多跨协同的多层次数据安全防护体系建设

文/骆　鉴　袁　昱*

摘要：近年来，数据安全相关法律、标准密集出台，社会面进入了数据安全强监管时代。金融业作为数据密集型产业，敏感数据积累速度和使用场景不断扩充，数据安全风险日趋严峻，而支付等银行核心业务高度依赖数据安全防护作为基础保障，建设数据安全防护体系刻不容缓。本文针对金融业数据安全防护体系建设中的若干痛点问题，提出了一种以数字化转型中的多跨协同理念为核心的指导思想，管理、技术、运营三位一体的多层次数据安全防护体系建设方案，并针对员工、外联、对客三大场景输出了落地实践，使得整个体系更加立体化、智能化，同时也更符合金融业特性。

关键词：多跨协同　数据安全　多层次防护

一、数据安全防护体系建设背景

（一）数据安全强监管时代来临

随着《数据安全法》《个人信息保护法》的正式实施以及配套法规、标准的相继落地，我国已初步形成了一整套指导各行业落实数据安全工作的顶层设计，数据安全法治时代随之到来。

金融业作为数据密集型产业，支付等各项银行核心业务高度依赖数据安全防护作为基础保障，因此行业监管部门对数据安全非常重视。人民银行起草了《中

* 作者单位：浙商银行股份有限公司。本文是根据作者 2023 年 9 月在第 12 届中国支付清算论坛数据安全分论坛上的发言整理。

国人民银行业务领域数据安全管理办法（征求意见稿）》，面向社会公开征求意见。国家金融监督管理总局也对《银行保险机构数据安全监管办法》开始征求意见，行业规范不断强化，数据安全强监管时代呼之欲出。

（二）金融业数据安全防护体系建设痛点

在这样的时代背景下，金融机构一直致力于加强数据安全防护体系建设，但仍面临诸多痛点与难点：一是由于金融业务的开放性，其数据供应链较长，数据产生、使用场景繁杂，数据流动快、泄露渠道众多，很难全面防护；二是金融机构往往从业人员较多，内部员工泄露数据的风险较大，难以提前防范；三是数据作为生产要素的价值释放要求数据更充分地流动和利用起来，而数据安全防护天然与这一诉求相矛盾，保护与利用的平衡点较难把握；四是当前产业界能供给的数据安全管控技术工具落后于监管要求，精准防护手段欠缺，防护有效性难以提升。

二、数据安全防护体系建设

为解决上述问题，浙商银行以数字化转型中的多跨协同理念为核心指导思想，结合金融行业相关行标与数据安全治理逻辑，构筑了管理、技术、运营三位一体的数据安全防护体系（见图1）。

