关于银行信息系统安全可控的思考

陈天晴

2014.10.23

安全可控一直是我们努力奋斗的目标！

1、安全是一个永恒的话题，其重要性怎么讲都不过分

2、安全是相对的，永远没有绝对的安全

3、安全的需求是随着发展而变化的

4、安全可控需实事求是，积极稳妥地推进

5、关于去IOE

6、安全可控与国产化

1、 安全是一个永恒的话题，其重要性怎么讲都不过分

银行业信息系统安全需求除了通常意义上的数据安全外，还有对整个信息系统的安全性、可靠性以及服务的及时性、持续性（24 x 365）、可恢复性的需求

银行业在电子化、信息化建设中，一直同步建设其信息安全系统，基本保障了整个银行业信息系统的安全运行，保障了客户的账户资金安全

没有发生过颠覆性安全事故　　(谢天谢地)

有力地支持和引领了银行业三十多年来飞跃式发展，从而有力地支持了国民经济三十多年的大发展!!!

银行信息化发展历史（典型银行）

互联网化时代

（2005年至今）

- 云架构、SOA、虚拟化、大数据应用、BCM、网上银行、互联网金融、移动金融

信息化时代

（2000年）

- Z系列主机、z/os、数据大集中，新一代综合系统，全功能银行系统（NOVA），B/S结构、网上银行，中间件，客户服务中心，中间业务平台，生产中心+灾难备份中心，数据整合、应用整合

电子化时代

（80、90年代）

- “七五”：通用微机及S系列小型机，M-150/240日立机与IBM 4381主机；专用系统，SNA网络体系；核心网点，账务处理
- “八五”：主机（IBM 4381+ES9000，M-660/860）、unix系统（HP9000，RS6000），混合网络，C/S模式，综合柜员，独立应用系统，面向客户
- “九五”：主机（IBM ES9000）+unix系统（HP、SUN、IBM），TCP/IP 网络；综合业务系统，数据库系统，ATM/POS/信用卡/电话银行，渠道整合

初期探索时代

（70年代）

- M-150应用

创新业务

- 电脑储蓄、电脑储蓄所、通存通兑、电子联行（80‘）
- 信用卡、自动取款服务、销售终端转账、电子汇兑（90‘初）
- 行内一卡通、一本通、代理业务、国际汇兑（90‘中）
- 自助银行、企业银行、电话银行（90‘末）
- 银联、一柜通、投资基金、外汇宝、纸黄金、金融e家、客户服务中心、现代支付服务、企业/个人征信、反洗钱（本世纪）
- 网上银行、移动银行、手机银行、私人银行、金融超市、互联网金融（继续中……）

2、安全是相对的，永远没有绝对的安全

什么是安全?（汤博：核电安全的基本问题）

第一、利益足够大，代价可承受，则可认可其是安全的

第二、安全是利益和代价的平衡；没有一件事情只有利没有弊；

第三、安全是可接受的风险

尽管安全非常非常重要，但也不能将安全绝对化

目前，我们必须：

- **正确处理开放和安全的关系：**

  安全不等于闭关锁国，不等于拒绝先进技术；(要知道现在已是国际互联网时代！)

- **安全和发展的关系**：必须**坚持抓好发展这一第一要务（习主席9.30讲话）**

  以安全保障发展，以发展促进安全；不发展就 最不安全（而决不能是安全了再发展!!!）

  我们的生活中处处都有风险（食品安全、环境安全、交通安全、医疗卫生安全…），

  但我们必须生活！只不过要努力将风险限于在相对可控的范围内（其实可控也是相对的）

3、安全的需求是随着发展而变化的

银行已进入互联网时代，对银行信息系统有更多、更高、更新的需求

电子化→信息化→互联网化 ;算盘→键盘→鼠标→滑屏

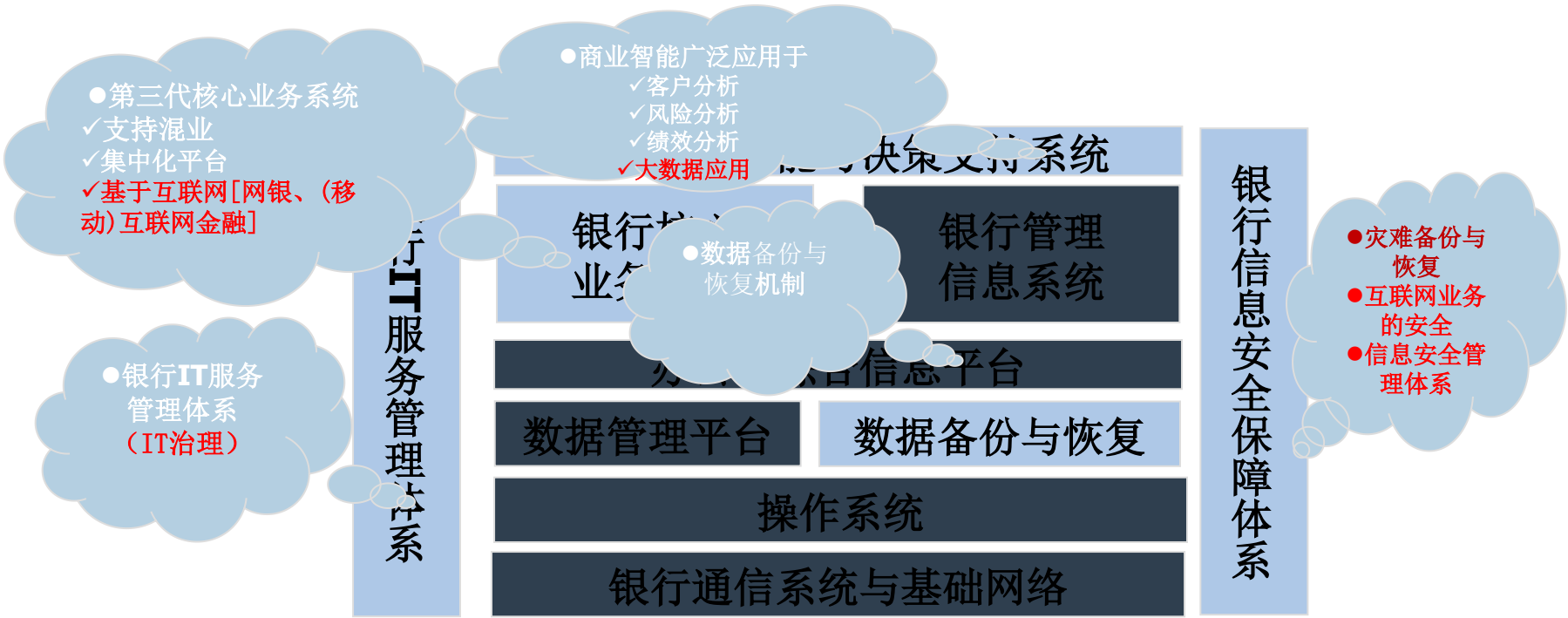
下一阶段：以综合服务为中心的智慧型银行(以服务为中心)

