财务公司如何数字化转型？给你打个样儿

日志易

客户介绍

浙江省能源集团财务有限责任公司（简称“浙能财务公司”）是经中国银保监会批准成立的非银行金融机构，成立于2006年8月28日，是浙江省能源集团有限公司控股的下属金融公司。浙能财务公司是新《企业集团财务公司管理办法》颁布以来成立的全国第一家财务公司，也是中国境内第一家引进国外战略投资者的财务公司。

经过多年IT运维建设，浙能财务公司已经建立起完善的运维体系，但随着大数据时代的到来，以及国家对网络安全等级保护管理要求的提高，公司急需建立一套日志集中管理分析系统来满足业务系统日志管理与分析的需求，进而实现运营分析、实时告警、事件回溯、故障的快速分析、追踪和定位以及满足合规审计等。

业务挑战

- 日志量大且格式繁杂，无法统一管理、规范并满足合规
- 故障定位有延迟，排障成本高而效率低
- IT 资产杂乱无章，安全性无法保障
- 运维数据无法及时呈现，价值密度低

为什么选择日志易

浙能财务公司目前处在由传统运维模式向智能运维模式的转型过程中，但仍无法高效实现数据统一采集管理、IT 资产管理，智能数据分析与指标智能可视化，快速分析故障定位根因等需求。

借此，浙能财务公司结合日志易自研搜索引擎Beaver的强分析能力，通过AGENT、SNMP、JMX等方式采集各系统运行信息，目前接入设备数量近200台，监控指标近7000个，触发器近3000个，自动发送告警信息至统一事件处理平台，在告警收敛、多事件关联分析、聚合处理等处理流程之后，向相关人员发送短信通知，生成事件工单，充分实现了数据统一管理与主动智能运维。

数据分析结果的多维智能可视化，同时也为浙能财务公司的业务运营提供了高效可靠的判断依据，同期配置的在线日志审计查询模块，满足了网络安全法对日志记录与存储的要求。

实现价值

轻松满足合规，智能日志分析

浙能财务公司建设了统一日志管理平台，能够对环境中的服务器、操作系统、数据库、应用程序、中间件、及安全设备等产生的日志，进行统一采集管理、规范存储，满足“重要日志数据需存储180天”的合规要求。此外，平台自动发送数据到指定的备份路径中，并支持对应的索引数据过期后手动恢复，供相关人员继续搜索分析。

日志易自研的Beaver是一个分布式搜索引擎，具备高可靠性和高性能。在Beaver的加持下，平台可通过系统自带或相关用户配置的规则解析日志，抽取关键字段，将非结构化的日志转化为结构化数据。此外，平台还支持时间文本索引和全文检索，配置了丰富的API用于索引、检索或修改大多数功能设置，实现TB级数据秒级检索溯源，让相应权限的工作人员可以像使用网络搜索引擎一样搜索日志数据。

统一资产管理，自动工单系统

在统一日志管理平台之上，浙能财务公司启用了日志易SIEM平台中的IT资产管理功能，通过CMDB数据库，相关人员可自定义管理资产的添加、修改、删除、查询和统计，并且将安全事件与资产相关联，实现了IT设备、IT服务等数字资产的统一管理。

工作人员可在平台上进行数字信息整合分析，实现数字资产高效管理，进而形成硬件、软件以及IT服务之间的物理和逻辑关系映射，将各部分的依赖关系可视化。如此，运维人员可轻松确定内部组件对业务运营的潜在影响，大幅提升流程运作效率，保证了资产数据的唯一性和准确性。

动态阀值告警，自动化巡检，安全智能运维

平台通过智能数据分析，解析提取不同类型的安全事件日志，统一标准化输出。之后，对比不同设备中的日志进行攻击溯源分析。平台支持行业内五大类数十种的主流机器学习和统计分析算法，对海量历史数据进行机器学习，实现动态趋势分析及预测。

同时，平台已经关联CMDB模块，通过对接各类漏洞扫描系统，可自动分析判断设备是否存在漏洞，同时关联设备详细信息，并可将信息自动推送给相关负责人。平台动态阀值预测告警体系已形成逻辑闭环，可大幅减少异常指标检测的发现时间，实现系统实时预警，为浙能财务公司的整个系统附上坚实的“金钟罩”。

浙能财务公司统一日志管理平台还配置了知识管理模块，内置海量安全知识，工作人员可在相应权限内进行检索学习，同时也可进行相应的设置。此外，平台可通过智能数据分析功能实现自动化巡检，并生成报表。

业务、运维、安全、性能总览，多维智能可视化大屏

日志易根据浙能财务公司需求，为平台配置了安全事件大屏、业务大屏、系统性能大屏以及事件总览大屏。

安全事件大屏： 可智能展示目前所有安全事件，定位异常攻击情况的分析结果，并以地图形式展示攻击来源。此外，安全大屏可实时展现设备登录情况，识别出包括非工作时间、绕过堡垒机登录等异常情况。

业 务 大 屏： 配置了N9系统，实现业务全网关指标可视化展现。

系统性能大屏： 对网络设备、主机设备、数据库等硬件性能进行可视化分析与展现，可快速定位性能问题。

事件总览大屏： 主要供运维监控人员使用，事件总览大屏实时汇总并展现系统中所有的异常事件，方便运维人员快速判断系统运行情况，当出现异常时可以快速定位问题，并进行处理，大幅提升运维效率，保障用户体验。

浙能财务公司统一日志管理平台基于日志易国产自研的高性能搜索引擎Beaver，搭配平台特有的SPL语言，对用户行为和业务运行状态进行多重关联分析，通过交互式、实时数据大屏来帮助运维人员发现、诊断业务问题，实时了解包括业务网关访问成功率、访问趋势环比、实时访问QPS、业务来源分布、VPN、网络、主机设备登录情况等各类指标的整体情况，真正实现了数字化管理，智能化运维。

