上海市公安局信息化项目用户需求编制大纲

一、封面

用户需求书

项目名称：智慧刑侦实战应用系统(2026 年升级改造)

责任单位：上海市公安局

项目负责人及职务：石朋飞　科长

联系人及电话：周美娟 13671525304

二、主要内容

（一）背景与现状概述

习总书记在全国两会期间发表的重要讲话，视野宏阔、立意高远，思想深邃、内涵丰富，具有很强的政治性、思想性、指导性、针对性，为我们做好工作指明了方向、提供了根本遵循。过去一年，以习总书记同志为核心的党中央团结带领全党全国各族人民，砥砺奋进、攻坚克难，经济运行总体平稳、稳中有进，高质量发展扎实推进，中国式现代化迈出新的坚实步伐。全国GA机关坚决贯彻落实习总书记重要指示精神和党中央决策部署，扎实做好维护安全稳定各项工作，为续写经济快速发展和社会长期稳定“两大奇迹”新篇章作出积极贡献。要准确把握保持社会和谐稳定新部署，努力把平安中国建设推向更高水平。要坚定不移贯彻总体国家安全观，在国家更加安全、社会更加有序、治理更加有效、人民更加满意上持续用力。要坚决捍卫国家政治安全，严密防范、严厉打击敌对势力渗透、破坏、颠覆、分裂活动，坚定维护国家政权安全、制度安全、意识形态安全。要坚决防范化解突出注意，结合开展“化解矛盾注意、维护社会稳定”专项行动，实质化解各类矛盾纠纷，确保社会大局持续稳定。要坚决维护公共安全，完善社会治安整体防控体系，依法严惩涉黑涉恶、电信网络诈骗等突出违法犯罪活动，深化安全生产治本攻坚三年行动，全力保护人民群众生命财产安全。

会议强调，要准确把握深化改革新机遇，不断提升GA机关新质战斗力。要完善GA机关机构职能体系，按照“党委领导、部级抓总、

省级主责、市县主战、派出所主防”的思路，稳步推进地方GA机关机构编制管理改革，着力构建职能科学、事权清晰、指挥顺畅、运行高效的警务管理体制。要建立完善“专业+机制+大数据”新型警务运行模式，推动警务运行更加协同高效。要强化大数据赋能实战，优化GA科技创新平台布局，为GA工作提供更加有力的支撑。

会议要求，要加强组织领导，周密安排部署，组织广大工作人员全面系统学、融会贯通学、联系实际学，迅速掀起学习贯彻热潮。要立足GA机关职责，认真研究谋划工作抓手和载体，提高创造性贯彻落实能力，确保在GA机关形成生动实践。要把学习贯彻全国两会精神与做好当前安保维稳工作紧密结合起来，切实以工作实绩检验学习贯彻成效。

2025年，为了全面贯彻落实党的二十大和二十届二中、三中全会精神，深入学习贯彻习总书记关于新时代GA工作的重要论述，认真贯彻中央政法工作会议、全国GA工作会议和全国GA厅局长会议精神，坚定拥护“两个确立”，坚决做到“两个维护”，坚持以人民为中心，坚持总体国家安全观，以党的政治建设为统领，以贯彻“四新”要求为主线，以“云剑—2025”行动为牵引，以深化刑侦改革为动力，以推进ZC中心建设为载体，以严格规范公正文明执法为要求，以锻造过硬刑侦铁军为保证，全面提升新质战斗力，精准打击各类突出犯罪，高水平推进GA工作现代化，为高质量完成“十四五”规划目标任务贡献刑侦力量。

重点抓好以下六个方面工作:

1、强化使命担当全力以赴护航发展大局

坚决捍卫政治安全，全力维护社会稳定，严打严防个人极端犯罪。主动服务高质量发展，严厉打击“沙霸”“矿霸”“村霸”等突出犯罪，持续深化打击海上走私犯罪，严厉打击假冒国企央企、对公侵财犯罪，严厉打击金融放贷、市场流通等行业领域黑恶犯罪，规范涉企执法行为，保护企业合法权益。

2、坚定必胜信念坚决打赢反诈人民战争

深化运用“四专两合力”，完善打击治理电信网络诈骗工作协调机制，统筹推进打防管治建宣各项措施，坚决打赢反诈人民战争，不获全胜，决不收兵。打好境外战场攻坚战，强力缉捕逃犯，强化务实执法合作，打掉一批涉诈园区、抓获一批涉诈人员。纵深推进打击缅北涉我犯罪专项工作整体战，做好缅北电诈集团头目骨干的诉讼工作。用足用好“两高一部”专门意见，全力开展境外移交人员审查和事件办理，确保整体打击、依法严惩。持续深化“断流”“拔钉”行动，抓金主、挖源头、斩链条。不间断发起集群战役、区域会战，坚决铲除黑灰产团伙，持续开展资金预警、见面劝阻，对易受骗人员开展精准宣传。全面实施联合惩戒办法，综合采取电信、金融、信用等惩戒措施，强力震慑犯罪。

3、坚持目标导向严厉打击各类突出犯罪

要以“云剑—2025”行动为牵引，组织优势警力，采取过硬措施，开展专项打击，确保打出声威、打出实效。纵深推进常态化扫黑除恶斗争，深化整治群众身边不正之风和腐败问题工作，强化大事攻坚，

打财断血、打伞破网，确保打深打透打彻底，强化打早打小，坚决将黑恶犯罪消除在萌芽状态。对一杀多人、个人极端、纵火投毒等重大敏感恶性事件，快速反应、及时侦破，继续组织命事积事攻坚。打源头、摧网络、捣窝点，消除枪爆隐患。强力打击惩治“隔空”猥亵、性侵等犯罪，继续开展拐卖儿童积事攻坚，坚决维护妇女儿童合法权益。严厉打击欺诈骗保、流窜盗窃、民资诈骗、养老诈骗等群众反映强烈的突出犯罪。强化文物犯罪事件攻坚，打击犯罪团伙，追缴涉事文物，构建文物安全工作新格局。

4、深化刑侦改革构建数字化ZC新模式

依托ZC中心，建立常态研判机制、专项攻坚机制、整体作战机制，统筹牵动各类ZC资源，全面提升数字化ZC能力。组建培育专业团队，整合ZC资源，集成专业能力，优化工作流程，精准开展打击，着力提升新型事件侦办能力，掌握攻防主动权。精确建立预测模型，精细开展预警反制，精准推动预防治理，做实做细主动警务、预防警务，推动ZC工作从事后被动打击向事前主动预防转型。

5、坚持守正创新开创刑侦工作现代化建设新局面

推动刑事技术迭代升级，做精传统勘查，做实新型勘查，深挖传统技术潜能，推广新技术新能力。加强ZC研判队伍建设，全面提升数字化ZC能力。大力推进警犬技术与前沿科技的深度融合，加大本土犬警用研发力度，积极拓展实战应用新领域，着力打造世界一流警犬技术团队。坚决整治执法突出问题，着力提升办事质量，不断健全制度体系。

6、强化政治引领全力打造过硬刑侦铁军

加强理想信念教育，大力弘扬新时代刑警精神，深入开展向乌国庆、崔道植同志等先进典型学习活动，大力传播刑侦正能量，不断增强刑警的职业荣誉感、自豪感。加强实战练兵，提高能力本领，全面强化正风肃纪，持续改进工作作风，保障工作人员执法权益，落实爱警暖警措施，全力锻造过硬刑侦铁军。

（二）目标与任务

依托ZC中心，建立常态研判机制、专项攻坚机制、整体作战机制，整合ZC资源，集成专业能力，优化工作流程，精准开展打击，着力提升新型事件侦办能力，掌握攻防主动权。精确建立预测模型，精细开展预警反制，精准推动预防治理，做实做细主动警务、预防警务，推动ZC工作从事后被动打击向事前主动预防转型。推动刑事技术迭代升级，做精传统勘查，做实新型勘查，深挖传统技术潜能，推广新技术新能力，积极拓展实战应用新领域。完善“专业+机制+大数据”新型警务运行模式，推动警务运行更加协同高效。要强化大数据赋能实战，优化GA科技创新平台布局，为GA工作提供更加有力的支撑。

智慧刑侦实战应用系统（2023年升级改造）的建设内容主要为刑事技术一体化实战应用、业务综合管理应用和反诈大数据应用的数字化ZC技术应用能力提升包括：HS特点核验、G重组率分析、GJ智能筛查、涉诈要素归集、易骗人群HX、涉诈链条阻断、涉诈事件研

判、反诈环节反查，共9个子应用建设。

（1）GJ智能筛查

统一集成、管理、调度各方资源，确保GJ筛查模型高效、按时、稳定、准确运行，最终产出高价值底库下发到基层进行处置反馈，形成闭环。提供逻辑清晰，易于操作的界面供各个角色的用户完成相应工作。同时，提供相关接口把模型结果赋能给其他单位部门，最大化发挥模型价值。

（2）HSF核查

为全市GA各警种提供高效的本地化HS识别服务，同时与上级HS系统及本省相关警种业务系统对接，系统能与上级HS库进行无缝对接和联动识别，实现对全国各省GA机关已采底库进行实时核验比对。使识别工作变得精准高效，同时可以深化HS识别在我省的其它应用。

（3）G重组率分析

构建全国范围的相关鉴定结果共享平台，实现各地GA机关之间的数据互通，确保鉴定结果的标准化输出，使数据无缝对接。此外，研发智能化数据分析工具，支持对共享鉴定结果的深度分析，提供更加精准的事件信息。通过这些措施，刑事技术一体化平台将能够更高效地利用相关物证，降低事件侦破的时间和经济成本，为打击犯罪提供坚实的技术支持。

（4）上海反诈数智平台（反诈大数据应用）

坚持实战为王、实效为先，以赋能反诈“打防管治建宣”体系为

牵引，以汇聚治理全量涉诈数据为根基，以应用人工智能技术为突破，建设全局性、集成式、智能化的反诈数智平台，实现“一屏通晓、一网统管”，助力反诈工作防范劝阻更精准、研判打击更深入。建设内容分为涉诈要素归集、反诈态势感知、受害人群HX、涉诈链条阻断、涉诈事件研判和反诈环节反查共3大功能模块。以全要素归集为根基，通过全态势感知、全人群HX、全链条阻断实现防范劝阻更精准，利用全事件研判实现研判打击更深入，进行全环节反查反哺平台优化完善。

1）涉诈要素归集

设定具体项目、统一格式标准、明确工作手势，实行“机器+人工”模式，做到前端应采尽采、末端应收尽收，侧端应汇尽汇。开展涉诈数据专项治理，构建电诈事件核心数据库，作为搭建全局反诈数字化平台的数据基座。

2）受害人群HX

研发“电诈受骗人群注意HX模型”，对不同类事复盘，建立标签体系，开展数据汇聚治理，建设训练模型，对全市全量筛查、分类筛查、循环筛查，分类锁定容易受骗群体，分级筛查潜在被害人员，为开展针对性宣传、精准性劝阻给予明确指引。

3）涉诈链条阻断

汇聚建立“两全H样本库（全量、全新）”，整合打通各系统间信息传导链路，完善“技术拦阻、预警劝阻、资金防阻”工作闭环。在技术拦阻方面，对接市TG局818、331等系统，推送H样本至TG

局开展布防拦截；接收TG局拦截信息开展宣防劝阻。在预警劝阻方面，在GA网互联相关系统，下发预警指令，汇集反馈信息；对接外单位相关系统，为街镇反诈中心开展宣传劝阻提供支撑。在资金防阻方面，打通上海城市金融网传输通道，推送H样本ZH至在沪中资商业YH拦截；建设反诈扫码模块，将大额取现、购买黄金、购买购物卡等纳入扫码范畴，开展拦截劝阻管控等工作。实现全量交互信息、动态评估成效、及时纠正偏差，为确保高效运转、有效阻断给出解决方事。

4）涉诈事件研判

整合总队目前掌握的全量资源，利用智研导侦机器人自动化开展资源的多轮次调用、循环调证，并构建相关知识图谱，实现全量机器自动初步研判并生成初研报告；对无法落地，通过智能辅助研判机器人的智能解答、智能指引功能，辅助开展人工二次研判（作战室），实现自动生成深研报告。

5）反诈环节反查

通过人工对相关情况全面倒查，研发反查模型，围绕“引流、诈骗、转账”等环节和“接报、研判、打击”等环节，逐个复盘反查注意隐患，实现“一键反查”、“全程反查”，推动解决通信、金融、互联网等行业管控治理漏洞，反哺提升内部防范宣传、防阻预警、研判打击等能力。

（三）设计方事

1、业务流程、数据和数据流分析

1.1 现有业务流程:

目前以刑侦数字化网上作战系统作为主干大系统，支撑“构建信息高度汇聚、资源充分整合、能力高效调用、研判一体合成、ZC 扁平联动”的建设目标，全面整合刑侦业务，扩展系统功能，深化数据应用，开发研判模型，服务刑事事件 ZC 的全过程。

1.2 新的业务流程:

智慧刑侦实战应用系统（2026 年升级改造）的建设内容主要为刑事技术一体化实战应用、业务综合管理应用和反诈大数据应用的数字化 ZC 技术应用能力提升。

2、总体框架

按照《上海智慧刑侦三年建设规划》的总体要求，着力提升 4 项刑侦核心专业能力（刑事技术专业能力、视频 ZC 专业能力、数据研判专业能力、非接犯罪攻防能力），刑侦数字化网上作战系统采用“1+3+N”总体架构开展建设，“1”是指刑侦数字化网上作战系统（刑侦数字化网上作战系统），“3”是指 3 个重点领域专业应用子模块（反诈、扫 H、JD、涉 Q 涉 B、刑事技术一体化、业务综合管理），“N”是指多数据多工具、多智能化应用。

3、功能和性能需求

3.1 功能需求

3.1.1.GJ 智能筛查

GJ 智能筛查应用是统一集成、管理、调度各方资源，确保 GJ 筛

查模型模型高效、按时、稳定、准确运行，最终产出信息下发进行处置反馈，形成闭环。提供逻辑清晰，易于操作的界面供各个角色的用户完成相应工作。同时，提供相关接口把模型结果赋能给其他单位部门，最大化发挥模型价值。包括以下几大功能模块:

模型标签体系管理: 模型标签体系贯穿系统的各个环节，既作为模型算法的计算依据，也确保数据治理的有章可循，同时在产出后提供给相关人员查看分析。随着系统的运行，标签体系也会随之发生变化，需要对其进行有效管理。本模块提供标签体系版本变更维护、标签体系内容维护等功能。

模型训练样本管理: 模型结果的准确性依赖训练样本的准确性、全面性。为了生成有效的样本，本模块提供各类事件和底库和对端反查功能，通过人工方式明确标签，生成样本数据。同时通过接口调用获取机器自动数据，最后按照相应规则合并人工和机器数据形成最终训练样本。

模型运行管理: 模型运行管理模块统一调度各方资源，最终产出数据，是本项目的重点内容，包括轮次版本管理、XGB 模型数据打标管理、XGB 模型执行管理、XGB 模型结果处理、第三维度数据对接处理、时空图模型收入数据打标管理、时空图模型执行管理、时空图模型结果处理、模型运行过程可视化、模型运行监控等功能。

模型结果研判: 模型产出结果后，进行抽查、分析，一方面确保结果没有大的偏差，另一方面分析模型优化的可能性。本模块提供辅助研判的功能，包括结果查看分析、结果态势分析、库管理、辅助研

判工具等功能。

模型预测结果处置：模型产出的结果需要下发并反馈。本模块提供下发、反馈上报、统计分析等功能。

模型结果对外赋能：为了扩大模型应用成果，向外提供服务。

每隔半个月对底库做一次筛查，对于每一轮筛查，首先获取当前底库数据，形成底库，然后启动 XGB 模型数据打标治理服务，生成最新标签数据，接着调用 XGB 模型运算服务为每个底库计算分值，大于某个阈值的构成待筛选底库，此底库的规模控制在几万以内，接着对这部分底库对接第三维度数据后启动时空图模型治理服务，补充相关标签数据后调用时空图模型运算服务，得到更准确的分值，大于某个阈值的底库作为最终发现的底库推送出去，进而下发，结果在系统中进行反馈。

业务流程：

1、发起一轮底库任务，记录轮次版本和本次任务；

2、初始化底库数据；

3、按 XGB 模型要求，调用服务，对底库打标；

4、调度 XGB 模型，输入有标签的底库，由其运算；

5、对 XGB 模型结果解析、保存、信息补充；

6、与第三维度系统对接，底库比对补充；

7、按时空图模型要求，调用数据治理服务，对可底库打标签；

8、调度时空图模型，输入打标的底库，由其运算；

9、对时空图模型结果解析、保存、信息补充；

10、底库处置：底库下发、基层反馈上报、信息统计;

11、结果对外赋能：提供底库分值获取、底库标签获取等服务;

12、对模型运行整个过程日志记录、监控和可视化。

3.1.1.1.模型标签体系管理

模型标签体系管理主要负责GJ模型计算运行过程中对分析主体对象按照标准化打标签，是整个系统运行在基础。

3.1.1.1.1.标签标准版本维护

提供对标签标准版本名称、版本号的维护，包括查询、新增、编辑、删除标签标准版本功能。

3.1.1.1.2.标签标准上传

提供批量导入xls、xlsx等格式的外部标签标准文件功能。

3.1.1.1.3.标签标准维护

提供对不同版本的标签标准进行详细标签维护功能，包括标签名称、标签映射名称、显示状态、跳转状态、标签标识码、排序号、版本号、数据源标记等数据项维护，提供对标签查询、新增、编辑、删除等功能。

3.1.1.1.4.标签标准导出

提供对不同版本的标签标准批量导出到xls、xlsx等外部格式文件功能。

3.1.1.2.模型训练样本数据管理

3.1.1.2.1.JS 人工反查

3.1.1.2.1.1.数据导入

提供模板下载，按照模板收集编号、类型，然后批量导入到系统，系统后台支持按照导入的编号从相应系统中抽取详细数据，为后续提供基础数据支撑。

3.1.1.2.1.2.底库反查

根据标签体系要求，提供功能页面，由人工录入底库相关标签信息，在打标过程中提供查看打标规则，调阅笔录，查看信息等功能，辅助了解情况。

3.1.1.2.1.3.对端反查

根据标签体系要求，提供功能页面，由人工录入底库相关标签信息，在打标过程中提供查看打标规则，调阅笔录，查看信息等功能，辅助了解对端情况。

3.1.1.2.2.WS 人工反查

3.1.1.2.2.1.数据导入

提供 WS 数据模板下载，按照模板收集 WS 的编号、类型，然后批量导入到系统，系统后台支持按照导入的编号从相应系统中抽取详细数据，为后续提供基础数据支撑。

3.1.1.2.2.2.WS 底库反查

根据标签体系要求，提供功能页面，由人工录入底库相关标签信息，在打标过程中提供查看打标规则，调阅，查看信息等功能，辅助

了解情况。

3.1.1.2.2.3.WS 对端反查

根据标签体系要求，提供功能页面，由人工录入对端相关标签信息，在打标过程中提供查看打标规则，调阅，查看信息等功能，辅助了解对端情况。

3.1.1.2.3.ZS 人工反查

3.1.1.2.3.1.ZS 数据导入

提供 ZS 数据模板下载，按照模板收集 ZS 编号、类型，然后批量导入到系统，系统后台支持按照导入的编号从相应系统中抽取详细数据，为后续提供支撑。

3.1.1.2.3.2.ZS 底库反查

根据标签体系要求，提供功能页面，由人工录入底库相关标签信息，在打标过程中提供查看打标规则，调阅，查看信息等功能，辅助了解情况。

3.1.1.2.3.3.ZS 对端底库反查

根据标签体系要求，提供功能页面，由人工录入对端底库相关标签信息，在打标过程中提供查看打标规则，调阅，查看信息等功能，辅助了解对端底库情况。

3.1.1.2.4.GJ 人工反查

3.1.1.2.4.1.GJ 数据导入

提供 GJ 数据模板下载，按照模板收集 GJ 的编号、类型，然后批量导入到系统，系统后台支持按照导入的编号从相应系统中抽取该批

的详细数据，为后续的人工反查提供基础数据支撑。

3.1.1.2.4.2.GJ 底库反查

根据标签体系要求，提供功能页面，由人工录入底库相关标签信息，在打标过程中提供查看打标规则，调阅，查看信息等功能，辅助了解底库情况。

3.1.1.2.4.3.GJ 对端底库反查

根据标签体系要求，提供功能页面，由人工录入对端底库相关标签信息，在打标过程中提供查看打标规则，调阅，查看信息等功能，辅助了解对端底库情况。

3.1.1.2.5.训练样本数据合成

3.1.1.2.5.1.获取机器反查数据

为了提供最终训练样本，调用数据治理服务接口，获取 JS 事件、WS 事件、ZS、GJ 的底库及对端底库的相关标签，以便进行标签合并工作。

3.1.1.2.5.2.人工反查与机器反查合并

按照标签数据合并规则，执行人工反查标签和机器反查标签，生成最终一致的训练标签数据。

3.1.1.3.模型运行管理

3.1.1.3.1.轮次版本管理

提供对 GJ 模型运行的版本名称、版本号、标签版本等内容的软次版本维护功能，用于记载每次制定模型分析任务时所属轮次版本及标签版本，包括轮次版本查询、新增、删除等功能。

3.1.1.3.2.待预测数据初始化

针对每个轮次任务，从库中筛选出符合分析目标进行数据处理、建表、加载等初始化工作，形成本轮模型数据。

3.1.1.3.3.XGB 模型输入数据管理

3.1.1.3.3.1.XGB 模型输入数据打标服务封装

待底库数据初始化后，系统需结合多维底库特征数据为每个底库打标处理，最终形成底库标签数据,作为 XGB 模型分析的输入数据，系统需将上述多维数据治理及打标封装成统一的服务供系统调用，输出标签数据库。服务封装支持多环境可移植性和稳定性，提供必要的异常数据处理、日志审计功能，满足实时性、准确性和安全性要求。

3.1.1.3.3.2.XGB 模型输入数据打标调度

在 XGB 模型输入数据打标服务封装后，提供灵活的调度功能，可以根据业务需要定时或实时触发 XGB 模型输入数据打标任务，调度过程中具备监控和日志记录能力便于跟踪调度情况。

3.1.1.3.4.XGB 模型执行管理

3.1.1.3.4.1.XGB 模型服务封装

将 XGB 模型算法封装成统一的服务供系统调用，提供加载模型、接收输入数据，输出分数结果，系统在每轮次模型执行时调用封装好的服务进行分析，旨在通过输入的特征数据分析预待测的分数。服务封装支持多环境可移植性和稳定性，提供必要的异常数据处理、日志审计功能，满足实时性、准备性和安全性要求。