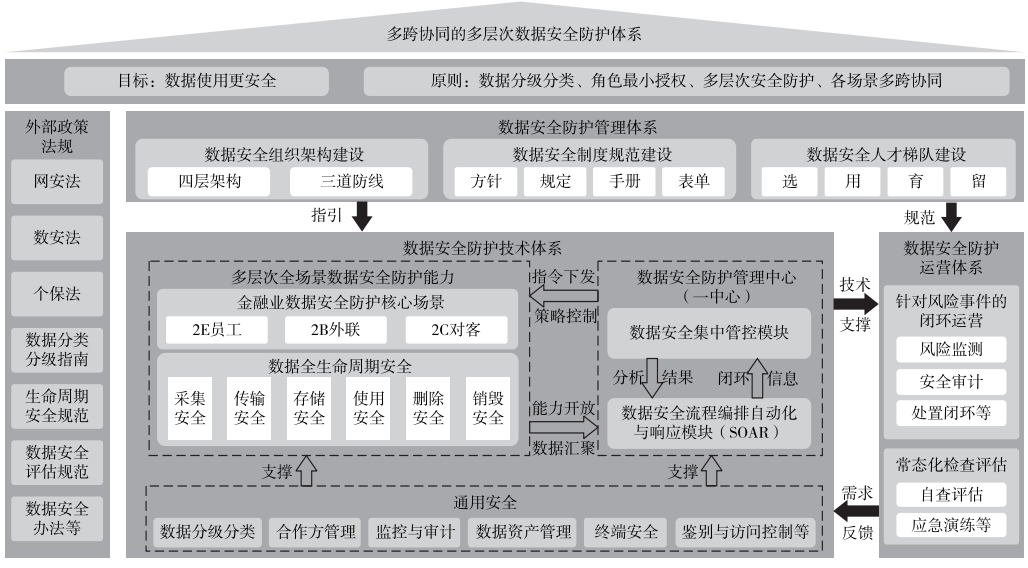

图1　多跨协同的多层次数据安全防护体系总体架构

管理、技术、运营三大体系涵盖了组织、流程、人员、技术、运营等数据安全相关事务，并在设计之初就考虑多部门、多业务、多产品融合联动的情况，在宏观层面贯彻了多跨协同的思路。管理体系是统领，技术体系是基础，运营体系则将相关安全产品与服务能力综合体现出来，三者相辅相成，构建了一个完整的数据安全防护体系。

（一）数据安全防护管理体系

管理体系是数据安全防护工作的统领与基础保障，应在现有的网络安全管理制度和网络安全组织架构下深化推进数据安全管理工作落地，形成多部门协同、齐抓共管、责任到岗到人的管理形式。通过管理体系建设，在数据安全领域落实金融科技风险三道防线并形成领导、管理、执行、监督的四层架构，强化数据使用者、管理者等各方的相关责任；同时，不断补充完善方针、规定、手册、表单构成的制度规范集，明晰各层级人员具体工作。

（二）数据安全防护技术体系

技术体系是以技术和相关产品为手段，结合金融机构自身的数据安全防护核心场景，提升预防、识别、处置数据泄露风险的能力和效率，实现保障数据安全的目标（见图 2）。

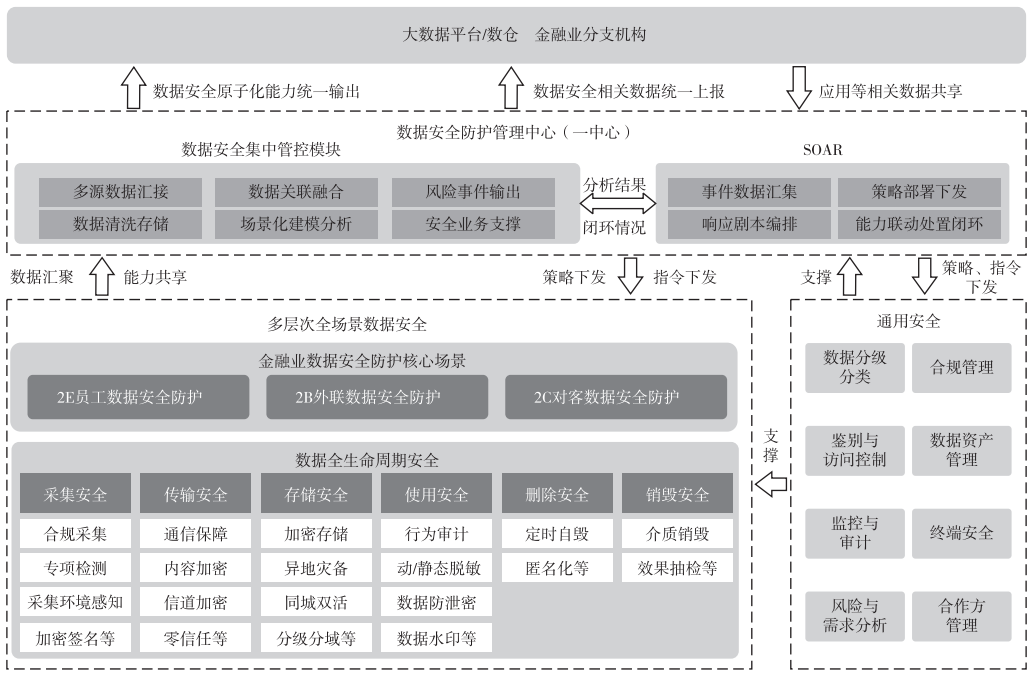

图 2　多跨协同的多层次数据安全防护技术体系架构

数据安全防护技术体系包括以通用安全为基础，多层次全场景数据安全防护能力为策略，数据安全防护管理中心为安全大脑的整套防护技术。

通用安全包含了所有数据安全防护场景下共性的基础防护能力，如数据分级分类、鉴别与访问控制、数据资产管理、终端安全、合作方管理、合规管理等。

多层次全场景数据安全是依据金融业数据安全防护的2E员工、2B外联、2C对客三大核心场景，进行针对性防护和管理的创新设计，将抽象的数据全生命周期安全技术与具象防护场景进行关联，形成更易于指导实操的建设方案。