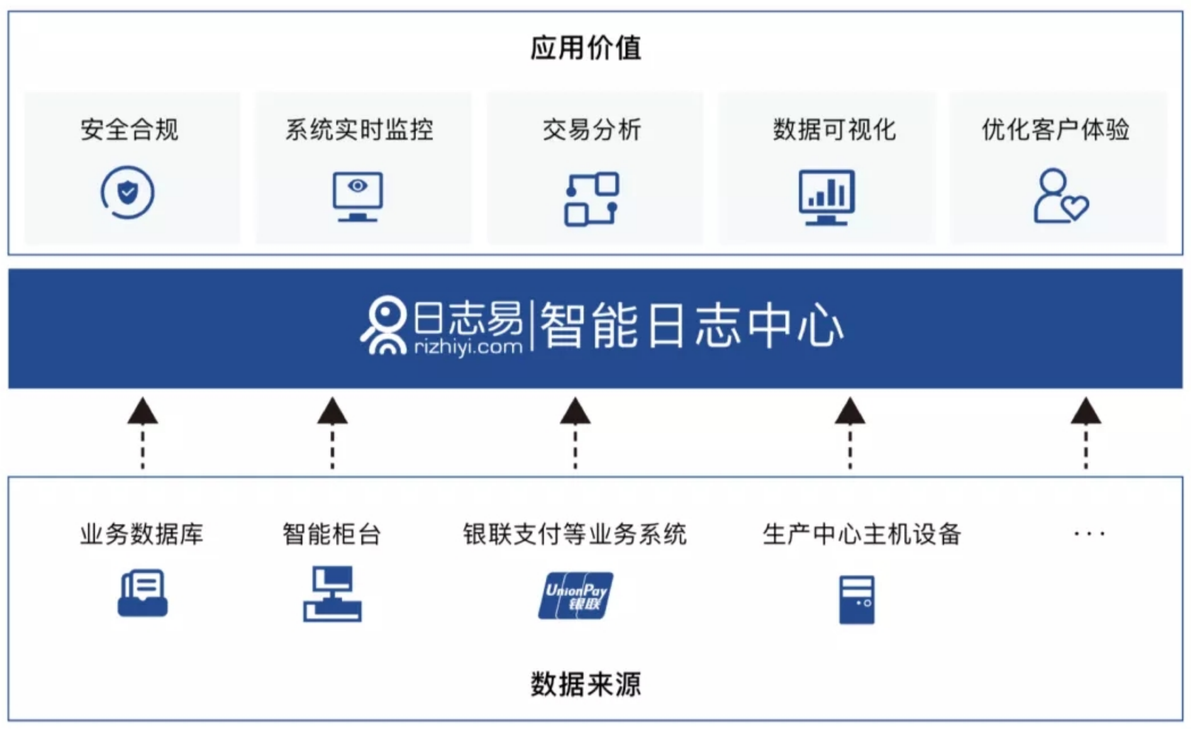
案例解读 | 实时监控业务状态，提升服务保障与用户体验

日志易

背景介绍

某城商银行：实时监控业务状态，提升服务保障与用户体验

该金融机构致力于提供综合性金融服务，自身IT基础设施建设完备，拥有独立运营的网银、手机银行等电子银行系统，为用户提供7*24小时的互联网业务支持。该金融机构为更好掌握自身IT系统状态及提升用户体验，选用日志易打造智能日志中心。



IT需求及挑战

- 日志数据量庞大且格式复杂，难以有效利用
- 无法掌握业务系统健康度，交易状态、风险不可控
- 出现突发性服务中断时，需消耗较长时间排查根源，难以保障用户体验
- 监控手段传统， IT人员投入大量精力、重复巡检

为何选用日志易?

该金融机构建设有互联网支付、短信平台、网贷、呼叫中心等数百个系统支撑自身业务数字化发展，IT系统在每笔交易背后都发挥着巨大价值。面对如此复杂多样且不断升级的系统环境，IT部门压力陡增，除要面临保障应用的正常运行需求外，在控制人员成本的基础上更需要面临日均近千万交易笔数的业务开展的基本要求。行方IT部门为能实时、清晰地了解自身系统运行状态，保障平台用户业务顺利完成，提升用户体验，决定选用日志易搭建智能日志中心，实现系统的实时监测、数据可视化、业务高可用等需求。

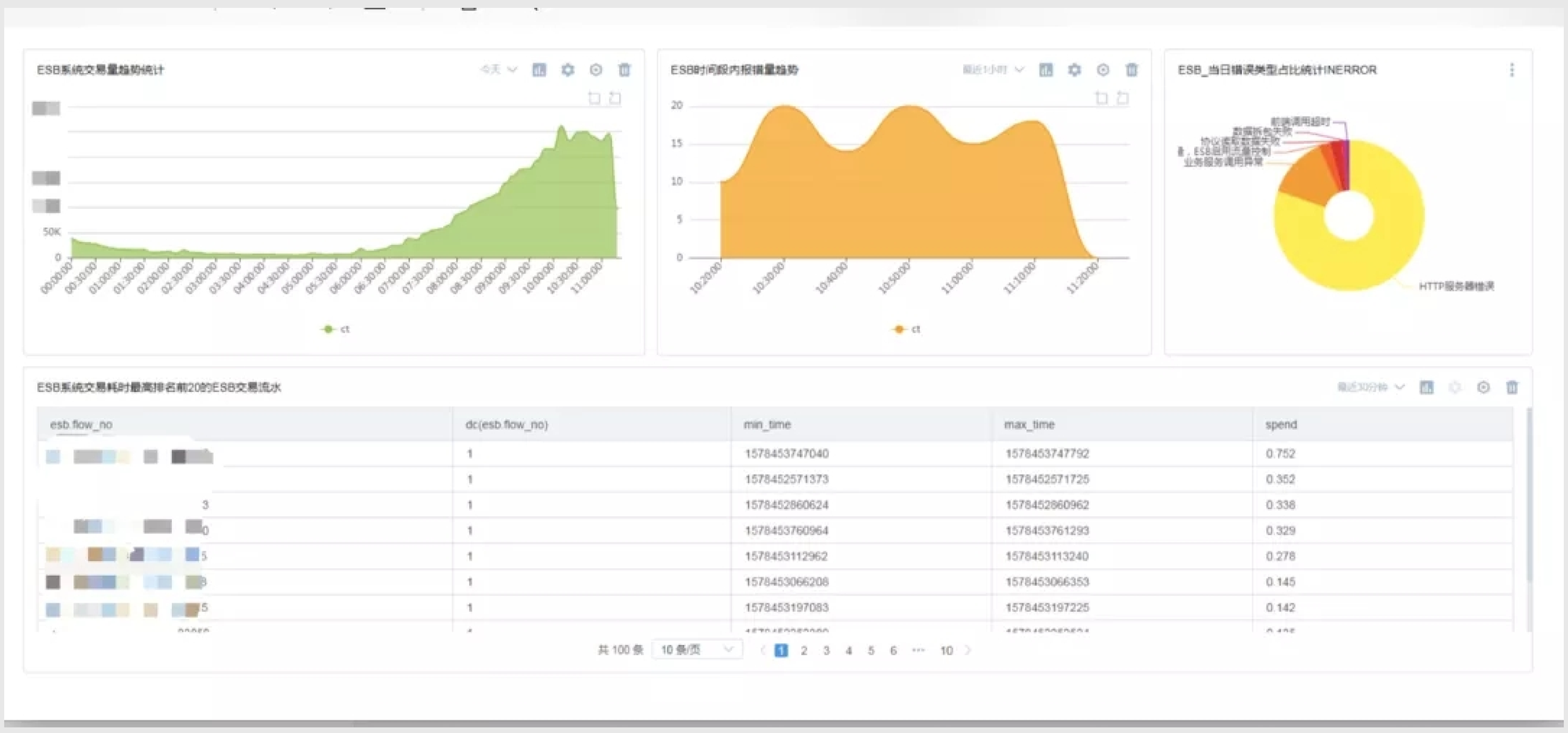
客户收益

日志数据集中管理，安全合规

随着该金融机构自身业务规模不断发展，其IT系统每时每刻都在产生海量日志数据，种类多样，包括交易、操作、应用系统等类型日志，这些数据散落在生产系统各个角落，难以集中管理，大部分日志在暂存一段时间后将被永久删除。根据国家等级保护及网络安全法要求，行方需对日志数据进行至少六个月的集中存储及必要分析。其借助日志易智能日志中心可实现日志数据的快速检索、数据分析及可视化，降低了IT人员操作风险，提升了日志数据的安全访问标准，满足安全合规要求。

异常交易监控及排障，降低业务风险

该金融机构IT部门除维护上百个系统的正常运行外，还需要管理各类主机、交换机、网络设备等，日常工作量大，难以实时发现系统异常。当支付、交易等业务出现失败时需重启跑批业务，若运维人员未及时发现、处理，会严重影响客户体验，行方也将面临投诉风险。该金融机构将数百个系统及数百台设备的日志数据统一采集到日志易平台进行管理后，IT管理员可按需对日志数据分析，辅助其实现跨系统交易实时关联查询，交易异常定位等需求。该金融机构IT人员反馈“目前我们可以实现在客户之前发现异常交易，并第一时间发现问题根源予以处理。日志易帮助团队省去了大量登陆服务器的操作，从而实现几分钟内即可发现问题并进行排查，数十倍地提升了处理异常的效率”。行方IT部门利用日志易建立近100个监控指标并汇总到近20个仪表盘进行可视化展示，业务健康状况清晰可见。