3.1.1.3.4.2.XGB 模型执行调度

在 XGB 模型算法服务封装后，提供灵活的调度功能，可以根据业务需要定时或实时触发模型分析任务，确保高效执行大批量底库分析，调度过程中具备监控和日志记录能力便于跟踪调度情况。

3.1.1.3.5.XGB 模型结果处理

3.1.1.3.5.1.解析保存底库基本信息

XGB 模型执行后,将结果中的底库基本信息进行解析并保存到系统中。

3.1.1.3.5.2.解析保存底库标签信息

XGB 模型执行后,将结果中的底库标签信息进行解析并保存到系统中。

3.1.1.3.5.3.保存底库原始数据包

XGB 模型执行后，将底库评分原始数据包，底库打标源业务数据包是指底库某类标签产生的业务原数据包备份保存到系统中，以便后续排查问题及回溯分析使用。

3.1.1.3.5.4.补充底库地域信息

已经产生的底库信息需进一步通过调用地域信息接口补充底库地域地址信息，以确保底库地域信息的准确性。

3.1.1.3.5.5.补充底库存在状态

已经产生的底库信息需进一步通过调用存在注销接口补充底库存在状态信息，以确保底库信息的准确性。

3.1.1.3.6.第三维度数据处理

3.1.1.3.3.1.三方查询数据申请

在 XGB 模型执行后产生的底库结果信息需进一步申请三方数据进行打标处理，三方查询数据申请通过提交申请数量、号码数量、申请时间信息以及以 xls 等格式的外部文件底库数据，提交由三方部门处理。

3.1.1.3.3.2.三方结果数据导入

三方部门接收到查询数据申请后根据底库信息和号码信息进行比对处理，生成符合模板要求的外部导入文件导入到系统，用于后续打标形成底库标签数据库。

3.1.1.3.3.3.辅助方查询数据导出

在 XGB 模型执行后产生的底库结果信息需进一步申请辅助方数据进行打标处理，系统提供辅助方查询数据筛选导出功能导出数据到外部文件提交由辅助方部门处理。

3.1.1.3.3.4.辅助方结果数据导入

辅助方部门将导出的查询数据根据底库信息和号码信息进行比对处理，生成符合模板要求的外部导入文件导入到系统，用于后续打标形成底库标签数据库。

3.1.1.3.7.时空图模型输入数据管理

3.1.1.3.7.1.时空图模型输入数据打标服务封装

在底库分析结果的基础上，系统需结合三方、辅助方部门提供的数据为每个底库作进一步打标处理，形成底库标签数据库，作为时空

图模型分析的输入数据，系统需将上述数据治理及打标封装成统一的服务供系统调用，输出底库标签数据库。服务封装支持多环境可移植性和稳定性，提供必要的异常数据处理、日志审计功能，满足实时性、准备性和安全性要求。

3.1.1.3.7.2.时空图模型输入数据打标调度

在时空图模型输入数据打标服务封装后，提供灵活的调度功能，可以根据业务需要定时或实时触发时空图模型输入数据打标任务，调度过程中具备监控和日志记录能力便于跟踪调度情况。

3.1.1.3.8.时空图模型执行管理

3.1.1.3.8.1.时空图模型服务封装

将时空图模型算法封装成统一的服务供系统调用，提供加载模型、接收输入数据，输出高和低底库分类，系统在每轮次模型执行时调用封装好的服务进行分析，旨在通过输入的底库结合三方、辅助方数据进一步分析并输出高和低底库分类。服务封装支持多环境可移植性和稳定性，提供必要的异常数据处理、日志审计功能，满足实时性、准备性和安全性要求。

3.1.1.3.8.2.时空图模型执行调度

在时空图模型算法服务封装后，提供灵活的调度功能，可以根据业务需要定时或实时触发模型分析任务，支持调度过程中具备监控和日志记录能力便于跟踪调度情况。

3.1.1.3.9.时空图模型结果处理

3.1.1.3.9.1.解析保存底库基本信息

通过调用时空图模型执行后,将结果中的底库基本信息进行解析并保存到系统中。

3.1.1.3.9.2.解析保存底库标签信息

通过调用时空图模型执行后,将结果中的底库标签信息进行解析并保存到系统中。

3.1.1.3.9.3.保存底库原始数据包

时空图模型执行后，将底库评分原始数据包，底库打标源业务数据包保存到系统中，以便后续排查问题及回溯分析使用。

3.1.1.3.9.4.补充底库地域信息

已经产生底库信息需进一步通过调用地域接口补充底库地域信息，以确保底库地域信息的准确性。

3.1.1.3.9.5.补充底库居住地坐标信息

已经产生的底库信息需进一步通过通过调用居住地坐标接口补充底库居住地坐标信息，以确保底库能在定图上定位。

3.1.1.3.9.6.补充底库存在状态

已经产生的底库信息需进一步通过通过调用存在注销接口补充底库存在状态信息，以确保底库信息的准确性。

3.1.1.3.10.模型运行过程可视化

可视化功能旨在帮助用户直观理解模型运行状态和预测结果，为

防控和决策研判分析提供可视化的数据支撑。

3.1.1.3.10.1.总体数据流转过程可视化

结合图表、数字及业务流程图等可视化手段综合展示总体数据流转过程。过程包括：待底库初始化、待底库打标处理、待底库标签数据库形成、XGB 模型执行、底库形成、底库打标、底库标签库形成、时空图模型执行、底库推送、底库处置反馈等。

3.1.1.3.10.2.本部数据更新情况可视化

待底库初始化后需与本部数据关联打标形成待底库标签数据库，系统通过图表可视化展示包括底库、基本信息、快卖底库、亲关系在内的本部数据更新情况，包括展示记录数、数据大小、更新频率、最后更新时间、更新状态等。

3.1.1.3.10.3.数据处数据更新情况可视化

待底库初始化后需与数据处提供的业务数据关联打标形成待底库标签数据库，系统通过图表可视化展示包括 30 多类数据处提供数据的更新情况，包括展示记录数、数据大小、更新频率、最后更新时间、更新状态等。

3.1.1.3.10.4.大中心数据更新情况可视化

待底库初始化后需与大中心提供的数据关联打标形成待底库标签数据库，系统通过图表可视化展示包括大中心提供数据的更新情况，包括展示记录数、数据大小、更新频率、最后更新时间、更新状态等。

3.1.1.3.10.5.三方数据更新情况可视化

底库需与三方提供的数据关联打标形成底库标签数据库，系统通过图表可视化展示包括各类三方、辅助方提供数据的更新情况，包括展示数据表、更新频率、最后更新时间、更新状态等。

3.1.1.3.10.6.XGBoost 模型运行原理可视化

通过图形化方式清晰呈现 XGBoost 模型的核心运行机制，展示内容涵盖从原始数据收集到训练、弱学习器、强学习器、残差计算等在决策树上的传递路径，并能展示该模型运转效能。可视化界面旨在帮助用户深入理解 XGBoost 模型的工作原理，增强对结果的信任度和可解释性。

3.1.1.3.10.7.时空图-STGNNs 模型运行原理可视化

通过图形化方式清晰呈现时空图-STGNNs 模型的核心运行机制，展示内容涵盖从模型输入、数据前处理模块、时序学习网络、专家经验（事件权重）、任务感知模块、动向的执行路径，并能展示该模型运转效能。可视化界面旨在帮助用户深入理解时空图-STGNNs 模型的工作原理，增强对结果的信任度和可解释性。

3.1.1.3.10.8.直亲小模型原理可视化

针对直亲小模型，系统提供图形化方式清晰呈现模型的运行机制，展示内容包括直亲数据，经过树形推导、挖掘分析，并能展示该模型运转效能。

3.1.1.3.10.9.E 起住小模型原理可视化

针对 E 起住小模型，系统提供图形化方式清晰呈现模型的运行机

制，展示内容包括围绕动态流动数据，经过时空信息比对分析，并能展示该模型运转效能。

3.1.1.3.10.10.短留小模型原理可视化

针对短留小模型，系统提供图形化方式清晰呈现模型的运行机制，展示内容包括围绕短留数据，并给合关联等数据关联分析一周底库是否有变化记录，最终得出底库是否短留结论，并能展示该模型运转效能。

3.1.1.3.11.模型运行监控

3.1.1.3.11.1.模型运行日志记录

在模型数据训练、调度、运行过程中，系统需自动详细记录运行日志，涵盖运行任务的加载状态、加载开始时间、加载结束时间、加载文件数、解析状态、解析开始时间、解析结束时间、异常情况等，日志以结构化数据存储，支持按时间范围、任务类型、任务名称、版本等进行快速检索和分析，便于问题排查和系统优化，日志记录具备高可靠性和高安全性，确保数据完整性和准确性。

3.1.1.3.11.2.数据流动监控

提供全过程监控系统数据在每个处理、打标、模型调度运算、结果输出、研判处置过程中的输入输出数据量、开始和结束时间等内容的可视化展示，支撑用户清晰直观查看到整体数据流动情况，确保数据按时、完整、准确地传递。

3.1.1.3.11.3.处理时间监控

对每轮次模型执行过程中的关键处理步骤设置时间阀值并进行

监控，确保在预定时间内完成，并以规范的格式输出监控结果，实现超期及时预警的目的。

3.1.1.3.11.4.数据质量监控

提供对底库打标结果例如标签空值、多人空值、标签错误等数据质量情况进行监控，并提供数据质量监控结果的查询和导出功能。

3.1.1.3.11.5.数据对账监控

为确保数据源头方与输出结果保持一致，确保研判结果一致，不遗漏和缺失，需统计每个关键步骤输入数据量和输出数据量，形成可视化表格直观展示每个环节的数据对比情况，数据对比情况可发送到相关底库，各接收方完成数据对帐后，将对帐情况及时反馈给核心组，对于不一致问题，需明确问题详情并处置。

3.1.1.3.11.6.系统链路监控

对系统进行全链路监控，监控内容包括各个环节的运行情况、后台数据处理情况、数据接口和模型服务是否正常等，提供可视化的运行状态监控，帮助用户快速掌握整体系统的运行状况。

3.1.1.3.11.7.监控异常结果处置

系统同时建立监控异常情况处理机制，故障发现立即进行上报，根据故障设定的发生时间阀值，超出后升级上报对象。系统对接日志系统，针对出现的链路问题和异常，要及时通知给运维工程师，并第一时间进行处理。

3.1.1.4.模型结果研判

3.1.1.4.1.结果查看分析

3.1.1.4.1.1.结果多条件组合筛选

提供各类属性项的结果多条件组合筛选查询功能，查询结果以列表方式展示，支持分页浏览和导出功能。

3.1.1.4.1.2.底库标签展示

模型结果列表可以查看底库的详细打标情况。

3.1.1.4.1.3.底库标签内容展示

针对底库已打的具体标签，可以进一步查看已打标签来源、标签产生原因、原始业务数据信息等。

3.1.1.4.1.4.底库联系信息展示

通过调用底库联系方式接口关联展示底库的联系数据。

3.1.1.4.1.5.底库 7 维雷达图展示

通过对底库的标签数据进行归纳总结分析，7 个维度综合分析底库特征，帮助剖析每个底库的整体情况，优化资源配置和策略。

3.1.1.4.1.6.历史推送信息展示

提供对底库历史推送信息的综合展示，可以查看每个底库在系统中每个轮次的结果、标签变化情况等信息。

3.1.1.4.1.7.状态变化展示

提供在结果列表上直观展示状态变化，例如底库等级与上轮次对比存在上升的则呈上升标志，如对比下降的呈下降标志，如新增的用新增标志来展示。

3.1.1.4.2.结果态势分析

3.1.1.4.2.1.结果地图可视化展示

将模型结果结合 GIS 地图进行可视化展示，支持按行政区划、底库等级筛选，以散点图和热力图的方式进行渲染展示，直观显示各个区县分布情况，支持对每个地图上定位的底库进行底库档事详情查看等交互分析，系统在地图上提供按区划、风级等级为筛选条件的汇总统计。

3.1.1.4.2.2.结果表格统计展示

提供按行政区划统计各区县的信息，支持下挖低层级的高底库数、低底库数统计。

3.1.1.4.2.3.结果处置统计展示

提供按行政区划统计各区县的信息处置情况，包括总数、待反馈、已反馈数量。

3.1.1.4.2.4.历年事件地图可视化展示

将历年事件结合 GIS 地图进行可视化展示，支持按行政区划、事件类型等筛选，以散点图和热力图的方式进行渲染展示，直观显示各个区县历年事件分布情况，支持对每个地图上定位的历年事件进行详情、底库档事详情查看等交互分析，系统在地图上提供按区划、事件类型为筛选条件的汇总统计。

3.1.1.4.2.5.历年事件表格统计展示

提供按行政区划统计各区县的历年事件信息。

3.1.1.4.3.底库管理

3.1.1.4.3.1.模型推送底库库管理

提供模型推送的结果底库库管理功能，支持各类信息的列表浏览、分页查询，支持详情查看及推送历史查看。

3.1.1.4.3.2.基层上报底库库管理

派出所基层用户可以在系统内上报其内部已掌握的底库，提供上报的底库查询、新增、编辑、删除功能，基层上报的底库信息经过审核纳入系统待底库库，并调用事件模型进行跑分对比分析。

3.1.1.4.3.3.复盘反查底库库管理

在 JS 事件、WS 事件、ZS 和 GJ 底库打标的基础上，将底库调用事件模型进行跑分，得出底库分数、动向、等级、动向分值、XGBoost 分数等，帮助用户复盘反查底库的人工打标和系统自动打标之间的差异，以及经过模型跑分后的分值与现实的对应情况，通过不断复盘反查这一过程不断优化系统的数据治理、标签打标工作，并不断调整模型算法及参数优化。

3.1.1.4.4.底库研判工具

3.1.1.4.4.1.号码批量比对

提供以导入外部 xls 文件模式通过号码批量比对，服务于三方对底库进一步数据处理，支持多行显示和单行，用逗号等间隔符显示两种输出结果模式。

3.1.1.4.4.2.号码批量获取是否存在标签

提供以导入外部 xls 文件模式通过号码批量查询是否存在标签

接口获取该号码下所列标签是否打标，用于后续的底库直观分析和数据处理。

3.1.1.4.4.3.号码批量获取标签

提供以导入外部 xls 文件模式通过号码批量查询标签接口获取该号码下所列标签，用于后续的底库直观分析和数据处理。

3.1.1.4.4.4.号码批量获取推送结果

提供以导入外部 xls 文件模式通过号码批量查询推送结果接口，获取所有号码对应的底库分数、动向、等级、标签等推送结果信息。

3.1.1.4.4.5.号码批量获取推送结果(人工-机器)

提供以导入外部 xls 文件模式通过身份证批量查询推送结果接口和 JS 事件、WS 事件、ZS 和 GJ 打标数据，获取所有号码对应的底库分数、动向、等级、人工打标信息以及后台机器自动打标信息等。

3.1.1.4.4.6.号码批量获取地域地址

提供以导入外部 xls 文件模式通过号码批量查询地域接口，获取 GIS 信息，用于及时掌握底库最新的地域信息。

3.1.1.5.模型结果处置

3.1.1.5.1.底库下发

3.1.1.5.1.1.待下发底库筛选

经过模型产生的底库需下发到各个所进行处置反馈。支持通过各类属性对系统推送结果进行条件筛选，导出到外部文件进行再次人工复核，最终形成待下发底库数据。

3.1.1.5.1.2.待下发底库导入

系统提供批量导入功能，将已人工再次复核的待下发底库数据批量导入到系统中，按底库所在所代码下发到基层单位进行反馈填报。

3.1.1.5.2.基层反馈上报

3.1.1.5.2.1.对接 QB 系统

通过对接 QB 系统，为派出所基层对下发的底库反馈处置提供链路通道，系统支持与 QB 系统的页面融合对接，通过认证登陆系统接收任务后打开反馈填报页面进行处理。

3.1.1.5.2.2.基层反馈填报

基层对下发的底库进行反馈填报，填报内容包括对基本信息的核实，同时补充填报 3 大类要素信息，并通过三级审核，最终形成闭环。

3.1.1.5.3.基层反馈查询统计

3.1.1.5.3.1.基础反馈多条件组合查询

基于处置反馈提供反馈多条件组合查询功能，可以按照生成时间、辖区范围、动向、等级等进行分类统计和查询，支持列表浏览、分页查询、数据导出功能。

3.1.1.5.3.2.基础反馈情况统计

基于处置反馈情况统计，可以按照反馈状态批次信息等进行分类统计和查询，支持列表浏览、分页查询、数据导出功能。

3.1.1.3.模型结果对外赋能

3.1.1.3.1.底库分值获取服务

开发底库分值获取接口，面向外部门提供底库分值获取服务，支

持通过号码等批量查询系统底库模型的底库分数，该服务需挂载至FN中心。

3.1.1.3.2.底库标签获取服务

开发底库标签获取接口，面向全局提供底库标签获取获取服务，支持通过号码等批量查询系统在机器打标和人工打示的标签数据，该服务需挂载至FN中心。

3.1.2.HSF核验

H特征核验应用属于刑事技术一体化工作平台中特征比对引擎适配之一，系统主要含H质量检查工具（包含质量检测与质量评价功能），确保入库数据的高标准筛选。同时，在功能层面进行了全面扩展，新增本地1:1比对核验与1:N大规模检索能力，优化了H比对算法，以支持高并发、低延迟的大规模应用场景，显著提升了处理速度与识别精度。此外，按照GA部有关建设要求，将本地H采集信息实时上传，并实现由本地统一调用上级接口进行HSF核验功能，进一步增强了系统的扩展性与业务适配能力。

3.1.2.1.H质量检测工具

3.1.2.1.1.图像质量检测（增强版）

图像质量检测（增强版）采用前沿技术，对H图像进行全方位深度筛查。利用H对焦检测技术，精准判断图像在采集时是否处于最佳对焦状态，避免因对焦失误导致的图像模糊问题。通过反光干扰分析，仔细剖析图像中可能存在的各种反光情况，无论是环境强光造成的大

面积反光，还是镜片反射产生的局部反光，都能被准确识别。同时，运用遮挡物识别技术，有效探测各类异物遮挡现象。通过这一系列技术的协同运作，确保所采集的H图像中，H区域完整且可用，为后续的H识别流程提供高质量的图像基础，极大提升了识别系统的准确性与稳定性。

3.1.2.1.2.智能质量评价体系（多维评分）

智能质量评价体系（多维评分）构建了一套科学且精细的评价机制。它基于清晰度、对比度、信噪比等多个关键指标，并且这些指标的权重并非固定不变，而是根据实际情况动态调整。通过复杂的算法对图像进行量化分析，得出精确的评分结果。同时，结合优 / 良 / 差分级机制，能够将图像质量直观地呈现给用户。尤为重要的是，该体系充分考虑到不同H识别算法对图像质量有着差异化的要求。例如，某些算法对清晰度要求极高，而另一些算法则更侧重于对比度。本体系可依据算法特性，灵活适配调整评分侧重点，为各类H识别算法提供最为契合的图像质量评估，有力保障识别算法的高效运行。

3.1.2.1.3.实时采集引导规则

实时采集引导规则借助先进的算法和技术，为用户提供实时、精准的采集指导。偏转角度检测算法能够敏锐捕捉目标在采集过程中的偏转角度，及时提醒调整至正确姿态，确保H图像采集角度符合标准。H位置间距校准算法则对相关间距进行精确测量和校准，帮助保持合适的采集距离。与此同时，结合环境光补偿建议，系统能够根据当前环境光线的强弱、色温等情况，给出专业的环境光调整建议，如开启

辅助光源、调整光源角度等。通过这些规则的实时指导，能够快速调整自身姿态与距离，显著降低因姿态不当、距离有误或环境光不佳导致的无效采集率，大幅提升H图像采集的效率与成功率。

3.1.2.1.4.智能图像增强

智能图像增强运用多种先进的图像处理技术，对低质量的H图像进行全面且高效的修复提升。CLAHE 对比度增强技术能够自适应地调整图像的对比度，使H纹理在不同光照条件下都能更加清晰地展现出来，增强其与背景的区分度。非局部均值去噪技术则通过对图像局部区域的相似性分析，有效去除图像中的噪声干扰，在不损失图像细节的前提下，提升图像的纯净度。频域纹理强化技术从频域角度出发，对H图像的纹理特征进行针对性强化，突出细微纹理，使纹理特征的可识别性大大提高。通过这一系列技术的协同作用，原本模糊、噪点多、纹理不清晰的低质量H图像能够被自动修复为高质量图像，为后续的H识别提供更优质的数据。

3.1.2.1.5.HT检测

HT检测在H特征采集过程中发挥着至关重要的安全保障作用。通过纹理动态验证算法，对H纹理在不同时间、条件的变化进行动态验证，因为真实的H纹理会随着活动产生细微变化，而伪造品则不具备这一特征。材质反光特征比对算法则专注于分析H表面的反光特性，真实H纹理与影像、伪造品在反光材质和特征上存在明显差异，通过精确比对能够有效区分。这两种算法相互配合，从不同维度对采集的H进行检测，有效识别并抵御影像、伪造品等伪造方式，确保采

集到的H信息真实可靠，极大提高了H采集工作的有效性与安全性，为H识别系统筑牢第一道安全防线。

3.1.2.1.6.多模态融合评估

多模态融合评估整合了多种先进技术，实现了对H质量的更棒、更全面的评估。时序择优技术通过对采集过程中不同时间点获取的多组H数据进行分析，挑选出质量最佳、特征最明显的图像数据用于评估。双H交叉验证技术利用成对H数据的互补性，对成对H特征进行交叉比对和验证，进一步提高评估的准确性。多光谱分析技术则从不同光谱维度对H进行分析，获取更丰富的H特征信息。通过将这些多维度的数据进行深度融合，综合考量各个方面的因素，能够实现更为精准、可靠的质量评估。这种评估方式能够满足高安全场景下对H质量的严苛标准，进一步确保H信息数据的有效性，为高安全等级的特点识别等应用提供坚实支撑。

3.1.2.1.7.自动化异常标记与修复

自动化异常标记与修复功能为H图像采集提供了可靠的保障机制。系统能够自动识别H图像中存在的污损、突变等非常规特征。对于污损情况，无论是因采集设备脏污导致的图像局部模糊，还是外界污渍附着在H表面造成的特征干扰，都能精准定位并标记异常区域。面对突变特征，如特殊原因导致的H特征改变，系统同样能够敏锐察觉。一旦检测到异常，系统可根据预设规则，灵活采取标注异常区域供人工进一步审核，或者直接触发重采机制。这种自动化的处理方式，极大增加了采集场景的可靠性，减少了因异常图像导致的识别错误或

