数据跨境流动的信息安全策略技术研究与实践

在信息社会和大数据时代，作为金融服务重要载体，金融数据不仅是银行经营管理的重要资产，更是国家基础性和战略性资源，事关国家政治安全和社会稳定。金融数据跨境流动对国家安全、网络安全、金融安全将产生越来越重要的影响。世界上越来越多的国家对数据跨境流动的干预愈加深入。对于跨境经营的商业银行来说，不可避免地面临满足各国数据跨境流动政策要求的复杂局面，对战略布局、经营管理、技术架构带来深远影响。

**研究背景**

随着经济全球化深入发展，农业银行稳步推进海外发展战略，不断拓展全球化经营服务，数据跨境流动日益增多，跨境数据保护压力持续增加。一方面，跨境金融服务离不开数据跨境流动的支撑。

**①银行经营管理内在要求境内数据流出。**例如跨境信贷业务，境外分支机构需要查阅境内客户评级信息；反洗钱合规审查，境外分支机构需要查阅境内客户交易信息。

**②全球重要银行风险控制要求境外数据流入。**例如集团客户统一授信，需要获取客户境外经营状况。

**③境外业务系统集中部署境内数据中心，数据处理运行集中化形成了境外分支机构数据跨境流动的现实状况。**另一方面，大数据、云计算等新技术的应用使得数据跨境流动变得十分寻常，数据跨境流动安全风险骤增，作为客户资金和信息的重要载体，银行肩负着保障客户交易安全和信息安全的重大责任，面临不同监管标准及境内外双重监管压力。

因此，在对全球主要经济体信息安全法规的核心要义深入研究基础上，如何在法律允许的范围内，以更优质安全的金融服务为导向，重新审视银行系统架构，明确技术改进策略，提升数据跨境流动安全保护能力，成为摆在农业银行科技部门面前的重要课题。

**全球主要国家信息安全法规要义解读及趋势分析**

1. **我国主要信息安全法规的解读。**

我国积极开展跨境数据流动管理的政策法规建设，2017年6月正式生效的《中华人民共和国网络安全法》明确实施跨境数据流动监管：“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制订的办法进行安全评估；法律、行政法规另有规定的，依照其规定。”

《网络安全法》一方面，明确规定在境内运营中收集和产生的个人信息和重要数据应当在境内存储，限制跨境流出。另一方面，明确向境外的机构、组织、个人提供电子或其他形式的数据即为数据出境。若因业务需要确需数据出境的，应征得个人信息主体的同意，同时要进行安全评估，并对评估结果负责，这又为合理安全的数据跨境流出预留了空间。

1. **境外各国信息安全的法规解读。**

以欧盟和美国为代表的境外监管机构已将信息安全上升到宏观审慎性政策高度，纷纷出台相关的法律法规要求。美国、欧盟、俄罗斯、德国、新加坡等多个国家或地区加强了信息安全相关的基础性立法。

美国是数据跨境流动的倡导者，数据政策相对宽泛和自由，但对金融服务、信用报告等特定领域的数据存储和流动有着极为严格的要求，对隐私数据限制或有条件允许数据跨境流动，将国家经济数据、政府管理数据、公共信息数据、敏感技术数据等视为“重要数据”进行严格出境管理。2016年9月更是发布了包含农业、受控技术信息、关键基础设施、应急管理、出口控制、金融等共计23类信息的受控非秘信息列表。

欧盟围绕个人隐私和数据保护制订了严格的法规，2018年5月25日起实施的《一般数据保护条例》（GDPR）是最重要的立法。一方面，明确个人作为数据主体的一系列权利，明确企业作为数据控制者、处理者的法定责任、数据保护原则和措施要求；另一方面，明确了数据跨境流动需要获得个人同意，建立了可信国家地区、评估认证、有约束力公司规则、同等保护水平的合同条款等合法通道，在确保境内外个人数据保护水平的基础上，为有序全的数据跨境流动提供空间。

1. **监管趋势分析。**

通过对全球主要国家网络信息安全法规的分析，数据跨境流动监管有以下四大趋势：

**一是**“数据自由流动”需求和“数据跨境流动”监管的冲突将长期并存。金融行业作为关键基础设施必是各国监管的重点，跨境经营的银行首当其冲面临各国不同标准的监管要求。

**二是**个人数据、非公开信息等数据保护要求和监管措施将进一步增强。企业作为数据控制者、处理者的责任与日俱增，数据分级保护、匿名化、存储加密等保护措施要求日趋细化。

**三是**数据出境概念存在逐渐拓宽的趋势，从采取数据存储国家地理边域为标准，向以数据主体国籍、数据处理者所有者国籍为标准延伸。例如GDPR明确保护对象是欧盟公民个人数据。

**四是**数据跨境流动限制规则标准不一，存在禁止数据离境、有条件解除数据流动禁止、数据本地备份基础上支持数据流动等不同规制模式。但在中国和俄罗斯的示范效应下，数据本地化存储的要求可能会成为一种趋势。

**农业银行数据跨境流动安全的技术策略选择及实践**

在金融科技时代，大数据、云计算、互联网等技术与全球经济生活深度融合，数据跨境流动是必然的，跨境经营的商业必须直面境内境外数据跨境流动的合规要求。农业银行科技部门按照集中化和本地化相结合的思路，制订了“坚守安全底线，构筑安全边界，数据分离协同再造，全方位完善技防体系，高标准规范技术管理”的技术策略，开展了如下实践探索。

