

中华人民共和国通信行业标准

YD/T 4213—2023

国际诈骗电话监控拦截技术要求

Technical specification for international telecommunication fraud
monitoring and blocking

2023-04-21 发布

2023-08-01 实施

中华人民共和国工业和信息化部 发布

目次

前言.....II

引言..... III

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

4 缩略语..... 1

5 诈骗电话监测总体技术架构..... 2

 5.1 诈骗电话原理..... 2

 5.2 诈骗电话监测技术架构..... 2

6 诈骗电话监控拦截技术要求..... 3

 6.1 信令采集技术要求..... 3

 6.2 监控分析技术要求..... 4

 6.3 投诉确认技术要求..... 7

 6.4 叫控制技术..... 7

前 言

本文件按照 GB/T1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》给出的规则起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：中国移动通信集团公司、中国移动通信集团设计院有限公司、中国联合通信集团有限公司、中兴通讯股份有限公司。

本文件主要起草人：张滨、袁捷、娄涛、冯运波、刘利军、廖奇、周晶、杜雪涛、冀文、王馨裕、李斌、招斯喆、于乐。

引 言

诈骗电话主要是指不法分子通过假冒公检法等权威部门电话号码，或邮政、银行等公众服务号码，向用户拨打诈骗电话，以恐吓、威胁等手段骗取钱财的诈骗行为。

近年来，诈骗电话愈演愈烈，已成为全社会关注的信息安全焦点问题，危害极为严重。诈骗电话在干扰正常通信秩序的同时，构成了对公民个人信息与财产安全的严重侵害，同时对电信运营商的业务开展与社会声誉造成了极大的负面影响。据公安部统计，2011 年以来，我国诈骗电话案件年均增长 70% 以上；2014 年，全国立案 50 余万起，造成损失 100 多亿元。

通信网络由各运营商互联互通组成，一点接入，全球可达。不法分子通常在国外利用 IP 电话进行改号并向国内用户拨打诈骗电话，由于国际上号码传送无统一规范，诈骗号码通常会被透传，且运营商无法验证号码的真实性，导致用户接到虚假号码的呼叫。据公安部门统计，来自国际的虚拟改号来电占诈骗电话总量的 80% 以上。

制订国际诈骗电话的监控拦截技术标准，采用技术手段，对国际诈骗电话进行封堵拦截已成为防范诈骗电话、保护客户利益的一项重要工作。

国际诈骗电话监控拦截技术要求

1 范围

本文件主要规定在网络侧对国际诈骗电话进行监控拦截的具体技术要求，主要包括：诈骗电话监测总体技术架构、网络信令采集要求、疑似诈骗电话行为分析、诈骗电话验证、诈骗呼叫拦截、诈骗电话统计分析等。

本文件适用于基础电信企业在国际/网间关口设备对国际诈骗电话开展技术拦截的场景。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

诈骗电话 telecommunication fraud

不法分子通过假冒公检法等权威部门电话号码，或邮政、银行等公众服务号码，向用户拨打诈骗电话，以恐吓、威胁等手段骗取钱财的诈骗行为。

3.2

国际诈骗电话 international telecommunication fraud

不法分子在境外利用 IP 电话进行改号，经过运营商国际关口设备，向国内用户发起的诈骗电话呼叫。

4 缩略语

下列缩略语适用于本文件。

CAP	CAMEL 应用部分	CAMEL Application Part
GMSC	网关移动交换中心	Gateway Mobile Switching Center

IAM	初始地址消息	Initial Address Message
SCP	业务控制点	Service Control Point
SIP	会话初始协议	Session Initial Protocol
VoIP	网络电话	Voice Over Internet Protocol

5 诈骗电话监测总体技术架构

5.1 诈骗电话原理

诈骗电话典型场景可归纳为两个阶段。

第一个阶段是“广泛撒网”。诈骗分子冒充邮政、银行、运营商等，以邮件包裹未领取、银行卡消费透支、手机欠费、社保卡到期等各种名义向大量用户群拨电话，吸引用户上钩。

第二个阶段是“重点诈骗”。一旦用户上钩，诈骗分子就会通过虚拟改号冒充公检法等权威部门，称用户身份证被盗用，并涉及洗钱、贩毒等重大犯罪案件，威胁和诱导用户将资金转账至所谓的“安全账户”从而完成诈骗。不法分子主要通过 VoIP 实现虚拟改号。

在传统电路交换网中，主叫号码基于交换机物理端口确定，用户无法自行修改。在 VoIP 环境下，不法分子可建立虚拟改号平台，任意修改源号码并接入到运营商网络进行落地。虚拟改号基本原理如图 1 所示。