以(移动)互联网为主要渠道的、强化客户体验（客户导向)的、提供全能型服务的智慧银行;

银行不再是一个地方，而是一种行为！ (kank3.0)

服务于国民经济的发展，服务于民生的宗旨不变!

中国银行业信息化发展趋势



银行信息化系统框架（黄色 表示可能发生变化的重点领域；红色表示重点加强和发展的系统）

银行发展进入新时代，对信息系统的安全可控提出更高要求

银监发[2014]39号文：

《关于应用安全可控信息技术　加强银行业网络安全和信息化建设的指导意见》

明确要求：到2019年，掌握银行业信息化的核心知识和关键技术，实现银行业关键网络和信息基础设施的合理分布，关键设施和服务的集中度风险得到有效缓解；安全可控信息技术在银行业总体达到75%左右的使用率

4、安全可控需实事求是，积极稳妥地推进

最近，几家银行的科技部门领导都发表了他们如何开展安全可控工作的文章，如：

中国工商银行科技部总经理吕仲涛的《构建”四为一体”的信息安全体系》

中国建设银行科技部总经理金磐石的《”产、用“战略联动，推动信息化自主可控进程》

广东 发展银行CIO王兵的《总体规划，稳步实施，通力协作，推进信息技术”自主可控”》等

工商银行的四为一体的信息安全体系：

组织体系是信息安全体系建设的保障

制度规范是信息安全体系建设的准绳

技术手段是信息安全体系建设的关键

管理措施是信息安全体系建设的根本

我个人认为：根据目前我们的综合条件，银行业作为信息技术的应用部门，其信息系统首先要努力实现应用级的安全可控！

(这是我们应该做的，也是能够做到的)

5、关于去IOE

首先，要明确去IOE的含义是什么？

是去IBM、ORACLE、EMC公司的所有产品和服务，进而去所有国外产品和服务？如果这样的话，则不可以为之，也不可能为之！

如果是指去以IBM的unix小型机、ORACLE的数据库管理系统、EMC的存储系统为代表的传统的封闭式数据处理技术机构，代之为以LINUX的x86PC服务器、内部数据处理系统和云存储的开发式云机构，可积极探讨！

第二，如何去？

— 我不提倡用”去”、“颠覆“等词语，建议用“迁移”、“重构”

—从技术角度上看，不是非此即彼，应选择适合的业务和应用场景

—目前来看， 银行核心的账户系统对数据一致性、客户信息安全性和系统运行的稳定性要求极高(实际上也是政府和客户对银行的要求)，不可轻易为之

—对于其他的、尤其是基于互联网的创新业务，可努力用开放式云架构来实现(市场行为，积极而稳妥；去IOE不等于国产化)

6、安全可控与国产化

— 必须支持国内产业，但也必须遵循实事求是、循序渐进的原则；

能做什么，先做什么；能用什么，先用什么；

建设银行推进信息系统自主可控与国产化的实践:

1、对于成熟的外围硬件产品，同等竞争

2、对于已比较成熟的非核心软件产品，要采取各种措施，积极推进国产化

3、对于逐步成熟的国产核心硬件产品，加快国产化替代的进度

4、对于暂时没有国产替代产品的门类，要通过架构调整或新技术应用，降低相关产品在整体架构中的使用比例

5、对于国内缺少成熟商用产品的基础软件，需要银行与产、研部门长期战略合作，共同孵化

6、在部分领域，试选用开源技术产品作为国产化“缺口”的补充

国产化与安全可控相关，但不是等于关系；国产化不是安全可控的全部

“产、学、研、用” 需要积极配合； 希望企业更紧密地贴近用户

最重要的是：我们必须保障银行业安全和可控，保障银行业务的持续运营和服务能力 →这是国家和社会对银行业的要求，也是对企业发展的支持

发展才能自强，科学发展才能永续发展！

（习主席9.30讲话）

谢谢！