《读书笔记》

风控要略
互联网业务反欺诈之路（上篇）
（马传雷、孙奇、高岳著）

消费金融风控联盟

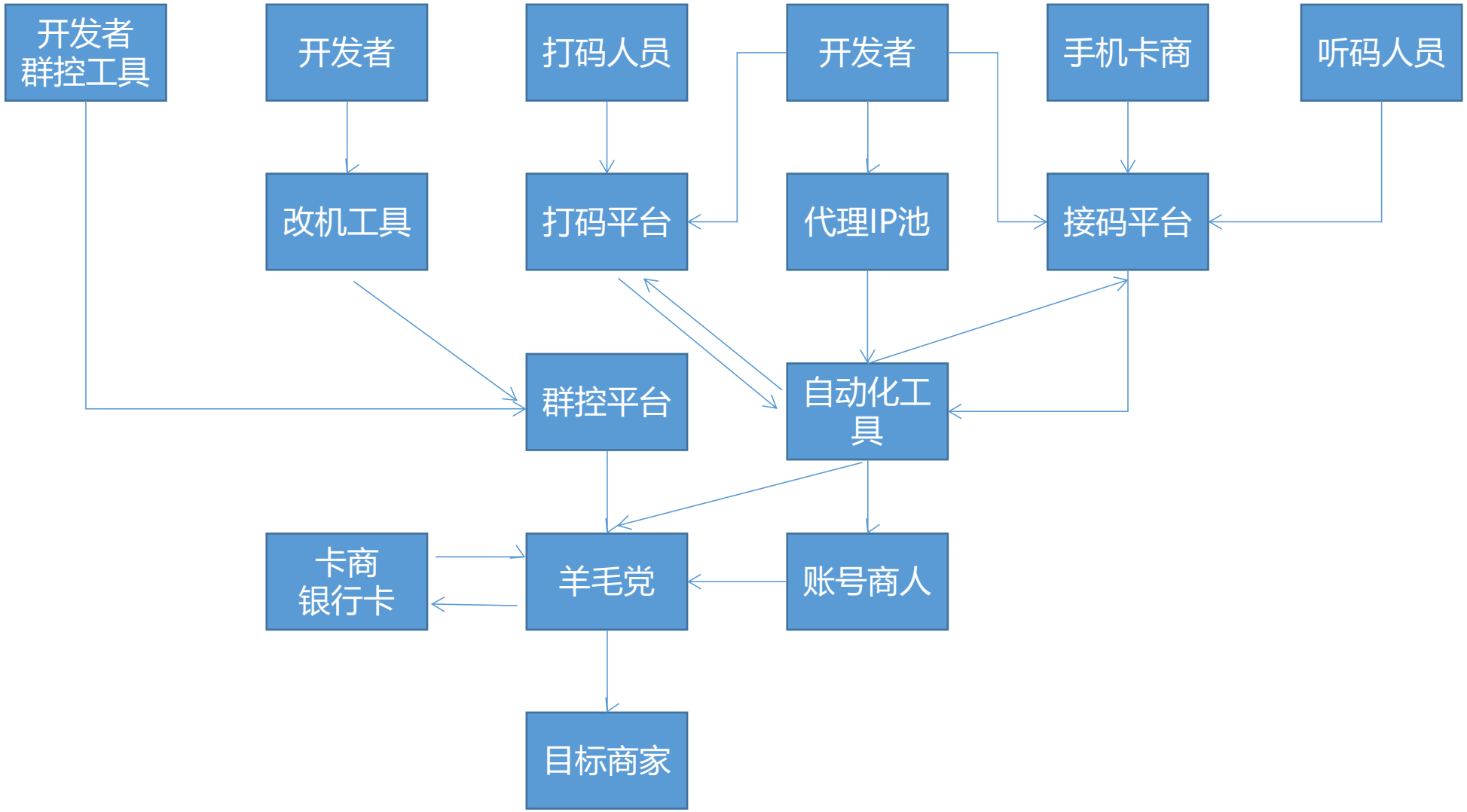
目录

一、洞察黑产 第1章黑产发展趋势

目录内容

一、洞察黑产 第1章黑产发展趋势

1.1黑产组织结构



一、洞察黑产 第1章黑产发展趋势

1.1黑产组织结构

反欺诈词典（1）

垃圾注册
在注册环节，使用虚假、不稳定的身份信息进行注册。如虚假号码、临时邮箱，或者使用脚本、注册机批量注册。账号命名常见有不规则英文组合、古诗词截取等。

薅羊毛
使用虚假身份或者自动化工具参与各类营销活动行为。如关注点赞、返现抽奖等。

黄牛/刷单
在合法销售途径以外，垄断、销售限量参与权或商品，并以此牟利的中介人成为黄牛。

众包
由多个独立的个人共同参与完成一项任务，参与薅羊毛的用户都是独立真实的用户。

一、洞察黑产 第1章黑产发展趋势

1.1黑产组织结构

反欺诈词典（2）

众包
由多个独立的个人共同参与完成一项任务，参与薅羊毛的用户都是独立真实的用户。

炒信
通过各种渠道和手段进行虚假交易，快速提升商户交易量、信用等级。

套利
由商户的发起薅羊毛行为，羊毛党和商家都能获利。

空包
虚假发送快递，发送空的快递或者包裹，为了提供真实的物流信息来规避平台的风控策略。

一、洞察黑产 第1章黑产发展趋势

1.2黑产成员分布

从年龄上区分，百分之五十黑产从业者年龄18-25周岁之间

黑产网络布控	• 通过蜜罐网络技术追踪黑产团伙，发现黑产人员聚集地(QQ、微信群、暗网等)使用AI机器人进行布控
机器学习聚合分析	• 采用机器学习算法对AI机器人采集的多渠道信息进行分析筛选。同时算法系统自我进化。
情报专家深入分析	• 对重要黑产攻击时间，情报专家分析，对黑产攻击手法溯源，为客户提供防御建议