1. **严标准高要求构筑安全边界。**

从物理机房、网络区域、应用部署等方面，以从严标准构建物理、网络和应用边界，形成企业内数据境内外部署的有效隔离。一是通过划定独立境外机房区、单独部署境外机构核心应用、与境内系统完全物理隔离等方式，建立物理安全边界。二是通过设立境外访问境内网络隔离区，建立网络安全边界。三是通过境外可访问应用实行白名单控制，所有可访问应用均在境外隔离区内落地，以权限最小化为原则，控制境外隔离区内应用向外的网络访问权限，建立应用安全边界。

1. **全方位完善技防体系。**

境外区部署双层异构防火墙，区分境外机构访问入口和境内业务互联入口，配置IPS、IPSEC等网络安全防护工具，部署防APT及流量回溯等系统，并进一步加强终端安全、用户认证、桌面安全防护、统一存储管理等信息安全手段。按等保三级的标准进行应用安全设计和建设，数据传输进行传输加密，对关键数据进行数据加密，信息访问上采取两重用户访问权限控制和操作留痕的设计，强化应用安全防控。

1. **围绕重点开展“数据分离、应用协同”再造。**

在客户信息管理、客户评级、客户授信等重点应用领域，按照“技术架构统一、境内外数据分离、优化数据访问控制”的原则进行系统架构再造。基于统一的技术平台，进一步改进松耦合的应用架构体系，境内外应用分离部署，支持境外数据本地化存放（如图1所示)。基于业务流程优化和跨系统流程调用，增加数据访问控制，实现安全控制下的数据透明互访。采用数据库透明加密、关键数据应用加密等技术，实现数据存储加密要求，全面灵活地应对境内境外各种监管要求。

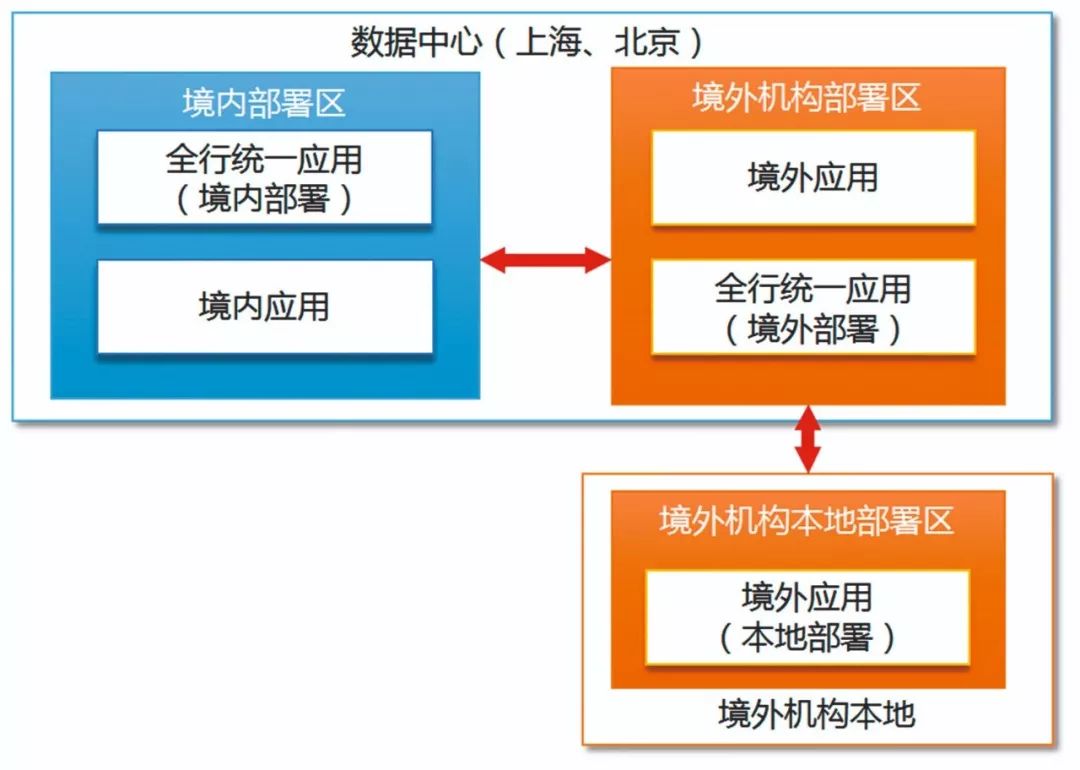


 图1  境内外数据部署应用架构体系

1. **多层次健全管理机制。**

对开发、测试、运维有严格的信息安全管控机制。与各境外机构签署规范统一的服务协议，构建同等保护水平的合同条款等数据跨境流动合法通道。

**结语**

技术策略只是数据跨境流动安全性解决方案的一个方面，要全面达到境内外双重监管要求，更需要**企业在业务经营战略中明确数据保护政策，从业务管理、制度流程、人员架构等方面建立全面的跨境数据流动管理机制。**首先，企业高管层要高度重视确定数据跨境流动中的数据保护政策、营造数据保护责任意识。多层次建立跨境数据保护制度，形成企业内部各部门数据保护责任和规则体系，明确数据收集、转移、存储、使用等各环节的具体安全管理要求。其次，要加强跨境数据安全监测，定期开展合规性检查，及时发现数据保护方面的漏洞并加以改进，防范数据安全风险。