日志易·ESB系统交易量趋势及异常统计分析

保障平台运营效率，提升用户体验

无论是在柜面业务还是电子银行业务办理，都涉及到多个系统的多个组件，如何保障各环节的稳定运行是IT部门的关键任务。利用日志易平台的采集、搜索、分析功能，IT人员由被动告知变主动发现，实现实时监控各组件及系统性能瓶颈，制定告警指标并发送给相关部门予以处理。行方运维人员反馈“短信平台向不同运营商提交短信后返回异常，但是运维人员无法实时发现此类异常，背负很大压力。通过日志易采集短信平台数据库数据，计算出异常短信条数，并制定‘如果大于20条，则触发短信平台运营商故障告警’的风控指标，大大提升平台运营效率。”监控一段时间后发现该故障是由短信服务商通道问题所引发，行方及时请该厂商进行升级完善，从而更好地提升了行方平台用户满意度及提升了IT人员的效率。

基于日志易智能日志中心，用户对自身IT数据资产有了更全面掌握：

- 满足安全合规要求，并形成IT日志数据管理标准化
- 监控及管理支付系统、数据库及应用系统等IT基础设施的可用性
- 分析识别业务交易超时、失败和错误等高风险事件
- 灵活的跨系统数据分析及可视化功能，帮助IT人员提高能效
- 优化提升客户在互联网端、设备应用端的体验

客户的声音

日志易系统投产后使用广泛，产品操作简单、灵活，针对各类系统日志的搜索变得尤为方便。同时，日志易自带监控模块，使得IT部门对自身系统运行监控的方式更丰富、更精确。

银行业解决方案丨一文读懂银行业如何挖掘日志大数据价值

日志易

背景介绍

银行业日志繁多复杂，日志“金矿”亟待挖掘

随着金融科技应用的不断深入，银行业面临着前所未有的机遇和挑战。伴随各种科技手段产生的数据，已经成为现代银行业的核心战略资产，对各类数据的有效挖掘分析，可以大幅提升银行的业务运营水平，提高盈利能力。

长期的业务发展为银行积累了大量的日志数据，大致可分为交易日志、运维和操作日志、应用日志、系统日志及网络日志，其中既有结构化的，也有非结构化的，涵盖业务数据以及IT运维数据等。传统的数据分析手段，往往很难兼顾各类数据的处理，因安全和权限等设计考虑，跨业务系统的数据分散孤立，难以发生关联，无法从整体视角监控业务健康度并进行优化。此外，这些日志大部分都被设置了清理策略，在暂存一段时间后将被永久删除，日志中隐藏的价值未被充分挖掘。

精准定位
针对具体需求，全能解决方案

依托自助运维平台，全行日志集中管理

业务挑战

a.因对接大量监控运维系统，主机需要安装多个Agent，且Agent资源消耗高；数据清洗依赖厂商；数据封闭，无法共享

b.作业平台、硬件存储器等设备无监管手段

c.远期数据使用频率低，保存成本低，调用成本高；近期数据使用频率高，保存成本高，调用成本低

d.用户群较多，管理员无法逐个进行维护、配置分析规则和输出页面

功能亮点

集中采集，超级Agent

实时分发，数据工厂

自助运维，全局展现

解决思路

1. 采集、预处理层，解决不同系统重复采数问题

按技术栈组织功能，启用进程资源控制机制；图形化封装正则表达式编写过程；流式技术解决动态窗口事件一致性分发。

实现价值

- 处理延时从秒级下降到毫秒级
- 计算模式增加动态滑窗功能
- 支持更多的分发目标对象
- 图形维护界面

2. 全域运维数据采集，监控覆盖无盲点

Agent加载插件，适配对应的设备类型；基于SPL的统计分析做告警规则。

实现价值

- 运维全覆盖
- 非标设备发生异常，实时告警

3. 互联网金融，解决高并发下的实时分析与应对

确定主KPI（失败原因、交易耗时、交易流水清单等）；权限下放，业务部门自行制定故障判断标准；根据功能码、点击量反向监控未上线成功的功能。

实现价值

- KPI内的故障，可设置实时微信告警，且在仪表盘展现
- 随时可增加新的监控规则
- 实时生成报表，版本功能码执行清单

4. 融合远近数据管理机制，解决高低频数据使用成本问题

近期数据，使用索引保存；远期数据，使用离线存储；近期数据自动滚动到远期数据存储区域。

实现价值

- 页面无缝查询近期或远期数据
- 后台自动转换数据集
- 无感流畅操作
- 远期数据查询返回延时远低于传统离线方案

5. 数据使用向导式，解决平台的推广技术门槛

通过权限配置，使功能和数据模块分离开；向导式分析配置，用户可自行制定分析规则。

实现价值

- 易推广，有助于提升企业各部门的参与度
- 易积累，使最终用户制定的分析规则更精准

日常运维降本增效，减少人工误操作

业务挑战

a.巡检任务技术难度低，可重复性高，容易出现人员懈怠情况；人工巡检数据，无法有效回溯分析规律
b.技术层面上，无法封堵所有可能的违规点，无法及时发现某些简易但违反安全制度的操作
c.日常运维存在大量申请登陆主机查日志的工单；必须进入ECC操作室登陆主机；存在一次分析需要登陆多台主机的问题
d.各部门运营均需重新进行数据收集、处理、分析等，工作量大，且涉及跨部门数据集成难度大