一、洞察黑产 第1章

1.3黑产专业化分工

随着技术的发展，大数据分析、深度学习和人工智能被广发应用到黑产当中。

一、洞察黑产 第1章

1.4黑产攻击规模

1、发生时间
电商平台通常在双11、双12、618

2、业务场景
注册登录占比40%以上

3、地域地点
华东地区占比40%以上，但是这里说的不是真实所在地，主要是IP归属地、手机号码归属地、设备等

4、欺诈IP地址
10%以上的欺诈行为来自自家宽带IP地址

一、洞察黑产 第1章

1.5电信欺诈黑产

在现实世界中还有一类更加凶残的黑产团伙--电信诈骗团伙。

这类黑产团伙的危害远远超过上文所说的羊毛党黑产。他们常常通过暗网等渠道购买大量公民隐私数据，

通过分析后选定欺诈目标，编写特定的剧本实施诈骗。

一、洞察黑产 第1章

1.6小结

所谓知己知彼百战不殆，在对抗之前，必须先对他们进行充分的了解。

黑产产业链之所以难以斩断，除技术因素之外，还和它形成的利益生态有很大关系。

当黑产团伙规模达到一定程度后，它就成了一种能够干扰互联网正常生态的力量。

一、洞察黑产 第2章黑产武器库概述

目录内容
2.1虚假号码
2.2代理IP
2.3设备伪造工具
2.4其他工具
2.5小结

一、洞察黑产 第2章黑产武器库概述

2.1虚假号码

1、定义

指的是运营商真实存在的手机号，但是这些手机号码未经实名制认证，可以替代他人接受验证码。

2、作用

互联网平台注册时，需要用手机号码接收验证码进行二次验证。

1）用户实名制

2）比邮件验证更便捷

3、互联网黑产产业链中，手机号是互联网欺诈活动的根源。

一、洞察黑产 第2章黑产武器库概述

2.1.1猫池

1、定义
英文名Modem，是一种用户控制和管理SIM卡的设备。猫池，由多个Modem模块组合而成。

2、组成
SIM卡槽、基带芯片、射频芯片、手机天线。
每个Modem都可以单独控制，收发短信和拨打电话。

3、使用
AT指令控制
酷卡/洗唰唰

一、洞察黑产 第2章黑产武器库概述

2.1.2短信验证码

1、定义
基本验证身份认证手段，某些平台把短信验证码当成唯一的验证方式。

2、组成
4-6位数字，随机性、有效期短

3、使用
猫池+软件配合就能够自动读取
为了对抗猫池，语音验证或者向制定号码发送一条短信

一、洞察黑产 第2章黑产武器库概述

2.1.3接码平台

1、定义
是虚假号码的集散地，中间人角色，链接卡商和下游黑产。

2、使用
提供一个卡端商程序给上游卡商，上下游卡商自行管理所有手机卡，程序把所有手机卡接收到的短信上传到接码平台。

3、作用
短信内容匹配、抽取、分发和结账

一、洞察黑产 第2章黑产武器库概述

2.1.4空号注册

目前已经比较少见
黑产与运营商勾结，没有投入市场使用的手机号码，即被大量接受短信验证码

2.1.5流量卡和物联网卡

1、流量卡
运营商推出来的，可以收发短信，注册账号，使用周期较短

2、物联网卡
运营商给物联网企业使用，某些企业低价转卖给黑产

一、洞察黑产 第2章黑产武器库概述

2.1.6手机rom后台

老人机团伙
1、定义
拥有自己开发手机rom系统，基于早期的MTK平台
提供电话、短信功能

2、使用
投放到市场售卖，并销售到贫困地区
当手机卡入手机卡后，rom中后台会通过短信方式上报对应手机号到黑产预埋的手机号中
rom后台屏蔽其短信，使用人无法察觉

一、洞察黑产 第2章黑产武器库概述

2.2代理IP

1、正向代理
屏蔽访问者IP

2、反向代理
企业中大量使用，用户可以访问多个网站资源，对用户而言，所有的资源都集中在一个域名下

3、类型
HTTP（S）、Socks，VPN

一、洞察黑产 第2章黑产武器库概述

2.3设备伪造工具

业务风控方除通过手机号、IP资源部署风控策略外，还会结合设备维度定制更加强有效的防控策略。因此黑产会通过各种方式和工具伪造移动设备信息。改机工具、模拟器和各种hook框架都是黑产常用作案工具。

