数据生命周期

数据安全治理，首先要能够发现数据流转行为。

内部系统的调用，外部系统的调用，数据库的读取等都属于数据流转。

数据流转的发现，依赖于完善的日志及日志解析。如果某系统日志未记录数据流转日志，那么就存在着黑洞，无法发现就无法预防风险，无法审计。

将所有系统的数据流转行为统一入库，不同系统使用不同标识符。不同系统按不同的行为规则进行安全审计。

数据加密，防黑客。数据必须经过自研系统才能正常使用解读。

时间-系统-接口-调用人-调用结果-IP

数据源：源数据库。mysql-audit，操作审计。

数据系统：业务系统，内部系统，消息队列，日志系统。完善的日志及解析及审计规则。

数据终端：员工PC电脑。DLP

能够发现是否有爬虫。

有用户在极短时间内，大批量调用某接口，可能存在爬虫或黑客攻击