安全态势感知，根据文件、应用及数据库表的操作日志和访问日志，以及 SQL 语句的解析、API 的调用等构建主体、设备、应用和数据库表的行为关系图谱，明确数据资产分布、数据流动情况，为动态掌控全局数据安全提供有力保障。**二是识别发现数据安全风险**。数据交互的复杂性和多样性对异常行为和潜在风险发现提出了更大挑战，需要根据数据流转关系对数据使用场景进行精准刻画，结合泄露风险监测、用户行为分析等相关技术手段，将风险识别全面深入到数据处理活动内容中，实现对数据安全威胁的及时预警和处置。**三是实现常态化安全运营**。通过定期开展数据安全专项审计工作，包括审查业务数据流转的各个环节是否存在安全隐患、个人信息及重要数据的保护措施是否满足合规要求、相关安全策略是否定期优化等内容，以实现持续的数据安全

保障运营。

四、解决数据安全痛点问题关键举措

面对上述的数据安全痛点问题，基于数据安全防护的实践与探索，本章节从个人信息保护、特权账号、动态授权、API 防护、面向全局的数据安全运营五个方面阐述解决痛点问题的关键举措。

（一）管理与技术结合助力个人信息保护合规落地

个人信息保护合规建设工作不仅仅是编制隐私政策文件、修改产品逻辑、增加提醒和通知等内容，还要将个人信息保护真正融入到日常的业务活动和产品管理中，从根本上建立个人信息保护合规体系，保障数据价值。

1.构建个人信息管理体系提供合规保障

基于现有数据安全管理机构建设情况，明确分管个人信息保护的组织机构。其工作职责包括但不限于：制定个人信息保护战略、隐私政策、个人信息安全事件处置机制等；统筹不同部门的个人信息保护工作重心、工作方法和计划，与业务发展进行平衡；协调安全、IT、法务等多个部门，体系化完善个人信息保护合规方案，避免个人信息保护合规风险。

2.识别监管要求聚焦个人信息保护合规重点

充分理解监管要求是个人信息保护合规工作的前提。现有法律法规和标准规范已提出了全面的个人信息保护要求，在个人信息处理过程中应充分考虑合规制度的建设及落实。同时，组织需要对自身的个

人信息保护现状开展合规评审活动，重点关注 APP 超范围收集个人信息、误导收集个人信息、SDK 越权收集问题等热点难点问题，提升整体个人信息保护工作的合规落地有效性。

3.技术检测嵌入个人信息保护全流程

组织收集个人信息的主要工具包括 APP、小程序、网站等，需要在工具研发、发布、运营各阶段嵌入合规要求。**研发阶段**提前规避合规问题能极大降低合规风险带来的成本，可通过合规培训、SDK 准入审核、合规评估等策略进行研发过程管理。同时采用技术手段进行合规评估，并根据风险容忍能力执行上架发布动作。**发布阶段**将合规检测技术嵌入到版本迭代过程中，通过对 APP 违规行为进行检测，实现对个人信息保护水平的合规性、有效性、完整性测试及验证，排查合规风险。**运营阶段**持续开展技术检测，通过访问控制策略、风险评估、应急处置等方式保障个人信息处理活动的合规性。

（二）特权账号安全治理持续强化安全内控

特权账号的安全治理，需要建立覆盖特权账号生命周期的管控机制，并通过技术手段持续监控特权账号的异常登录、权限变更等潜在风险，确保特权账号安全的可知、可管、可控、可查。

1.建立特权账号安全管理机制

在账号产生阶段建立特权账号纳管机制。新系统、新设备在投产和扩容时，应及时收集其中的特权账号，并与系统上线的业务流程进行联动，确认此系统的特权账号已纳入特权账号安全管理系统进行统一控制。

在账号存储阶段明确特权凭证的安全策略管理。建立一套行之有效的密码安全策略，包括建立密码申请机制、密码定期修改机制、密码安全策略等。其中密码申请机制，应仅允许具备管理权限的用户通过审批的方式获取所需的账号密码；密码定期修改机制，应建立定期的密码修改任务单，完成密码修改重置工作；密码安全策略，应明确密码复杂度要求、唯一性要求、不重复要求等。