2.3.1改机工具

1、互联网业务平台常见规则
1）每个注册账号仅限参与一次
2）每个手机号仅限参与一次
3）每台设备仅限参与一次

2、改机工具
1）更改手机串号
2）更改手机型号
3）更改MAC地址
4）更改无线名称
5）更改手机运营商、手机号码

一、洞察黑产 第2章黑产武器库概述

2.3.2多开工具

1、定义
不root七年同事开启多个相同应用程序

2、种类
LBE平行空间、360分身大师、多开分身等

2.3.3Root/越狱工具

1、定义
Android和IOS悦悦指的是操作系统管理员的权限状态

2、使用
root和越狱操作都是有一定风险的，很多有可能造成手机系统瘫痪
root和越狱并不意味着设备一定是黑设备，只是风险比较高

一、洞察黑产 第2章黑产武器库概述

2.3.4Xposed

2.3.5Cydia Substrate

2.3.6Frida

2.3.7硬改工具

2.3.8脱机挂

2.3.9备份恢复/抹机恢复

2.3.10模拟器

2.3.11订制浏览器

2.3.12自动化脚本

一、洞察黑产 第2章黑产武器库概述

2.4其他工具

2.4.1位置伪造器

2.4.2群控

2.4.3工具集

一、洞察黑产 第2章黑产武器库概述

2.5小结

在业务安全领域和黑产的对抗，很大程度是技术和资源的对抗。

新的欺诈手段层出不穷，趋势互联网平台和风控厂商不断构建更先进的防控体系来保证业务安全。

而黑产团伙在金钱的驱动下也不断将新的技术用于欺诈攻击，实现现有的防御体系。

对于风控从业者，必须对黑产的技术手段和攻击模式有深入了解。

二、体系构建 第3章反欺诈体系建设思路

目录内容
3.1动态防控理念
3.2防控体系构建
3.3小结

二、体系构建 第3章反欺诈体系建设思路

互联网黑产攻击行为特点

1、团伙化

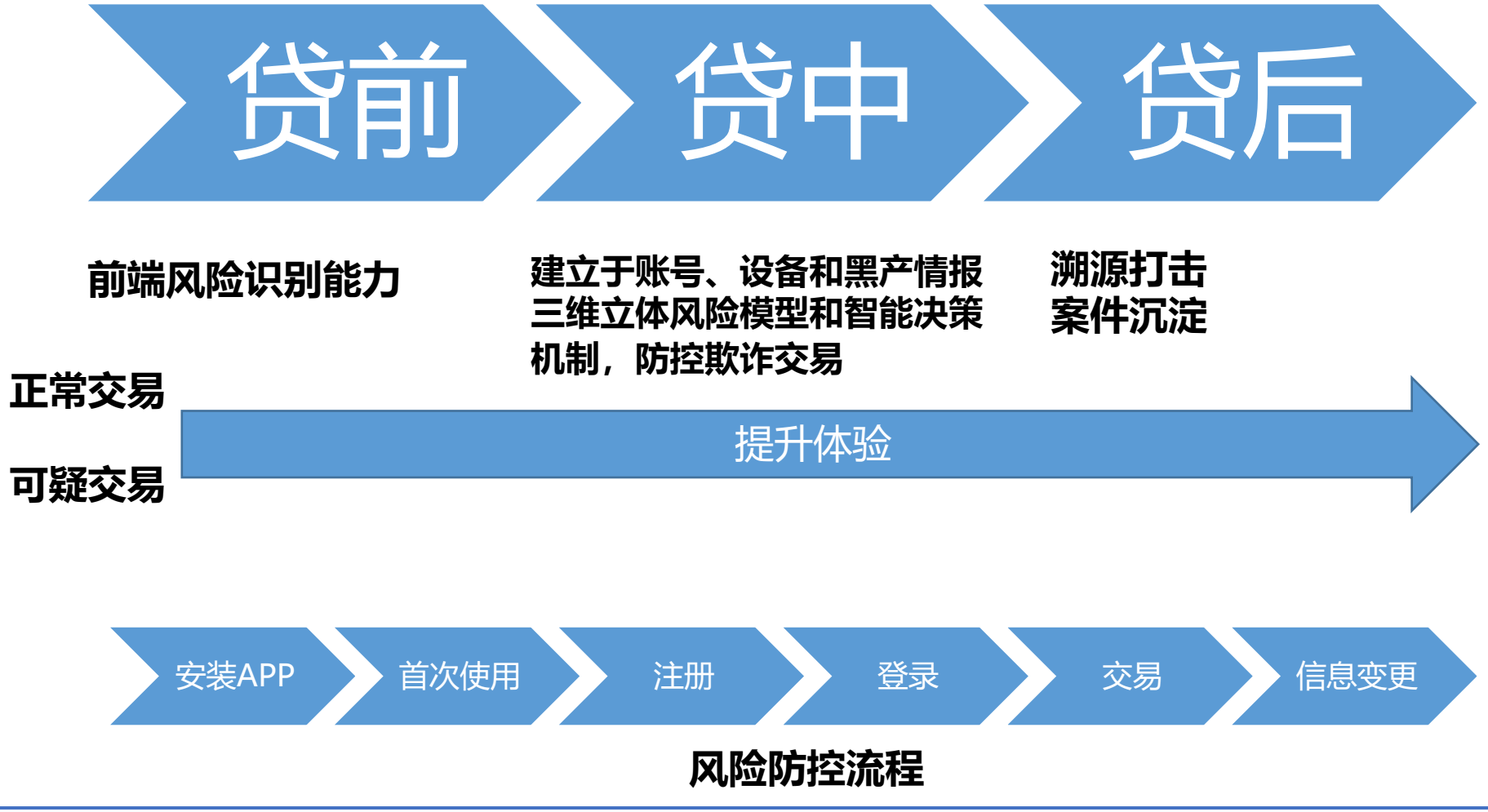
2、专业化

3、强对抗性

4、跨行业

二、体系构建 第3章反欺诈体系建设思路

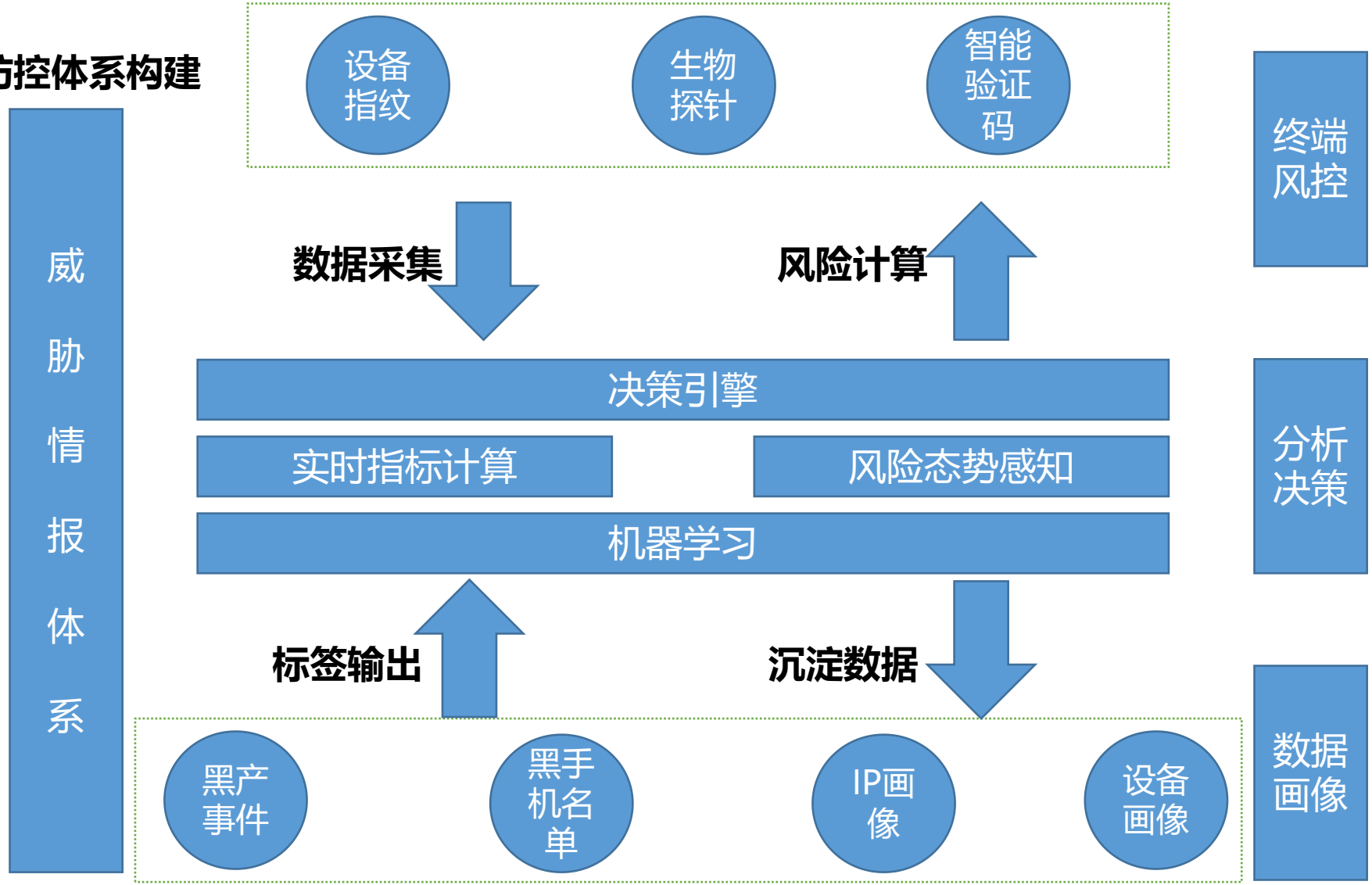
3.1动态防控理念



风险防控流程

二、体系构建 第3章反欺诈体系建设思路

3.2防控体系构建



二、体系构建 第7章风控中暑枢决策引擎系统

3.3小结

通过实战总结提炼而成的动态防控理念。

依据此风控理念，我们构建贯穿事前、事中、事后的业务全生命周期风控体系，通过终端风险识别能力、云端智能决策和黑产数据画像实现多层次、全场景的业务风控。

二、体系构建 第4章风控核心组建设备指纹

目录内容

二、体系构建 第4章风控核心组建设备指纹

4.1设备指纹的原理