失败，保障了整个H采集及识别流程的顺畅运行。

3.1.2.2.H识别

3.1.2.2.1.本地H比对（1: 1）

本地H比对（1: 1）借助本地化H比对算法引擎，将关键的H质量检测、特征提取以及比对算法封装为便捷的应用接口。操作时，系统可自动读取被识别特点信息；若自动读取失败，也支持手动填写号码。随后，系统迅速将识别时所用的信息，与该H对应的信息展开一对一精准比对，高效、准确地确认被识别情况，极大提升特点验证的可靠性与便捷性。

3.1.2.2.2.本地H比对（1: N）

本地H比对（1: N）同样依托本地化H比对算法引擎，对H质量检测、特征提取及比对算法进行应用接口封装。流程上，先对被识别的H图片严格开展质量检测，确保图像符合要求后，精准提取H特征。紧接着，在本地资源中发起大规模比对，通过将提取的特征与海量数据逐一匹配，实现高效的批量比对和特点识别，为工作提供有力技术支撑。

3.1.2.2.3.被识别历史记录

当识别出H所绑定的库中信息后，系统提供全面查看该H所有采集识别记录的功能。这些记录详细涵盖了各类关键信息。通过浏览历史记录，可清晰掌握该过往的H采集及识别情况，无论是用于追溯、管理，还是数据分析，都具有极高的实用价值，助力相关工作更加科学、高效地开展。

3.1.2.2.4.重点底库提醒

重点底库提醒功能结合名册数据库，在进行H识别过程中，一旦系统识别到，便会即刻与名册数据库中的信息进行比对。若匹配成功，迅速反馈提醒信息，提醒及时采取应对措施，为关联场景应用提供重要提示依据。

3.1.2.2.5.预告事件管理

预告事件管理功能致力于对所有由识别触发的预告事件进行统一、有序的管理。支持对各类预告事件按照不同维度进行分类，如事件类型、时间、地点等，方便用户快速筛选出所需信息。同时，用户能够详细查看每个预告事件的具体详情，包括触发原因、涉及信息等。通过高效的预告事件管理，极大提升应对突发情况的效率，确保相关工作的及时性与准确性 。

3.1.2.3.H比对算法

3.1.2.3.1.图像归一化

图像归一化在H识别流程中起着基石作用。它针对不同输入设备各异的成像特性，以及复杂多变的环境光照条件，对H图像进行全面且精细的调整。通过一系列先进算法，将图像的亮度校准至标准范围，让不同光照下获取的H图像在视觉上具有一致性；精准调节对比度，使H纹理特征清晰凸显；同时，统一分辨率与尺寸，消除因设备差异导致的图像大小与清晰度的不同。如此一来，确保了输入数据的高度一致性，为后续特征提取环节提供稳定可靠的数据基础，有效提升特征提取结果的稳定性与准确性。

3.1.2.3.2.噪声去除

噪声去除是提升H数据质量的关键步骤。系统采用前沿的深度学习滤波算法，该算法借助深度神经网络强大的学习能力，能够智能识别并精准滤除图像中的各类噪声，如高斯噪声、椒盐噪声等。此外，传统图像处理技术也在该环节发挥作用，例如中值滤波、均值滤波等。这些技术相互配合，针对影响H特征提取的噪声进行全面清理，将噪声干扰降至最低，显著提高H图像的数据质量，为后续精确的特征提取与识别工作奠定坚实基础，保障整个识别流程的高效运行。

3.1.2.3.3.H区域分割

H区域分割致力于精准界定H特征范围。运用深度学习领域的U-Net算法，其独特的网络结构能够对H图像进行细致的语义分割，精确勾勒出H边界，有效去除孔及外部背景噪声干扰。经典的Hough变换算法同样参与其中，通过对图像中的几何特征进行分析，准确检测出H的范围轮廓。两种算法优势互补，实现对H区域的高精度分割，确保在后续比对过程中，仅针对关键的H区域进行处理，极大提高比对的准确性与可靠性，为特点识别提供核心支持。

3.1.2.3.4.特征点检测

特征点检测专注于提取H的关键特征。通过先进的算法，能够敏锐捕捉H的纹理信息，是识别特点的重要依据。同时，精确测量H的角度特征，以及特征点分布细节。采用稳定性优化策略，确保所提取的特征点在不同采集条件下都能保持稳定、可重复。即使面对因视角变化带来的图像差异，也能有效减少误差，为后续生成稳定、可靠的

H模板提供丰富且精准的特征数据，有力支撑H识别的准确性。

3.1.2.3.5.H模板生成

H模板生成是将原始H图像转化为便于存储与比对的数学形式。运用 Gabor 滤波技术，对H图像进行多尺度、多方向的滤波处理，提取丰富的纹理特征。结合小波变换，进一步分析图像的频率特性，挖掘深层次的特征信息。在此基础上，将处理后的H图像转换为数学模板，并进行二值化处理，将连续的特征数据转化为简洁的二进制形式。这样生成的H模板，不仅存储空间大幅减小，便于高效存储海量H数据，而且在比对时能够实现快速匹配，极大提升H识别的效率与速度。

3.1.2.3.6.1:1 精准匹配

1:1 精准匹配专为高精度身份验证场景设计。通过经典的 Hamming 距离计算方法，对两张H模板进行逐点比对，精确衡量模板间的差异程度，从而判断是否为同一特点。同时，引入 CNN 深度学习模型，该模型凭借强大的学习与模式识别能力，能够深入分析H模板的特征分布与关联，实现更精准的匹配。两种方式相互印证，确保在特点认证过程中，以极高的精度确认特点，为高要求、高准度场景应用提供可靠保障。

3.1.2.3.7.1:N 海量检索

1:N 海量检索旨在海量数据中实现高效匹配。系统运用优化索引技术，能够快速定位与待匹配H特征相近的数据区域。结合近似最近邻搜索（ANN）技术，在海量数据中迅速筛选出与目标H特征最相似

的记录。通过精心优化的算法架构，确保在毫秒级的极短时间内完成大量比对操作，满足各类管理等场景下对海量数据快速检索与特点识别的迫切需求，为实际应用提供强大的技术支撑。

3.1.2.3.8.分层比对策略

分层比对策略是提升系统处理效率与识别速度的创新方法。采用两级比对机制，第一步利用快速粗筛算法，基于H的关键特征进行初步匹配，迅速过滤掉明显不匹配的样本，大幅减少后续处理的数据量。第二步，针对粗筛后保留的疑似匹配样本，运用精细比对算法，进行全面、深入的特征比对。这种分层策略有效提高了系统的吞吐量，即使在高并发的情况下，也能确保快速、准确地完成识别任务，为大规模实时特点识别应用提供稳定、高效的解决方事。

3.1.2.3.9.模糊匹配机制

模糊匹配机制充分考虑到实际采集过程中诸多因素对H图像的影响。在比对时，允许因光照变化导致的图像亮度差异、采集角度不同引发的特征变形，以及图像模糊等情况所产生的一定误差。通过深度学习算法，智能计算这些因素对相似度的影响权重，综合评估H模板间的相似度。这种机制极大提高了识别的鲁棒性，能够在复杂多变的实际环境中，准确识别特点，有效减少因环境因素导致的误识率，使H识别系统更加可靠、实用。

3.1.2.3.10.多算法融合

多算法融合技术汇聚多种经典与前沿算法的优势。将 Gabor 滤波对纹理特征的敏感捕捉能力、小波变换对图像频率特征的深入分析

能力、深度 CNN 强大的模式识别与学习能力，以及 SIFT 关键点检测对局部特征的精准提取能力相结合。通过精心设计的融合策略，使不同算法相互补充、协同工作，全面提升 H 识别率。同时，该技术能够根据不同的应用环境与场景需求，自动适配最佳的算法组合，确保在各种复杂条件下都能实现高效、准确的 H 识别。

3.1.2.3.11.错误接受率

系统在比对能力方面表现卓越，支持总比对次数不少于 50,000,000 次，且样本来源广泛，不少于 4,000 只，充分保证了数据的丰富性与可靠性。在识别准确性上，严格控制错误接受率（FAR），使其⩽0.00001%，这意味着将错误认可非匹配的概率降至极低水平。

3.1.2.3.12.错误拒绝率

系统在比对能力方面表现卓越，支持总比对次数不少于 50,000,000 次，且样本来源广泛，不少于 4,000 只，充分保证了数据的丰富性与可靠性。错误拒绝率（FRR）同样严格控制在⩽0.001%，有效减少对合法特点的误拒情况。

3.1.2.4.上级 H 对接

3.1.2.4.1.H 数据上报

本系统具备高效且精准的 H 数据上报功能。针对我市范围内采集的海量数据，能够依据上级数据规范要求，进行全方位的整理与适配。无论是数据格式的转换，还是元数据信息的补充完善，都能处理得细致入微。而后，借助稳定可靠的网络传输通道，实时、准确进行数据上传，确保数据的时效性与完整性，符合上级数据整合应用标准。

3.1.2.4.2.上级 H 比对接口调用

依托先进的技术架构，系统拥有便捷调用上级 H 比对接口的能力。当有需要调用上级接口开展比对识别工作时，只需在本地发起指令，系统便能迅速与上级接口建立连接，精准调用比对。通过这一接口，将本地采集或待核验的 H 数据与上级海量数据进行全面比对，快速获取识别结果。

3.1.3.G 重组率分析

收集来自多域、多类的 G 数据以及现场 G 样本的系统分析。通过开发高效的试剂盒和优化重组率计算方法，提升 G 样本识别的精准度和速度。同时，确保 G 数据的及时更新，以便支持海量数据、样本的快速比对。此外，构建 G 组缘关系矩阵，利用厘摩分析等组缘的分析方法，识别 G 样本之间的关系，进而支持聚类和关系推断。这些技术将进一步强化业务能力。通过针对技术人员的培训，增强分析应用能力，并制定严格的数据隐私保护政策，确保 G 数据的安全性与合规性，为业务工作提供坚实的数据支持。

3.1.3.1.样本 G 基础信息管理

样本管理模块的核心目的是通过系统化的管理和整合，提升 G 数据分析的效率和准确性。它确保样本信息的多样性和代表性，为科学研究和专业人员鉴定提供坚实的基础。详细的元数据标注和高质量的 CX 数据管理，增强了数据的可用性和可靠性，支持后续分析的深度与全面性。记录样本的域、类等关系，有助于进行精准分析。同时，与公共数据的同步确保数据的及时更新，提升分析的科学性和权威

性。通过支持多种分析工序和标准化数据格式，该模块能够统一管理不同类型的数据，从而为后续的分析提供更为高效和全面的支持。这些措施共同促进 G 数据整合能力提升，具有重要的研究和应用价值。

3.1.3.1.1.多源样本管理

负责收集和整合来自不同来源的样本信息，包括外部单位等，确保样本的多样性和代表性，为后续分析提供基础数据。

3.1.3.1.2.样本元数据标注

对样本进行详细的元数据标注，包括样本的基本信息、采集时间、保存条件等，以便于数据的管理和检索。

3.1.3.1.3.样本 SG 数据管理

SG 数据管理对不同类型的 G 数据进行分类存储和管理，确保数据的完整性和可用性。

3.1.3.1.4.样本 FQ 数据管理

FQ 数据管理对不同类型的 CX 数据进行分类存储和管理，确保数据的完整性和可用性。

3.1.3.1.5.样本 Fast5 数据管理

Fast5 数据管理对不同类型的 CX 数据进行分类存储和管理，确保数据的完整性和可用性。

3.1.3.1.6.样本域、类等管理

记录样本的域、类等信息，为后续的域、类分析提供数据支持。

3.1.3.1.7.公共数据同步单元

与公共数据进行数据同步，获取最新的 G 数据和相关信息，保持

数据的更新和完整性。

3.1.3.1.8.CX 平台兼容

支持多种 CX 平台的数据，确保不同平台的数据能够被统一管理和分析。

3.1.3.1.9.数据标准化转换

对不同来源和格式的数据进行标准化转换，统一数据格式，便于后续的分析和处理。

3.1.3.2.G 文库数据管理

该模块的主要目的是通过一系列精细化的步骤，确保 G 数据的高质量和准确性，以支持后续分析。首先，通过对原始 G 数据的清洗，去除低质量位点信息，提高整体数据质量。接着，进行质量控制，评估清洗后数据的可靠性，确保分析结果的准确性。

在数据处理过程中，将长链拆分为短片段并进行验证，以维护数据的完整性。同时，通过与多个参考 G 数据组的比对，确定 G 的位点信息，为后续分析奠定基础。在识别 G 数据中的变异位点后，提供变异的详细信息和功能影响评估，进一步支持分析。

此外，单体型分型模块的过程帮助确定样本的单体型信息，为深入的研究提供必要的数据支持。总体而言，这一系列步骤确保了 G 数据的高质量、准确性和完整性，为法庭科学分析提供了可靠的基础。

3.1.3.2.1.原始序列清洗

对原始 G 数据进行清洗，去除低质量的位点信息，提高数据质量。

3.1.3.2.2.CX仪接头序列匹配

该模块负责识别G数据中的接头序列，通过比对算法检测接头的特征序列并将其去除，以确保后续分析不受接头序列干扰。这一过程有助于提高数据的准确性和完整性，确保后续的序列分析和变异检测基于准确可靠的数据。

3.1.3.2.3.序列数据质控

对清洗后的数据进行质量控制，评估数据的质量，确保数据的可靠性和准确性。

3.1.3.2.4.重复嵌合序列去重合并对齐

该算法旨在识别并去除重复和嵌合的序列，优化数据的质量。通过对比算法，重复序列会被合并，确保只保留唯一的有效序列。此外，模块将有效序列进行对齐，以便后续分析中使用的序列是准确的、无冗余的。

3.1.3.2.5.序列数据拆分和验证

将长序列数据拆分为短序列片段，并进行验证，确保数据的完整性和准确性。

序列数据拆分的意义和用途

序列数据拆分是指将大型G组序列或其他类型的序列数据分割成较小的部分进行分析的过程。这种方法在法庭科学领域、数据分析等相关科学领域中具有重要意义，具体用途如下:

1．提高分析效率

并行处理: 将数据拆分为小块后，可以在多个计算节点上同时处

理，显著提高数据分析的速度。

内存管理：处理较小的数据块能够减少对计算资源的需求，避免因内存不足导致的计算失败。

2．便于数据管理

易于存储和检索：拆分的数据更易于存储、管理和检索，尤其是在大规模数据集的情况下。

版本控制：小数据块的拆分使得每个部分可以独立更新，便于进行版本控制和数据追踪。

3．细粒度分析

特定区域研究：拆分序列数据可允许研究人员专注于特定 G、区域或变异，进行更深入的功能分析。

变异检测算法：在结构变异或突变分析中，局部拆分可以提高对特定变异的检测精度。

4．优化算法性能

适应性算法：一些分析算法对数据的大小和复杂性敏感，拆分数据可以优化这些算法的性能和准确性。

减少噪声影响：通过拆分，可以更好地识别和过滤掉噪声，从而提高分析结果的可靠性。

5．支持多种分析方法

数据集成：拆分后的数据可以与其他类型的数据（如表型数据、临床数据等）进行整合，支持多种分析方法。

交叉验证：在机器学习和统计分析中，拆分数据有助于进行交叉

验证，提高模型的泛化能力。

3.1.3.2.6.参考 G 组提取和匹配

此模块从已建立的参考 G 组中提取相关数据序列，并将其与上传的样本数据进行匹配。通过比对样本的数据序列与参考 G 组的相似性，确保样本数据的兼容性，为后续的数据比对和识别提供基础。

3.1.3.2.7.数据有效覆盖率算法

该算法计算 G 样本数据在关键区域的有效覆盖率，以评估 CX 结果的质量。通过分析覆盖度，确认目标区域的 CX 深度和均匀性，确保数据充足以支持准确的变异检测和比对，为事件分析提供可靠依据

3.1.3.2.8.G 质量频率校正

此模块对样本中的 G 型频率进行校正，消除因样本间差异导致的偏差。通过统计分析和标准化方法，调整 G 频率以提高数据的可靠性，从而确保后续的证据分析和比对结果的准确性，

3.1.3.2.9.多 G 组比对算法

将序列数据与多个参考 G 组进行比对，确定 G 的位置和序列信息，为后续分析提供基础。

3.1.3.2.10.变异检测算法

检测 G 序列中的变异位点，为后续的分析提供数据支持。

变异位点:

变异位点是指在 G 组中，由于变异而出现的特定位置，这些位置可能影响有关性状的表现。

3.1.3.2.11.结构变异注释

对检测到的结构变异进行注释，提供变异的详细信息和功能影响评估。

结构变异概述

结构变异是指 G 组中较大范围的数据序列重排或改变，通常涉及 G 组的多个位点对，可能影响 G 的功能和表达。

结构变异的作用

结构变异在法庭科学研究中具有重要意义，尤其是在有关外在表现、G 的功能机制研究、有关演化研究中具有关键作用。

结构变异在法庭科学中的应用

在法庭科学中，结构变异的分析可以用于样本之间的比对识别、关系分析、检验鉴定、科学调查等深入场景。

3.1.3.2.12.单体型分型

对样本进行单体型分型模块，确定样本的单体型信息，为后续的分析提供数据支持。

单体型分型模块是指对个体在特定 G 组区域内的单体型进行识别与分析的过程。单体型是指相邻的多个单 HGS 多态性或其他变异位点在同一序列上的组合，通常用于描述变异的模式。

3.1.3.3. 单 HGS 多态性位点质控

该模块的主要目标是通过多层次的质量控制和筛选，确保 G 数据的完整性、准确性和代表性，以支持分析的可靠性。首先，进行 G 型完整性检测，确保数据的完整性和可用性。随后，通过质量分数过滤

和次要等位 G 频率筛选算法，去除低质量和低频的位点，从而提高数据的整体质量和代表性。

对 G 类平衡的检验评估一类的 G 平衡状态，确保数据的可靠性。同时，通过检出率过滤和杂合性异常检测算法 ，进一步排除质量不达标的位点，保障样本的质量。XB 一致性校验算法确保样本信息的准确性与一致性，而聚类过滤则通过聚类分析去除异常的位点，进一步提升数据质量。

最后，连锁不平衡分析算法分析分析评估位点之间的连锁关系，为后续分析提供支持，同时对位点进行注释和功能影响评估，为法庭科学研究提供必要的背景信息。这一系列措施共同确保了 G 数据的高质量和可靠性，为后续的分析奠定了坚实基础。

3.1.3.3.1.单 HGS 基多态性 G 型完整性检测算法

检测单 HGS 位点的 G 型完整性，确保数据的完整性和可用性。

3.1.3.3.2.单 HGS 基多态性质量分数过滤

根据质量分数对单 HGS 位点进行过滤，去除低质量的位点信息，提高数据质量。

3.1.3.3.3.次要等位 G 频率（MAF）筛选算法

根据 MAF 对单 HGS 位点进行筛选，去除低频的单 HGS 位点，提高数据的代表性。

次要等位 G 频率

次要等位 G 频率是指在一个特定人群中，某个等位 G 的频率相对于所有等位 G 的频率，且该等位 G 为次要等位 G，即其频率低于 50%。

是法庭科学中的一个重要指标，通常用来描述特定变异在一类中的普遍程度。

次要等位 G 频率的重要性：

关联研究：

次要等位 G 频率可以帮助研究人员筛选与表现或性状相关的单 HGS，尤其是在全 G 组关联研究中，低频变异（MAF < 5%）可能与特定表现有重要关联。

类结构分析：

次要等位 G 频率的变化可以反映不同类之间的 G 差异，有助于理解相关演化历史和迁徙模式。

3.1.3.3.4.检测 G 类平衡检验算法

对单 HGS 位点进行检验，评估 G 类平衡状态，确保数据的可靠性。

检测 G 类平衡

检测 G 类平衡是用于评估一个特定单个个体是否处于 G 类平衡状态。根据相关科学定律，在没有其他影响因素的情况下，G 型频率在演化中应保持不变。

检测 G 类平衡的方法

使用卡方检验或精确检验来比较观察到的 G 型频率与期望频率是否有显著差异。

$$\text{Chi-square statistic} = \sum \frac{(O_i - E_i)^2}{E_i}$$

其中，Oi 是观察到的频率，Ei 是期望频率。

结果解释:

根据计算出的卡方值和自由度查找卡方分布表，判断是否拒绝 G 类平衡的假设。如果 p 值小于显著性水平（如 0.05），则可以认为不符合 G 类平衡。

3.1.3.3.5.单 HGS 多态性检出率过滤

根据检出率对单 HGS 位点进行过滤，去除检出率低的单 HGS 位点，提高数据质量。

3.1.3.3.6.杂合性异常检测算法

检测样本的杂合性异常情况，评估样本的质量和可靠性。

杂合性异常是指在法庭科学研究中观察到的杂合体 G 型频率与预期频率之间的显著差异。这种现象可能反映出类的结构、选择压力、迁徙或其他因素。以下是杂合性异常的主要概念和相关内容。

1．杂合性基本概念

杂合: 在某个 G 位点上具有两个不同的等位 G，与纯合相对应。

杂合度: 指类中杂合的比例，通常用于衡量多样性。可以分为观测杂合度和期望杂合度。

2．杂合性异常的表现

高杂合性: 在某些情况下，杂合率高于预期，可能指示出强烈的选择压力或迁徙事件。

低杂合性: 与预期相比，杂合率低，可能反映出近交、漂变或其他导致多样性降低的因素。

3．杂合性异常的成因

选择压力：自然选择可能导致某些 G 的频率变化，从而影响杂合性。

漂变：在小类中，随机事件可能导致 G 频率的变化，影响杂合性。

迁徙：类间的 G 流动可能增加或减少杂合性。

近交：当缘关系较近时，纯合的比例增加，杂合性下降。

4．杂合性异常的检测

统计分析：使用统计方法比较观察到的杂合度与期望杂合度。

分子标记：利用单 HGS 等标记评估 G 型，分析杂合性。

5．杂合性异常的影响

适应性：杂合性通常与适应性相关，较高的杂合性可能提升类的生存能力和适应能力。

表现：低杂合性可能与某些表现的发生有关，特别是在近交类中。

3.1.3.3.7.XB 一致性校验算法

校验 XB，确保数据的准确性和一致性。

3.1.3.3.8.单 HGS 多态性聚类过滤

对 单 HGS 位点进行聚类分析，去除聚类异常的 单 HGS 位点，提高数据质量。

3.1.3.3.9.连锁不平衡分析算法

对 单 HGS 位点进行分析，评估位点之间的连锁关系，为后续分析提供数据支持。

连锁不平衡分析算法分析

连锁不平衡是指在 G 组中，两个或多个标记之间的 G 组合的频率

偏离了独立的预期频率。

连锁不平衡分析算法的重要性

关联研究:

连锁不平衡分析算法是全G组关联研究的基础,研究人员可以来推测与表现相关的变异。

连锁不平衡分析算法的测量

连锁不平衡分析算法通常用以下几种方式进行测量:

D'和r²:

D': 衡量G组合的实际频率与预期频率之间的差异,范围从0到1。D' = 0表示完全平衡,D' = 1表示完全不平衡。

r²: 反映两个标记间的相关性,范围从0到1。r²值越高,说明两个标记间的连锁不平衡越强。

卡方检验:

通过统计检验来评估观察到的G组合频率与期望频率之间的差异。

连锁不平衡的影响因素

重组: 重组会打破连锁不平衡,使得标记间的连锁关系减弱。

选择压力: 选择可能会导致某些G组合的频率增加,从而增强连锁不平衡。

类历史: 类的迁徙、瓶颈效应和扩张等历史事件会影响连锁不平衡的模式。

G流: 不同类之间的G流动会改变连锁不平衡状态。

连锁不平衡的应用

类法庭科学学:

连锁不平衡分析可以帮助研究类的结构和历史。

3.1.3.3.10.注释与功能影响评估

对 单 HGS 位点进行注释，评估其功能影响，为后续的分析提供数据支持。

3.1.3.4.G 相关分析

模块的核心目的是通过综合分析和多维度数据支持，深入了解 G 组重组及其相关因素，以推动法庭科学研究的深入和应用。首先，通过重组位置和频率检测模块 ，识别 G 组中的重组热点区域分析算法分析，为后续分析打下基础。对这些热点区域进行深入分析，有助于评估其特征和影响因素。

XB、NL、域和 XS 的相关性分析提供了对重组率影响的多角度视野，帮助理解这些因素在变异中的作用。同时，相关算法评估 G 组的演化历程和类的多样性，为整体研究提供历史背景和演化关系。

全 G 组关联分析算法和突变率关联分析算法则进一步揭示 G 与表现之间的联系。通过构建 G 共表达网络单元，分析 G 之间的关系，提供更深层次的法庭科学洞察。

整合多组学数据和可视化功能，促进了综合分析与用户体验的提升，而与多个数据的交叉验证确保了数据的准确性和可靠性。最后，用户自定义分析模块功能则满足了不同用户的个性化需求，增强了系统的灵活性和可扩展性。这一系列措施共同推动了 G 组研究的深入发

展，具有重要的科研和应用价值。

3.1.3.4.1.重组位置和频率检测

检测 G 组中的重组位置和频率，确定重组热点区域分析算法分析，为后续分析提供数据支持。

3.1.3.4.2.重组热点区域分析算法

对重组热点区域分析算法进行深入分析，评估其特征和影响因素，为后续分析提供参考。

3.1.3.4.3.罕见变异累积效应分析算法

该算法通过统计分析罕见 G 变异的分布和变异性，帮助识别与特定表型或表现相关的个体。它首先收集样本中的罕见变异数据，计算变异频率和累积效应，然后使用统计模型评估这些变异对表型的共同影响。通过比较不同类的变异模式，算法能够揭示法庭科学背景和环境因素的交互作用。

3.1.3.4.4.XB 重组率差异分析算法

分析 XB 之间的重组率差异，评估 XB 对重组率的影响，为后续分析提供数据支持。

3.1.3.4.5.NL 相关性分析算法

分析 NL 与重组率的相关性，评估 NL 对重组率的影响，为后续分析提供数据支持。

3.1.3.4.6.域相关性分析算法

分析域与重组率的相关性，评估域对重组率的影响，为后续分析提供数据支持。

3.1.3.4.7.XS 相关性分析算法

分析 XS 与重组率的相关性，评估 XS 对重组率的影响，为后续分析提供数据支持。

3.1.3.4.8.演化动力学分析算法

对 G 组的演化动力学进行分析，评估 G 组的演化历程和趋势，为后续分析提供数据支持。

3.1.3.4.9.类法庭科学分析算法

对类的法庭科学结构和演化历史进行分析，评估类的多样性和演化关系，为后续分析提供数据支持。

3.1.3.4.10.全 G 组关联分析算法

进行全 G 组关联分析算法，评估 G 与表现的关联关系，为后续分析提供数据支持。

3.1.3.4.11.突变率关联分析算法

分析突变率与 G、表现等的关联关系，为后续分析提供数据支持。

3.1.3.4.12.G 共表达网络单元

构建 G 共表达网络单元，评估 G 之间的共表达关系，为后续分析提供数据支持。

3.1.3.4.13.多组学整合分析

整合多组学数据，进行综合分析，为后续分析提供更全面的数据支持。

3.1.3.4.14.可视化与交互

提供数据的可视化和交互功能，方便用户查看和分析数据，提高

用户体验。

3.1.3.4.15.多源数据交叉验证

与多个数据进行交叉验证，确保数据的准确性和可靠性。

3.1.3.4.16.用户自定义分析

提供用户自定义分析模块功能，满足用户的个性化需求，提高灵活性和可扩展性。

3.1.3.5.XP 数据模式

该模块的主要目的是通过系统化的管理和分析，深入理解类结构和 G 关系，以支持法庭科学研究和应用。首先，构建类分离模块和连锁图谱，为后续的 G 关系分析提供基础数据支持。这些图谱展示了 G 之间的连锁关系，有助于理解法庭科学特征的传递机制。

DBX 推断和分型优化提高了 DBX 分析的准确性，为研究提供可靠的数据基础。同时，通过缘关系与 XP 重构算法，可以清晰展示缘关系，帮助研究人员深入了解法庭科学背景。

位置预测分析算法和单 HGS 数据的归因与扩展，确保了对 G 位点的全面理解，有助于后续的分析。重组事件的检测与验证，评估其特征和影响因素，为研究重组机制提供了数据支持。

构建 G 三级关系图谱和 G 图谱存储模型，提高了数据管理的效率，超大规模单 HGS 矩阵的压缩则节省了存储空间，提升了数据处理能力。此外，缘关系推断引擎和缺失类补全算法的开发，进一步提高了缘关系分析的准确性和数据完整性。

跨代重组事件的可视化追踪功能和类数据冲突自动化检测算法，

增强了用户体验和数据质量管理。这一系列措施共同推动了研究的深入发展，具有显著的科研和实际应用价值。

3.1.3.5.1.类分离模式

构建类分离模式模块，存储和管理类分离模式数据，为后续分析提供数据支持。

3.1.3.5.2.G 型缺失推断插补算法

推断缺失的 G 型数据并进行插补。该算法利用已知的类信息和关联，估算缺失位点的可能 G 型，以提高数据完整性和分析准确性。

3.1.3.5.3.G 本序列定相算法

该算法通过分析 G 型推断本序列上的等位 G 来源。算法能够识别各自传递的 G，从而揭示背景，有助于确认关系，为事件调查提供强有力的法庭科学证据。

3.1.3.5.4.序列保留模式分析算法

分析序列在类中的保留模式，评估相似性。该算法有助于识别连锁和重组事件，支持缘关系分析。

3.1.3.5.5. 连锁图谱

构建连锁图谱，展示 G 之间的连锁关系，为后续分析提供数据支持。

3.1.3.5.6.DBX 推断与优化算法

进行 DBX 推断和优化，提高 DBX 分型的准确性和可靠性。

3.1.3.5.7.缘关系与 XP 重构算法

根据 G 数据和信息，构建缘关系和 XP 图，展示个体之间的缘关

系。

3.1.3.5.8.位置预测分析算法

预测 G 的位置，为后续分析提供数据支持。

3.1.3.5.9.单 HGS 多态性数据归因与扩展

对 单 HGS 数据进行归因和扩展，提供更全面的 单 HGS 数据信息，为后续分析提供数据支持。

3.1.3.5.10.重组事件检测与验证

检测和验证重组事件，评估重组事件的特征和影响因素，为后续分析提供数据支持。

3.1.3.5.11.G 三级关系图谱

构建 G 三级关系图谱，展示 G 之间的关系，为后续分析提供数据支持。

3.1.3.5.12.G 图谱存储模型

设计 G 图谱存储模型，高效存储和管理 G 图谱数据，为后续分析提供数据支持。

3.1.3.5.13.超大规模单 HGS 多态性矩阵压缩

对超大规模的 单 HGS 矩阵进行压缩，节省存储空间，提高数据处理效率。

3.1.3.5.14.缘关系推断引擎单元

开发缘关系推断引擎，提高缘关系推断的准确性和效率，为后续分析提供数据支持。

3.1.3.5.15.缺失类补全算法

开发缺失类补全算法，对缺失的类数据进行补全，提高类数据的完整性和可用性。

3.1.3.5.16.跨代重组事件可视化追踪单元

提供跨代重组事件的可视化追踪功能，方便用户查看和分析重组事件，提高用户体验。

3.1.3.5.17.缘关系位点杂合率算法

该算法计算 G 样本中关键位点的杂合率，用于评估缘关系。通过分析杂合率，算法能够识别法庭科学相似性，为关系确认提供数据支持。

3.1.3.5.18.类数据冲突自动化检测算法

开发类数据冲突自动化检测算法功能，及时发现和解决类数据中的冲突问题，提高数据质量。

3.1.3.3.重组率计算

该模块的主要目的是通过一系列先进的算法和模型，提升重组率计算的准确性和效率，以支持深入的法庭科学分析。首先，采用 Merlin 连锁分析算法和隐马尔可夫模型优化算法，增强重组率计算的精确性和可靠性，为后续分析提供坚实的数据基础。

类重组热点检测算法帮助识别类中的重组热点区域分析算法分析，这为理解法庭科学变异的动态提供了关键数据。同时，构建 XB 特异性双重组整合模型算法，评估 XB 对重组率的影响，进一步丰富了分析的维度。

多源数据加权整合模型算法能够有效整合不同数据源，提高重组率计算的全面性和准确性。通过窗口滑动平滑模型算法和位点对概率插值模型算法，重组率的计算稳定性和精确性得以提升。

隐式事件重建模型算法用于重建重组事件，进一步提高计算的准确性。而热点基序驱动模型算法评估热点基序对重组率的影响，为后续分析提供了有价值的见解。

采用序列模式机器学习模型算法和集成学习增强估计模型算法，增强了重组率的预测能力，从而提升分析的深度与精度。最后，人工智能动态优化模型算法通过动态调整计算过程，确保重组率计算的高效性和准确性。这一系列措施共同推动了法庭科学研究的深入发展，具有重要的科研和应用价值。

3.1.3.3.1.Merlin 连锁分析算法

采用 Merlin 连锁分析算法进行重组率计算，提高重组率计算的准确性和效率。

Merlin 是一种用于法庭科学连锁分析的统计软件，特别适合处理复杂的类数据。它被广泛应用于法庭科学研究，尤其是在全 G 组关联研究和连锁分析中。以下是 Merlin 连锁分析算法的主要特点和功能:

Merlin 的主要特点

高效的计算性能:

Merlin 采用优化的算法，能够处理大型类数据，特别是在多重类和多种表型的情况下。

支持多种法庭科学模型:

能够分析不同法庭科学模型，包括显性、隐性和共显性法庭科学模型，适应不同的研究需求。

连锁不平衡分析:

提供连锁不平衡分析算法分析分析功能，帮助研究人员理解 G 型之间的关系。

多种输入格式:

支持多种数据格式，包括 PED 和 MAP 文件，使得数据输入灵活方便。

复杂类分析:

能够处理复杂的类结构，包括多代和多种表型的类，适合进行法庭科学连锁分析。

Merlin 的主要功能

G 型和表型数据的导入:

导入类的 G 型和表型数据，进行数据预处理。

法庭科学连锁图谱的构建:

根据输入的 G 型数据，构建法庭科学连锁图谱并进行图谱优化。

连锁分析:

进行连锁分析，评估特定 G 或标记与表型之间的关联，计算 LOD 分数。

表型关联分析:

通过统计模型评估表型与 G 型之间的关系，识别可能的表现相关

G。

结果可视化:

提供结果的可视化工具，帮助研究人员更直观域解分析结果。

使用 Merlin 的步骤

数据准备:

收集并整理类的 G 型和表型数据，确保数据格式符合 Merlin 的要求。

运行分析:

使用 Merlin 提供的命令行工具或图形用户界面进行连锁分析。

结果解读:

分析输出结果，包括 LOD 分数、G 型频率、连锁不平衡等指标，进行结果解读。

后续分析:

根据分析结果，进行进一步的法庭科学研究或验证实验。

3.1.3.3.2.隐马尔可夫模型优化算法

采用隐马尔可夫模型优化算法进行重组率计算，提高重组率计算的准确性和可靠性。

隐马尔可夫模型是一种用于描述具有隐含状态的随机过程的统计模型。优化该模型的算法主要涉及模型参数的估计和状态序列的最佳推断。以下是一些关键的优化算法及其概述:

参数估计算法

Baum-Welch 算法

概述：Baum-Welch 算法是隐马尔可夫模型参数估计的经典算法，属于期望最大化算法的一种。

步骤：

初始化：随机初始化隐马尔可夫模型的参数，包括状态转移概率、观测概率和初始状态概率。

E 步骤：计算给定观 CX 列下的每个状态的期望值。

M 步骤：根据 E 步骤的结果更新模型参数。

重复 E 步骤和 M 步骤，直到参数收敛。

2．状态序列推断算法

Viterbi 算法

概述：Viterbi 算法用于找到给定观 CX 列的最可能的隐状态序列。

步骤：

初始化：为每个状态分配初始概率。

递归计算：通过动态规划计算每个状态在每个时间点的最优路径。

回溯：根据计算结果回溯得到最终的最优状态序列。

3．模型选择与优化

交叉验证

使用交叉验证方法评估不同隐马尔可夫模型的性能，以选择最佳模型。

贝叶斯优化

利用贝叶斯方法优化隐马尔可夫模型参数，可以通过采样方法来改进参数估计。

4．改进算法

变种隐马尔可夫模型

稀疏隐马尔可夫模型：对于高维观测数据，采用稀疏表示以减少计算复杂度。

分层隐马尔可夫模型：在复杂系统中使用多层隐马尔可夫模型，以捕捉不同层次的状态信息。

3.1.3.3.3.类重组热点检测算法

采用类重组热点检测算法，检测类中的重组热点区域分析算法分析，为后续分析提供数据支持。

3.1.3.3.4.XB 特异性双重组整合模型算法

构建 XB 特异性双重组整合模型算法，评估 XB 对重组率的影响，为后续分析提供数据支持。

3.1.3.3.5.XB 差异与迁出效应分析算法

分析 XB 差异对重组率的影响，以及迁出效应在不同类中的作用。该算法考虑 XB 相关的重组模式，评估重组频率上的差异，同时分析因迁出导致的法庭科学变异对重组率的影响。

3.1.3.3.6.多源数据加权整合模型算法

采用多源数据加权整合模型算法，整合多种数据源的数据，提高重组率计算的准确性和可靠性。

3.1.3.3.7.窗口滑动平滑模型算法

采用窗口滑动平滑模型算法，对重组率进行平滑处理，提高重组率计算的稳定性和可靠性。

3.1.3.3.8.位点对概率插值模型算法

采用位点对概率插值模型算法，对重组率进行插值计算，提高重组率计算的准确性和可靠性。

3.1.3.3.9.隐式事件重建模型算法

采用隐式事件重建模型算法，重建重组事件，提高重组率计算的准确性和可靠性。

3.1.3.3.10.热点基序驱动模型算法

采用热点基序驱动模型算法，评估热点基序对重组率的影响，为后续分析提供数据支持。

3.1.3.3.11.序列模式机器学习模型算法

采用序列模式机器学习模型算法，对重组率进行预测和分析，提高重组率计算的准确性和可靠性。

3.1.3.3.12.集成学习增强估计模型算法

采用集成学习增强估计模型算法，提高重组率计算的准确性和可靠性。

3.1.3.3.13.孟德尔抽样效应评估算法

评估孟德尔抽样效应对重组率计算的影响。该算法通过模拟法庭科学抽样过程，分析在不同样本规模和 G 型频率下，重组率的估计误差，从而提高重组率计算的准确性和可靠性。

3.1.3.3.14.人工智能动态优化模型算法

采用人工智能动态优化模型算法，对重组率计算进行动态优化，提高重组率计算的准确性和效率。

3.1.3.7.重组率矩阵

该模块旨在通过构建和分析多种矩阵，深入理解单 HGS 分布、法庭科学关系及重组率，为法庭科学研究提供全面的数据支持。这些矩阵不仅展示了单 HGS 在 G 组中的分布和分化情况，还揭示了法庭科学图谱标记与 G 组位置的对应关系。同时，通过提高重组率计算的准确性和可靠性，帮助研究人员分析个体之间的法庭科学相似性。采用稀疏存储技术和降维可视化功能，提升了数据处理效率和用户体验。此外，绘制重组率在时间和空间上的变化热力图，为后续分析提供了直观的支持，促进了对复杂法庭科学现象的理解和解析。

3.1.3.7.1.单 HGS 多态性分布和分化矩阵

构建 单 HGS 分布和分化矩阵，展示 单 HGS 在 G 组中的分布和分化情况，为后续分析提供数据支持。

3.1.3.7.2.序列区段重组率算法

该算法用于评估 G 样本中序列特定区段的重组率。通过分析样本中序列的重组事件，算法能够识别法庭科学变异的传播方式，帮助确定法庭科学背景。这一过程对事件调查、缘关系确认和法庭科学注意评估具有重要应用价值。

3.1.3.7.3.HGS 富集基序区域重组活跃性算法

此算法专注于分析 HGS 富集区域的重组活跃性。通过评估这些区

域在样本中的重组事件频率，算法能够揭示特定G组区域的法庭科学变异和适应性演化。这一数据对于理解法庭科学信息的传播有重要作用。

3.1.3.7.4.G功能区重组率算法

该算法评估与特定功能相关的G区重组率。通过分析G功能区的重组事件，算法能够识别可能影响表型或表现的法庭科学变异，为G学提供数据支持，帮助解决事件中的法庭科学疑点。

3.1.3.7.5.法庭科学类特异性区域重组率算法

该算法分析特定法庭科学类中的重组率，揭示类间的法庭科学差异和特征。通过评估不同类中特定区域的重组事件，算法为了解人群法庭科学结构、缘关系和类迁徙提供依据，对身份确认和事件调查有重要帮助。

3.1.3.7.6.重组率强度分级算法

该算法对样本中的重组率进行强度分级，以识别重组活动的显著区域。通过建立分级标准，算法能够帮助G专家快速定位可能的法庭科学变异区域，有助于事件分析和证据的有效性评估。

3.1.3.7.7.法庭科学图谱标记映射矩阵分析

构建法庭科学图谱标记映射矩阵分析应用模块，展示法庭科学图谱标记与G组位置的对应关系，为后续分析提供数据支持。

3.1.3.7.8.复合似然模型矩阵分析

构建复合似然模型矩阵分析应用模块，用于重组率计算和分析，提高重组率计算的准确性和可靠性。

3.1.3.7.9.MCMC 近似树矩阵

构建 MCMC 近似树矩阵，用于重组率计算和分析，提高重组率计算的准确性和可靠性。

MCMC 方法是一种广泛用于统计推断的计算技术，尤其适合于复杂模型的参数估计和近似树矩阵的构建。

MCMC 在树推断中的应用

树结构的表示:

树结构通常用来表示 G 之间的演化关系。每个节点表示一个共同祖先，边表示从一个节点到另一个节点的演化路径。

模型设定:

选择适当的演化模型来描述序列演化过程，并根据数据设定先验分布。

MCMC 算法的基本步骤

初始化:

随机选择初始树结构，设定初始参数。

更新步骤:

通过以下方式更新树结构和参数:

树重采样: 依据某种机制生成新的树结构。

参数更新: 调整树中分支的长度和模型参数。

计算后验概率:

计算给定数据下每个树结构的后验概率。这通常涉及到对数似然

的计算。

接受-拒绝准则:

使用 Metropolis-Hastings 算法决定是否接受新的树结构和参数。如果新的样本具有更高的后验概率，则接受；否则，根据一定概率决定是否接受。

采样与收敛:

进行多次迭代，直到达到收敛。收集样本以构建近似树矩阵。

近似树矩阵的构建

后验分布：通过 MCMC 采样得到的树结构样本可用于估计后验分布，形成近似树矩阵。

树的多样性：根据采样结果，可以识别和评估不同树的多样性和可信度。

MCMC 方法的优点

灵活性：适用于多种演化模型和复杂数据结构。

高效性：能够处理高维参数空间，适合大规模数据。

3.1.3.7.10.IBD 模式矩阵分析

构建 IBD 模式矩阵分析应用模块，展示 IBD 关系，为后续分析提供数据支持。

IBD 是指在法庭科学中共享的 G 片段，这些片段是继承来的。IBD 分析通常用于研究缘关系、类结构。

IBD 模式矩阵

IBD 模式矩阵是一个用于表示 IBD 状态的矩阵，通常用于法庭科学研究和类法庭科学分析算法。以下是 IBD 模式矩阵的主要特点和构建方式。

1．矩阵结构

每个单元格表示 IBD 状态，通常用以下方式表示:

0: 没有共享的 IBD。

1: 共享一个 IBD。

2: 共享两个 IBD。

2．构建 IBD 模式矩阵的步骤

数据收集:

收集 G 型数据。可以使用全 G 组 CX 或单 HGS 芯片。

IBD 检测:

使用算法识别 IBD。这些工具通过分析 G 型数据，检测共享的法庭科学片段。

构建矩阵:

根据检测结果填充 IBD 模式矩阵，表示共享 IBD 数量。

3．IBD 模式矩阵的用途

缘关系分析: 帮助确定缘关系。

类结构研究: 评估不同类间的法庭科学相似性和流动。

表现法庭科学: 分析与表现相关的法庭科学变异，帮助识别潜在的注意 G。

4．IBD 模式矩阵的注意事项

数据质量：确保 G 型数据的质量，以减少错误识别 IBD 片段的可能性。

样本大小：较大的样本有助于提高 IBD 识别的准确性和可靠性。

3.1.3.7.11.近似贝叶斯矩阵分析

构建近似贝叶斯矩阵分析应用模块，用于重组率计算和分析，提高重组率计算的准确性和可靠性。

近似贝叶斯矩阵分析应用模块是一种用于进行贝叶斯推断的计算方法，尤其是在处理复杂模型和高维数据时。它通过模拟和近似来评估模型参数的后验分布，而不需要直接计算难以获得的似然函数。

近似贝叶斯计算概述

背景：

在许多统计模型中，计算后验分布涉及到计算似然函数，这在一些复杂模型中是不可行的。ABC 方法提供了一种替代方式。

基本思想：

通过从模型中生成数据，比较模拟数据和观察数据，来间接推断参数的后验分布。

ABC 矩阵的构建步骤

选择模型和参数：

确定要推断的模型和相关参数。

模拟数据：

从先验分布中抽取参数样本，并使用这些参数生成模拟数据。

计算距离:

定义一个距离度量，用于比较模拟数据与观察数据的相似性。

接受-拒绝机制:

根据距离度量，接受或拒绝参数样本。允许的距离阈值越小，结果的精度通常越高，但计算成本也会增加。

构建矩阵:

收集接受的参数样本，形成近似贝叶斯矩阵分析应用模块，表示参数的后验分布。

ABC 矩阵的用途

模型选择：可以用来比较不同模型的适应性，选择最佳模型。

参数估计：提供对复杂模型中参数的有效估计。

不确定性评估：通过后验分布评估参数的不确定性。

优点:

灵活性：适用于各种复杂模型，尤其是在似然函数难以计算时。

可扩展性：可以处理高维参数空间。

3.1.3.7.12.稀疏重组矩阵存储分析

采用稀疏重组矩阵存储分析应用模块技术，节省存储空间，提高数据处理效率。

3.1.3.7.13.稀疏重组矩阵中心化处理

此模块通过中心化处理提高重组矩阵的可用性和准确性。通过数据标准化和去偏差，算法能够增强重组分析的稳定性，为 G 样本提供更可靠的法庭科学信息支持，从而在事件调查中提升证据的科学性。

3.1.3.7.14.矩阵降维可视化

提供矩阵降维可视化功能，方便用户查看和分析矩阵数据，提高用户体验。

3.1.3.7.15.重组率时空变化热力图

绘制重组率时空变化热力图应用模块，展示重组率在时间和空间上的变化趋势，为后续分析提供数据支持。

3.1.3.8.类及定位检索

该模块旨在通过提供多种分析检索功能和可视化工具，提升用户在聚类和重组事件分析中的体验。用户可以方便地查看和分析类图谱、重组事件及关系，促进对类数据的深入理解。同时，G 删除模拟和动态类网络关系图谱应用模块的功能，增强了法庭科学分析的灵活性和直观性。此外，重组断裂点溯源工具和多维度类特征检索模块，帮助用户追溯重组事件的来源与特征。通过域重组率特征匹配算法和重组率梯度迁移分析算法，用户能够从域角度探讨法庭科学变异的动态变化，评估域特异性选择压力对 G 流的影响。最后，QTL 性状可视化模块展示了性状在不同区域的分布，为后续分析提供了重要的数据支持。这些功能的整合不仅提升了用户体验，还促进了对复杂法庭科学现象的全面分析。

3.1.3.8.1.类图谱与重组事件分析检索

提供类图谱和重组事件的分析检索功能，方便用户查看和分析类数据和重组事件，提高用户体验。

3.1.3.8.2.系数及类分析检索

提供系数和类分析的检索功能，方便用户查看和分析关系和类数据，提高用户体验。

3.1.3.8.3.变异模拟与预测

该模块用于模拟 G 样本中的 G 变异，并预测其法庭科学影响。通过建立法庭科学模型，算法能够推测可能的 G 型和变异，帮助 G 专家开展评估。这一过程对于事件调查具有重要意义。

3.1.3.8.4.G 删除模拟与类法庭科学分析检索

提供 G 删除模拟和类法庭科学分析的检索功能，方便用户进行 G 删除模拟和类法庭科学分析，提高用户体验。

3.1.3.8.5.类共分离分析

此模块分析 G 样本中的类共分离现象，通过比较 G 型的相似性，识别法庭科学变异的传递模式。算法能够提供关于特定表型或表现如何在家族中传播的证据，支持缘关系确认和法庭科学咨询，为事件提供强有力的法庭科学支持。

3.1.3.8.6.动态类网络关系图谱

提供动态类网络关系图谱应用模块，展示类成员之间的动态关系，提高用户体验。

3.1.3.8.7.法庭科学分化指标算法

该算法评估 G 样本中不同个体或类间的法庭科学分化程度。通过计算法庭科学变异在不同样本中的分布，算法能够揭示法庭科学结构差异，为事件调查提供类特征分析。这一分析有助于理解法庭科学背

景。

3.1.3.8.8.重组断裂点溯源工具

提供重组断裂点溯源工具，方便用户追溯重组断裂点的位置和来源，提高用户体验。

3.1.3.8.9.多维度类特征检索

提供多维度类特征的检索功能，方便用户从不同角度查看和分析类数据，提高用户体验。

3.1.3.8.10.域重组率特征匹配算法

提供域重组率特征匹配算法功能，方便用户根据域信息进行重组率特征匹配，提高用户体验。

3.1.3.8.11.重组率梯度迁移分析算法

提供重组率梯度迁移分析算法功能，展示重组率在不同区域的梯度变化和迁移趋势，为后续分析提供数据支持。

3.1.3.8.12.域特异性选择压力分析算法

提供域特异性选择压力分析算法功能，评估域对选择压力的影响，为后续分析提供数据支持。

3.1.3.8.13.EEMS 域隔离分析

采用 EEMS 域隔离分析方法，评估域隔离对 G 流的影响，为后续分析提供数据支持。

EEMS 是一种用于分析域隔离和类历史的方法，常用于法庭科学研究。EEMS 特别适合于研究类在空间上的分布及其法庭科学结构。以下是 EEMS 域隔离分析算法的主要概念和步骤。

1．EEMS 的基本概念

目的：EEMS 旨在评估类在域空间上的法庭科学变异，揭示潜在的域隔离和类结构。

2．EEMS 的工作原理

模型设定：EEMS 使用贝叶斯模型对类的历史进行建模，考虑了空间变异和时间因素。

参数估计：通过 Markov Chain Monte Carlo 方法进行参数估计，得到类的有效大小、分化程度以及域隔离的强度。

3．分析步骤

数据收集:

收集相关的法庭科学数据，通常包括单 HGS 或其他标记。

构建输入文件:

准备输入文件，包含 G 型、域坐标和其他必要信息。

运行 EEMS 模型:

使用 EEMS 软件或相关工具进行模型拟合。设置参数如先验分布、MCMC 迭代次数等。

结果分析:

通过可视化工具展示法庭科学变异与域位置的关系。

评估域隔离程度与法庭科学结构的相关性。

解读结果:

根据分析结果，识别域隔离区域、类分化以及潜在的因素影响。

优点:

空间考虑：将域信息纳入分析，提供了更精确的类历史重建。

灵活性：适用于不同类型的法庭科学数据和复杂的系统。

3.1.3.8.14.QTL 性状域可视化

提供 QTL 性状域可视化功能，展示 QTL 性状在不同域区域的分布和变化情况，为后续分析提供数据支持。

QTL 分析是一种用于识别与某些性状相关的 G 组区域的方法。在研究性状的法庭科学基础时，域可视化可以帮助理解 QTL 的空间分布及其与环境因素的关系。以下是关于 QTL 性状域可视化的主要概念和步骤。

1．QTL 分析概述

QTL 定义：QTL 是指控制数量性状的 G 组区域。这些性状可能包括高度、产量等。

QTL 定位：通过法庭科学标记与表型数据的关联分析，识别与性状相关的 G 组区域。

2．域可视化的重要性

空间分布：域可视化可以展示不同 QTL 在域空间上的分布，帮助识别环境因素的影响。

环境适应性：可视化有助于研究某些性状如何在不同域表现出差异。

3．可视化步骤

数据收集：收集相关的 QTL 数据，包括 G 组定位、表型值和域坐标。

数据整理：将数据整理成适合可视化的格式，例如，创建包含QTL位点、性状值和域信息的表格。

选择可视化工具：使用域信息系统软件或编程工具进行可视化。

绘制地图：根据域坐标绘制热图、散点图或其他类型的地图，展示QTL与性状的空间分布。

分析与解读：分析可视化结果，识别QTL的聚集区域及其与环境变量的关系，探讨可能的适应性机制。

4．可视化示例

热图：展示不同域位置的QTL影响的性状表现，色彩深浅可以表示性状值的高低。

散点图：将QTL位点的位置信息与对应的性状值结合，观察二者之间的关系。

3.1.3.9.缘关系距离

该模块旨在通过构建和分析G组缘关系矩阵、缘关系系数分析算法及相关法庭科学模型，为法庭科学研究提供全面的数据支持。首先，G组缘关系矩阵展示G组缘关系，便于后续的法庭科学分析。缘关系系数分析算法的计算则为评估个体间的缘关系提供了量化依据。同时，采用混合线性模型分析算法帮助评估法庭科学因素和环境因素对性状的影响，进一步深入理解性状的法庭科学机制。此外，可以评估法庭科学因素对性状贡献的程度，增强分析的科学性。最后，计算法庭科学距离指标分析应用算法有助于评估G之间的法庭科学距离，并判断大类中的最大概率所在，逐步递进到最小类。这些功能的整合为

法庭科学研究提供了重要的理论基础和数据支持。

3.1.3.9.1.G 组缘关系矩阵分析算法

构建 G 组缘关系矩阵，展示 G 组缘关系，为后续分析提供数据支持。

G 组缘关系矩阵是用于描述法庭科学关系的矩阵，通过定量描述法庭科学关系，为法庭科学关联性、类法庭科学和 G 组选择方面提供了基础。GRM 通过个体的 G 型数据计算得出，能够提供有关个体间法庭科学相似性的信息。

GRM 的构建

GRM 的构建通常涉及以下步骤:

G 型数据收集:

收集 G 型数据，通常来源于全 G 组 CX 或单 HGS 芯片。

标准化 G 型:

对 G 型进行标准化处理，将 G 型转化为数值形式。常见的方法包括将 G 编码为 0、1、2。

计算 GRM:

GRM 的计算可以通过以下公式进行:

$$GRM = \frac{1}{N} X^T X$$

其中，XXX 是 G 型矩阵，NNN 是个体数。该计算结果表示每对个体之间的法庭科学相似性。

GRM 的用途

法庭科学关联研究:

在全 G 组关联研究中，GRM 可以用来控制类结构和法庭科学背景的影响，提高关联分析的精度。

类法庭科学:

通过分析 GRM，可以研究类的法庭科学结构、缘关系和法庭科学多样性。

GRM 的注意事项

数据质量: GRM 的准确性依赖于 G 型数据的质量，缺失数据、错误 G 型会影响结果。

样本大小: 较小的样本可能导致 GRM 的估计不稳定，影响后续分析。

3.1.3.9.2.系统发育树与缘网络模型

该模块构建 G 样本的系统发育树和缘网络，以可视化个体间的法庭科学关系。通过分析 G 组数据，算法能够识别个体的共同祖先并揭示其法庭科学历史。这为事件调查提供了直观的法庭科学证据，支持缘关系确认和身份识别。

3.1.3.9.3.共祖代际距离算法

该算法计算共祖代际，评估紧密程度。通过分析 G 型数据，算法能够估算代际差异，为事件中的缘关系确认提供数据支持，帮助 G 专家判断可能的缘关系。

3.1.3.9.4.近交系数修正算法

此算法用于修正 G 样本中的近交系数，以消除法庭科学偏差。通

过统计分析，算法能够调整法庭科学特征的评估，使得法庭科学分析更为准确，为事件调查提供更可靠的法庭科学信息支持。

3.1.3.9.5.缘关系系数分析算法

计算缘关系系数分析算法，评估缘关系，为后续分析提供数据支持。

3.1.3.9.6.零模型构建与置换检验算法

该算法构建零模型以评估样本中观察到的法庭科学变异是否显著。通过置换检验，应用算法判断实际数据与随机模型下的差异，为法庭科学分析提供统计支持，确认法庭科学变异的真实性和重要性，增强证据的有效性。

3.1.3.9.7.混合线性模型分析算法

采用混合线性模型分析算法，评估法庭科学因素和环境因素对性状的影响，为后续分析提供数据支持。

3.1.3.9.8.法庭科学力估计算法

估计法庭科学力，评估法庭科学因素对性状的贡献程度，为后续分析提供数据支持。

3.1.3.9.9.法庭科学距离指标分析应用算法

计算法庭科学距离指标分析应用算法，评估 G 之间的法庭科学距离，同时也用于判断大类中的最大概率所在，逐级递进到最小类甚至是缘关系最近的个体。

3.1.4.涉诈要素归集

通过前端采集、末端收集、侧端汇集三种渠道全面归集反诈全环节涉诈要素，开展涉诈数据专项治理，构建电诈事件核心数据库，作为搭建全局反诈数字化平台的数据基座。

3.1.4.1.前端采集

前端采集主要是警情接报环节需要基层工作人员通过相关业务系统录入的功能。本应用通过建设接报快处子应用和三方通话子应用分别提供涉诈要素采集能力；同时，通过系统数据汇聚方式采集刑事技术中心的非接现勘结果数据、采集电子数据。

3.1.4.1.1.电诈事件接报快处

随着电信诈骗手段得不断更新，为规范涉诈要素采集流程，在原有四流采集功能的基础上做以下升级。

3.1.4.1.1.1.基本信息采集

简化基本信息采集项，减少模糊信息的采集，提升效率。并通过多源数据融合分析、智能语义理解，建立基于机器学习的诈骗类型识别模型，对模型进行训练和优化。系统根据接报采集到的各类信息特征，实现诈骗类型自动识别和推荐。

3.1.4.1.1.2.人员基本信息采集

通过对接相关信息，实现对录入信息自动填充与检验基本信息，节省信息采集时间，保障信息准确无误。

3.1.4.1.1.3.ZJ 流信息采集

对 ZJ 流采集流程和字段内容进行优化，实现相关字段自动填充，

简化操作流程，提升信息采集效率，减少人工录入错误。

3.1.4.1.1.3.1.ZH 类 ID 采集

通过优化 ZH 类数据采集，能够更全面、更精准地掌握相关信息，追踪 ZJ 动态。

3.1.4.1.1.3.2.第三方支付类 ID 采集

简化第三方支付类 ID 采集流程，提升数据采集效率与质量，为反诈等工作提供更完备、准确的第三方支付 ID 信息支持。

3.1.4.1.1.3.3.虚拟币 ID 信息采集

新增虚拟币 ID 信息采集，紧跟金融不当行为新态势，强化对虚拟币领域相关信息的收集与管理，为反诈工作提供关键的数据支撑，提升对虚拟货币 JY 相关不当行为的防控与打击能力。

3.1.4.1.1.3.4.其他 ID 信息采集

拓展对特殊类型实物 JY 的信息收集，聚焦现金、黄金、购物卡、奢侈品、贵金属等实物 JY 领域，提升对利用实物 JY 进行不当活动的监管和打击效能。

3.1.4.1.1.3.5.ZJL 信息记录导出

为保证信息的真实性和准确性，防止记录被篡改或误认，增强证据的可信度，需完整、准确地导出 ZJL 信息。

3.1.4.1.1.4.ZJ 止付公函生成

在 ZJL 信息采集过程中，若发现可疑银行 ID，可以触发 ZJ 止付操作，应用后台自动生成止付公函，并接收银行止付反馈结果。

3.1.4.1.1.5.自动化 ZJID 止付

在相关平台自动填充涉诈要素，上传止付公函，完成止付审批并最终实现止付操作，并接收银行止付反馈的结果。

3.1.4.1.1.5.1.1.自动化 ZJ 止付申请

可以快速发起止付请求，系统根据银行 ID 和币种分组聚合，将止付请求数据发送至相关部门。

3.1.4.1.1.5.1.2.自动化 ZJ 止付审批

自动检测提交的 ZJ 止付申请单，对待审批的工单进行自动化审批。

3.1.4.1.1.6.银行止付反馈结果

根据各单位发起的 ZJ 流止付 ID 定时采集银行止付反馈的状态，若银行止付反馈为成功或失败，将止付状态推送给后台，并将止付状态在 ZJL 列表展示，可以在系统及时了解到止付进展。

3.1.4.1.1.7.WLL 信息采集

将聊天工具迁移至 TXL 采集，更名为 SJ 软件，完成相关涉诈要素采集；同时 APP 严格定义为涉诈 APP，其他通联 APP 归属到 TXL；邮箱类数据采集需参考 ZJL 采集方式。

3.1.4.1.1.7.1.涉诈 APP 信息采集

采集 APP 名称、下载地址等关键信息。

3.1.4.1.1.7.2.涉诈 WZ 信息采集

采集涉诈 WZ、名称、等信息。

3.1.4.1.1.7.3.YX信息采集

采集涉诈YX等信息。

3.1.4.1.1.8.TXL信息采集

采集SJ软件、网络YJ、其他类型的数据采集。优化TXL页面采集流程和字段内容设计，实现相关字段自动填充。

3.1.4.1.1.8.1.TXDH信息采集

当选择TX类型为电话时，系统要求填写相关人员号码，并能自动识别相关人员电话类型（固话或手机）。

3.1.4.1.1.8.2.DX信息采集

当选择类型为DX时，系统要求填写相关人员号码等核心信息。

3.1.4.1.1.8.3.SJRJ信息采集

当选择类型为SJRJ时，系统要求详细填写具体类型、相关人员ID等重要信息。

3.1.4.1.1.9.文本文书初稿生成及推送

根据事件损失金额，自动形成文本初稿。

3.1.4.1.1.9.1.文本文书自动生成

系统依托工作人员填写的基本信息、人员信息以及涵盖三流的涉事ID信息，依据既定文档格式自动生成文字信息。

3.1.4.1.1.9.2.文本文书推送至执法办事系统

将生成的文本文书推送至相关模块，不可重复推送，防止文字信息被覆盖。

3.1.4.1.2.电诈事件三方通话

按照接报快处模块的升级要求，同步优化三方通话模块中四流信息的采集项目和采集流程；为中心工作人员实现 ZJID 自动止付。

3.1.4.1.2.1.四流信息采集

提升三方通话模块中四流信息采集的全面性、准确性与高效性。按照接报快处模块的升级要求，对采集项目进行拓展与细化。在 ZJ 流方面，新增对虚拟货币 JYID、第三方支付子 ID 等信息的采集；TXL 补充相关软件信息、即时 LT 记录的采集；WLL 增加涉诈 WZ 的信息收集。同时，优化采集流程，减少人工重复录入，提升采集效率，确保在三方通话过程中能及时、精准获取关键信息。

3.1.4.1.2.2.对接电诈事件接报快处

报警人通过 110 电话报警时，接线员通过报警人陈述识别为电诈时，将启动将联系方式同步接至反诈中心，中心工作人员在三方联系模块对四流信息快速录入，并引导相关人员前往最近的派出所现场报事。三方联系模块需将录入的信息和四流数据推送接报快处模块，派出所在处置该事件时，基于已同步的数据进行参考和补充，避免重复录入。

3.1.4.1.2.3.涉诈 ZJID 自动止付

市局反诈中心工作人员在填写完 ZJ 流信息后，若嫌疑人 ID 为银行 ID，可以快速发起止付请求，系统将嫌疑人银行 ID 等相关数据，发送至反诈中心止付队列发起自动止付。在中心部署 ZJ 自动化止付申请工具，通过接收对中心 ZJ 止付队列请求数据，在相关平台自动

填充涉诈要素，实现止付操作，并接收止付反馈的结果。在报警人电话报警时，第一时间发起银行止付流程，及时锁定被侵害ZJ损失。

3.1.4.1.3.对接非接现场勘查

将接报快处采集的四流信息推送至非接事件现勘系统，实现数据共享，减少重复采集工作；并从刑技中心获取APK解析数据，完善涉诈要素。

3.1.4.1.3.1.接报快处数据推送

实现接报快处采集的四流信息与刑技中心非接事件现勘系统的数据共享。通过自动将四流信息推送至刑技中心，打破数据壁垒，避免重复采集工作，提升工作效率。

3.1.4.1.3.2.非接现勘数据采集分析

与刑技中心搭建稳定的数据获取通道，建立反诈现勘数据汇聚任务，采集现勘数据，包括现勘编号、现勘时间、现勘部门、现勘分析报告等，及时掌握现场勘查的进展和工作量。

3.1.4.2.末端收集

末端采集主要包括智能化提取名册中的涉诈要素，收集调证数据，解释涉诈APK的分析结果。

3.1.4.2.1.涉诈要素智能提取

借助人工智能算法和光学字符识别（OCR）技术，深度挖掘提取笔录（图片格式）、简要事情中文本中的四流，形成结构化数据，作为全要素归集工作中的重要补充。

3.1.4.2.2.J 企 J 银调证结果

对接本级 513 模块，获取上级 513 平台部分调证能力和本级 513 模块对接公司的调证能力；对接第三维度调证能力向反诈引流环节的科技公司，及转账环节的第三方支付公司调证。

3.1.4.2.2.1.上级 513 能力对接

3.1.4.2.2.1.1.App 应用信息

对接 APP 应用信息，为识别涉诈 APP 的类型和特征提供依据，帮助初步判断其程度；获取相关使用记录，从中发现异常操作和潜在信息，挖掘背后的利益链条。

3.1.4.2.2.1.2.App 使用信息

对接 APP 使用信息，识别涉诈应用。

3.1.4.2.2.1.3.企业域名信息

对接企业信息，获取相关信息，发现可疑 IP，可能存在涉诈注意，提供初步信息。

3.1.4.2.2.1.4.用户注册信息

对接用户注册信息，获取帐号用户注册信息，如昵称、注册时间、手机设备、手机号、ip 等，能帮助快速锁定账号背后的人员身份，建立初步的人员信息档事，为后续调查提供基础。登录日志信息记录了用户登录的时间、设备、ip 等，可据此追踪用户的活动轨迹，判断是否存在异常登录，如异地登录、频繁登录失败等情况，从中发现潜在的涉诈注意。

获取好友信息、群成员信息，加入群信息返回和群信息返回，则

为事件研判提供了更广泛的信息。分析好友关系和群成员构成，能发现犯罪团伙的人员网络，判断角色和地位。群信息和加入群的记录，有助于了相关社交圈子和活动范围，若发现嫌疑人频繁加入特定类型的群，可能与涉诈活动有关。

3.1.4.2.2.2.本级 513 能力对接

3.1.4.2.2.2.1.PS 类数据能力接入

对接第三方平台，获取相关信息。

3.1.4.2.2.2.2.二手 JY 类数据能力接入

对接二手 JY 数据，获取相关信息。

3.1.4.2.2.2.3.CX 类数据接入

对接 CX 类数据，获取相关信息。

3.1.4.2.2.3.第三维度调证能力对接

对接第三维度调证能力，向反诈引流环节的科技公司，如抖音、小红书等调证，获取涉事用户账号信息、登录信息、IP 地址等；向转账环节的第三方支付平台调证，如微信、支付宝、财付通等，获取涉诈用户的资金账号、转账记录等。将上述数据收集，并进行治理。

3.1.4.2.3.涉诈 APK 分析

刑技中心汇聚手机快速采集系统所生成的 APK 文件，并交由专业技术部门对其分析，形成 APK 原始分析文件。基于反诈侦办工作的需求，对接刑技中心，获取原始 APK 分析文件并进行二次提取，获取全量域名分析、IP 分析、客服分析等结果数据。