在账号使用阶段明确特权账号使用的安全管控措施。在访问管理方面，统一管理所有相关的安全会话操作，并通过密码安全设施分发密码，在对特权账号不可见的情况下直接访问目标主机设备，以防止特权账号凭证暴露。在权限控制方面，对重要级别高的数据采取高级别的操作权限控制，针对核心业务、核心数据等采取动态工单授权申请审批机制和会话实时控制等方法，确保重点业务系统任何时刻不能被单个账号直接操作。

在账号销毁阶段建立账号删除/回收/冻结机制。需重点关注第三方临时访问场景，通过设置一次一密策略，在账号使用完毕后，立即更改密码，降低密码被窃取、二次共享或人为扩散的风险。针对系统升级、维护、下线等变更过程或人员交接、转岗、离职等流程，建立账号回收冻结机制，及时对特权账号进行回收/冻结/删除，防止因管理的疏忽造成特权账号变成幽灵账号。

2.运用特权账号技术管控手段

特权账号自动发现能力。通过自动化的账号扫描和检测手段，及时发现应用系统、数据库等包含的特权账号信息，并通过账号管理系

统进行账号整理，全面了解组织特权账号使用情况，扫除因为僵尸账号、幽灵账号造成的安全隐患。

特权凭证安全保管能力。采用安全存储技术建立存放特权账号密码、访问权限配置、密码访问日志等关键数据的安全环境。例如密码保险箱的安全存储技术，以密码保险箱为单位存放特权账号相关信息，并定义不同的访问权限。每个密码保险箱都有自己的授权用户，只有这些授权用户可以访问存储在密码保险箱中的账号密码信息，并配置相应策略动作，如查看密码，删除密码等。

3.开展特权账号持续监测运营

加强对特权异常行为监测预警能力。需要确保所有的特权操作都在监测管控之下，**一是**能够针对操作指令进行解析，识别操作指令；**二是**通过 OCR 文字识别等方式识别图形协议，审计特权用户操作内容；**三是**针对特权账号的文件传输，记录传输文件名和目标路径。通过统计分析、关联分析等技术手段深度分析特权账号的行为信息，构建特权用户整体画像。其中包括特权用户的 IP、账号、权限等基本属性，以及行为轮廓、特权行为、通联关系等行为属性，持续监控特权账号行为，及时发现账号威胁，以便迅速处置响应。

加强特殊场景特权账号安全治理能力。在应用系统与其他应用程序之间的交互认证场景中，存在用户名与密码互相调用的情况，因此通常会出现应用系统将账号及密码明文写在代码或配置文件中的现象，此类明文密码暴露会给组织带来极大安全风险。在账号安全管理过程中，必须将这类账号纳入管理并进行重点整改。