功能亮点

自动化巡检，行为操作审计　　智能告警、管办分离　　关键设备细颗粒性能对比

解决思路

1. 日常巡检自动化，解决人工效率、准确性、数据积累问题

基于对象、KPI做相对应的检测脚本；数据做标准化时间戳处理，形成历史纪录。

实现价值

- 单次巡检，可配置异常告警
- 可快速分析过往巡检历史数据
- 巡检结果，可设置为IT可视化的一部分

2. 操作类数据审计，解决安全制度执行的有效性监管问题

收集堡垒机、工单等系统的数据，做判断基准；收集各设备对象数据做分析数据源；将操作数据与基准数据做匹配分析。

实现价值

- 实时告警绕堡垒机、高危指令等行为
- 报表提醒非变更窗内的操作行为、对象、人物等

3. 日志管理Web化，免去人员误操作风险

部署Agent，实时采集运行日志；做区域Agent代理，解决流量并发问题；一键安装，Agent安装权限下放给使用部门。

实现价值

- 工位Web方式查询日志
- 分析规则业务部门可自定义

4. 关键设备性能基准化，解决长周期历史运行规律问题

以时间为主维度，对比不同的KPI，找出异常KPI；以KPI为主维度，对比不同的历史周期，确定异常的时间范围。

实现价值

- 平台可自动报告某个对象或指标存在异常
- 规则清晰，且支持实时调整

5. 自动化运营，建设智慧营业厅

利用日志易提供的运维数据集中优势，省去人工整理数据的工作任务；利用日志易提供的数据工厂功能，实时捕获清洗后的数据。

实现价值

- 降低人工成本，各部门可将精力聚焦于业务
- 各部门运维需求可快速完成交付，提升运维效率

故障快速排查定位，追溯根因全局可视

业务挑战

a.无法实时知晓当前业务系统的运行状态与相关联对象是否有异常
b.大多数管理员，无法度量系统运行的健康度

功能亮点

业务运行拓扑图　　交易状态追溯表　　交易明细窗口查阅

解决思路

1. 业务拓扑图，可视化业务及支撑对象的实时状态

采集全部对象的日志、记录数据；数据做结构化，并时间对齐；按业务逻辑，组织拓扑展现视图；指标数据，采用时序、对比等多种方式。

实现价值

- 业务状态实时展现，系统状态量化
- 关键节点指标实时展现
- 关键路径清晰可见

2. 业务运维标准化，建立全行业务运维的KPI体系

建立标准的KPI指标（交易量、交易耗时、交易状态等）。通过分析应答报文、按渠道号分析和统计；通过历史数据，提供多日同时段数据环比趋势。

实现价值

- 标准化输出业务系统的运行状态
- 运行指标时间轴趋势展现，波峰波谷一目了然

3. 时间窗，解决关键事件的小范围快速信息定位

所有数据都是使用标准化时间格式；时间范围工具，输入参数，自动±时间窗口。

实现价值

- 大幅缩短排查故障时间
- 以时间作为参数，自动化传递到其他对象数据，效果更精准

端到端全链路分析，运营决策有据可循

业务挑战

a.每一笔交易都对应海量日志，人工无法快速准确地判断故障点
b.对于单笔交易是否存在风险，无参考基准，无法判断
c.在各个系统间，无法判断请求方或应答方是否按照约定执行了正确逻辑

功能亮点

运行指标数据化、决策化，运行分析智能化

解决思路

1. 微服务调用链，解决业务端到端全流程监控问题

在各业务系统的模块调用入口，外挂“微服务调用框架”代码，使得每一笔交易都能记录父或子进程号，响应时间等数据。

实现价值

- 实现单笔交易的端到端全流程可视化
- 可快速定位故障，异常根因清晰明了

2. 运营日志数字化，量化业务系统的性能状态

基于开始、结束、线程号，判断单笔交易；基于历史同时间（1分钟），做安全基准；使用中位数算法，避免历史故障事件对基准偏差影响。

实现价值

- 单笔交易的性能可视化，可决策化
- 单个交易码的交易性能可视化，可决策化
- 业务系统的交易性能可视化，可决策化

3. 交易轨迹链路化，解决请求应答的匹配问题

定位请求报文、应答报文；结构化报表，形成字段列表；根据交易流水号、内部ID、及其他相同字段值相似的数量多少，推荐请求、应答报文组合。

实现价值

- 不再需要人工梳理业务系统之间的关系
- 可自动串联跨系统之间的请求、应答报文
- 交易路径可视化，进程清晰可见

总结

目前，已有多家银行头部客户依托日志易建设了统一日志管理中心，实现了日志数据的合规审计、统计分析、日常运维降本增效、系统故障链路可溯、运营决策有据可循等需求，充分利用了日志数据的深层价值。

部分银行业客户

中国人民银行、中国银行、建设银行、交通银行、招商银行、广发银行、华夏银行、兴业银行、浦发银行、平安银行、山东城商行联盟、北京银行、江苏银行、徽商银行、甘肃银行、富滇银行、农信银、山东农信、山西农信、重庆农商行、无锡农商行、百信银行、瑞穗银行（中国）

案例｜日志易助力保险企业，展现大数据惊人洞察力

日志易

背景介绍

伴随着大数据、区块链、云计算、人工智能、移动互联等新一代信息技术的不断发展与应用，金融科技（FinTech）风起云涌，传统保险企业的运营流程正受到科技和大数据带来的巨大冲击。

而在众多挑战中，海量的日志数据可以说是保险企业运维保障的一大难关，如何管理好这些日志数据，并从中挖掘更深层次的价值，已成为企业当前亟待解决的问题。

保险行业日志现状

1 日志来源众多，格式复杂

在保险企业中，各类网络设备、安全设备、操作系统、数据库、中间件、业务系统都会产生日志数据，格式多样，日志格式不规范，存储复杂且分散，缺乏统一收集和管理的平台。

保险核心系统日志

```
2017-11-13 16:44:33,415 [[ACTIVE] ExecuteThread: '15' for queue: 'weblogic.kernel.Default (self-tuning)'] INFO
cn.sinosoft.webservice.server.infservice.impl.EasyScanInterface - 系统编号：001,系统访问用户名:null
2017-11-13 15:37:02,832 [Thread-3794002] INFO
cn.sinosoft.core.service.qualitycontrol.impl.QualityControlServiceImpl - 影像文件转移通过,单证号码：03000 * * * * *
27471,业务类型：BQ,单证类型：010015
```

linux日志

```
<86>Nov 04 16:29:57 presale-lmx02 sshd[11503]: pam_unix(sshd:session):session opened for user root by (uid=0)
```

防火墙日志

```
<190>Nov 04 16:31:51 2809109150008447(root) 4424361f Traffic@FLOW: SESSION: 10.219.70.195:52996->220.181.7.
165:80(TCP), interface ethernet0/2, vr trust-vr, policy 16, user -@-, host- , policy deny
```

apache日志

```
218.22.19.234 -- [04/Nov/2017:16:32:51 +0800] " POST /bulk/cd30b146c3d74c3dab23fdadcca9a114/tag/log/ appna
me/nqd_0002 HTTP/1.1" 200 64 " http://wldf.hy-game.com/nqd/login.html?user=1176603288&server=MTM5LjE5OS
4xOTEuMjM2fDgwNTF8aHR0cDovL3dsZGYuaHktZ2FtZS5jb20vbnFkLw==&key=1FB0D940618783EA125BC6F80ABD4
1FC&time=150609198&site=nqd_0002&platform=qidian&sign=97E19817A06CD606C346B5BC910C4D11&extparam
=%7B%7D " " Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom...5.0.2883.87
Safari/537.36 " "-" 0.001 0.001
```