1、设备指纹通过收集客户端设备的特征属性信息并将其加密上传到云端，然后通过后台的算法计算分析为每台设备生成唯一设备ID来标识这台设备。

2、手机操作系统和浏览器厂商为了方便用户与开发者获取用户的设备信息，预留了一些API供应用程序使用。

3、用户和开发者可以通过这些API获取客户端相关的软硬件信息，这些信息因设备而已，设备指纹通过部分的差异信息来生成完全独立的设备ID。

二、体系构建 第4章风控核心组建设备指纹

4.2设备指纹的技术实现

4.2.1Android设备指纹

针对Android作弊环境的监测方法

1、通过安装包监测安装的作弊环境

2、通过特定特征识别ROOT环境

3、使用多样方案采集同一字段信息

4、它能够个通用性的作弊原理识别运行的作弊框架hook（JAVA、NATIVE）

5、通过特定特征识别运行的作弊工具和模拟器

二、体系构建 第4章风控核心组建设备指纹

4.2.2IOS设备指纹

IOS设备指纹风险识别技术

1、通过使用hook原理识别技术检测运行的作弊工具

2、通过特定作弊工具特征识别的作弊工具

3、通过特定特征识别越狱环境

4、寻找特定的空间储存设备标识

5、对抗hook改机

6、对抗备份和抹机

二、体系构建 第4章风控核心组建设备指纹

4.2.3Web设备指纹

识别浏览器端异常环境

1、通过特定特征识别hook

2、通过特定特征识别JS是否被篡改或正在被调整

3、通过浏览器特殊方式存储设备标识，防止储存的标识被删除

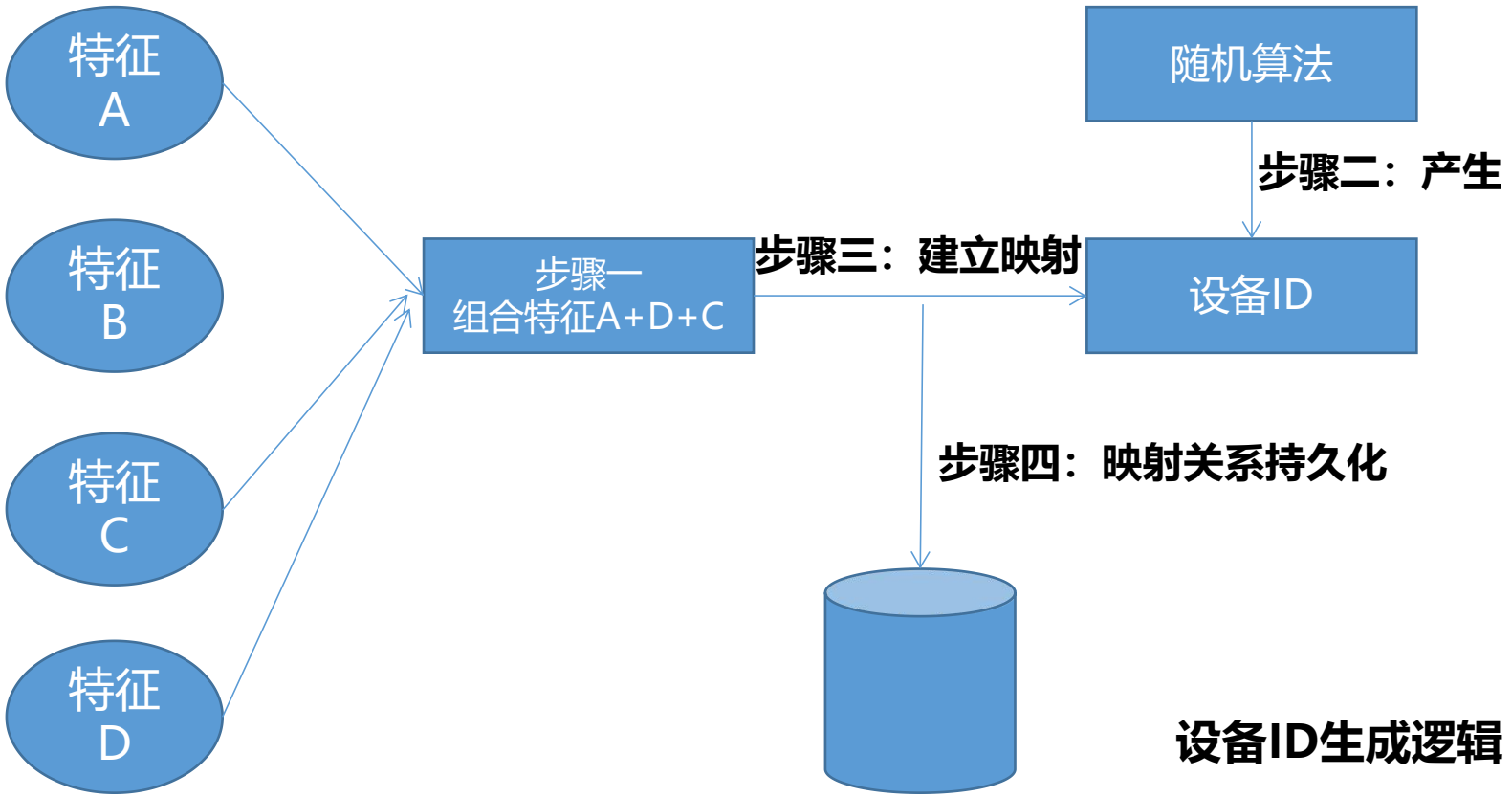
Web设备指纹实现过程

1、设备指纹的稳定性，即需要收集较为稳定的设备信息

2、作弊环境监测，即保证当前Web设备指纹采集到的信息都是真实的

二、体系构建 第4章风控核心组建设备指纹

4.2.4设备ID生成与恢复逻辑



设备ID生成逻辑

二、体系构建 第4章风控核心组建设备指纹

4.2.4设备ID生成与恢复逻辑

设备ID恢复逻辑

二、体系构建 第4章风控核心组建设备指纹

4.2.5被动式识别技术

在设备指纹中会应用一些被动式识别技术，行业成为被动式设备指纹。

这种设备指纹是在终端设备与后台服务器建立连接的过程中，从网络报文中提取多个维度的特征集，

在后台使用机器学习算法识别终端设备。

这类被动式的设备指纹，在没有完全流量的情况下，仅利用建立连接的过程数据是很难生成一个唯一设备ID，

但是可以用于设备验真（验证设备参数是否真实，未被篡改）。

二、体系构建 第4章风控核心组建设备指纹

4.3代码保护

4.3.1JS代码混淆技术

1、定义
代码混淆（obfuscation）是增加黑产静态分析难度而牺牲运行效率的一种技术方案。
通过逻辑变换算法等技术手段将受保护的代码转换为难以分析的等价代码的一种技术方案。