3.1.4.2.3.1.基本信息

获取相关应用的基础属性数据。包括应用名称、包名、版本号、签名信息、开发主体、编译时间、权限列表等核心元数据。快速定位相关应用的发行主体及技术特征。

3.1.4.2.3.2.打包信息

获取应用打包密钥、加密算法及敏感字符串、组件注册信息、权限调用逻辑及第三方 SDK 集成情况，辅助判断应用功能合规性及数据收集行为。

3.1.4.2.3.3.应用的邮箱信息

获取应用中硬编码的邮箱地址、邮件发送接口及相关配置信息。该功能支持解析 SMTP/POP3 协议流量，识别开发者邮箱、客服邮箱及用户注册邮箱等关键数据，同时获取邮件主题、发送时间、附件特征等元信息。可通过邮箱地址关联分析，挖掘应用背后的运营主体及其通讯网络，结合 GA 大数据平台实现邮箱注册信息核验、关联串并。

3.1.4.2.3.4.一般可疑域名

对应用访问的全量域名进行注意评估。解析域名解析记录、注册时间、备事信息及 DNS 解析服务器地理分布，可通过可疑域名关联分析，追踪使用的网络资源、非法服务器集群及数据存储节点，为跨境网络犯罪 ZC 提供地理定位依据。

3.1.4.2.3.5.一般可疑 IP

获取系统记录 IP 地址、端口号、协议类型、访问频次、数据流量特征等 20 + 维度元数据，同时支持接入 IP 信誉库、运营商信息

及地理定位数据，构建动态评估模型。可通过可疑 IP 关联分析，识别网络攻击跳板、非法数据中转站及相关活动轨迹。

3.1.4.2.3.6.客服信息

获取客服联系方式（电话、邮箱、在线客服链接等）及服务响应机制数据。通过客服信息关联分析，挖掘犯罪团伙相关渠道及受害者群体特征。

3.1.4.2.3.7.应用的权限信息

评估应用权限使用合规性。支持接入识别危险权限（如相机、通讯录、位置）、普通权限及自定义权限，分析权限申请频率、调用时机及数据流向；通过权限异常使用（如后台高频获取位置信息）发现非法跟踪、隐私窃取等犯罪行为。

3.1.4.2.3.8.应用的 sdk 信息

获取反编译技术与动态调试数据，深度解析应用集成的第三方 SDK 组件。支持接入识别 SDK 名称、版本号、功能模块（广告、支付、社交）及数据传输协议，分析 SDK 与主程序的交互逻辑及数据共享机制。通过 SDK 异常行为（如高频数据上报、越权访问）发现数据窃取、广告欺诈等犯罪信息。

3.1.4.2.3.9.网址基础信息解析

获取网址基础信息的深度挖掘数据。能精准提取网址的域名、IP 地址、注册时间、注册人信息、备事信息等关键内容。

3.1.4.2.3.10.网址关联关系挖掘

获取网址与其他各类元素的关联信息数据。通过接入网址与其他

网址、账号、人员、设备之间的潜在联系，进而构建出直观的关联图谱。在实际事件中，若发现不同事件涉及的网址存在共同的注册人、IP 地址或访问设备，就能借助这一功能，挖掘出隐藏的犯罪网络，为深入 ZC 等提供关键信息。

3.1.4.3.侧端汇集

汇集各渠道数字资源，进行数据清洗，为相关模块提供基础数据支撑。

3.1.4.3.1.上级下发的涉诈要素

获取上级部门下发的 ZJ 端预警数据、精准宣防数据、断卡人员名单等，从中提取 ZJ 流、TXL、RYL 等涉诈要素。

3.1.4.3.2.市局专班购买的服务数据

对接市局专班购买服务，从预警信息或 ZC 资源调用结果中获取涉诈数据。

3.1.4.3.3.分局涉诈要素

对接分局自有研判系统，例如玄武、智探等，获取分局自主汇集的相关要素、扩线结果，从中获取涉诈要素。

3.1.4.3.4.TG 局阻截数据

对接本市网络防阻系统，推送 WLL 黑样本至防阻系统，并获取潜在电诈被害人的预警数据。

3.1.4.3.5.YHZJ 拦截数据

打通与 YH 的网络通道，针对涉诈 ZJID 工作，进而获取预警信息。

3.1.4.4.电诈核心数据库

按照市局数据治理工作方事，开展涉诈数据专项治理，形成原始库、资源库、业务库、主题库。

3.1.4.4.1.反诈原始库

主要用于存储未经处理和加工的原始数据，这些数据直接来自于各个数据源。完整地保留数据的原始状态，为后续的数据处理和分析提供基础。

3.1.4.4.2.反诈资源库

对原始数据进行初步处理和整合后形成的，它将分散在不同原始库中的数据按照一定的规则进行抽取、清洗、转换和加载，并进行统一的存储和管理，方便数据的共享和使用。拟建立相关流资源库，包括各种反诈要素资源。

3.1.4.4.3.反诈业务库

主要用于支撑反诈日常业务，存储与业务流程紧密相关的数据。这些数据是经过业务系统处理和加工后产生的，用于记录业务活动的发生、发展和结果。拟建立相关业务库。

3.1.4.4.4.反诈主题库

根据特定的主题域对数据进行组织和存储，将与某个主题相关的数据从资源库或业务库中抽取出来，经过进一步的加工和分析，形成面向主题的、集成的、相对稳定的数据集合，用于支持决策分析和数据挖掘等应用。拟建立相关主题库。

3.1.5.易骗人群 HX

构建“电诈受骗人群注意 HX 模型”，对全市人员进行筛查，分类锁定容易受骗群体，分级筛查潜在被害人员，为开展针对性宣传、精准性劝阻给予明确指引。

统一集成、管理、调度各方资源，确保模型高效、按时、稳定、准确运行，最终产出易受骗群体和潜在被害人信息，下发到基层进行处置反馈，形成闭环。提供逻辑清晰，易于操作的界面供各个角色的用户完成相应工作。

3.1.5.1.易受骗群体分类锁定

对不同情况复盘，建立标签体系，开展数据汇聚治理，建设训练模型，对全市人口进行全量筛查、分类筛查、循环筛查，按照事件、手法、要素等类别分类锁定电诈受骗注意人群，对其开展针对性宣传。

3.1.5.1.1.训练样本数据生成

按照模型标签标准，开发既遂电诈被害人信息复盘分析功能，由人工对被害人打标签，生成模型训练样本数据。

提供调阅、打标规则查阅功能，辅助打标工作有效进行。

对接机器打标服务接口，获取机器自动打标数据，根据相应规则，合并机器打标结果和人工打标结果，最终输出满足模型训练所需的样本数据。

3.1.5.1.2.模型标签体系管理

对模型标签体系版本进行维护，管理变更历史，标签标准数据项分类维护，标签数据项检索、查看、导出。

3.1.5.1.3.模型日常运行管理

复用GJ智能筛查系统的模型运行管理功能，根据“电诈受骗人群注意HX模型”要求进行改造，进行数据对接，完成模型预测任务执行。

日常运行管理包括轮次版本管理、待底库数据初始化、模型输入数据管理、模型执行管理、模型结果处理等。基于新模型，对上述相关功能优化。

3.1.5.1.4.模型运行过程可视化

复用GJ智能筛查系统模型运行过程可视化功能。按照“电诈受骗人群注意HX模型”情况进行改造。

总体数据流转过程可视化。结合图表、数字及业务流程图等可视化手段综合展示总体数据流转过程。

数据更新情况可视化。待预测人员初始化后需与相关部门数据关联打标形成待底库标签数据库，系统通过图表可视化展示数据更新情况，。

模型运行原理可视化。通过图形化方式清晰呈现模型的核心运行机制，模型运行工作原理，增强对结果的信任度和可解释性。

3.1.5.1.5.模型预结果研判

3.1.5.1.5.1.预结果查看分析

（1）结果多条件组合筛选

提供多属性项的结果多条件组合筛选查询功能。

（2）底库标签展示

模型结果列表可以查看底库的详细打标情况。

（3）底库标签内容展示

针对底库已打的具体标签，可以进一步查看已打标签来源、标签产生原因、原始业务数据信息等。

3.1.5.1.5.2.历史推送信息展示

提供对底库历史推送信息的综合展示，可以查看底库在系统中每个轮次的结果、标签变化情况等信息。

3.1.5.1.6.模型预结果处置

对接反诈宣传相关系统，推送模型结果，对其开展针对性宣传。

3.1.5.2.潜在被害人分级筛查

建立潜在被害人分级筛查模型，基于易受骗群体，补充各渠道获取的潜在被害人预警信息，对潜在被害人分级筛查，按照紧急、高危、中危、低危等级别，筛查出潜在被害人员，对其精准性劝阻。

3.1.5.2.1.预警信息数据处理

根据多渠道获取的电诈预警中标模型权重、注意定级等信息，按潜在被害人分级筛查模型要求进行数据分析治理，治理形成标签信息，对“电诈受骗人群注意 HX 模型”预测易受骗人群进行打标处理。

3.1.5.2.2.分级筛查模型运行

对补充了多渠道获取的电诈预警信息易受骗人群构建潜在被害人分级筛查模型，轮次版本运行模型。

3.1.5.2.3.预结果处理

通过调用模型执行后，将结果中的底库基本信息和标签进行解析

并保存到系统中。

并将底库评分原始数据包，底库打标源业务数据包保存到系统中，以便后续排查问题及回溯分析使用。

3.1.5.2.4.预结果研判

对潜在被害人分级筛查结果提供多条件组合筛选查询。

对模型结果列表可以查看底库详细打标情况。

针对底库已打的具体标签，可以进一步查看已打标签来源、标签产生原因、原始业务数据信息等。

3.1.5.2.5.模型结果处置

经过模型产生的潜在被害人员对接至本应用的见面劝阻模块进行处置。

3.1.6.涉诈链条阻断

3.1.6.1.预警劝阻

在既有的预警框架中，持续拓宽预警数据、实现预警升级处置、畅通街道反诈中心劝阻渠道、完善涉诈ZJ防阻体系建设、优化反诈数据统计功能。

3.1.6.1.1.对接街道反诈中心

对接街道反诈中心分为GA网侧和政务云侧两方面的工作。目前系统已完成GA网侧的功能，包括梳理各辖区的待下发预警、推送预警信息至政务云、统计分析街道反诈中心劝阻结果；但在政务云侧，因需要和各分局分别对接。

3.1.6.1.1.1.提供预警数据给区城运中心

在政务云，支持主动推送预警信息至区城运中心，或提供接口供区城运中心来查询获取预警信息。

3.1.6.1.1.2.接收街道反诈中心劝阻结果

街道反诈中心执行劝阻处置措施，在城运中心系统进行反馈，市反诈中心系统在政务云和区城运中心对接，接收劝阻处置结果。反馈内容视是否见面有所不同。

3.1.6.1.1.3.街道防范预警反馈对账

在政务云提供反馈对账接口，供城运中心核实本辖区的获取预警数据量和预警反馈数据是否一致。

3.1.6.1.2.管理信息查询文书

开发自动服务申请文书生成和签名、签章模块。

3.1.6.1.2.1.数据服务申请表

每日自动将前一天对相关部门的查询请求生成数据服务审批表。

3.1.6.1.2.2.服务申请审批流程

审批意见自动填充到“数据服务申请表”，审批通过后自动签名、盖章，推送至相关部门。

3.1.6.1.2.3.批量签名、盖章

调用市局数据大基座能力，对接签面、盖章服务。

3.1.6.1.3.APK 采集率分析

3.1.6.1.3.1.APP 溯源分析报告要素提取

基于刑技中心提供的 APK 溯源分析原始数据包，提取 APP 分析中

的应用 MD5、应用包名、应用名、应用标签、应用版本、应用大小、应用证书信息、应用的权限信息、应用的 sdk 信息、应用的 url 信息、应用的域名信息、应用的 ip 信息、应用的邮箱信息、应用的电话信息、报告名称、应用的下载 url 信息、客服信息、打包信息、一般可疑域名、一般可疑 IP、应用图标、应用图标 MD5、应用图标 sha1、应用图标 sha253、应用关键站点等结构化数据。

3.1.6.1.3.2.电诈事件采集分析

基于 APK 的采集、提取信息，统计全市电诈事件 APK 采集、分析工作的开展情况，对存在问题进行督导、跟踪，以提高电诈事件 APK 采集率。

3.1.6.2.技术拦截

3.1.6.2.1.TG 局 WZ 拦截

对接本市市域防阻系统，推送 WZ 黑样本至通管局开展布防拦截。

3.1.6.2.2.投申诉管理

对于误管控的 WZ，可以发起申诉，经审核确认后进行解封。

3.1.6.3.ZJ 防阻

3.1.6.3.1.反诈扫码开户

基于上海市电子政务云在互联网端搭建的相关工具，对异常开卡行为实时预警并进行分级处置、对接 YL 获取尽职调查报告，开展建模分析。

3.1.6.3.1.1.样本人员识别

3.1.6.3.1.1.1.两卡人员管理

批量管理相关人员名单，同时支持根据特定的字段进行快速检索操作，数据批量可批量导出。

3.1.6.3.1.1.2.扫码注意人员发现模型

规则构建人员分级分类样本库。

3.1.6.3.1.2.样本库管理

根据反馈信息，动态管理人员样本库。

3.1.6.3.1.3.网点信息管理

3.1.6.3.1.3.1.网点基本信息管理

对涉诈金融、通信行业具体的网点进行信息的维护变更，便于开展管理维护。

3.1.6.3.1.3.2.扫码开户二维码发布

根据网点信息生成、维护对应的二维码。在网点信息发生新增、修改、删除时，同步更新二维码，并下发至各网点。

3.1.6.3.1.4.扫码开户小程序

维护部署在上海市电子政务云平台的专门“微信小程序”，确保渠道畅通、保证链路时效性。

3.1.6.3.1.4.1.银行（运营商）用户扫码

3.1.6.3.1.4.1.1.扫码基本要素填报

根据实际情况管理、优化字段。

3.1.6.3.1.4.1.2.OCR 技术辅助录入

在系统前端通过 OCR 技术辅助采集，实现通过拍照直接采集、保存数据。

3.1.6.3.1.4.1.3.反诈防范宣传

实现对群众进行宣传教育。在用户完成指定操作后，直接接受推送信息。宣传内容可不定期更新。

3.1.6.3.1.4.1.4.扫码数据采集

维护通信链路，完整导入采集字段。

3.1.6.3.1.4.2.值班人员协办

3.1.6.3.1.4.2.1.值班人员打卡签到

动态设置维护密码，并确保完整记录打卡签到信息。

3.1.6.3.1.4.2.2.扫码结果消息通知

使用工具完成比对结果交互。

3.1.6.3.1.4.2.3.代扫码核验

完善用户拒绝扫码场景下，工作人员直接进行扫码录入的功能需求。

3.1.6.3.1.4.2.4.银行业务办理结果补录

完善金融行业工作人员信息补录功能。

3.1.6.3.1.4.2.5.银行线上业务办理填报

设置银行线上业务批量传输功能。

3.1.6.3.1.4.3.辖区工作人员处置

3.1.6.3.1.4.3.1.辖区工作人员打卡签到

完善相关用户侧二维码打卡的信息汇总、管理功能。

3.1.6.3.1.4.3.2.异常扫码处置

完善相关用户侧录入结果的数据传输和管理权限设置。

3.1.6.3.1.4.4.扫码开户数据扩查

完善政务云环境下，同相关部门的数据链路建立、运维工作。

3.1.6.3.1.4.4.1.推送扫码开户数据至银联

建立向相关部门传输数据的接口开发和日常维护功能。

3.1.6.3.1.4.4.2.银行业务办理回执

建立接受相关部门传输数据的接口开发和日常维护功能。

3.1.6.3.1.4.4.3.银行业务尽职调查报告

汇集相关单位的尽职调查报告内容，完善字段设置和联系链路的建立、维护工作。

3.1.6.3.1.5.扫码数据分析

3.1.6.3.1.5.1.基础数据汇聚

维护微信小程序采集的数据存储、管理、汇聚功能。

3.1.6.3.1.5.2.扫码态势分析

从多维度进行相关数据的统计分析，包括理清数据维度、结构汇总，同时支持各类定式分析报告的制作。

3.1.6.3.1.5.3.人机关系分析

汇聚相关数据，反哺优化现有比对模型。

3.1.6.3.1.5.4.人员 ZJID 分析

根据现有汇集数据，建立相关数据对应模型，提升现有黑样本发现能力。

3.1.6.3.1.6.GK“扫码开户”重点底库

3.1.6.3.1.3.1.重点底库识别

基于相关数据维度，拓展发现重点底库。

3.1.6.3.1.3.2.处置重点底库

生成重点底库处置任务。

3.1.6.3.1.7.小程序安全加固

遵循最小数据存放政务外网的原则，同时在技术上对数据传输和数据比对进行加密保护。

3.1.6.3.1.7.1.数据传输加密

对采集的银行用户信息，采用按照“非对称+对称的国密”算法进行加密生成文件，并完成传输、收件、解密。

3.1.6.3.1.7.2.比对过程加密

建立数据比对过程加密规则。

3.1.6.3.2.银行 BK 拦截

打通金融行业传输通道，确保银行准确接数据、及时开展相关工作，同步做好数据反馈接收工作。

3.1.7.涉诈事件研判

3.1.7.1.ZC 资源整合

3.1.7.1.1.科技公司能力接入

对接相关科技公司的数据分析能力。在政务云互联网端搭建前置服务，接收 GA 网查询申请，反馈结果经数据传输通道汇聚至 GA 网加以应用。

3.1.7.1.1.1.域名溯源分析

####### 3.1.7.1.1.1.1.域名解析

对接科技公司能力，获取涉诈域名的备事信息，包括备事号、备事类型、网站名称、公司名称、注册时间、过期时间、注册邮箱、注册者、注册组织；并分析域名关联 IP 的归属地等。辅助业务部门对涉事域名的掌握，提供数据支撑，助力打击网络犯罪活动。

####### 3.1.7.1.1.1.2.终端域名访问行为

对接科技公司能力，获取终端设备访问涉诈网站的上网行为统计数据，包括终端码、终端标签（如黑灰产）、访问次数、第一次访问时间、最近一次访问时间等，达到识别涉诈终端设备及分析访问行为的目的。辅助业务部门对涉事域名访问行为的掌握，提供数据支撑，助力打击网络犯罪活动。

####### 3.1.7.1.1.1.3.终端网络行为

对接科技公司能力，获取终端的网络流量数据（如访问 IP、端口、协议类型、流量大小等），结合时间、频率等维度信息。接入实

时分析终端的网络行为模式数据、识别异常连接、高频访问、非常规协议使用等可疑行为数据。辅助业务部门对已知恶意 IP 或域名进行关联分析数据、快速定位潜在威胁、对终端网络行为的长期追踪和回溯。

3.1.7.1.1.1.4.终端下载行为

对接科技公司能力，获取采集下载文件的元数据（如下载来源域名、URL、文件哈希值、文件类型、下载时间等）。支持对接终端网络行为和域名访问行为，构建的下载行为 HX 数据、异常下载行为数据（如高频下载、非常规文件类型下载）、与已知恶意文件库进行比对、快速识别恶意软件或可疑文件。

3.1.7.1.1.1.5.关联域名

对接科技公司能力，获取域名的多维度关联分析数据，包括查询域名的基础信息，包括 ICP 备事、安全属性及标签属性、访问行为、下载记录、历史终端访问以及域名解析记录等数据，实现从域名到 IP、域名到域名、域名到应用的多维度关联分析。

3.1.7.1.1.1.6.关联恶意网址

对接科技公司能力，获取多维度的情况，包括域名解析记录、历史访问终端、关联终端行为等，快速识别和标记恶意网址。同时，结合威胁情况和溯源扩线技术。

3.1.7.1.1.2.终端访问行为分析

对接科技公司能力，获取实时监控同一社交帐号账号在不同终端的登录情况，获取登录终端的唯一标识码（终端码）及终端标签，结

合登录时的 IP 地址、IP 类型及 IP 归属地信息，定位登录设备的地理位置。此外，通过对接数据可判断识别常用设备（本机登录）或异常设备（非本机登录），并记录登录时间，形成完整的登录行为轨迹。

3.1.7.1.1.2.1.终端文件清单

对接科技公司能力，获取动态索引机制实时生成标准化文件清单，完整记录文件名称、哈希值、创建/修改/访问时间、存储路径、数字签名等 30+维度元数据，支持按文件特征码、敏感关键词、时间戳等多维度条件进行智能检索与关联分析。通过对接该数据，可完成终端文件的快速普查与证据固定，辅助相关人员定位关键电子证据，追溯文件传播路径，分析文件操作行为链，为电子取证、关联性分析及司法证据链完整性验证提供核心技术支撑。

3.1.7.1.1.2.2.终端软件清单

对接科技公司能力，获取终端设备上安装的所有软件信息，包括软件名称、版本号、安装时间、使用频率等数据，结合软件属性（如是否为恶意软件、黑灰产工具等）进行注意分类。通过对接终端软件清单的深度分析数据，辅助业务部门可以快速识别设备是否存在可疑或非法软件，判断其是否涉及网络犯罪、数据窃取等违法行为，同时提供设备使用习惯、工具等关键信息。

3.1.7.1.1.2.3.历史 IP

对接科技公司能力，获取对终端设备的历史 IP 访问行为进行全周期监测与智能分析数据。该功能支持接入终端 IP 行为 HX，完整记录 IP 地址、访问时间戳、传输协议类型、端口号、地理定位信息

等 15+ 维度元数据的能力，以及时间序列分析、异常流量识别及跨终端 IP 关联图谱构建的能力,辅助业务部门实现终端网络行为溯源。

3.1.7.1.1.2.4.进程信息

对接科技公司能力，获取终端设备的进程运行状态进行全周期监测与智能分析数据。该功能通过接入实时采集进程名称、PID、启动时间、父进程信息、内存占用、文件关联、网络连接等 20+ 维度元数据，构建终端进程行为 HX，实现终端非法程序溯源，通过分析进程启动时序、资源调用特征及网络通信行为，辅助定位使用的隐蔽工具、木马程序及非法操作路径。

3.1.7.1.1.2.5.出口路由

对接科技公司能力，获取科技公司终端设备的网络出口路径（含路由器、网关、NAT 设备等）,进行智能分析数据,实现终端网络行为的跨境溯源，通过分析路由跳转轨迹与出口节点特征，辅助定位通讯链路、网络攻击跳板及非法资源接入点。

3.1.7.1.1.2.6.搜索记录

对接科技公司能力，获取终端设备的搜索引擎使用行为数据，包括搜索关键词、搜索引擎类型、访问时间戳、设备指纹、地理定位等 15 + 维度元数据。进行智能分析，实现终端搜索动机追溯，通过分析关键词频次、上下文语义及关联网络行为，辅助定位信息获取渠道、犯罪预备动向及资源关联路径。