2 海量数据，管理困难

保险企业每日产生的日志数据量巨大，并且分散在不同的服务器，运维人员无法集中查看日志，也无法基于海量数据进行数据挖掘及用户行为分析。

3 日志查询原始

很多传统保险企业的日志查询方式相对比较原始，只能使用 less、grep 和 awk 等常见的 linux 指令，无法多维度查询，查询结果慢，并且有风险。

4 无法实时告警

由于缺乏日志分析平台，导致企业无法进行日志的业务逻辑分析和告警，也无法发掘日志的内在价值。

5 日志利用价值低

由于业务系统黑盒，企业不能进行业务逻辑分析，因此，无法细粒度掌控系统全局健康状况。

日志易解决方案

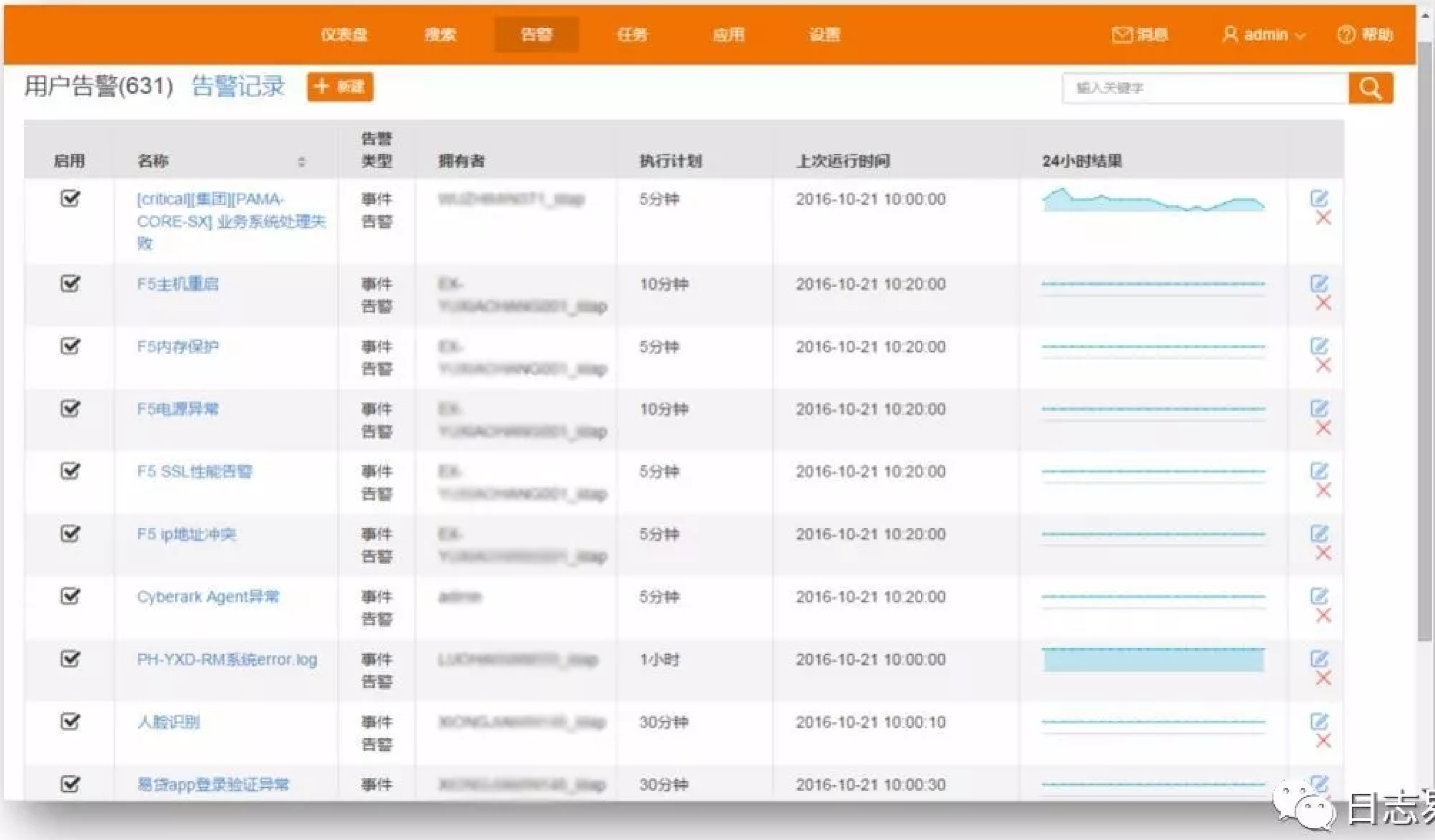
针对保险行业当前日志数据管理现状，日志易搭建统一日志云平台，接入保险企业各业务系统、网络安全设备等日志数据，通过日志易日志分析平台，统一收集、管理日志，并进一步挖掘日志价值，帮助企业进行运维监控、安全合规审计及业务数据挖掘，从而助力保险企业最终实现智能运维。

1 日志集中管理

日志易可统一采集网络设备、防火墙、中间件、保险业务系统、内外部接口（如空中电子签名、保险承保、支付确认）等的日志，提供搜索查询功能，支持多维度查询。利用日志易的海量日志秒级搜索和分析能力，可辅助运维人员快速发现异常，并进行溯源排障。

2 性能、稳定性监控告警

保险企业可利用日志易搭建综合告警平台，分析对比承保业务量趋势，输出趋势图报表，对承保调用过程中各业务环节的耗时进行分析，日志易提供承保调用核保、见费请求承保等关键环节的实时监控、拐点告警功能。



3 核心业务统计分析

日志易还可对契约、保全、续期、理赔等保险核心系统的业务进行汇总、分析，根据关联字段查询详细的业务流程状态，实现业务端到端分析。

保险客户案例场景

针对保险行业当前日志数据管理现状，日志易搭建统一日志云平台，接入保险企业各业务系统、网络安全设备等日志数据，通过日志易日志分析平台，统一收集、管理日志，并进一步挖掘日志价值，帮助企业进行运维监控、安全合规审计及业务数据挖掘，从而助力保险企业最终实现智能运维。

业务端到端分析

某保险企业的车险承保业务经常出现响应缓慢，但无法确定缓慢原因。希望通过日志易对日志进行分析，定位异常时间及位置。

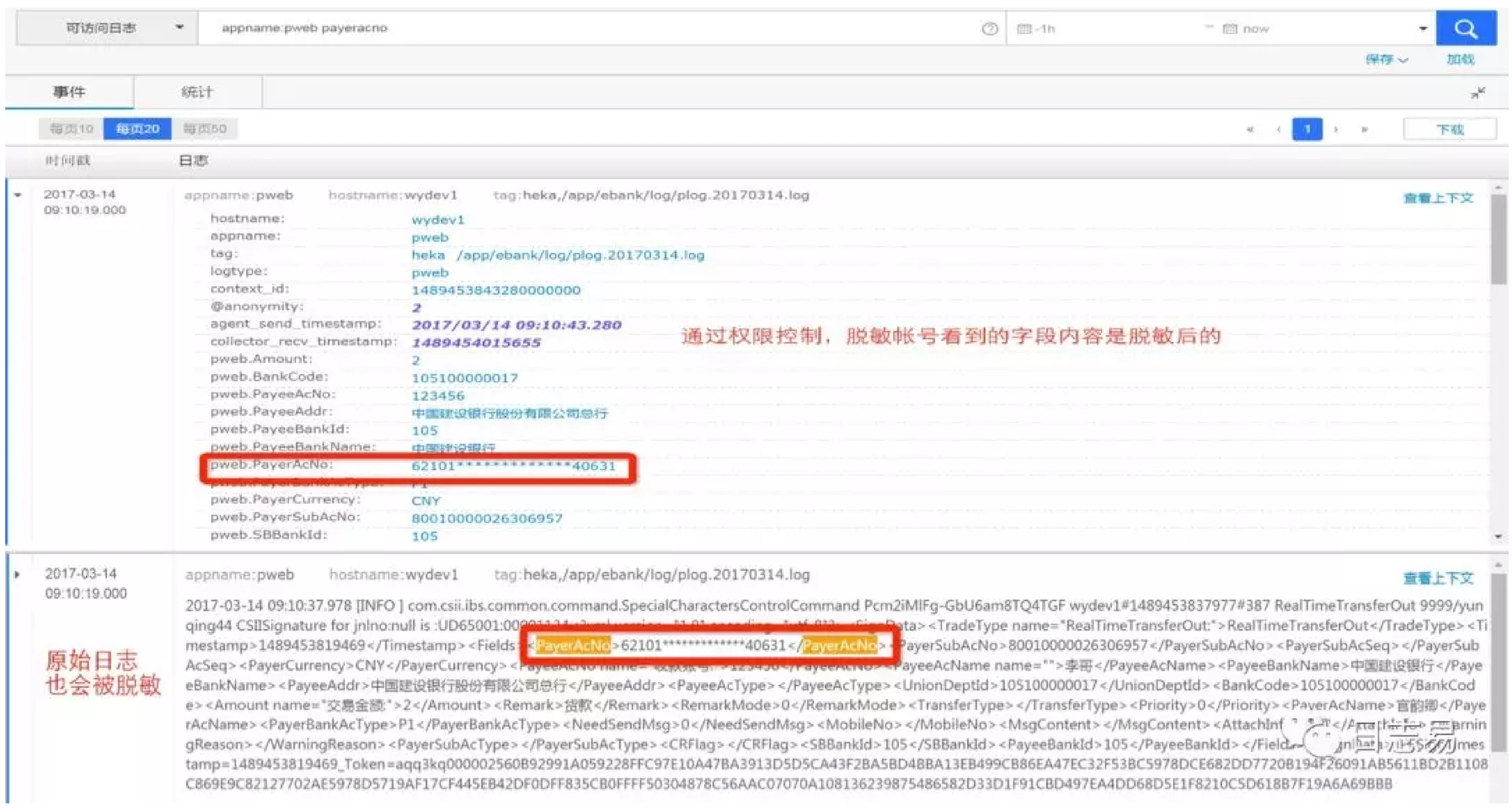
通过日志易承保业务趋势图，可将近期承保业务量进行对比，发现 发生响应缓慢日期的业务量较少，故判定不是由业务量引起的响应缓慢。再通过承保调用各环节业务高峰期每 2 分钟平均耗时分析，可以发现承保调用核保与见费请求承保平均耗时非常大，最高耗时达到 10 秒。