2、分类
1）布局混淆

2）数据混淆

3）控制混淆

4）预防混淆

二、体系构建 第4章风控核心组建设备指纹

4.3.1.1布局混淆

1、删除无效代码

2、标识符重命名

二、体系构建 第4章风控核心组建设备指纹

4.3.1.2数据混淆

4.3.1.2.1数字混淆

1、定义
数字混淆主要是使用进制转换、数字拆解等方法对代码进行混淆保护

2、进制转换

3、数学技巧

4、数字拆解

二、体系构建 第4章风控核心组建设备指纹

4.3.1.2.2布尔混淆

1、定义
取值范围比较固定且范围非常小，混淆手段较多。

2、类型转换
从一个值从一个类型隐式的转换到另一个类型的操作。

3、构造随机数

4.3.1.2.3字符串混淆

Mealy机

字符编码

其他

二、体系构建 第4章风控核心组建设备指纹

4.3.1.3控制混淆
定义

4.3.1.3.1不透明谓词

4.3.1.3.2插入冗余代码

4.3.1.3.3控制流平坦化

二、体系构建 第4章风控核心组建设备指纹

4.4小结

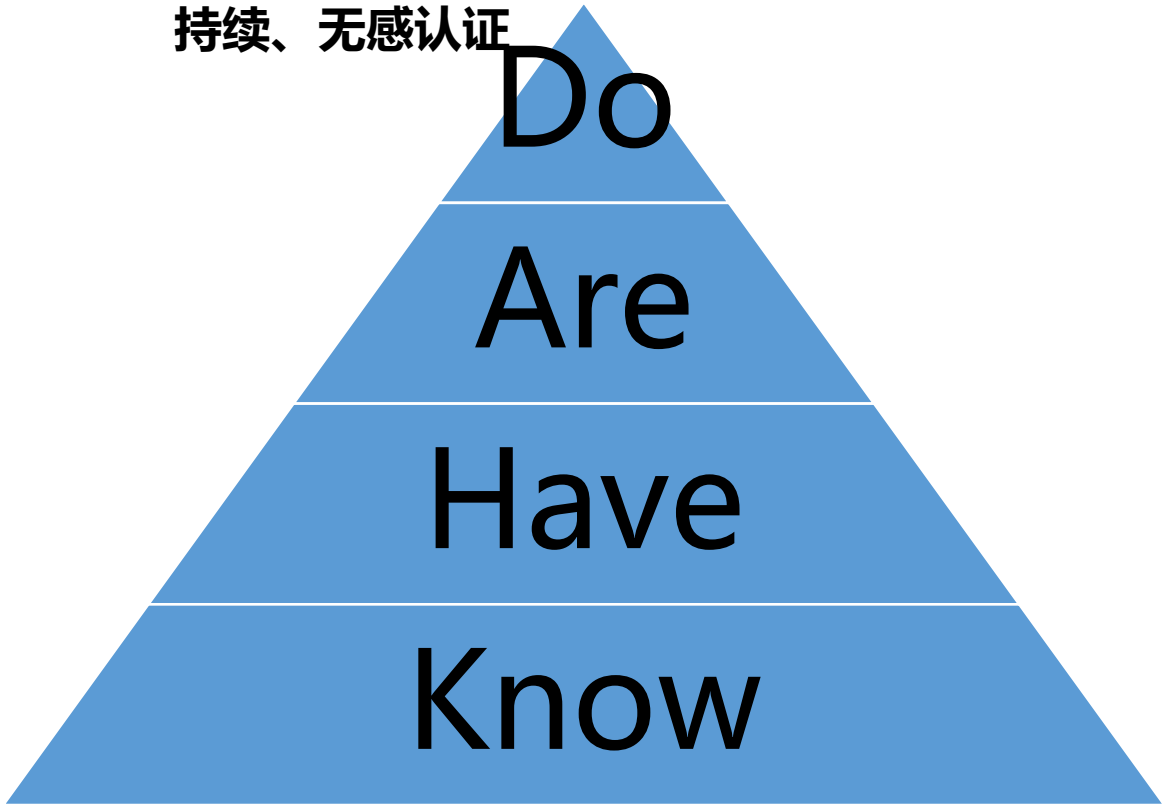
风控体系中为移动终端生成唯一标识的设备指纹设备。

设备ID的稳定性和唯一性是对立的，在设计设备ID恢复逻辑时需要权衡考虑。

设备指纹的应用场景非常广泛，常见的如网银APP的设备识别、APP推广安装激活计费、APP注册营销及业务接口发爬虫拉去数据等。

二、体系构建 第5章基于用户行为的生物探针

持续、无感认证



身份认证的层次

你持有的行为证明了你就是你

只有你拥有的生物特征

只有你拥有的物品

只有你知道的信息

二、体系构建 第5章基于用户行为的生物探针

5.1生物探针

二、体系构建 第5章基于用户行为的生物探针

5.2无感认证

无感认证可以在用户登录场景提供轻量级的风控能力。

无感认证的应用情景

5.2.1无感认证的基础

5.2.2无感认证的构建

二、体系构建 第5章基于用户行为的生物探针

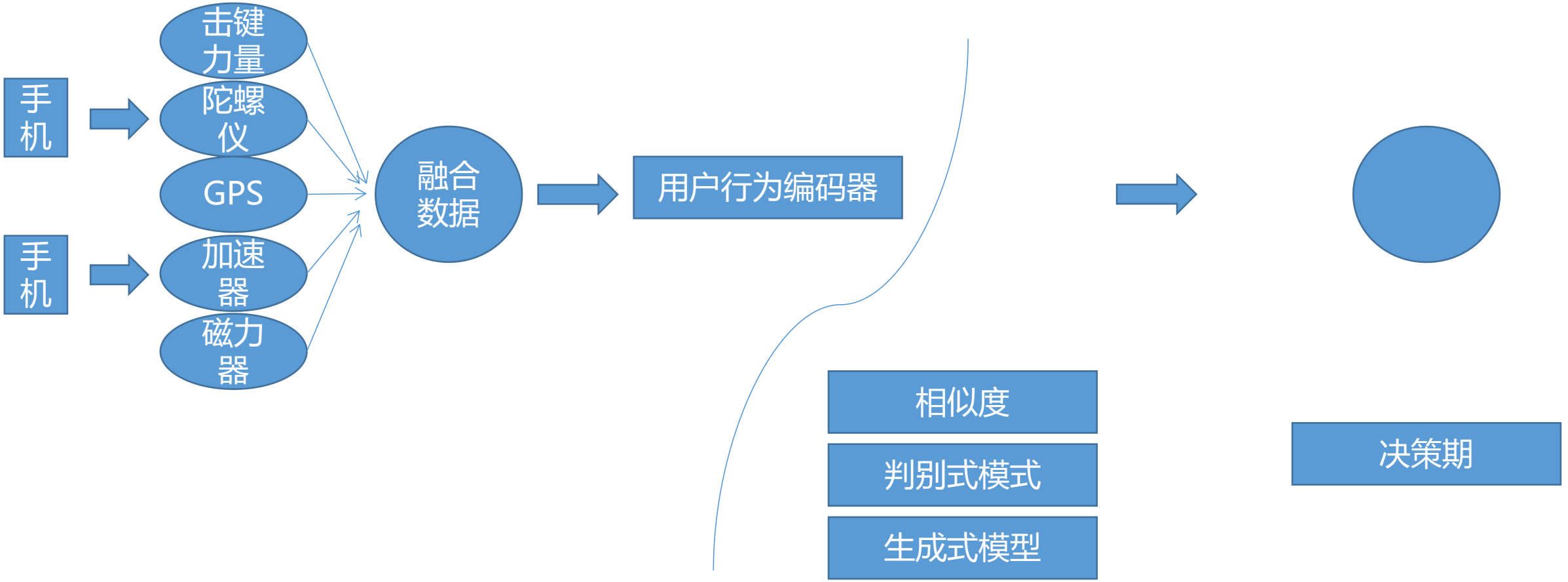
5.2.2无感认证的基础

无感认证的验证系统的构建思路

数据采集（输入空间）

生成用户行为习惯空间（特征空间）

在空间中映射一个点或分布



二、体系构建 第5章基于用户行为的生物探针

5.3生物探针的应用场景

应用场景

1、登录场景

2、小额转账免短信场景

3、支付免密场景

4、信用卡、消费、信贷申请场景

二、体系构建 第5章基于用户行为的生物探针

5.4小结

生物探针与设备指纹相比，其缺点是采集上报的数据包较大，容易受网络波动影响。

未来可以通过终端智能计算、5G边缘计算解决网络传输带来的问题。

生物探针未来在风控领域必然有广阔的应用前景，融合了移动安全、5G和机器学习三大技术领域，

能够提供更强的风控效果和更优雅的客户体验。

二、体系构建 第6章智能验证码的前世今生

目录内容
6.1验证码的诞生
6.2验证码的攻防
6.3设计一款优秀的验证码
6.4小结

二、体系构建 第6章智能验证码的前世今生

6.1.验证码的诞生

2000年，雅虎公司面对的问题：一些恶意的计算机程序伪装成青少年在个在线聊天室，收集聊天者信息并且散发其他公司的促销广告。为了对抗这些恶意程序的攻击，雅虎工程师依照图灵测试的思路，设计了一种完全由计算机自动生成，并判断回答者是否是一个真实人类的反向图灵测试。