数据安全防护管理中心（以下简称“一中心”）作为安全大脑，牵引各单点安全产品的信息汇聚与能力融合，形成数据多跨融合、能力协同联动的立体式防御体系，进一步提升数据安全风险发现、预警与处置的效能。

技术体系建设的核心是“一中心”，以分层解耦的架构设计思路入手可将“一中心”划分为数据子系统、能力子系统和应用子系统（见图3）。数据子系统汇聚了原先离散的多源异构数据，形成了原始库、业务库、知识库等支撑上层业务调用；能力子系统一方面提供了智能编排响应能力来统一调控多元防护能力，另一方面通过大数据建模分析能力对汇聚后的数据进行多维度分析；应用子系统通过集中管控模块完成了数据安全风险的最终研判，通过SOAR模块编排的标准化SOP完成对数据安全风险的智能处置，最终形成了风险告警、分析、研判、预警、处置的完整管控闭环。

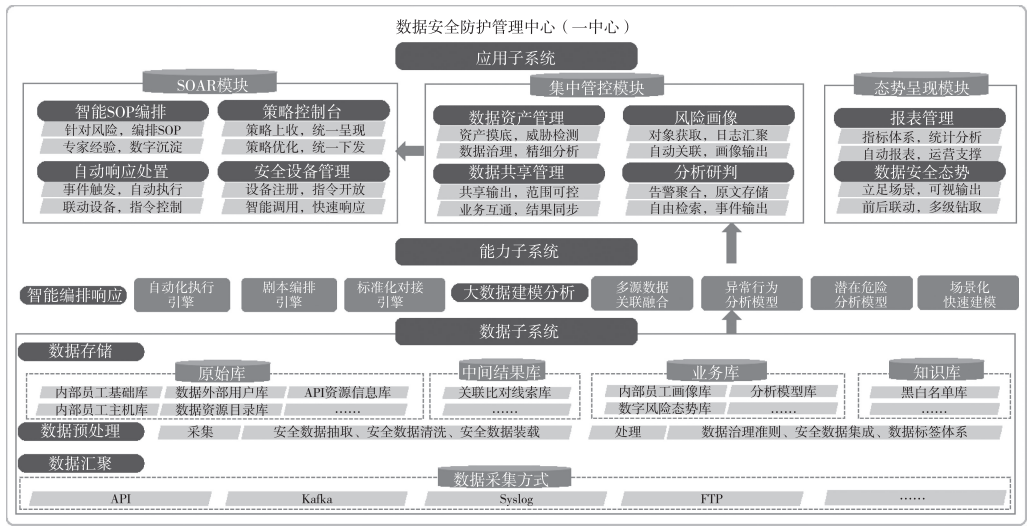

图3　数据安全防护管理中心架构

“一中心”在技术体系中承担安全大脑和指挥中枢的角色，统筹调度终端层、接入层、主机层、数据层等多层次的防护能力全面覆盖“三场景”，提前发掘和处置各类数据安全风险，实现数据安全风险的全面防控。

（三）数据安全防护运营体系

运营体系将数据安全防护与生产业务有机融合，跨业务条线进行运营协同，降低泄露风险、数据合规风险，保障数据安全。数据安全运营以技术体系提供的各项能力、工具为支撑，将各类制度、规范落实成具体可执行的工作：一方面，形成常态化的检查评估机制，对数据安全防护体系建设成效定期巡检，不断查漏补缺；另一方面，重点针对风险事件开展事前、事中、事后的全链路闭环运营，真正压降数据安全风险（见图 4）。