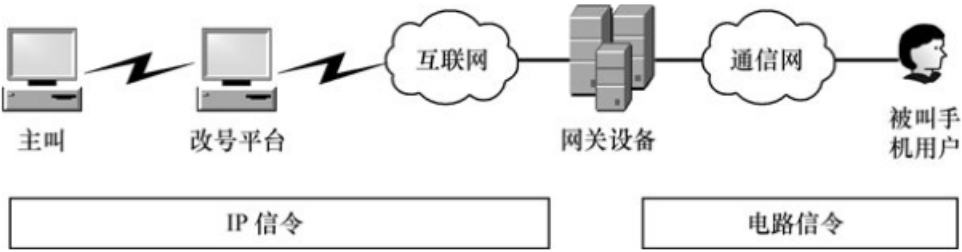


图 1 虚拟改号基本原理

- a) 诈骗分子通过客户端与改号平台发起连接，此时访问请求中同时携带原主叫号码和修改后的号码；
- b) 改号平台将 SIP 信令的 From 头域修改为诈骗分子修改后的号码，例如公检法等权威部门的号码，并在 IP 网络中传递 SIP 信令
- c) SIP 信令通过电信网网关设备落地后转换为七号信令，并在其 IAM 消息的主叫号码字段插入 From 头域中的号码；
- d) 被叫用户接到诈骗电话，来电显示为诈骗分子修改后的号码。

目前，各运营商间主叫号码传送的具体方式国际标准没有统一规范，通常情况下，互通设备会对号码进行透传，且不验证所传递号码的真实性。诈骗分子通常利用此漏洞，在境外搭建改号服务平台并在电信运营商进行 VoIP 落地，修改主叫号码后呼叫国内用户进行诈骗活动。

5.2 诈骗电话监测技术架构

基于对诈骗电话特征的研究，诈骗电话的呼叫特征主要包括高频呼叫、含有特服号码（例如 11185

等）、伪装公检法权威部门电话等。基于上述特征，诈骗电话的监测拦截过程应包括下面 3 个方面。

- 诈骗电话监控与发现：在网络侧监测相关数据，通过实时话务触发及离线信令采集等方式，基于呼叫特征对国际来电中的诈骗电话进行筛选识别，发现疑似国际诈骗电话号码。
- 诈骗电话验证与确认：依托客户投诉数据，对疑似国际诈骗电话进行验证确认。
- 诈骗电话拦截：对国际诈骗号码发起的后续呼叫，在全国范围对诈骗电话进行系统拦截。

依据诈骗电话监测拦截过程，诈骗电话监控拦截系统总体架构应包括 4 个模块，分别是信令采集模块、监控分析模块、投诉确认模块和呼叫控制模块，如图 2 所示。

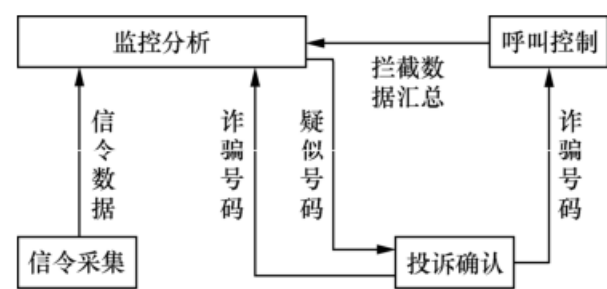


图 2 诈骗电话监控拦截系统总体架构

6 诈骗电话监控拦截技术要求

6.1 信令采集技术要求

关口设备信令数据采集能力不同，系统应支持实时信令数据采集和准实时信令数据采集两种方式，如图 3 所示。

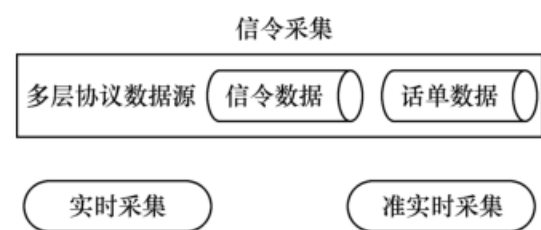


图 3 信令数据采集模块

6.1.1 信令数据采集

信令数据采集是指在通信过程中，对相关控制层面及数据层面信息进行采集的过程。一般来说，可通过相关软件收敛通信信息完成采集工作，或者通过采用硬件的方式，例如采取高阻跨接等方法收敛采集信令数据。

6.1.2 实时采集

针对支持实时触发的关口局设备，应将主叫号码具有“00”前缀的国际话务触发至信令采集模块的 SCP 中，由该模块实时采集 SCP 生成的国际来话呼叫话单。

信令采集模块应支持对网间关口局或国际关口局触发的呼叫来源进行区分，并将采集到的数据提供给监控分析模块。信令采集模块应支持全信令和简化信令两种采集方式，并可通过开关方式进行控制。