二、体系构建 第6章智能验证码的前世今生

6.1.1验证码的本质

6.1.2验证的发展

二、体系构建 第6章智能验证码的前世今生

6.2验证码的攻防

6.2.1.1传统识别方法

1、对图片做二值化处理

2、通过腐蚀去除剩下的噪点

3、利用一种垂直投影的方法

4、对所有的字符进行规范化

二、体系构建 第6章智能验证码的前世今生

6.2验证码的攻防

6.2.1.2AI识别方法

6.2.2新型验证码的识别

6.2.2.1滑块拼图验证码识别

6.2.2.2图文点选验证码识别

6.2.2.3打码平台

6.2.3对抗黑产的方案

6.2.3.1新的验证类型

6.2.3.2轨迹模型

6.2.3.3多维度赋能

二、体系构建 第6章智能验证码的前世今生

6.3设计一款优秀的验证码

6.3.1设计标准

6.3.2设计实战

6.3.2.1空间旋转码验证

6.3.2.2空间推理码验证

二、体系构建 第6章智能验证码的前世今生

6.4小结

验证码是历史悠久的风控产品。

从风控角度分析，验证码是抵御攻击的最后一道防线。

从用户体验的角度分析，验证码又是一个有可能影响用户体验感受到的风控产品。

验证码的最理想状态是对正常用户无感，对异常用户弹框。

二、体系构建 第7章风控中枢决策引擎系统

目录内容

二、体系构建 第7章风控中枢决策引擎系统

1、定义

决策引擎是整个风控体系的核心枢纽，踏实买你想风控运营人员设计的，

以规则编辑和规则执行为主要任务的计算，通常还包含了灰度测试、数据统计分析等功能。

作为风控体系的中枢系统，决策引擎会对接终端风控系统、实时指标计算平台、风控数据画像、机器学习和模型平台等各类风控子系统，集中进行风险计算和决策。

2、特点

1）灵活性

2）易用性

3）实时性

二、体系构建 第7章风控中枢决策引擎系统

7.1规则引擎

1、定义

规则引擎是决策引擎的核心，模块主要包括规则管理、规则推送、规则执行等。

2、应用场景特点

1）流程分支复杂，条件判断多，常规编码难以实现，维护成本高

2）不确定性需求多，频率高，随时可能发生业务变更

3）业务规则变更要求实时生效

4）业务变更不依赖开发人员，可以由业务人员直接进行业务变更

二、体系构建 第7章风控中枢决策引擎系统

7.1.1脚本引擎

7.1.2开源规则引擎