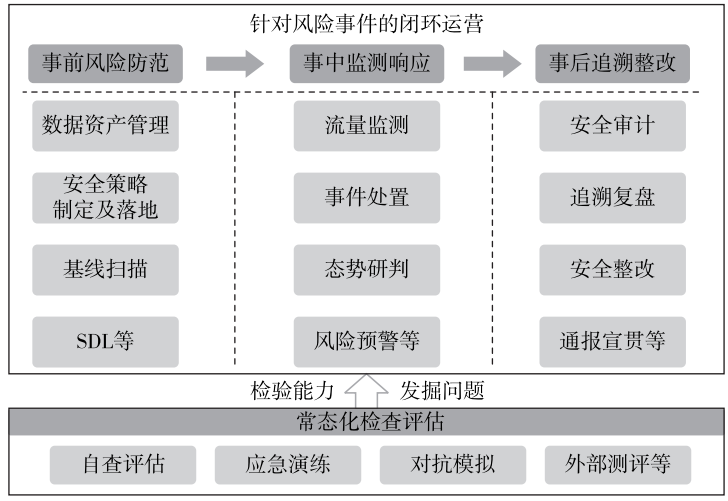

图 4　多跨协同的多层次数据安全防护运营体系架构

具体来说，常态化检查评估主要围绕数据资产、安全漏洞等要素，通过评估、演练、对抗等多种运营手段主动发掘短板、问题，并进一步有针对性地强化数据安全防护的各项能力、优化各类防护策略。

针对风险事件的闭环运营则从事前风险防范、事中监测响应到事后追溯整改，建立起针对风险事件的监控预警流程，形成全链路的数据安全运营体系，将风险压降至可控范围。具体安全防护运营机制如下：

一是事前清查资产底数。通过数据使用主体、数据访问客体、数据访问行为三大类数据的汇聚，输出员工主体、访问 IP 主体、结构化数据、非结构化文件

和应用系统这五本资产台账；进一步通过主体、行为、客体的关联关系刻画，以可视化方式产出员工、IP 和应用系统的三张风险画像，帮助运营人员快速定位问题。

二是事中做好风险分析挖掘。在专家人工分析研判积累的经验基础上，基于“一中心”分析能力，构建“异常行为分析 + 潜在威胁分析”的分层式模型，使得智能化、自动化的分析能力可以广泛适配各类场景，深度挖掘各类风险、问题。

三是事后快速整改闭环。依托“一中心”所具备的剧本编排、自动化调度引擎等能力构建针对各类别数据安全风险的闭环处置剧本，自主碰撞 IP 信誉、资产、原始流量等信息库实现智能化追踪溯源，有效提升数据安全运营的自动化、智能化程度。

三、数据安全防护体系应用与成效

浙商银行构筑的数据安全防护体系，具体应用在 2E 员工、2B 外联、2C 对客三个场景的全面防护上。

（一）2E 员工数据安全防护场景

2E 场景重点关注的是办公网、开发测试网、生产网等全网环境下内部员工的操作风险与数据泄密风险的挖掘、预警与处置。多跨协同的多层次数据安全防护体系落地应用方案如下：

一是构建多层次防护体系。终端防护层通过终端准入、桌面安全、防病毒等技术产品的部署保障入网设备安全、可信；接入防护层针对跨网区访问，配备防火墙、IPS 入侵防御、WAF 应用防火墙等多种接入防护设备实现精细化访问控制；数据防护层对员工的用数行为通过 DLP 数据防泄露、数据容器、数据安全监控与预警等进行管控和审计；控制层依托“一中心”对员工的操作行为进行分析与预警，挖掘与溯源数据操作不合规行为或泄密风险，及时下发指令控制员工用数权限。

二是构建 IPDR 全过程的安全策略体系。即识别（I）资产，对服务器、终端、数据、员工身份进行识别，完成资产梳理；防护（P）策略，对相关安全资产落实数据脱敏、数据水印、数据加密、外发外拷、邮件外发等安全控制策略，

确保数据自身安全；监控（D）行为，针对内部异常访问、远程访问、员工异常行为、数据变更、数据索取等高风险操作行为进行监控和分析，实现风险深度挖掘；响应（R）处置，针对不同类风险，自动启动 SOP 调用各安全能力对相关员工进行降权、限额、追踪、问责等处置，最终落实员工数据防泄露安全管控闭环。

三是构建员工防泄露安全闭环管控。在运营层面上通过终端与数据安全系列产品的数据多跨融合、能力联动处置，完成内部员工数据安全管控闭环，形成多层次的立体式防护，实现了员工用数动态脱敏、外发/外拷审批、离职泄密预判、数据定时自毁等应用，覆盖了员工用数的各个具体场景。现该场景覆盖了全国所有 304 家分支机构约 1. 8 万名员工及近 2 万台终端，并在 2023 年 1—8 月期间阻断潜在终端泄密事件 751 次、泄密邮件 8486 封，完成 14. 1 万份敏感文件的全生命周期智能管控；同时通过融合数据、建模分析成功事先挖掘了一小部分离职前有泄密动向的员工并完成了警示、问责等处置，有效提升了风险事前管控能力，压降了内部数据泄露风险。