由此，便对承保调用核保与见费请求承保环节进行实时监控，拐点告警，将生成的趋势图制作报表内容，方便每天查看。并对业务系统健康度进行实时监控，包括交易量、业务耗时监控、异常事件监控、内存释放监控，以查找响应缓慢原因。

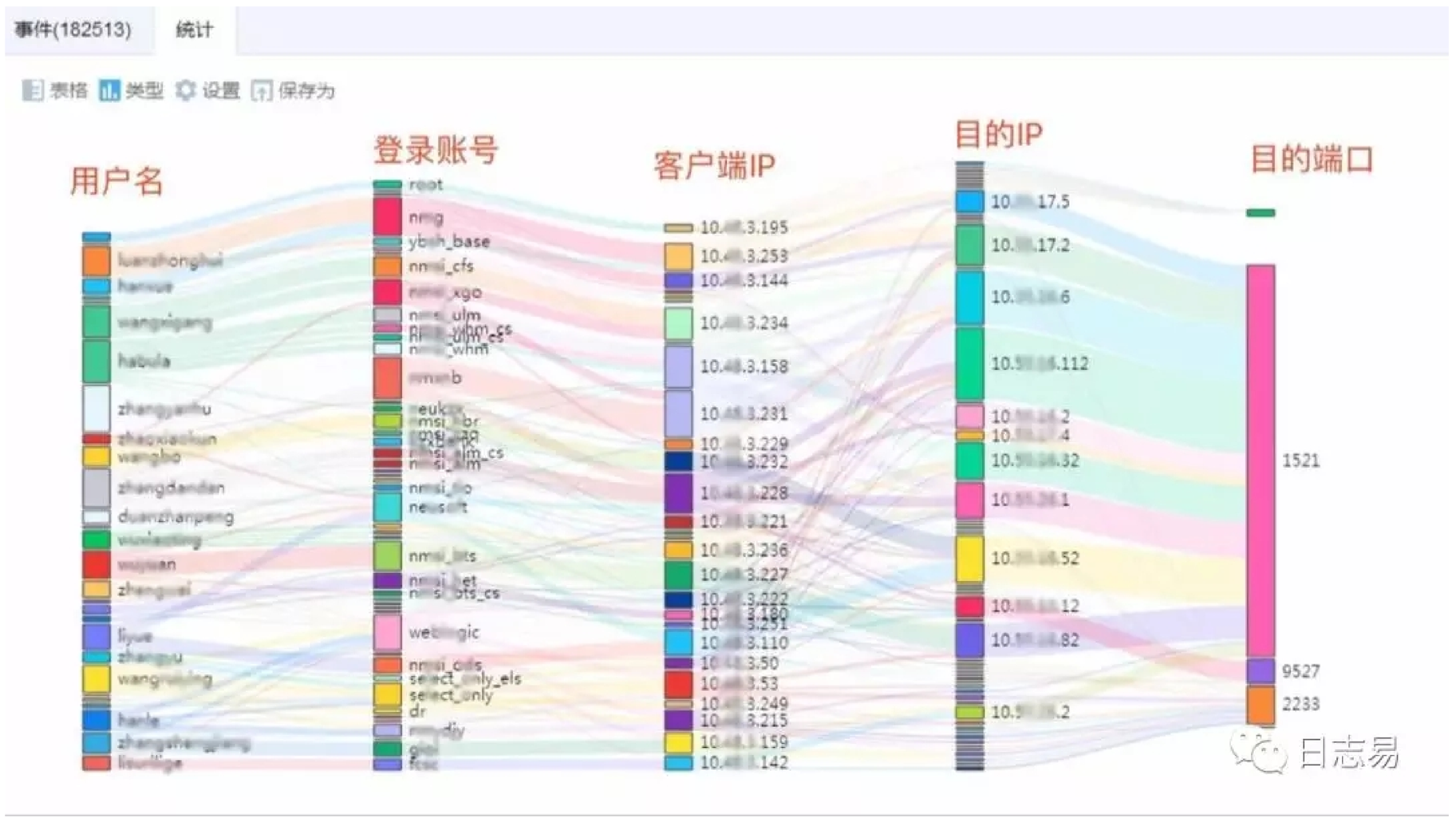
安全合规

为应对国家网络安全要求，某保险企业要求对企业日志数据进行不少于 6 个月备份管理，并对用户敏感数据进行脱敏处理。此外，还需要日志易对内网行为进行分析。

日志易可通过权限控制，使脱敏账号只能看到脱敏后的字段内容，对原始日志和下载后的日志内容进行脱敏，可以全方位保证数据安全性。



此外，日志易还可对企业内部用户的异常操作行为进行分析，包括僵尸账号发现、异常登录统计、高权限切换发现、高风险命令统计等，通过实时监控系统登录数据，有效发现“暴力破解”行为，并同时生成服务器主机失败登录、异常用户登录等不同类型日报，方便企业查看。



机器学习的应用

随着人工智能技术的不断成熟及完善，智能运维已经越来越多的出现在运维人的视野，因此，日志易近两年来也逐步将机器学习算法引入产品中，通过根因分析、数据概要等，缩短故障恢复时间（MTTR），提升运维工程师工作效率，助力保险企业落地智能运维。

日志易解决方案价值

日志统一接入、分用户展现

保险企业部署日志易后，由日志易统一接入日志源，方便日志留存取证，从而避免了监控、故障定位等操作对生产系统的侵入。此外，日志易可针对不同用户提供独立的数据视图，从源头杜绝交叉影响及敏感信息泄露。

即时搜索，快速排障

日志易提供海量信息秒级查询功能，可以协助开发人员快速发现系统异常,辅助运维工作人员的排障工作。

实时告警，提前预防

通过日志易设置高危关键字监控，一旦系统有涉及高危关键字的异常，便会以短信、邮件、电话等方式即时发出告警，及时通知相关人员系统异常情况。

决策依据好帮手

日志易借助业务统计报表可以掌握业务趋势，通过接口调用统计为扩容、性能问题排查提供参考信息，辅助工作人员进行决策，让决策有的放矢。

用户及系统画像

企业可通过日志易平台实时掌握用户访问特征及系统运行特征, 对可能出现的安全问题及用户偏好迅速做出反应。

案例 | 通过全局链路监控分析实现企业邮箱故障快速定位

日志易

背景介绍

随着企业业务的发展壮大，协同办公工具在内外部信息管理方面的必要性日益凸显。企业邮箱作为最基础的协同办公工具之一，对现代化企业的办公效率有着重要影响。

中大型公司都会搭建自己的企业邮箱服务，并且使用专业的安全邮件网关过滤掉外网的垃圾邮件、病毒邮件，拦截内部发送外网的涉密邮件，保证工作的合规性和安全性。但日常使用中难免遇到邮件发送失败、接收失败和异常退信等情况，这就需要对邮件发送和接收整个链路进行针对性的监控，以便迅速解决问题，保障办公效率。