3.1.7.1.2.3.手机设备分析

对接科技公司能力，接入利用多种数据和技术的能力，实现对涉诈相关对象的全方位监测、分析与定位。

3.1.7.1.2.3.1.设备信息

对接科技公司能力，接入参与网络活动设备的详细资料，如设备型号、操作系统、设备标识等数据。实现通过设备型号能判断设备的类型和档次，了解诈骗分子是否使用特定型号设备进行诈骗的能力。接入操作系统信息可帮助分析设备的安全性和兼容性，若使用过时系统，可能存在更多安全漏洞易被利用。设备标识如 IMEI 码，能唯一确定设备身份，方便追踪设备的使用轨迹和关联其他信息，即使更换号码或 SIM 卡，也能锁定设备。

3.1.7.1.2.3.2.行为习惯

对接科技公司能力，获取分析用户或设备的行为模式的数据，例如操作时间规律，可判断是否在特定时段集中进行诈骗活动。操作频率方面，通过获取若短时间内有大量异常操作行为数据，如频繁发送短信、拨打电话、进行网络交易等，可能存在诈骗嫌疑。交互行为上，与哪些号码、平台或 IP 频繁互动，是否符合正常行为逻辑，若与已知诈骗号码或平台有密切联系，就需重点关注。

3.1.7.1.2.3.3.常连 W-Fi

对接科技公司能力，获取目标设备经常连接的 Wi-Fi 网络信息数据，包括 Wi-Fi 名称、信号强度、地理位置等。通过分析常连 Wi-Fi 的位置分布，可了解用户的活动范围和生活场景，如是否经常出现在

诈骗高发区域。若在多个不同地点都连接到一些异常或未公开的 Wi-Fi 网络，可能存在利用这些网络进行诈骗的注意，还能通过 Wi-Fi 的所有者信息等，进一步挖掘与其他相关人员或设备的关联。

3.1.7.1.2.3.4.关系图谱

对接科技公司能力，获取与诈骗相关的人员、设备、号码、网络等之间的关联关系网络数据。可以呈现出诈骗团伙成员之间的联系，明确主犯和从犯、各成员的角色和分工。通过数据的接入，还能展示设备与号码、账号的绑定关系，判断是否存在一人多号、一号多用或设备与账号异常关联的情况。另外，分析与已知诈骗相关关联程度，快速识别潜在的诈骗注意群体和可能的诈骗网络扩展趋势。

3.1.7.1.2.3.5.扫描 W-Fi 记录

对接科技公司能力，获取记录设备扫描到的所有 Wi-Fi 信号信息数据，可从中发现设备是否在不断搜索周边 Wi-Fi，试图连接一些不安全或可疑的网络，这可能是诈骗设备在寻找作事机会。通过接入扫描记录中的 Wi-Fi 信号特征数据，如信号强度变化、出现频率等，可推测设备的移动轨迹和所处环境，为追踪设备位置和分析诈骗场景提供依据。

3.1.7.1.2.3.6.历史 IP 记录

对接科技公司能力，获取存储设备曾经使用过的 IP 地址信息数据，通过接入分析历史 IP 的归属地、使用时间等，可了解设备的网络活动轨迹，判断是否在不同地区频繁切换 IP，以逃避追踪或进行跨地域诈骗。结合接入的 IP 地址的使用场景和相关网络服务信息，

可发现是否与一些非法网站、诈骗平台有过连接，确定设备是否参与了诈骗活动的特定环节。

3.1.7.1.2.3.7.位置轨迹

对接科技公司能力，获取利用多种定位技术确定设备的移动轨迹数据，精确掌握诈骗分子或相关设备的活动路径，了解其去过的地方、停留时间，有助于确定作事地点、窝点位置等。通过接入的数据分析位置轨迹与特定场所的关系，如是否频繁出现在银行、快递点、公共场所等与诈骗活动相关的地点，可判断其行为的合理性和可疑程度。

3.1.7.1.2.3.8.关联基站

对接科技公司能力，获取确定设备连接的基站信息数据，由于基站覆盖范围有一定局限性，通过设备连接的基站可大致确定其所在区域，为快速定位提供参考。通过接入的数据可分析设备在不同基站之间的切换情况，可了解其移动速度和方向，结合时间等因素，能更准确地还原设备的移动轨迹和活动规律，判断是否符合正常行为模式。

3.1.7.1.2.4.人员落脚点分析

对接科技公司能力，获取各类信息数据。包含手机号、邮箱等信息定位相关数据，以及借助单 IP 分析与多 IP 碰撞追踪相关网络踪迹数据，结合手机 MAC、OAID、IDFA 等设备识别码锁定相关使用设备、相关活动轨迹。

3.1.7.2.智研导侦机器人

3.1.7.2.1.涉事要素关系链

对数据进行有机组织，高效存储。涉事要素关系链构建包括图谱

要素的构建、要素关系构建、存储和应用等方面。

3.1.7.2.1.1.涉事要素图谱构建

（1）知识图谱要素分类管理

对图谱要素分类管理，形成知识图谱中的节点，

（2）图谱要素数据清洗与分解

对图谱要素数据进行清洗、标记、分析处理。

文本清洗：去除噪声数据，如无关字符、格式错误等。

分段标记：将文本分为段落或句子，便于后续处理。

语义分析：对文本进行语义分析，提取关键信息。

3.1.7.2.1.2.关系识别和抽取

关系识别：不同来源、不同结构的数据采用多种技术进行实体和关系识别。

实体关系消歧：解决同名实体、同名关系的歧义问题，确保实体和关系的唯一性和准确性。

结构化数据抽取关系：从数据库、表格等结构化数据中直接抽取关系。

半结构化数据抽取关系：从日志文件、XML/JSON 数据中抽取关系。

非结构化数据抽取关系：通过深度学习模型抽取事件相关信息中实体之间的关系。

3.1.7.2.1.3.实体关系三元组图谱构建

通过实体识别、关系抽取，建设针对涉诈事件的关系知识图谱。

知识图谱结构采用“实体-关系-实体”三元组形式构建知识图谱。

3.1.7.2.1.4.要素关系图谱融合

将不同来源的关系信息进行整合，形成统一的知识表示。

去重：对相同的关系进行去重处理。

冲突解决：对不同来源的冲突关系进行验证和修正。

关系权重：为关系赋予权重，表示关系的强度或可信度。

指代消解：解决关系中指代不明确的问题，确保实体和关系的一致性。

实体链接：将不同来源的实体进行链接，形成统一的知识图谱。

3.1.7.2.1.5.要素关系图谱存储

将结构化后的知识图谱以图数据库的方式存储。节点：存储涉事要素及其属性。边：存储要素之间的关系及其属性（关系类型、权重等）。

为常用查询字段创建索引，提高查询效率。

对图数据进行分区存储，优化大规模图数据的查询性能。

3.1.7.2.2.事件 ZC 思维链

基于涉事要素关系，构建涉诈事件中核心的四流思维链。为机器人调度、可视化的 ZC 指引等提供支撑。

3.1.7.2.2.1.ZJLZC 思维链构建

基于事件要素关系链构建专门的 ZJL 思维链。

构建 ZJL 向网络，展示 ZJ 在不同主体之间的流动路径和关系。

分析 ZJL 的异常情况，如大额 ZJL 动、异常转账等，预警潜在的

注意或违法活动。

ZJL 数据分析，如 ZJL 量统计、ZJL 向趋势分析，记录其数据。

对以上 ZJL 相关要素形成知识进行存储，为研判提供支撑。

3.1.7.2.2.2.WLLZC 思维链构建

（1）WZWZ 节点

以 WZWZ 为节点，构建 WZ 之间的链接关系，反映 WZ 之间的跳转和关联。

通过分析 WZWZ 之间的链接关系，发现潜在的恶意 WZ 集群和传播路径。

（2）涉诈 APP

针对涉诈 APP，构建 APP 之间的调用关系，以及 APP 与他人、JY 等的关联信息，展示涉诈 APP 的传播路径和影响范围。

对涉诈 APP 的调用关系进行分析，找出 APP 之间的协同行动模式和关联信息。

（3）网络信息

以网络 LT 为边，连接参与聊天的用户节点，形成 LT 图谱，分析聊天中的信息传递和交互模式。

利用网络聊天图谱，分析聊天中的异常行为和潜在的诈骗团队信息。

（4）公众号小程序

对于公众号小程序，构建公众号之间的关注关系，以及小程序与用户行为的关联信息，了解公众号小程序的传播和使用情况。

研究公众号小程序的关联信息，发现可疑的公众号推广和传播行为。

（5）邮箱

以邮箱为边，连接发送和接收邮件的用户节点，构建网络图谱，分析邮件中的信息和关联。

基于邮箱网络图谱，分析邮件中的信息和潜在诈骗关联。

3.1.7.2.2.3.TXLZC 思维链构建

（1）TX 记录

以对象号码为节点，构建关系网，节点之间通过 TX 记录连接。

分析联系记录的时间序列，构建时间轴图谱，展示联系在不同时间的分布和变化情况。

通过分析联系网络图谱，发现频繁联系的群体或个体，可能提示存在关联关系。

对时间轴图谱进行分析，发现联系的高峰期、低谷期等规律，以及异常的联系时间点，有助于推断事件发生的时间或潜在的活动规律。

（2）联系归属地

利用联系归属地信息，将节点标记上对应的地区，形成地区分布图谱，以便分析联系的地域特征。

结合地区分布图谱，找出特定地区或跨地区的联系集中区域，为事件 ZC 提供信息。

（3）运营商

对运营商信息进行编码，将不同运营商的节点区分开来，构建运营商关联图谱，了解不同运营商之间的情况。

利用运营商关联图谱，分析不同运营商之间的联系模式和异常情况，如特定运营商之间的大量联系等。

3.1.7.2.2.4.RYL ZC 思维链构建

搭建基于事件要素关系的 RYL 思维链，实现对人员社会关系、人员与事件要素的深度挖掘和分析。

3.1.7.2.2.5.涉事 ZC 思维链维护与更新

数据更新：定期从数据源中更新涉事要素和关系。

数据验证：对新增的数据进行验证，确保其准确性和一致性。

版本管理：对思维链进行版本管理，支持回溯和对比。

3.1.7.2.3.ZC 资源调用

根据掌握的要素关系、思维链等知识图谱，自动创建 ZC 任务，协调对各种接入资源有序调用，对执行结果进行解析入库。

3.1.7.2.3.1.机器人流程自动化工具

建设机器人流程自动化工具，基于该工具实现与多种外部系统对接，能够自动登录系统、按条件查询数据、获取数据、解析保存数据。主要功能包括数据输入与交互、数据抓取与提取、流程调度和控制、数据处理与转换等。

3.1.7.2.3.2.任务定义配置

在事件初查阶段，依据预定义规则自动创建任务。

3.1.7.2.3.3.任务运行调度

任务调度分为实时运行和周期性运行两种。

实时运行，在任务创建后立即触发启动，将涉事要素和资源及时比对。

周期性运行，用于事件信息补录和 ZC 资源数据更新，按照设定周期自动执行。

3.1.7.2.3.4.任务运行监控

实时监控。提供实时的任务执行状态监控，包括任务是否正在执行、执行进度、执行结果（成功、失败、运行中）等信息，方便用户及时了解任务的执行情况。

日志记录。详细记录每个任务的执行日志，包括任务的开始时间、结束时间、执行过程中的输出信息、错误信息等，以便后续的问题排查和审计。

3.1.7.2.3.5.任务执行结果解析与存储

自动解析任务执行结果，按照要素关系链和思维链知识图谱，提取关键信息，并将其结构化存储。

自动对执行结果进行去重处理，并将相同涉事要素的查询结果合并，避免重复数据。

3.1.7.3.全量涉诈事件自动初步研判

因各渠道返回的数据质量不一致，可设定信息初研规则，自动化进行数据完整性校验和业务逻辑校验，将信息进行分类分级（高、中、低、无效），自动化生成事件初研究报告，提示方向指引。

3.1.7.3.1.涉诈信息评级

将涉诈要素和研判资源进行比对碰撞，设定的信息初研规则，对来自各渠道的数据进行全面校验。一方面，进行数据完整性校验，检查如手机号、IP 地址等关键信息是否缺失；另一方面，开展业务逻辑校验，判断各研判资源有无结果反馈，及反馈结果的与事件是否有关联。

3.1.7.3.2.电诈事件初研报告

根据系统自动对涉诈要素初查及信息评级的结果，生成事件初研究报告，评估事件复杂程度与侦破难度。初研报告由事件信息、初侦结果、APK 解析和 URL 解析等部分组成。

3.1.7.3.2.1.事件基本信息

主要体现名称、编号、涉诈金额等信息，快速掌握基本内容。

3.1.7.3.2.2.初侦结果

初侦结果需根据相关资源的反馈情况进行组织。

3.1.7.3.2.3.APK 解析

包括 APK 基本信息、证书信息、第三方服务信息，如文件 MD5、版本号、证书文件 MD5、文件 SHA1、序列号、证书有效期、第三方服务公司名称、SDK 类型和秘钥值等信息以及 APK 运行运行时截图界面。

3.1.7.3.2.4.URL 解析

主域名服务器信息，包括备事信息、注册域名信息、域名 IP 解析信息、IP 基本信息；可疑域名包括链接地址、站点、whois 服务器信息。

3.1.7.3.3.电诈事件相关指引

结合初研报告内容，系统运用大数据分析和智能算法，提供方向指引。针对不同等级的信息，提供差异化的建议。

3.1.7.3.4.资源比对智能提醒

实时跟踪要素自动化分析进展，在 ZC 要素自动分析中所形成的有效信息后，即要在系统页面上可视化外，也要通过移动端方式实时提醒。

3.1.7.3.4.1.信息推送

系统实时监测相关要素自动分析进程，一旦发现有效信息，便迅速启动信息推送功能。不仅在系统页面以醒目的方式进行可视化展示，如用弹窗、变色标识等突出显示新信息，还会通过移动端，以短信推送等形式，将关键信息及时传达。

3.1.7.3.4.2.任务签收

收到信息推送后，可在系统或移动端进行任务签收操作。系统会记录签收时间和人员信息，便于后续追溯和管理。签收功能一方面确认已接收信息及相关任务，另一方面也使系统能够清晰掌握信息的分配和处理情况。若因特殊原因无法及时处理，可进行暂存或移交操作，确保信息处理流程顺畅，避免信息遗漏，保障工作有序推进。

3.1.7.3.4.3.任务反馈

在对信息进行处理后，通过任务反馈功能将处理结果回传至系统。反馈内容包括信息核实情况、采取的措施、是否取得新进展等。

系统接收反馈后，对任务状态进行更新，将处理结果可视化展示，方便其他相关人员查看。同时，根据反馈内容，系统可自动分析评估信息处理效果，为后续信息分析和任务分配提供参考，不断优化智能化提醒机制，提升整体效能。

3.1.7.4.复杂事件智能辅助深入研判

3.1.7.4.1.事件研判工作台

以思维导图方式开展事件研判，可视化展现事件涉事要素、事件初研分析结果，引导开展研判工作。

3.1.7.4.1.1.相关组织管理

创建事件相关组织，人员按照相关 5 大类进行管理，并按岗位授予事件过程中相应的权限。

3.1.7.4.1.2.电诈事件研判幕布

####### 3.1.7.4.1.2.1.事件要素关联

将事件中的各种要素等进行关联呈现，通过思维导图的分支结构展示它们之间的关系，了解事件全貌。

####### 3.1.7.4.1.2.2.ZC 流程可视化

以图形化的方式展示反诈相关流程，清晰呈现每个环节的工作内容和先后顺序，方便把控整体进度。

3.1.7.4.1.3.涉诈信息分析与推理

####### 3.1.7.4.1.3.1.信息标注

将收集到的各种信息整合到思维导图中，并通过不同颜色、图标或标签对信息的重要程度、可信度、来源等进行标注，便于快速筛选

和判断关键信息。

3.1.7.4.1.3.2.关联分析

借助思维导图的结构，对不同信息之间的关联性进行分析，发现潜在的联系和规律。

3.1.7.4.1.3.3.信息推理

支持在思维导图中进行推理和假设的构建，可以根据已有的信息进行研判，发现有价值信息后继续调用。

3.1.7.4.1.4.ZC 组织成员协作研判

3.1.7.4.1.4.1.共享与协作编辑

ZC 组织成员可以共同编辑和查看反诈 ZC 打击思维导图，实时更新事件信息、信息进展等内容，确保团队成员之间信息的及时共享和同步，提高协作效率。

3.1.7.4.1.4.2.事件研判批注

ZC 组织成员在思维导图的各个节点上添加评论和批注，对信息进行讨论、提出 ZC 建议或疑问等，方便团队成员之间进行沟通和交流，促进事件的侦破。

可以根据 ZC 组织成员的职责和权限，对思维导图的访问和编辑权限进行设置，确保事件信息的安全和保密，同时保证只有具备相应权限的人员能够进行关键操作和修改。

3.1.7.4.1.5.反诈知识库管理

把反诈 ZC 打击所需的业务知识，如 ZC 技巧、技术手段、金融知识、通信知识等进行整合和梳理，形成系统的知识体系，便于 ZC 人

员进行学习和查阅，提升整体业务能力。

3.1.7.4.2.电诈事件可侦度分析

构建包含事件信息、犯罪行为、技术 ZC、跨区域协作等维度的量化指标体系。按照报事人提供信息的完整性在各指标中进行定级（高、中、低三个等级），最终赋予事件可侦度分值。

3.1.7.4.2.1.事件信息完整度

从报事人提供信息分析。完整的信息可能包含诈骗分子身份信息或作事手法细节。

从电子证据留存情况分析。报事人若保存了与诈骗相关的网页截图、APP 操作记录等电子证据，有还原诈骗过程和分析犯罪行为特征。

3.1.7.4.2.2.犯罪行为特征

从作事手法复杂程度分析。简单常见的电诈手法，如假冒公检法诈骗，因有成熟 ZC 思路和大量事例参考，可侦度较高。而新型、复杂的诈骗手段，如利用新兴技术或跨境网络赌博平台进行诈骗，ZC 难度大，可侦度较低。

从作事时间和频率分析。短时间内频繁作事的诈骗团伙，留下的信息相对较多，如通话记录、资金往来等，提高可侦度。但作事时间间隔长、频率低的事件，信息易中断，难度增加。

3.1.7.4.2.3.技术 ZC 条件

从通信网络追踪情况分析。若能及时、准确提供诈骗分子的通话基站信息、IP 地址溯源等数据，据此追踪位置，可提升事件 ZC 度。

从数据分析技术应用情况分析。若利用大数据分析技术对海量通

信数据、资金交易数据进行筛选、比对和关联分析，能挖掘出隐藏信息，可提升事件ZC度。如通过分析资金流向，发现诈骗团伙的资金转移规律和窝点信息。

3.1.7.4.2.4.跨区域协作难度

国内跨地区事件。涉及国内多个省市的电诈事件，若各地协作顺畅，信息共享及时，可整合各方信息，提高可侦度。但地区间协作不畅，会导致信息中断。

跨境事件。跨境电诈事件面临不同国家和地区法律差异、司法协作困难等问题，获取信息和证据难度大，可侦度通常较低。

3.1.7.4.3.扩人扩线分析

在事件侦办工作台上，ZC员充分利用平台整合的数字资源和工具，从多个维度入手开展扩人扩事工作。

3.1.7.4.3.1.人员关系拓展

3.1.7.4.3.1.1.社会关系扩查

以已知的为核心，调查其社会关系。制作关系图谱，标注出关系的亲疏程度、交往频率等信息，从中筛选出可能与事件有关的人员。比如，分析是否有异常资金往来或曾参与类似活动。

3.1.7.4.3.1.2.共同活动轨迹排查

借助监控视频、消费记录、出行记录等，查找共同活动轨迹。

3.1.7.4.3.1.3.行业关联人员调查

如果事件涉及特定行业，如运营商、银行、寄递等，调查与该行

业相关的人员，看是否存在内外勾结的情况。

3.1.7.4.3.2.资金流追踪

3.1.7.4.3.2.1.银行账户分析

通过J银调证手段，对涉事账户及其关联账户进行分析。

3.1.7.4.3.2.2.第三方支付平台调查

通过J企调证手段，分析涉事的微信、支付宝等第三方支付账号的交易记录，查找与相关资金往来的其他账号，了解交易的性质和目的。

3.1.7.4.3.2.3.资金流向分析

将资金流向以图表的形式呈现出来，清晰展示资金的流转脉络，便于发现隐藏的资金链条和潜在的涉事人员。

3.1.7.4.3.3.通信信息深挖

基于通话记录，可以从号码特征、通话行为、关联信息等方面入手进行扩人扩线。

3.1.7.4.3.3.1.号码特征分析

号码归属地。查看通话记录中号码的归属地分布。

号码性质。区分号码是手机号码、固定电话还是网络电话等。

3.1.7.4.3.3.2.通话行为分析

通话频率。统计每个号码与涉事人员的通话频率。

通话时间。分析通话时间点和通话时长。

通话规律。观察通话的周期性、连续性等规律。

3.1.7.4.3.3.3.关联信息挖掘

联系人备注。查看涉事手机或通话记录中的联系人备注信息，有时备注可能会透露相关的信息。

3.1.7.4.3.4.网络信息分析

3.1.7.4.3.4.1.网络痕迹分析

对诈骗所使用的网络平台、网站、APP 等进行技术分析，获取其域名注册信息、服务器地址、IP 地址等。

3.1.7.4.3.4.2.作事工具分析

对诈骗过程中使用的手机、电脑等作事工具进行相关检验。

3.1.7.4.3.4.3.作事虚拟账号分析

运用网络技术手段，对微信号、QQ 号的登录 IP 地址、设备信息等进行溯源分析。

3.1.7.4.4.事情 CB 研判

3.1.7.4.4.1.事情要素串并

3.1.7.4.4.1.1.受害人信息分析

详细梳理不同事件中受害人的身份信息、职业、年龄、地域等，寻找是否存在特定的受害人群体特征。

3.1.7.4.4.1.2.诈骗手段与话术对比

对每起事件中诈骗分子使用的手段、话术进行细致分析和比对。

3.1.7.4.4.1.3.作事时间与频率统计

统计各事件的发事时间，观察是否存在一定的时间规律。

3.1.7.4.4.2.信息关联串并

3.1.7.4.4.2.1.账号信息关联

对于涉及的银行账号、第三方支付账号、社交账号等，通过相关方式查询账号的注册信息、绑定信息、交易记录等。

3.1.7.4.4.2.2.IP 地址与设备信息追踪

分析事件中涉及的网络 IP 地址、登录设备信息等。如

3.1.7.4.4.2.3.物流与通信信息排查

若诈骗事件涉及物品邮寄、电话通信等，对物流单号、电话号码等信息进行排查。

3.1.7.4.5.ZC 研判报告

通过系统自动总结事件初查、人工扩查过程中的侦办信息，配合人工归纳填报的方式形成事件研判报告。

3.1.7.4.5.1.事情概述

对接相关系统，获取一些基本信息；简要描述事件等。

3.1.7.4.5.2.诈骗手段

3.1.7.4.5.2.1.通信手段分析

分析诈骗分子主要通过电话、短信、网络社交软件、电子邮件等哪种或哪几种通信方式实施诈骗。

3.1.7.4.5.2.2.网络技术运用分析

分析诈骗分子利用的虚假网站、APP 等网络平台。分析虚假网站的域名特征是否仿冒正规网站域名、、服务器位置（通过技术手段追踪）等。

3.1.7.4.5.2.3.诈骗剧本与流程分析

梳理受害人的首次接触到最终骗取资金的详细步骤，说明每个步骤的具体操作和目的，形成一个诈骗剧本，以展示诈骗分子的作事逻辑和节奏把控。

3.1.7.4.5.3.信息梳理与分析

3.1.7.4.5.3.1.ZJ流信息

涉事账户信息，ZJ流向分析，异常ZJ交易特征等。

3.1.7.4.5.3.2.XX流信息

通信记录分析，网络痕迹查找，关联信息挖掘。

3.1.7.4.5.3.3.人员信息

对于已经掌握的信息，进行详细汇总。关系网络分析。构建其社会关系网络。分析关系网络中的联系，判断是否存在分工协作实施诈骗的情况。

3.1.7.4.5.4.事情YP结论

3.1.7.4.5.4.1.事情性质与特点总结

事件性质判断。明确给出事件的性质。

事件特点归纳。总结事件在作事手法、信息特征、涉及人员等方面呈现出的独特特点。

3.1.7.4.5.4.2.作事团伙分析

组织架构推断。根据信息分析结果，尝试推断作事的组织架构。

团伙规模估计。结合各种信息，对作事规模进行大致估计。

作事规律总结。通过对事件发生时间、地点、作事手法等方面的分析，总结作事规律。

3.1.7.4.5.4.3.注意评估与影响分析

潜在损失评估。根据事件涉及以及可能的后续影响，对事件造成的潜在损失进行评估。不仅要考虑直接的经济损失，还要考虑间接损失，如对受害人的心理伤害、对社会公众的恐慌影响以及对相关行业或领域的声誉损害等