（三）零信任数据动态授权赋能精细化管控

数据安全访问的痛点是信任问题，零信任数据动态授权体系是数字化时代解决信任问题的手段。

1.数据动态授权策略准备阶段

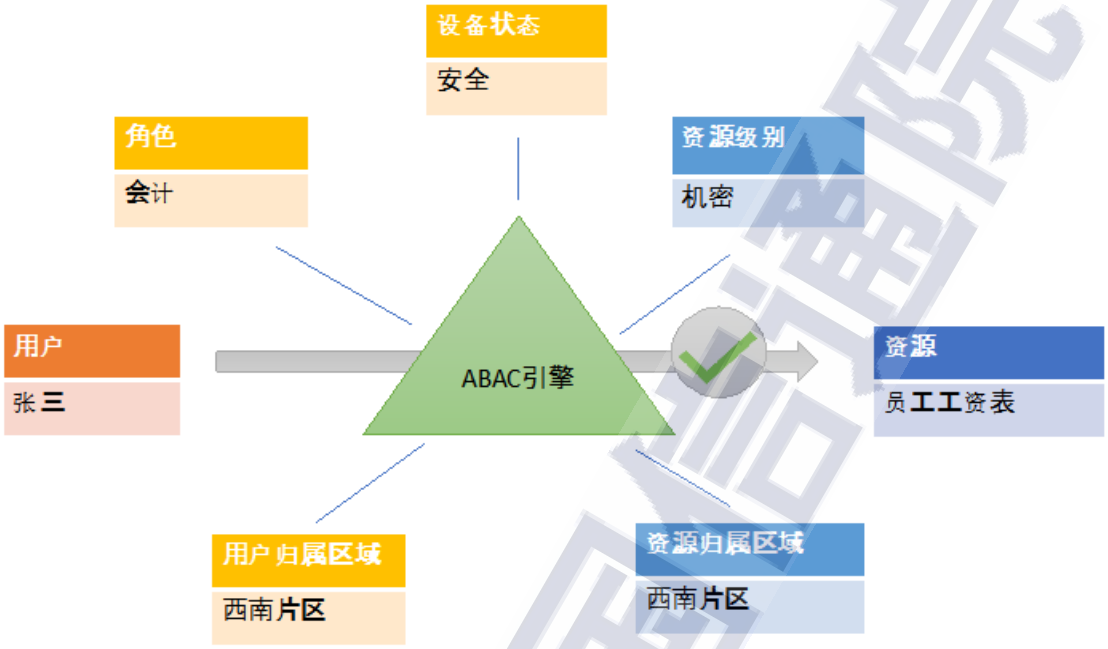
基于统一的元数据管理和数据分级分类结果，构建数据视图。数据视图便于组织对数据建立全面认知，有助于了解数据的位置及使用情况等基本信息。通过持续跟踪和分析元数据状态，结合数据分类分级结果，驱动组织形成动态数据访问策略，为数据动态授权体系的建设提供基础能力。

明晰数据访问上下文，构建身份视图。身份视图主要解决主体身份信任问题，主体身份信任根本上是解决“是什么部门的什么人、在什么地方、因为什么任务、访问了什么数据里的什么字段”的问题。通过明晰数据访问上下文，将用户身份、数据类型、访问意图等信息关联起来；通过上下文评估，对组织范围内的人员、设备、终端应用等主体进行细致刻画，构建身份、设备、应用等实体的全局身份视图。基于身份视图明确制定策略所依赖的各种信息，从而更精准的对主体信任进行评估，解决主体身份信任问题。

2.数据动态授权策略建设阶段

基于数据视图、身份视图构建动态访问策略。在零信任架构下，采用基于属性的访问控制机制（Attribute Based Access Control，简称 ABAC），从实体安全、身份可信、业务合规三个目标出发，依赖数据视图、身份视图等内容，如图 4 所示，通过角色、访问主体所在地