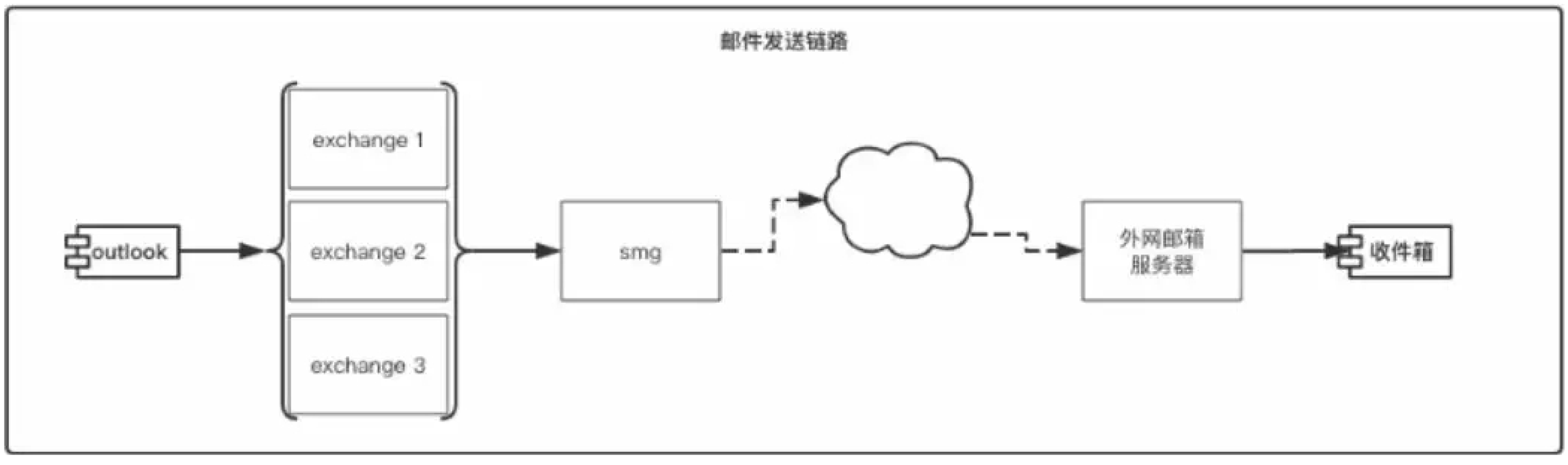
客户场景分析

某大型证券公司业务范围较广，工作的合规性及安全性要求较高。该企业在处理邮箱服务异常情况时，通常会根据邮件的发送时间和标题来确定大致范围，然后逐个登录服务器查看日志。此种方式效率较低，需要很长时间才能定位故障问题。

日志易团队从邮件的整体链路情况和日常故障场景两方面入手分析，使用全局监控手段来帮助运维人员快速定位问题，以缩短时间消耗，减少人工投入。

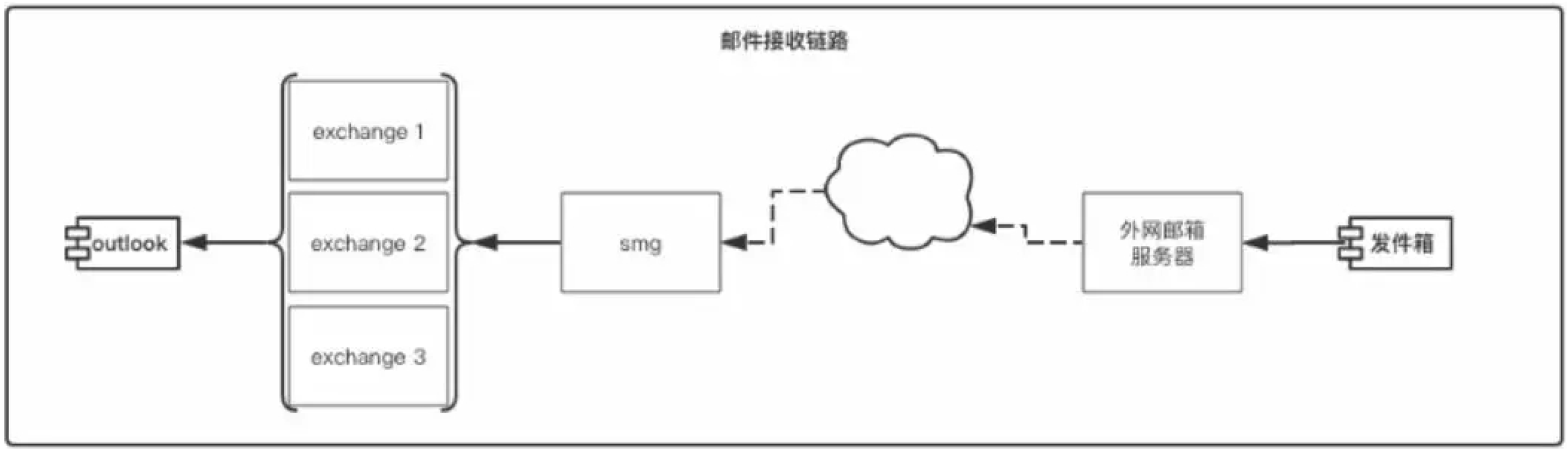
从邮件的整体链路情况进行分析，邮件链路可拆分为内网邮件发送链路及外网邮件接收链路两部分。

内网邮件发送链路是指用户在企业内网发送邮件的过程，用户通过 Outlook 进行邮件发送，邮件先到达 Exchange 邮件服务器组，该服务器组将对邮件进行转发，转发后的邮件到达 SMG 邮件网关，该邮件网关会对邮件的内容进行合规检查，检查通过后，邮件发送到外网的邮箱服务器，由收件人进行邮件接收。



【图1 内网邮件发送链路示意图】

外网邮件接收链路与内网邮件发送链路相反，邮件先由外部进入内网，经 SMG 邮件网关对原始邮件进行垃圾邮件过滤或邮件安全扫描等检查后，才会转发到内网。



【图2 外网邮件接收链路示意图】

根据上述邮件链路，对该企业日常故障场景进行分析，已知内网邮箱为 emailckeck@xxx.com.cn，外网邮箱为 cland@xxx.com，可得出以下几种故障情况：

1.Exchange 无 emailckeck 邮箱的发送记录，邮件投递失败；

2.Exchange 有 emailckeck 邮箱的发送记录，但 SMG 无记录，邮件投递失败；

3.SMG 无 cland 邮箱的接收记录，邮件接收失败；

4.SMG 有 cland 邮箱的接收记录，但 Exchange 无记录，邮件接收失败。

解决方案

根据整体链路情况，需要将 **Exchange 日志和 SMG 日志进行采集、解析及关联分析，最后将整体运行情况进行展示，并对异常情况进行告警分析及发送。**

将内网邮件发送及外网邮件接收情况进行汇总，可根据某些参数判断链路是否正常。如在下面的 SMG 内部邮箱发送链路分析中，当 smg_ct 及 exchangec_ct 同时为 1 时，status 字段会显示邮件链路正常，其他情况均为异常。而内部邮箱发送链路和外部邮件发送链路都正常时，代表整体邮箱服务正常。