- 全信令：信令采集模块完整记录由呼叫触发到用户挂机的全信令消息，并提取主被叫号码、通话时长、振铃时长等字段，以供分析模块进行综合特征策略分析时使用。
- 简化信令：信令采集模块简单记录呼叫触发的相关信令消息，并提取主被叫号码、通话开始时间等字段，以供分析模块进行基本策略分析使用。

6.1.3 准实时采集

针对不支持实时触发的关口局设备，信令采集模块应通过信令监测系统采集关口局设备的 ISUP 信令，并以准实时的方式将信令提供给监控分析模块。

保留系统或数据接口，使得该模块可以与本运营商、其他运营商和安全厂商的相关系统进行连接和数据共享，实现联动治理。

6.2 监控分析技术要求

监控分析模块是系统的核心模块，应提供以下两方面功能，如图 4 所示。

- a) 基于信令采集数据以及话单数据，结合分析策略，实现对数据多维度分析。
- b) 对诈骗电话呼叫信息进行统计，生成统计报表供管理人员分析使用。

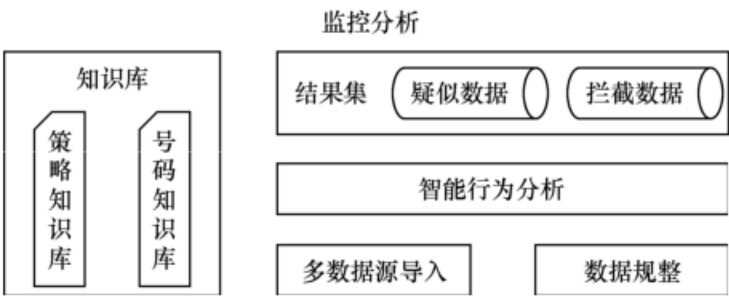


图 4 监控分析模块结构

6.2.1 数据规整

监控分析模块应提供数据规整功能，对采集到的信令或话单数据进行无效数据清理、缺失数据整理、数据类型格式统一、多维度数据整理等操作，最终生成入库分析表，输出数据格式见表 1。

表 1 入库分析表

字段	说明
callingNumber	主叫号码
calledNumber	被叫号码
Commit_time	入库时间
ringtime	振铃时长
CallDuration	通话时长
serverCode	业务编码
CallingHlr	主叫归属地区号（带 0 区号）
CalledHlr	被叫归属地区号（带 0 区号）

表 1 入库分析表（续）

字段	说明
call_result	呼叫处理结果：
	0：正常接续
	1：拆线
	2：路由桥接
callType	呼叫类型
MSCAddress	触发智能业务的 MSC 编号
CallEndTime	通话结束时间
CallingVLR	关口局所在地区：
	（IDP 中 locationNumber 对应的区号，带 0 区号）
serviceKey	业务键

6.2.2 智能行为分析

监控分析模块应具备如下两种分析能力：基于号码特征的分析识别和基于呼叫行为的分析识别。智能识别策略见表 2。

表 2 智能识别策略表

识别策略		功能
基于号码特征的分析识别	号码精确匹配	该规则主要对主叫号码是否与特殊号码完全匹配进行分析
	号码模糊匹配	该规则主要对主叫号码尾号连续若干位与特殊号码是否匹配进行分析
	号码格式匹配	该规则主要对主叫号码与《网间不规范主叫号码判定细则》（工信厅信管[2018]16 号）中的号码规范结构是否匹配进行分析
	“0086” 号码匹配	该规则主要对 “0086” 号码与《关于加强电信网不规范主叫号码拦截工作的通知》（工信部信管函【2017】17 号）》中的要求是否匹配进行分析
基于呼叫行为的分析识别	主叫呼叫频次	该规则对主叫号码的呼叫频次进行分析。可配置低于（含等于）、高于（含等于）阈值
	被叫号码离散度	该规则对被叫号码的离散度进行分析
	接通率	该规则对主叫号码的接通比例进行分析。接通率=接通次数/主叫呼叫频次
	呼叫时间间隔	该规则对主叫号码的呼叫时间间隔进行分析。可配置低于（含等于）、高于（含等于）阈值
	通话时长	对主被叫间的通话时长进行分析。可配置低于（含等于）、高于（含等于）阈值
	振铃时长	该规则对被叫号码振铃时长进行分析。可配置低于（含等于）、高于（含等于）阈值

表 2 智能识别策略表（续）

识别策略		功能
基于呼叫行为的分析识别	用户位置	针对主叫号码格式为“0086+移动用户号码”的情况，结合核心网存储的用户位置与用户境外漫游情况进行比较分析
	呼叫转移状态	对通话的呼叫转移状态进行分析。可配置呼叫转移状态开启或关闭