7.1.3商业规则引擎

7.1.4几种规则引擎实现方案的对比

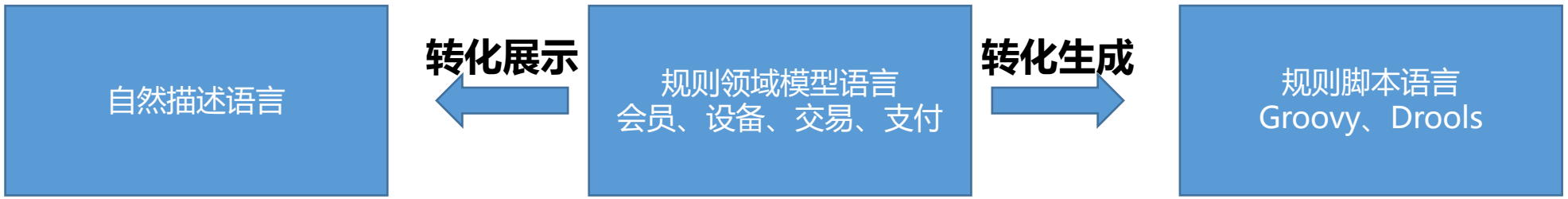
二、体系构建 第7章风控中枢决策引擎系统

7.2规则管理

1、如何储存和执行

1）用户交互使用自然语言

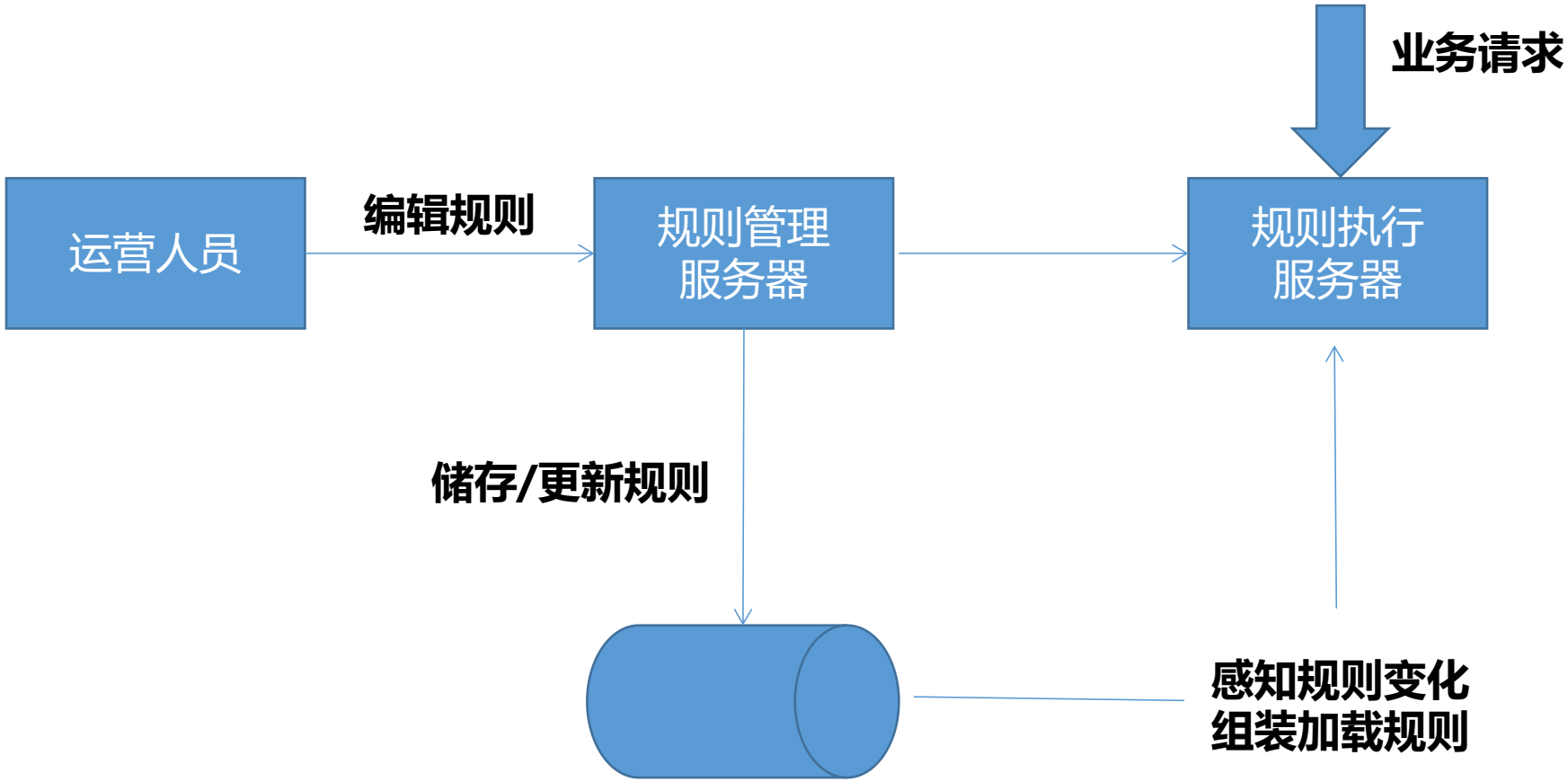
2）领域化的规则使用规则表示语言



规则转化和执行

二、体系构建 第7章风控中枢决策引擎系统

7.3规则推送



二、体系构建 第7章风控中枢决策引擎系统

7.4规则执行

1、执行步骤

1）数据输入到规则引擎

2）规则引擎根据场景选择规则集

3）规则领域模型转换模块，把规则集转换成脚本语言

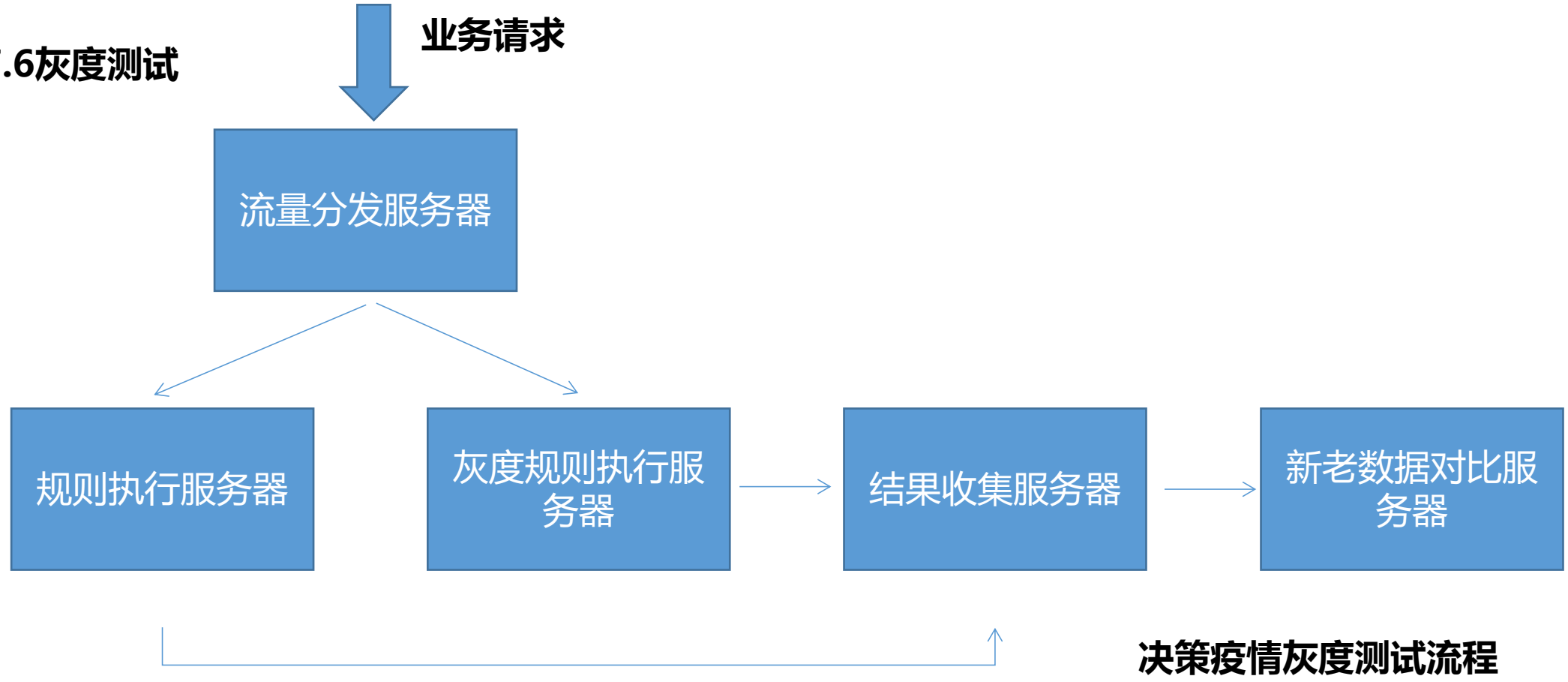
4）脚本引擎加载脚本语言

5）脚本引擎接受数据，执行规则

二、体系构建 第7章风控中枢决策引擎系统

7.5外部系统集成

7.6灰度测试



决策疫情灰度测试流程

二、体系构建 第7章风控中枢决策引擎系统

7.7小结

实时决策系统中的核心组件决策引擎，包括决策引擎中的规则引擎、规则管理、规则推送、规则灰度等。

决策引擎作为业务反欺诈系统的核心必备组件，对风控运营人员快速调整策略至关重要，需要重点保障稳定性和易用性。

二、体系构建 第8章海量数据的实施指标计算

8.1实时指标计算概述

指标类型	示例	可能关联风险
频度-出现次数统计	IP最近5分钟注册次数	次数过多一般对应场景：垃圾注册、短信轰炸
	手机号最近1小时接受短信次数	
频度-关联个数统计	1天内同一设备接受短信的手机号个数	个数过多一般应对场景：群控设备、群控账号
	7天内同一设备充值的账户个数	
活跃天数	账户最近7天内活跃次数	活跃次数过少一般对应场景：僵尸用户
	设备最近1个月活跃次数	
移动距离	设备最近1小时移动距离	移动距离过远一般对应场景：虚假定位
	设备最近24小时移动距离	
常用习惯	账户最近7天常用设备账号	常用信号或城市不一致一般对应场景：账号被盗
	账户组件30天常用登录城市	
趋势计算	账户最近1天内多变交易支付金额递增	支付的趋势一般对应场景：刷卡盗刷
	账户最近1天先小额后大额支付	
其他	账户最近5分钟密码连续错误次数	连续错误一般对应场景：账户暴力破解