邮件链路通讯详情 SMG日志分析

smg_内部邮箱发送链路详情 最近7小时

time	send	recv	excha…	smg_ct	excha…	status
10:00:00	emailcke ck@xxx. com.cn	cland@x xx.com	邮件链路连通性测试-2018 0528_10 00	1	1	邮件链路正常
09:00:00	emailcke ck@xxx. com.cn	cland@x xx.com	邮件链路连通性测试-2018 0528_09 00	1	1	邮件链路正常
08:00:00	emailcke ck@xxx. com.cn	cland@x xx.com	邮件链路连通性测试-2018 0528_08 00	1	1	邮件链路正常
07:00:00	emailcke ck@xxx. com.cn	cland@x xx.com	邮件链路连通性测试-2018 0528_07 00	1	1	邮件链路正常
06:00:00	emailcke ck@xxx. com.cn	cland@x xx.com	邮件链路连通性测试-2018 0528_06 00	1	1	邮件链路正常
05:00:00	emailcke ck@xxx. com.cn	cland@x xx.com	邮件链路连通性测试-2018 0528_05 00	1	1	邮件链路正常
04:00:00	emailcke ck@xxx. com.cn	cland@x xx.com	邮件链路连通性测试-2018 0528_04 00	1	1	邮件链路正常

smg_外部邮箱发送链路详情 最近7小时

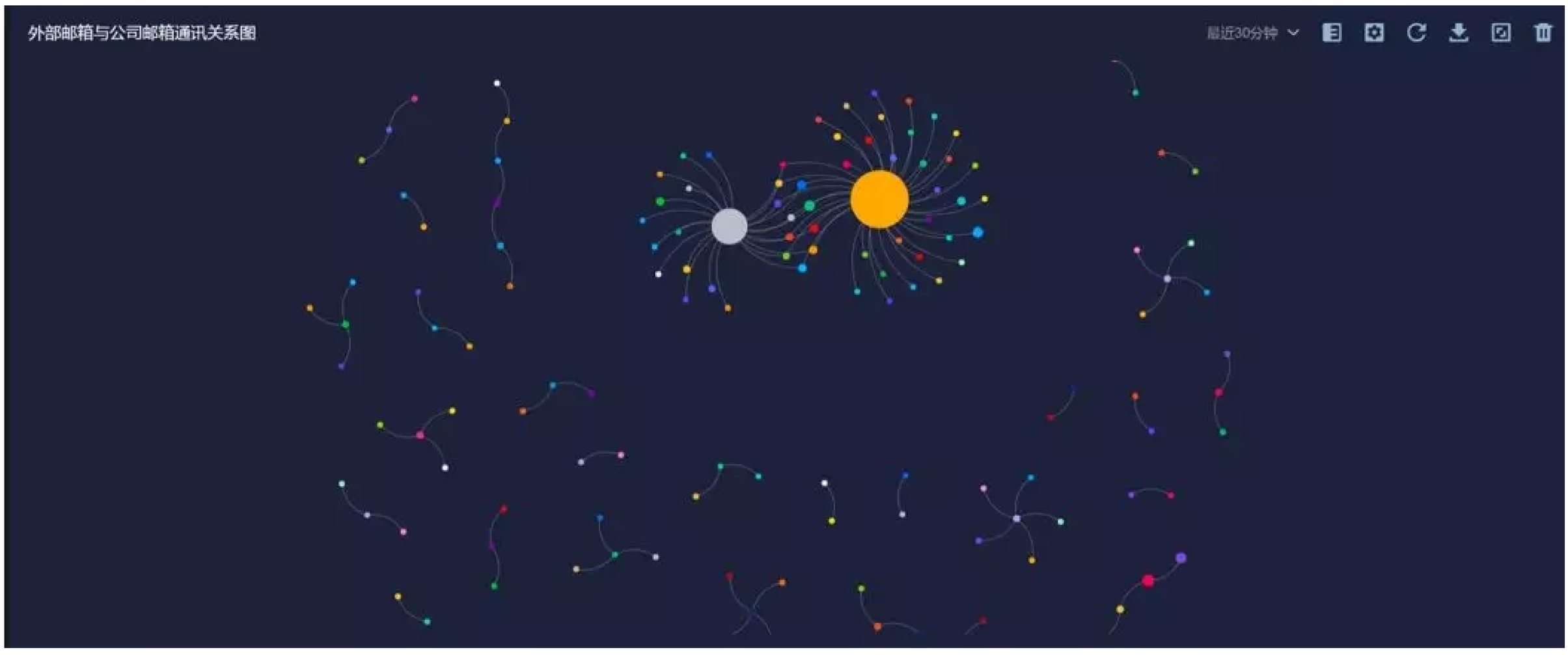
time	send	recv	excha…	smg_ct	excha…	status
10:00:00	cland@x xx.com	emailcke ck@xxx. com.cn	邮件链路连通性测试-2018 0528_10 01	1	1	邮件链路正常
09:00:00	cland@x xx.com	emailcke ck@xxx. com.cn	邮件链路连通性测试-2018 0528_09 01	1	1	邮件链路正常
08:00:00	cland@x xx.com	emailcke ck@xxx. com.cn	邮件链路连通性测试-2018 0528_08 01	1	1	邮件链路正常
07:00:00	cland@x xx.com	emailcke ck@xxx. com.cn	邮件链路连通性测试-2018 0528_07 01	1	1	邮件链路正常
06:00:00	cland@x xx.com	emailcke ck@xxx. com.cn	邮件链路连通性测试-2018 0528_06 01	1	1	邮件链路正常
05:00:00	cland@x xx.com	emailcke ck@xxx. com.cn	邮件链路连通性测试-2018 0528_05 01	1	1	邮件链路正常
04:00:00	cland@x xx.com	emailcke ck@xxx. com.cn	邮件链路连通性测试-2018 0528_04 01	1	1	邮件链路正常

【图3 SMG链路详情分析图示】

当邮箱发送情况出现故障分析中的 4 种情况时，会发送告警给邮箱管理员，点击告警详情中的查询链接可以直接钻取到仪表盘告警界面。

邮箱异常行为分析

根据外部邮箱和公司邮箱的离散关系，还可以分析出是否有针对内网邮箱的邮件轰炸及异常发件邮箱，并可通过配置邮件网关进行屏蔽过滤。



【图4 外部邮箱与公司邮箱通讯关系图】

日志易的监控及故障定位能力不仅仅体现在企业邮箱故障定位上。通过日志易可以构建一个完整的多维度监控体系，既可以从横向对多种设备进行关联分析，也可以从纵向快速发现单一设备或系统的异常故障，深挖故障原因，从而为企业构建全面完整的运维分析平台。

关于日志易

北京优特捷信息技术有限公司（简称：日志易）是国家级专精特新“小巨人”企业，专注于机器大数据平台、服务和解决方案的开发，致力于帮助各行业用户挖掘和利用机器数据价值，提升数字化运营能力，轻松应对IT及业务挑战。公司推出**智能日志中心、SIEM安全大数据分析平台、观察易、智能运维平台、数据工厂、日志易大屏**等系列产品，一站式解决机器数据采集、清洗、存储、搜索、分析、可视化等需求，帮助企业轻松实现查询统计、业务关联分析、监控告警、安全信息与事件管理SIEM、用户与实体行为分析UEBA、智能运维AIOps、IT可观察性等应用场景。

联系我们

咨询热线：400-085-0159
官网地址：www.rizhiyi.com

关注日志易微信公众号，接收更多行业资讯和干货内容

扫码添加日志易官方交流微信，进入行业交流群，还有随机福利发送~