区、访问主体设备状态等属性进行授权决策，实现对数据权限的动态精细化管控。



来源：奇安信科技集团股份有限公司

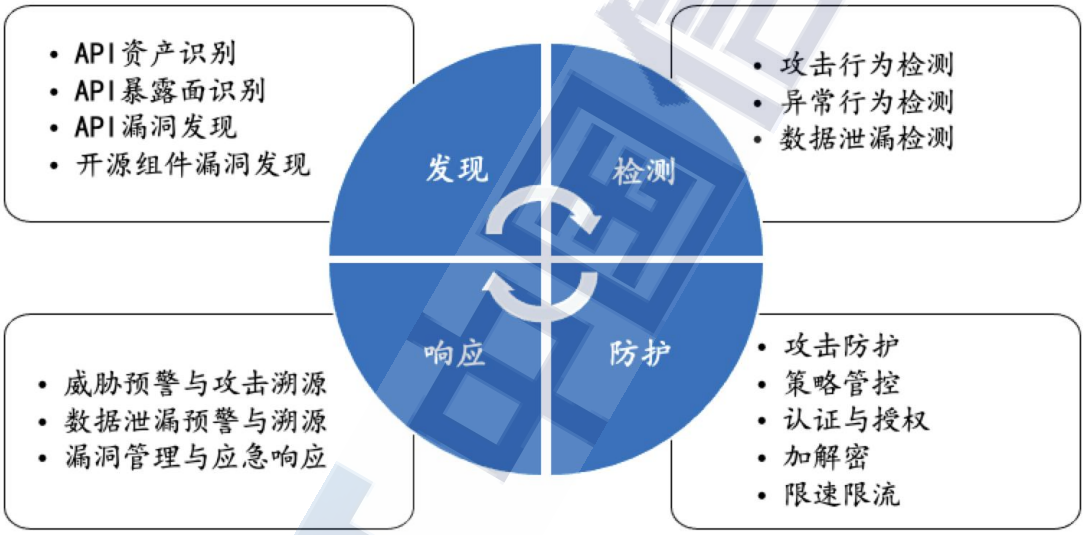
图 4 基于属性的数据动态授权机制

3.数据动态授权策略持续信任评估阶段

通过访问活动合规分析、访问主体信任评估、威胁行为持续发现三方面落实评估工作。**一是**开展访问合规性分析，对可执行的业务规则和现有访问控制机制进行评估，通过监控访问行为维护数据的完整性及业务安全，**二是**通过对身份、行为等多源数据的分析，实现对每一次访问行为的信任评估。用户行为若存在安全风险，信任评估结果将无法满足访问控制要求，则不被授予访问资源的权限或被终止权限。**三是**通过行为分析、关联分析等方式发现隐藏在正常活动模式下的恶意活动。通过对主体、资源、行为属性的持续挖掘与运营，落实持续信任评估。

（四）完善 API 安全防护体系的闭环建设

API 安全问题的最佳解决方案是在 API 的设计过程嵌入安全思想，实现安全内生。API 安全建设的落地需要结合现状需求以及实战化的安全经验，发现并收敛 API 使用过程中的风险。通过将 API 的安全能力和组件，嵌入到业务体系，构建自适应的内生安全机制。可以按照“发现”、“检测”、“防护”、“响应”的安全模型进行 API 安全体系建设，如图 5 所示。



来源：奇安信科技集团股份有限公司

图 5 API 安全防护体系

1.以 API 资产为视角的漏洞与风险发现能力

组织的 API 安全建设，需要将安全能力与业务过程高度融合。在南北向、东西向路径进行持续监测、持续分析、动态防护。

首先是 API **的资产发现与管理能力**。组织应对自身 API 部署情况进行全面排查，梳理统计 API 类型、活跃接口数量、失活接口数量等资产现状。通过对 API 进行深度的资产梳理和发现，帮助组织了

解不同应用程序使用的 API 以及 API 对应的业务属性。

其次是 API **漏洞发现能力**。随着攻击面和攻击手段的变化，应建立持续挖掘 API 相关漏洞的能力和机制，做好补丁管理，并在引入第三方组件时充分考虑组件自身安全，避免第三方组件引入的漏洞。

最后是 API **滥用发现能力**。加强 API 在运行时的外部风险感知和阻断能力建设尤为重要，可以及时准确的感知 API 的滥用情况，并阻断攻击者的进一步行动。

2.面向 API 的攻击和数据泄漏检测能力

加强 API 安全检测能力。**一是**持续检测针对 API 漏洞的攻击行为，并通过大数据分析及人工智能技术对攻击告警进行攻击事件还原和攻击溯源。**二是**检测逻辑异常攻击，通过构建 API 调用链可视化能力，将请求经过的每一个节点都记录下来，形成一个完整的调用链监控系统，当发生请求调用异常或回溯安全事件时，可清晰定位到具体环节。**三是**检测异常行为，基于可扩展的行为检测模型，实现对异常访问行为等的实时监测分析，并对比正常行为基线，快速发现异常。

强化数据异常流转及泄露检测能力。**一是**开展敏感数据识别，依托数据分类分级的结果，梳理 API 数据类型，并对 API 访问的数据进行持续监测评估。通过自动梳理 API 接口中的敏感数据流，生成 API 接口与敏感数据的映射，确保对敏感数据的持续监控。**二是**开展数据流转检测，应构建全面的数据流转监控体系，通过识别各类 API，对其传输内容进行精细化检测来明确“谁通过什么方式的 API，传输了什么类型的敏感数据”，实现敏感信息流转可视化。**三是**构建威胁

情报检测能力，通过检测分析手段，快速定位攻击行为，并对攻击行为进行溯源，实现在攻击行为产生恶劣影响之前及时感知已失陷主机，从而提前预警并响应，以降低恶意攻击行为对内网造成的影响和损失。