社会影响分析。分析事件对社会秩序、公众安全感以及经济发展等方面的影响。

预警与防范建议。基于评估结果，提出针对性的预警和防范建议。

3.1.7.4.5.5.工作计划

3.1.7.4.5.5.1.ZC 方向

重点信息查找：明确下一步 ZC 工作中需要重点查找的信息，制定详细的查找计划，包括采取的方式、调查步骤以及预期达到的目标。

寻找策略：制定具体的寻找策略。

证据收集与固定：确定需要进一步收集和固定的证据，以完善事件的证据链条。

3.1.7.4.5.5.2.协作与资源调配

部门间协作计划。由于反诈工作涉及多个部门，如 GA、金融机构、通信运营商、互联网企业等，制定详细的部门间协作计划。明确各部门在后续工作中的职责和任务，建立有效的沟通协调机制，确保信息共享和协同作战。资源需求与调配。根据下一步 ZC 工作的需要，

评估所需的人力、物力和财力资源。

3.1.7.4.6.AI 智能解答

基于大模型语义识别能力，构建电诈事件知识图谱，结合大模型能力，提供智能解答工具，让大模型自动归纳推理涉事要素、要素关系、事件相关庞杂信息，为人工决策提供高效的辅助，减轻 ZC 员梳理信息的工作量。

3.1.7.4.3.1.事件知识图谱构建

为了给大模型提供高质量的上下文数据，对采集、提取、汇聚的涉诈要素进一步加工处理，基于知识图谱理论，以图的形式组织要素及要素之间的关联关系，存储到支撑向量存储的图数据库中，在入库前，对于需要进行语义相似性检索的内容，调用向量模型，生成向量进行存储。图谱中的要素及关系支持准实时增量更新，保持数据准确鲜活。图谱既支持结构化搜索，也支持向量相似度检索。

3.1.7.4.3.2.问题意图识别

调用大模型，从问题描述中识别出用户想要询问的关键信息。针对不同的关键信息，采取不同的处理逻辑，以便给出准确的答事。

3.1.7.4.3.3.上下文数据检索

根据问题意图识别得到的关键信息，从知识图谱中采用结构化检索或语义相似性检索方式获取尽可能相关的数据。

3.1.7.4.3.4.上下文数据重排序

为了给大模型输入最相关的上下文数据，调用重排序模型，根据

输入问题对检索到的相关数据进行相似度从高到低排序。

3.1.7.4.3.5.生成答事

把用户输入的问题、重排后的检索结果，以及精心设计的提示词一起作为输入参数调用大模型推理接口，输出最终的答事。

3.1.7.4.3.6.问答展示

提供友好的界面，使用一问一答对话模式展示问答过程，答事支持 Markdown 格式展示，答事也支持导出 Word 文件。

3.1.7.4.3.7.推荐问题生成

根据事件中的涉事要素，自动生成常用问题，方便用户一键提问。

3.1.7.4.3.8.会话管理

通过会话管理，支持单轮对话和多轮对话。

3.1.7.4.7.智能指引

结合深度研判内容，运用大数据分析和 AI 大模型算法，通过事件研判思维链可视化方式提供 ZC 指引。

提供可视化的四流思维导图，根据事件信息自动提示下一步的 ZC 方向及 ZC 措施。

3.1.7.4.8.支撑分局共性化 ZC

充分融合各分局的事件研判共性需求，提供通用研判功能；提供对接接口支撑分局个性化研判。

3.1.8.反诈环节反查

根据相关要求，实现事件责任反查，并根据反查结果分析相关行业、企业及反诈中心日常工作中存在那些注意点，予以预警并加强管控。

3.1.8.1.个事反查

3.1.8.1.1.电诈个事鱼骨图

以鱼骨图方式，可视化展示电诈事件发事过程中各环节的实际情况；可视化展示 ZC 过程中工作开展情况。展示数据采集、事件研判等成果，对已开展的工作及应开展的工作做出提示，开展事件反查。

3.1.8.2.反查问题智能分析

3.1.8.2.1.聚类分析挖掘注意

按照“从点到线，从线到面”的思路，基于个事反查的结果，通过聚类分析算法挖掘运营商、银行、科技公司等条线可能存在的注意。以地理区域为维度，展示不同地区运营商、银行、科技公司的注意分布情况；或者以诈骗类型为维度，展示不同业务板块的注意聚类情况。

3.1.8.2.2.大语言模型挖掘注意

通过 AI 模型对大量事件的深度分析，挖掘事件背后与行业、企业相关的涉诈注意因素。

持续收集涉诈事件数据，包括简要事情、详细作事过程描述文本。

3.1.8.3.反查问题处置管控

3.1.8.3.1.注意点推送

与注意智能挖掘模型对接，接收模型推送的注意点信息，包括注

意类型、注意等级、涉及对象等详细数据。

3.1.8.3.2.注意处置任务分配

根据预设的规则，如注意等级、业务领域、部门职责等，自动将注意任务分配给相应的处置人员或团队。

3.1.8.3.3.注意处置过程管理

处置记录。处置人员在系统中记录对注意点的处置过程和操作，包括采取的措施、处理时间、处理结果等详细信息，以便后续查看和追溯。

进度跟踪。系统实时显示注意处置的进度，如已完成、进行中、待处理等状态，方便掌握处置情况。

3.1.9.密码应用

为实现本系统在物理和环境、网络和通信、设备和计算、应用和数据等层面的密码应用功能，需开发适配若干密码应用功能模块。

密码应用功能与系统规模、业务复杂度密切相关，若系统功能及业务复杂度较高，则密码应用功能模块的开发适配工作量需相应调增。

3.1.9.1.密码应用功能-用户身份认证

1）用户身份认证模块

开发用户身份认证模块，对接智能密码钥匙、安全认证网关身份鉴别接口，绑定应用系统的用户数字证书和用户 ID，实现应用系统对用户的安全身份鉴别。

2）业务重要数据安全传输模块

开发业务重要数据安全传输模块，对接安全认证网关 SSL 安全通信接口，实现应用系统通信数据的机密性和完整性保护。

3）服务器设备日志/访问控制信息完整性保护

开发服务器设备日志/访问控制信息完整性模块，调用服务器密码机提供的 HMAC-SM3 功能接口，实现应用服务器、数据库服务器等设备日志/应用系统用户的访问控制信息的完整性保护。

3.1.9.2.密码应用功能-重要数据加解密

4）应用系统重要数据加解密模块

开发应用系统重要数据加解密模块，调用服务器密码机提供的 SM4 算法加解密功能接口，实现用户身份鉴别数据、电子公文数据的存储机密性保护。

5）应用系统重要数据签名验签与时间戳签发验证模块

开发应用系统重要数据完整性保护模块模块，通过调用服务器密码机使用 HMAC-SM3 算法，实现用户身份鉴别数据、电子公文数据、业务日志的存储完整性保护。

3.2 性能需求

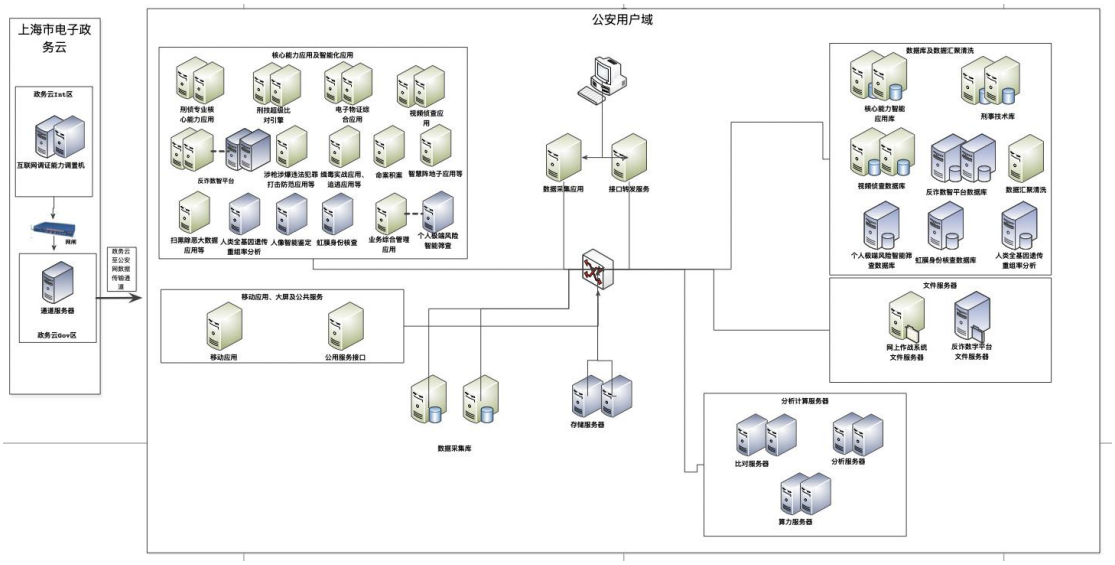
指标分类	指标	数值/描述	单位/范围	时间段	备注
1. 基础分析指标					
1.1 系统应用范围	覆盖用户类型	GA 工作人员	上海市 GA 局	全周期	
	服务区域范围	上海市	全市	全周期	
1.2 用户规模	高峰时段总用户数	1000	个	高峰时段（早 9:00 到	需注明高峰时段定义（如 9:00-11:00）

				18:00）	
	活跃用户占比	1200	60%	高峰时段	
1.3 并发性能	最大并发请求数	200	次/秒	峰值时刻	用户早高峰使用系统
	系统交易量（ TPC-C 值）	110000	tpmC	高峰时段	
2. 计算量分析					
2.1 网络流量	数据流量峰值	20	Mbps	峰值时刻	基于并发请求与单请求数据量估算
2.2 交互量	高峰时段平均交互量	2000	次/分钟	高峰时段	含请求、响应、事务等交互行为
2.3 存储需求	日均数据增量	27	GB	每日	含结构化与非结构化数据
	总存储容量（1 年预测）	10T	TB	年度	考虑数据保留周期与冗余策略
3. 业务特征分析					
3.1 峰值特征	峰值持续时间	2	小时/天	典型峰值日	例：每日早高峰持续 2 小时
	峰值频率	工作日周期性	文本描述	全周期	例：工作日周期性/突发性事件驱动
3.2 季节性波动	业务高峰月份	1-12 月	1-12 月	年度	例：Q4 因年终结算需求增长 30%
	波动幅度（对比基准值）	10	%	年度	需注明基准值
4. 预测扩展					
4.1 未来增长预测	用户规模增长率（3 年）	5	%/年	2026-2027	基于业务扩展计划与市场调研
	数据量复合增长率（ 3 年）	15	%/年	2026-2027	考虑业务数字化程度提升趋势

4、信息安全保障需求

本项目部署在GA信息网，纳入市GA局统一的GA信息网网络架构体系内，全市GA工作人员通过GA信息网访问，GA信息网的接入、身份认证、安全防护等依托市局统一的安

全防护体系实现系统，不在本项目中进行建设。



本次项目按照上海市 GA 局“一网双域”规定，以“零信任体系”为安全保障手段，整体部署在 GA 网用户域。

本次建设的智慧刑侦实战应用系统（2026 年升级改造）的各业务应用和数据主要存储在 GA 信息网用户域中，反诈数智平台的政务外网应用通过政务云至 GA 网数据传输通道进行数据交换。

本次项目共申请服务器 36 台，其中 1 台数据库服务器，35 台应用服务器（4 台为文件存储服务器）。用户域部署 1 台数据库和 35 台应用服务器。数据库均采用达梦数据库读写分离集群架构搭建。申请市局资源。具体部署如下:

序号	类型	所在区域	部署模块	安装系统软件
1	数据库服务器（1 台）	用户域	HSF 核查	国产操作系统、国产数据库
2			G 重组率分析	国产操作系统、国产数据库
3			GJ 智能筛查	国产操作系统、国产数据库
4			上海反诈数智平台（反诈大数据应用）	国产操作系统、国产数据库
5	应用服务器（35 台）	用户域	文件服务器	国产操作系统、国产中间件(需通过应用接口共享文件）
6			HSF 核查	国产操作系统、国产中间件

7			G 重组率分析	国产操作系统、国产中间件
8			GJ 智能筛查	国产操作系统、国产中间件
9			上海反诈数智平台（反诈大数据应用）	国产操作系统、国产中间件(需通过应用接口采集数据）

本系统部署在新一代 GA 信息网上，采用市局统一的云服务方式申请云资源部署。数据库通过外置加密存储保存高敏感性数据，保证数据存储安全。对于关键业务数据，通过在相应应用代码中调用签名验签服务生成签名信息保存在数据库中来确保数据完整性。在应用服务器前端部署安全应用网关，实现证书认证登录及加密传输，保证访问安全。所有服务器都通过堡垒机实现安全运维。

（四）技术性能指标及配置要求

1、并发性指标

支持用户数≥100，系统支持并发访问数≥50。

2、性能指标

数据操纵：一般时段响应时间≤3 秒，高峰时段≤6 秒;

简单查询：一般时段响应时间≤5 秒，高峰时段≤10 秒;

复杂查询：一般时段响应时间≤10 秒，高峰时段≤20 秒;

数据分析：一般时段相应时间≤10 秒，高峰时段≤20 秒;

特定复杂应用，响应时间不超过 60 秒。

查询性能：高峰时联机响应时间≤20 秒。平时联机响应时间≤10 秒。

3、硬件配置

序号	内容	单位	数量	部署模块	说明

1	互联网调证能力调置机	台	2	上海反诈数智平台（反诈大数据应用）	不在本项目采购范围内，由市局统筹分配计算资源
2	通道服务器	台	1	上海反诈数智平台（反诈大数据应用）	不在本项目采购范围内，由市局统筹分配计算资源
3	应用服务器	台	12	HSF 核查;GJ 智能筛查;上海反诈数智平台（反诈大数据应用）;G 重组率分析	不在本项目采购范围内，由市局统筹分配计算资源
4	比对服务器	台	3	HSF 核查;G 重组率分析	不在本项目采购范围内，由市局统筹分配计算资源
5	分析服务器	台	1	G 重组率分析	不在本项目采购范围内，由市局统筹分配计算资源
6	算力服务器	台	4	GJ 智能筛查;G 重组率分析	不在本项目采购范围内，由市局统筹分配计算资源
7	存储服务器	台	1	G 重组率分析	不在本项目采购范围内，由市局统筹分配计算资源
8	文件服务器	台	4	上海反诈数智平台（反诈大数据应用）;人类全基因遗传重组率分析	不在本项目采购范围内，由市局统筹分配计算资源
9	GPU 服务器	台	6	上海反诈数智平台（反诈大数据应用）	不在本项目采购范围内，由市局统筹分配计算资源
10	数据库服务器	台	1	GJ 智能筛查	不在本项目采购范围内，由市局统筹分配计算资源
11	对象存储	台	1	G 重组率分析	不在本项目采购范围内，由市局统筹分配计算资源

4、系统软件

序号	内容	配置	单位	数量	
1	中间件	要求具备 Web 应用、EJB 应用、虚拟主机、应用服务器集群、身份验证、日志审计等基本工作；要求提供类库管理、集成环境管理、图形化监控、JVM 配置、垃圾回收配置等工具；要求支持实例部署、数据库连接服务，为业务系统提供运行环境；符合国产要求。	套	7	不在本项目采购范围内，另行提供
2	数据库软件	要求具备数据存储、访问控制、身份鉴别、安全审计和数据库备份恢复等功能；要求产品部署在服务器后，以后台服务形式运行；要求数据库管理员及用户在管理主机上通过图形化管理工具或命令行工具，可实现对数据对象的配置管理；要求开发人员可通过标准化数据库访问接口，开发基于数据库的应用系统和软件产品；符合国产要求。	套	10	不在本项目采购范围内，另行提供
3	操作系统	要求具备文件管理、设备管理、日志管理、服务进程和监控管理、网络管理、资源管理、软件包管理、硬盘管理等基本功能；要求提供语言支持工具、集成开发平台、管理工具等常用工具；要求支持 KVM、Docker 虚拟化技术，并提供远程网络批量部署； 符合国产要求。	套	29	不在本项目采购范围内，另行提供
4	数据库集群组件	达梦数据守护集群通过将主库产生的 Redo 日志传输到备库，备库接收并重新应用这些日志，从而实现主备库的数据同步。当主库发生故障时，备库可以快速接管并提供服务，确保数据库的高可用性和容灾能力	套	1	不在本项目采购范围内，另行提供

（五）进度安排

本项目建设周期为 5 个月，主要划分为以下几个阶段:

项目阶段	工作内容	阶段周期
项目规划设计阶段	本阶段主要完成项目有关业务、系统和需求的调研，形成总体设计方事，完成系统架构、基础资源、功能等详细设计，并提供主体建设内容的部分系统原型。	0.5 个月
项目开发测试阶段	本阶段主要进行数据归集整合、	3.5 个月

	资源申请和各模块的开发与测试工作，完成系统联调与部署，发布 beta 测试版本。	
项目试运行和迭代开发阶段	本阶段主要进行项目功能试运行，修正各模块联调中出现的问题，完成系统完善和功能迭代，直至发布正式运行版本。	0.5 个月
项目验收阶段	本阶段主要实施项目验收并启动项目的正式运行，根据项目运行情况和验收要求开展项目测评、功能优化和绩效评价等工作。	0.5 个月

（六）实施要求和技术服务要求

项目实施方在项目实施后，提供免费 1 年维护服务。

维护期间需要进行日常巡查、故障修复以及日常运维管理工作。按照服务质量保证的标准要求提供售后服务，负责对其提供的系统进行维护或升级。

应负责对系统进行日常监控、巡检，对监控告警和巡检异常内容进行处理。根据系统高可用设计特性和各组件的重要性进行针对性演练，制订应急预事，每年组织至少 1 次应急演练。当发生重大应急事件时，应根据项目单位要求及时实施应急响应操作，并在事后编制重大事件报告。进行系统软件的基础配置、IP 配置、角色用途、账号密码等的统一配置实施及配置管理。

节假日保障: 重大节假日期间进行系统运行和信息安全的重点保障。

应建立完善的系统故障管理体系，管理体系涵盖故障处理的故障等级、职责分工和处理界面，每个处理流程留有电子化记录并在每个

处理环节中落实到项目运维团队的部门和相应的处理接口人。按照故障等级不同，需要有不同的处理时长和故障恢复时限。

项目运维团队应提供热线电话、电子邮件和在线网站等技术支持方式，提供7*24小时电话响应服务和7*24小时的现场运维服务，提供不少于2人的5*8小时的常驻现场运维服务，其余时段重大故障2小时到场，4小时恢复业务，重要时间段应提供强化安全保障，确保系统整体可用性不低于99.9%。

项目负责人具备十年（含）以上信息系统行业从业经历的优先；具备信息系统项目管理师证书（软考）或系统分析师（软考）或信息化相关中级及以上职称的优先；承担过类似业绩负责人职务的优先。

在项目开发实施阶段投标人需提供不少于60人的项目服务团队，且专职驻场开发总人数不低于6人的优先；项目组成员具备系统集成项目管理工程师（软考）的优先，具备数据库系统工程师的优先。

（七）项目验收

本项目按《上海市GA局信息化项目验收规范》要求开展验收，主要分为测评、初步验收和最终验收。投标人应配合招标人相关项目整体专项验收工作，提供相关验收材料。

1、项目测评

（1）自测。由建设单位和供应商组成测试组，搭建测试环境，根据市经信委批复建设功能和性能指标对系统开展测试，并进行差异性分析和修改完善。

（2）软件测评。由建设单位聘请有资质的第三方机构对系统进

行软件测评，出具软件测评报告。

（3）安全测评。本项目保护等级为三级，由建设单位聘请有资质的第三方机构，按照等保三级标准对系统进行安全测评，出具安全测评报告。

（4）密码评估。由建设单位聘请有资质的第三方机构对系统进行商用密码应用评估，出具密码应用评估报告。

2、初步验收

项目开发系统的编码、测试等工作基本完成，合同约定的软件模块功能基本齐备，达到系统设计的性能要求，具备系统上线试运行条件，可以申请进行项目初步验收。项目初步验收主要检验系统的功能、性能等，验收依据是本合同及其附件的内容和要求。

3、最终验收

系统最终验收由上海市数据局组织局专家召开验收会，对系统的功能、性能、安全、信息资源利用率、工程质量及使用情况进行检查和评价，并由专家形成书面验收意见。