（二）2B 外联数据安全防护

2B 场景下核心关注 API 自身安全性、合规性及外部风险调用行为的预警、处置等。通过多跨协同的多层次技术体系，完成了对外联流量的全面监控与解析，实现了所有 API 的统一管理，并在此基础上实现了 API 资产管理、API 数据安全态势感知、敏感信息外联监测预警、数据安全事件追溯等应用，保障数据外联可信、受控。

运营层面主要是依托大数据融合分析能力针对异常访问、敏感信息交换、特权账号滥用等情况进行实时分析，对风险接口和异常调用行为等进行禁用、限流、限频、溯源等智能处置。

依托技术、运营体系的建设，浙商银行完成了 5 万多个常用 API 接口和 423 个核心数据库的全面监控和防护，监测并修复 API 相关漏洞 1765 个；通过数据融合分析挖掘出真正存在泄密风险与合规风险的 API 接口 152 个并全部完成整改，防范了外联中的数据合规与泄露风险。

（三）2C 对客数据安全防护

2C 场景下核心关注隐私合规、交易风险及黑灰产撞库窃密等行为，重点防范攻击窃密与数据盗用等风险。对互联网访问通过异构防火墙、IPS 入侵防御、

动态防御、人机验证、限额控制、动态脱敏等多层次能力进行监控与防护，同时对客户交易行为落实大数据事中风控机制，最后通过“一中心”挖掘高可信度黑灰产撞库IP或其他风险行为，并下发指令至WAF或防火墙作封禁、隔离或通过系统自动提升安全强度（增加交叉认证）、线下人工认证等方式提升安全等级。

浙商银行将网上银行、手机银行等在内的所有2C业务应用纳入数据安全监测、防护范畴，形成IP机器行为登录、暴力破解行为等分析模型，挖掘了高置信度黑灰产IP 371个并完成了闭环管控，有效防范了攻击窃密，压降了数据盗用风险。

四、未来展望

数据安全防护体系仅是数据安全宏观体系中最基础的一部分，要真正发挥数据作为生产要素的价值，隐私计算是一个很重要的方向。浙商银行目前选择了多方安全计算作为探索方向，在联合营销、行业纵向联合风控等场景下，与各参与方共同就隐私数据进行联合分析与建模，整个过程中不泄露任何一方持有的数据，实现了数据可用不可见。在某一放贷场景的实验中，相比传统建模，多方安全计算建模AUC（准确率）提升13%，KS（好坏样本区分度）提升39%，Recall/Lift（与随机选择相比模型提升）提升20%，建模效果提升显著。后续浙商银行也将继续探索隐私计算的更多场景和技术，合规利用数据的同时创造更多价值。

在数据安全的建设工作中，金融机构不仅自身要落实好相关工作，也需要产业界的产品、服务等大力支持，更需要监管部门的监督与指导，同时也要加强与高校、院所的产学研合作，共同促进法律法规不断完善，促进行业不断规范，促进数据要素合规利用，共建金融行业数据安全生态圈，助推数字经济加速发展。

参考文献

[1] 李雪妮，闫树，魏凯，等．数据安全治理能力评估方法［S］．北京：中国质检出版社，2021.

[2] 李雪妮，闫树，刘雪花．数据安全治理框架及实践总体模型研究［J］.

通信世界，2021（17）.

［3］李晓伟，吴迎，邹彧，等．数据安全治理体系与技术研究［J］．信息通信技术与政策，2021，47（8）.

［4］中国信息通信研究院．数据安全治理实践指南 1.0［EB/OL］.［2021－12－ 27］． http：//www. caict. ac. cn/kxyj/qwfb/ztbg/202107/p020210720377857004616. pdf.

［5］张峰，于乐，马禹昇，等．数据安全分类分级研究与实践［J］．信息通信技术与政策，2021，47（8）.

［6］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 4.0［EB/OL］.［2022－05－27］． https：//dsj. guizhou. gov. cn/xwzx/gnyw/202206/t20220609 _ 74678503. html.

［7］马力，陈广勇，张振峰，等．信息安全技术网络安全等级保护基本要求［S］．北京：中国标准出版社，2019.

［8］杨国正．守正创新 构筑多层次数据安全防护体系［J］．金融电子化．2021（5）.

［9］朱红儒，刘贤刚，胡影，等．信息安全技术数据安全能力成熟度模型［S］．北京：中国标准出版社，2019.