3.构建以 API 为主体的安全防护能力

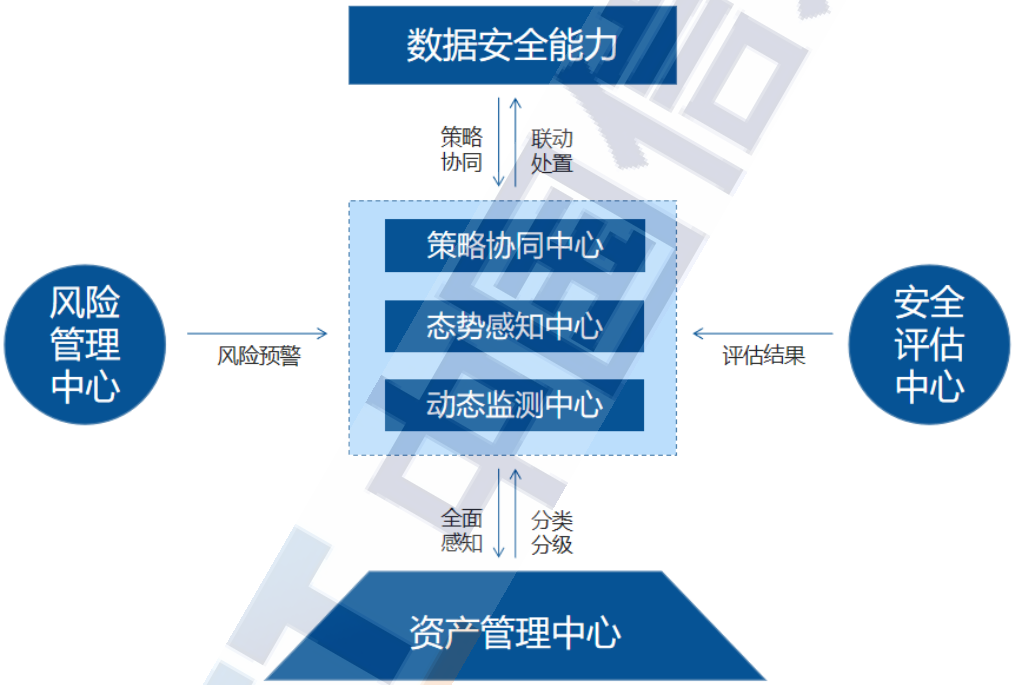
API 接口的安全防护能力建设，包括但不限于：**认证授权体系**，基于零信任理念，实现统一的认证授权机制，对所有的 API 内部、外部访问执行可信认证策略；**访问控制**，认证成功后，还需针对不同的应用执行不同的访问控制策略，并提供完整的访问控制日志；**数据加解密能力**，应对 API 中敏感信息的交互进行加密或脱敏，减少敏感信息的泄露风险；API **限流限速**，需考虑系统的处理能力，对 API 请求进行限流防护，缓解基于 API 的 DDoS 攻击，防止资源消耗在无意义或恶意的 API 请求上。

4.建立持续运营与快速响应能力

首先应建立威胁预警能力，基于业务流量，细化分析攻击行为，并结合攻击者历史情报信息对攻击者的资源、手法、意图等进行关联跟踪分析，进而构建攻击者情报库，对攻击者进行持续跟踪，实现提前预防。**其次是构建漏洞管理与响应机制**，通过构建持续挖掘 API 相关漏洞的能力来实现风险预防，并开展补丁管理，应对不断变化的攻击面及隐秘多变的攻击手段。**最后是建立威胁分析与处置能力**，对所有威胁日志进行深度分析，实现对所有 API 的统一监控与威胁事件感知，达到快速处置的目的。最终形成一套“预防为主、快速响应、精准处置”的应急响应管理体系。

（五）围绕数据安全态势感知统筹数据安全运营

数据安全运营是以数据资产发现为前提，分类分级为手段，审计和监测为依托，持续风险管理为核心，实现及时发现异常、快速响应处置的安全闭环流程。通过管理流程、技术平台、运营专家的深度融合，建立一套完整全面的数据安全运营态势感知中心，指导数据安全体系建设，如图 6 所示。



来源：奇安信科技集团股份有限公司

图 6 数据安全运营总体架构

1.盘清家底：以数据资源为核心的资产管理

通过对目标环境中的数据资产，尤其是敏感数据资产，进行全面清查、摸排，了解数据资产类型、数据资产分布、数据资产权限、数据资产使用等信息，并深入分析业务系统之间的关联性，完善数据资产目录。