基于号码特征的识别策略包括但不限于如下策略。

- **公检法号码精确匹配：**对主叫号码去除“00”前缀后与国内某公检法部门号码完全相同的国际来电判定为疑似诈骗号码。
- **公检法号码模糊匹配：**对尾号与国内某公检法部门号码完全相同的国际来电判定为疑似诈骗号码。
- **特服号码模糊匹配：**对呼叫频率高、且尾号为邮政（11185）、银行（95553）、社保（12333）等服务号码的国际来电判定为疑似诈骗号码。
- **紧急呼叫号码模糊匹配：**对呼叫频率高、且尾号为紧急呼叫号码的国际来电号码，如 110 等，判定为疑似诈骗号码。
- **号码格式匹配：**对号码格式不符合《网间不规范主叫号码判定细则》中相关要求的国际来电号码判定为诈骗号码。
- **“0086”号码匹配：**对格式为“0086+固定用户号码”的国际来电号码、且被叫号码不属于各电信企业分配的漫游号段或其他合法平台号码的判定为诈骗号码；对格式为“0086+移动用户号码”，且经核验该手机号码的用户状态和位置等信息，显示该移动用户号码未启用或未漫游至境外的国际来电号码判定为诈骗号码。

基于呼叫行为的分析识别应支持通过逻辑回归识别、决策树识别等模型对用户的通话时长、通话未接通次数（或比例）、释放次数（或比例）等用户行为进行分析挖掘，从而发现疑似诈骗号码。

监控分析模块基于上述识别算法发现疑似诈骗号码后，发送给投诉确认模块进行进一步验证。

6.2.3 数据统计

数据统计报表应包括以下内容：

- 可根据分析策略类型、触发省份、运营商类型和时间粒度，统计疑似号码数量、呼叫频次等信息。
- 可根据分析策略类型、触发省份、运营商类型和时间粒度，统计已确认诈骗号码的数量、诈骗类型、拦截量等信息。
- 可根据分析策略类型、触发省份、运营商类型和时间粒度，统计各省拦截量 top5 的已确认号码的数量、呼叫频次、拦截量等信息。
- 可根据分析信令话单中 GT 地址、GT 与运营商映射表，统计国际来话主叫来源企业等信息。
- 可根据分析策略类型，查询系统分析识别的疑似诈骗号码，并支持疑似号码的导入导出功能。

6.3 投诉确认技术要求

投诉确认模块应提供疑似国际诈骗号码与投诉样本数据比对的功能，一旦主叫号码与被投诉号码完全相同，则判断此号码为诈骗电话号码，并将该号码同时输出到呼叫控制模块和监控分析模块。呼叫控制模块对诈骗号码进行拦截；监控分析模块通过内部数据通道，读取投诉确认模块发现的诈骗电话号码，存储在结果集中进行策略调优，如图 5 所示。

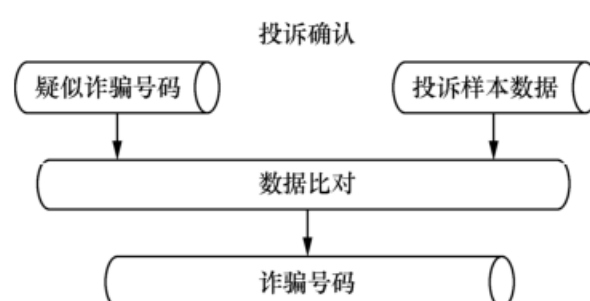


图 5 投诉确认模块

投诉确认模块除支持对疑似号码发起的国际呼叫进行验证之外，还应支持对疑似号码话单文件和投诉样本文件进行归档管理，具体要求为：

- 应支持按照指定的规则（例如日期）进行投诉样本文件归档管理，支持在线保存 1 年、离线保存 3 年；
- 应支持疑似号码呼叫记录话单的归档管理，支持在线保存 1 年、离线保存 3 年。

保留系统或数据接口，使得该模块可以与本运营商、其他运营商和安全厂商的相关系统进行连接和数据共享，实现联动治理。

6.4 叫控制技术要求

根据关口局设备的信令触发方式，呼叫控制模块应支持诈骗号码的实时拦截和非实时拦截功能，包括：

- a) 若关口局设备采用实时信令触发方式，应由呼叫控制模块对后续通话进行实时监控，并对该诈骗号码发起的通话进行实时拦截；
- b) 若关口局设备采用非实时信令触发方式，应由人工在关口局设备手工配置黑名单，对诈骗号码发起的后续呼叫进行拦截。