反欺诈业务中经常使用的指标类型

二、体系构建 第8章海量数据的实施指标计算

8.2实时指标计算方案

8.2.1基于数据库SQL的计算方案

8.2.2基于事件驱动的计算方案

8.2.3基于实时计算框架的计算方案

8.2.3.1Storm介绍

8.2.3.2Spark Streaming介绍

8.2.3.3Flink介绍

8.2.3.4三种实时计算框架对比

8.2.4实时指标计算方案对比

二、体系构建 第8章海量数据的实施指标计算

8.3反欺诈实时指标计算实践

8.3.1实时指标计算引擎原型

某个风控反欺诈业务场景需求如下，在一个登录风险识别规则集中，需要计算基于设备号属性的多个指标

1、设备在最近5分钟登录次数

2、设备在最近1小时登陆过的账户个人

3、设备在最近1天内登陆过账户个数

4、设备在最近1天使用过的IP个数

5、设备在最近1天的GPS位置移动距离

二、体系构建 第8章海量数据的实施指标计算

实时指标计算引擎的优点

1、速度快

2、节省Nosql内存

3、同一属性新指标上线快，无需积累数据

8.3.2数据拆分计算

优点

1、按需要储存数据

2、使用指标查询时，不浪费网络宽带和应用内存

二、体系构建 第8章海量数据的实施指标计算

缺点：

1、数据不具有可复用性

2、同一主属性新指标需要数据积累

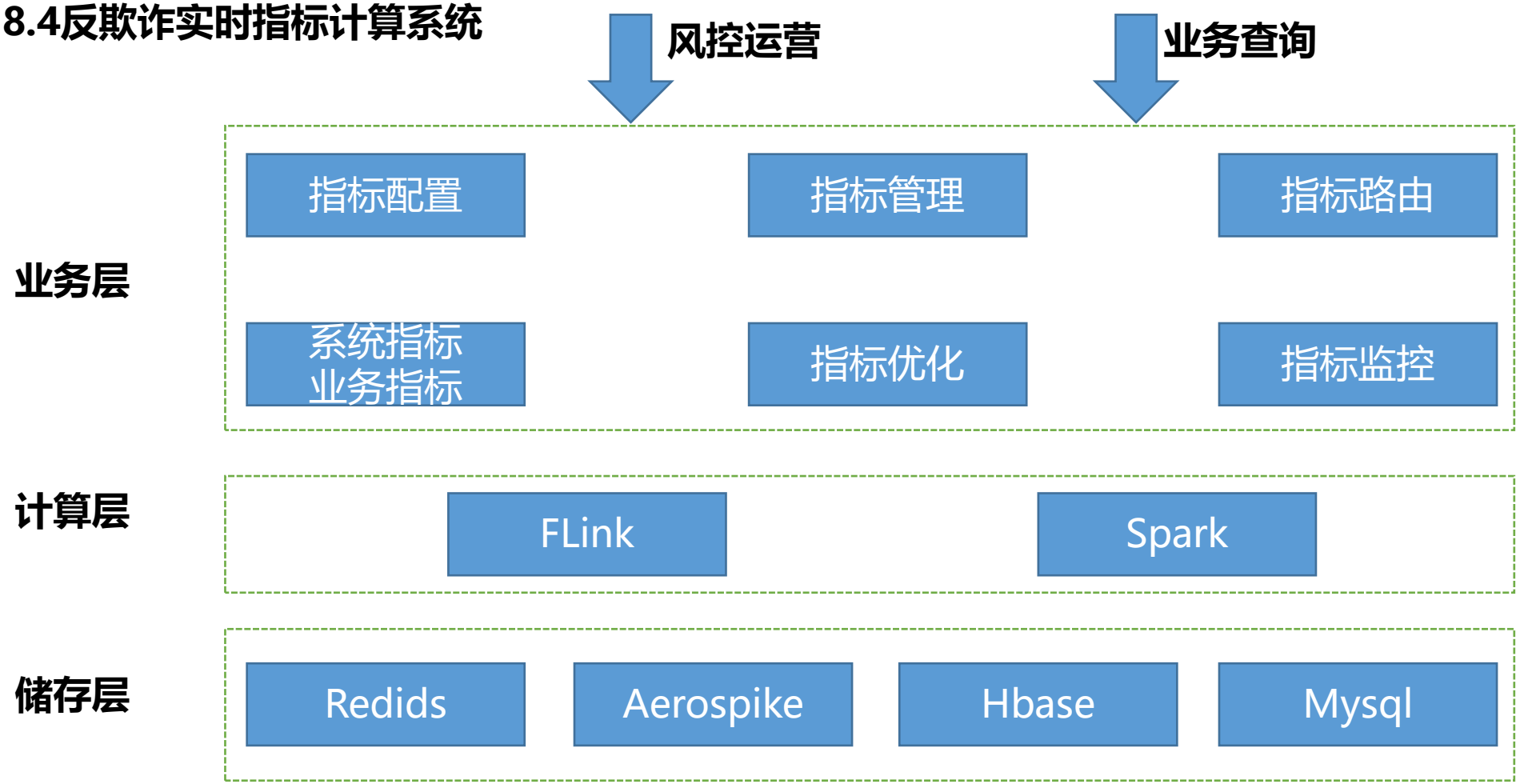
8.3.3分片计算

8.3.5引入Flink

8.3.5Lamda架构

二、体系构建 第8章海量数据的实施指标计算

8.4反欺诈实时指标计算系统



实时指标计算系统架构

二、体系构建 第8章海量数据的实施指标计算

8.5小结

当前各大中型互联网公司在风控反欺诈业务中，基本都创建了基于开源或自研技术的实时指标计算平台。

实时计算框架凭借其稳定可靠、开发高效等特点，已经成为实时指标计算系统必不可少的核心模块。

二、体系构建 第9章风险态势感知系统

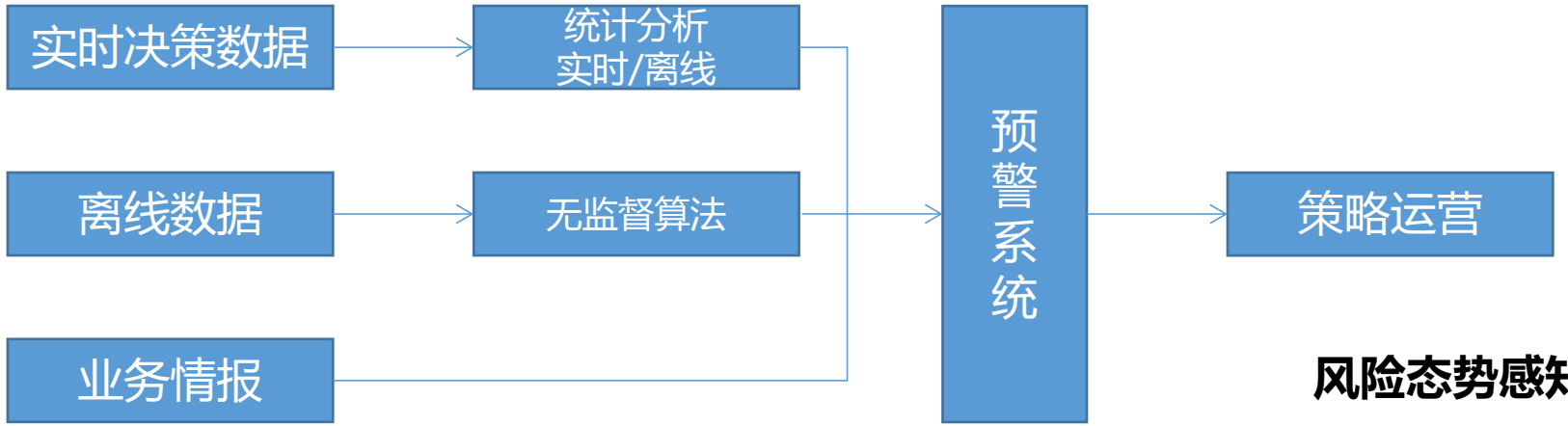
目前面临的挑战

1、专业的水平差异性

2、黑产攻击收发多变

3、运营人员操作风险

4、产品和系统bug



风险态势感知系统整体流程

二、体系构建 第9章风险态势感知系统

9.1基于统计分析的方法

1、核心风险事件数据

主要指分开系统中产生的数据，包括实时决策系统的入参、出参、中间计算结果、决策结果

2、核心业务数据

主要指业务自身的核心数据指标，和具体业务场景有关，如电商、O2O、直播等各不相同

二、体系构建 第9章风险态势感知系统

9.1.1核心风控指标数据

1、调用量

2、拒绝率和拒绝变化率

3、人审率和人审变化率

4、PSI

5、字段获取率

二、体系构建 第9章风险态势感知系统

9.1.2核心业务数据

1、交易金额的同比/环比数据

2、退货率的同比/环比数据

3、地域分布

4、商家分布数

5、类目分布数据

6、营销优惠券的使用数据

二、体系构建 第9章风险态势感知系统

9.2基于无监督学习的方法

一般步骤

1、特征抽取

2、建立连通图

3、组群聚类

通过无监督学习方法发现风险后，可以和实施决策进行对比。

如果无监督学习方法比实时决策的增益率高，则需要关注当天的数据，业务有被攻击的可能

二、体系构建 第9章风险态势感知系统

9.3基于欺诈情报的方法

举个例子

一个欺诈情报风险态势感知预警实例，通过语义分析可以准确提取情报主题（客户名）、类型（薅羊毛）手法（新用户抽奖）等信息，及时预警给风控运营人员进行针对性防控

二、体系构建 第9章风险态势感知系统

9.4预警系统

1、同比

2、环比

3、均值

4、最大值

5、最小值

6、欺诈情报特定类型

7、无监督算法增益率

以上的指标，可以用调用量、时间等数据进行条件组合

二、体系构建 第9章风险态势感知系统

9.5小结

系统故障、运营疏忽、黑产技术绕过等原因会导致实时决策系统产生漏杀和误杀

数据驱动、AI驱动的及时有效的风险态势感知系统是被动运营转主动运营，人工运营转自动化的必经之路

二、体系构建 第10章风险数据名单体系

10.1名单体系的价值

10.2名单体系的设计

1、需要明确哪些数据可以用于建立名单，确定名单数据的关键。常见名单主键：手机号、身份证号、银行卡、IP和各类设备标识

2、需要明确标签的类别

以手机号码名单建立过程为例阐述名单的体系设计

基本属性特性、使用特征、风险特征

二、体系构建 第10章风险数据名单体系

10.3名单体系的生命周期

10.4名单体系质量管理

对名单数据的质量进行监控，常规的方式就是持续评估数据的命中率和误杀率。

我们使用的误杀评估方案是按照时间切片统计其趋势，即收集策略效果情况、客户投诉等多方面的因素综合量化评估其变化趋势。

二、体系构建 第10章风险数据名单体系

10.5小结

作为风控体系的基础设施之一，黑名单系统既可以用于拦截黑产攻击，也可以生成风险标签成为复杂业务模型的输入参数，其价值和重要性在当前黑产攻击手段不断翻新的情况下依然不可低估。

二、体系构建 第11章欺诈情报体系

1、定义

黑产团伙在使用哪些资源和技术手段危害互联网业务的正常运营，包括但不限于获取刷单、薅羊毛等黑产攻击事件细节、黑产新型的作弊工具及黑产使用的各类资源信息。

2、趋势

黑产掌握的数据和资源（IP和手机号）非常丰富，对移动安全和机器学习领域的新技术也能够非常快速应用于实战。

欺诈情报的价值在于，帮助防御方更快捷的掌握相对丰富的黑产动态和信息，更快速、更准确的决策。

二、体系构建 第11章欺诈情报体系

11.1情报采集

一般通过卧底黑产网络、监控黑产论坛等方式进行。

根据采集内容和方式不同，分为：数据情报、技术情报和事件情报。

11.1.1数据情报

能够沉淀手机号、IP、设备及邮箱账号等黑产名单数据的情报信息。

11.1.2技术情报

针对某一种欺诈技术的详细信息，包括原理、用途、危害等。

11.1.3事件情报

情报体系获取的某欺诈事件即将发生，正在发生或已经发生过的信息均可成为事件情报。

二、体系构建 第11章欺诈情报体系

11.2情报分析

文本情报的分析过程

二、体系构建 第11章欺诈情报体系

11.3小结

欺诈情报体系的效果取决于运营和数据分析能力，通过运营打入黑产团伙内部获取更多的情报来源。

通过数据分析快速挖掘、判断高价值情报，两者缺一不可。