2.联防联控：以分类分级为核心的策略协同

数据安全的策略协同需要围绕分类分级结果展开，以实现对不同类别、不同级别数据资产的差异化防护能力设计和安全策略配置。同时，联动数据链路上的数据安全措施，打通策略配置通道和日志及告警上报通道，并结合具体的数据安全防护组件，统一下发安全策略，以实时监测数据的防护能力状态，及时感知薄弱环节并进行策略的自动调整，保障数据业务和安全管控的全面协同。

3.流动监测：以业务流程为核心的动态监测

通过数据流动监测，动态掌控数据安全状态。面对复杂的数据流动态势，开展数据内部使用、外发共享等业务流程的梳理，通过摸排数据使用情况，识别数据的流动路径、访问主体等关键因素，明晰数据在组织内部的流动情况，构建一幅连接“数据、业务、主体”的数据流动业务视图。

4.风险分析：以行为分析为核心的风险管理

及时发现数据安全风险是开展数据安全运营工作的重要一环。数据安全风险分析基于在数据流转监测环节中对数据使用场景的精准刻画，以风险分析引擎为技术基础，辅以丰富的分析策略，灵活检测不同场景下的数据安全风险，并采取有效的处置流程进行跟踪响应，真正实现可控的风险管理。

5.安全评估：以安全合规为核心的持续评估

开展数据安全评估工作是安全合规的需要，也是组织自身数据保

护的需求。数据安全评估工作需充分考虑监管要求、数据安全现状、风险分析结果等因素，其评估内容包括但不限于数据管理组织架构、数据管理制度等内容。为保障评估工作的有效性和准确性，应以技术工具为支撑落实数据安全评估执行，发现数据安全薄弱环节，提出整改措施。

6.持续运营：以态势感知为核心的安全运营

全面的数据安全态势感知是数据安全运营持续开展的核心。数据安全态势感知，以数据资产管理和分类分级为底座；面向数据处理活动实现数据流动的全面监测、数据安全风险的快速发现；依托策略联动机制拉通实体防护能力，实现风险的快速处置；定期开展安全评估，确保安全能力行之有效。最终实现面向全流程的数据安全管理，构建持续的数据安全运营保障能力。

五、数据安全建设发展建议

数据安全体系建设需要全局考虑已经逐步达成共识，而如何深化数据安全体系建设亟需理念创新。

（一）聚焦关键环节完善数据安全能力建设

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安全痛点问题，明确重点环节，按照有序推进、分步建设的实施路线，以组件化方式落地并完善数据安全能力建设。

（二）结合业务流程深化数据安全工作开展

频繁的数据交互和复杂的业务流程为组织带来严峻的数据安全挑战，数据安全的持续保障工作仍存在较大提升空间。需要进一步融合安全与业务，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，进而指导数据安全能力建设，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。

（三）高度重视技术创新破局作用

随着零信任、隐私计算等新理念新技术的出现，为解决数据安全难点问题带来破局思路。通过对数据安全技术发展趋势的持续关注，提前布局技术研发与应用，抢先推动数据安全能力建设创新，实现数据安全体系建设的持续优化。

参考文献

[1] 全球数字经济新图景（2020 年）——大变局下的可持续发展新动能. 中国信息通信研究院.

[2] Data Breach Investigations Report 2021. Verizon.

[3] APP 违法违规收集使用个人信息监测分析报告. 国家计算机网络应急技术处理协调中心、中国网络空间安全协会.

[4] Cost of a Data Breach Report 2021. IBM.

[5] Enterprise API Security Survey2021. Imvision.

[6] 隐私保护计算与合规应用研究报告（2021 年）. 中国信息通信研究院安全研究所.

[7] 数据安全治理实践指南（1.0）. 中国信息通信研究院云计算与大数据研究所.

[8] 大数据平台安全研究报告. 中国信息通信研究院安全研究所.

[9] 网络安全先进技术与应用发展系列报告-零信任技术. 中国信息通信研究院安全研究所、奇安信科技集团股份有限公司.

中国信息通信研究院 云计算与大数据研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：13581661287

传真：010-62304980

网址：www.caict.ac.cn