国 际 电 信 联 盟

ITU-T X.1246

国际电信联盟
电信标准化部门

修正 1
(05/2022)

X系列：数据网，开放系统通信和安全性

网络空间安全 – 反垃圾信息

电信组织反语音垃圾邮件技术

修正 1

ITU-T X.1246 建议书（2015）– 修正1

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1 – X.199
开放系统互连	X.200 – X.299
网间互通	X.300 – X.399
消息处理系统	X.400 – X.499
号码簿	X.500 – X.599
OSI组网和系统概貌	X.600 – X.699
OSI管理	X.700 – X.799
安全	X.800 – X.849
OSI应用	X.850 – X.899
开放分布式处理	X.900 – X.999
信息和网络安全	
一般安全问题	X.1000 – X.1029
网络安全	X.1030 – X.1049
安全管理	X.1050 – X.1069
生物测定	X.1080 – X.1099
安全应用和服务（1）	
组播安全	X.1100 – X.1109
家庭网络安全	X.1110 – X.1119
移动安全	X.1120 – X.1139
网页安全（1）	X.1140 – X.1149
应用安全（1）	X.1150 – X.1159
对等网络安全	X.1160 – X.1169
网络身份安全	X.1170 – X.1179
IPTV安全	X.1180 – X.1199
网络空间安全	
网络安全	X.1200 – X.1229
反垃圾信息	**X.1230 – X.1249**
身份管理	X.1250 – X.1279
安全应用和服务（2）	
应急通信	X.1300 – X.1309
泛在传感器网络安全	X.1310 – X.1319
智能电网安全	X.1330 – X.1339
验证邮件	X.1340 – X.1349
物联网（IoT）安全	X.1350 – X.1369
智能交通系统（ITS）安全	X.1370 – X.1399
分布式账簿技术（DLT）安全	X.1400 – X.1429
应用安全（2）	X.1450–X.1459
万维网安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500 – X.1519
漏洞/状态信息交换	X.1520 – X.1539
事件/事故/启发式信息交换	X.1540 – X.1549
政策的交换	X.1550 – X.1559
启发式和信息请求	X.1560 – X.1569
标识和发现	X.1570 – X.1579
确保交换	X.1580 – X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600 – X.1601
云计算安全设计	X.1602 – X.1639
云计算安全最佳做法和指导原则	X.1640 – X.1659
云计算安全实施方案	X.1660 – X.1679
其他云计算安全	X.1680 – X.1699
量子通信	
术语	X.1700 – X.1701
量子随机数发生器	X.1702 – X.1709
QKDN安全框架	X.1710 – X.1711
QKDN安全设计	X.1712 – X.1719
QKDN安全技术	X.1720 – X.1729
数据安全	
大数据安全	X.1750 – X.1759
数据保护	X.1770–X.1789
IMT-2020安全	X.1800–X.1819

ITU-T X.1246建议书

电信组织反语音垃圾邮件技术

修正1

摘要

语音通信是电信网络提供的一项基础服务。随着语音通信的发展，语音垃圾邮件也对终端用户和网络运营商产生越来越消极的影响。通常，语音垃圾邮件的内容范围从商业广告到有攻击性的色情内容，为终端用户和网络运营商带来了许多消极的影响。语音垃圾邮件会引诱、骚扰、威吓甚至恐吓用户和网络资源。为了避免这些消极的影响，保护用户权益，维持网络稳定性，网络运营商将加大反语音垃圾邮件的力度。

ITU-T X.1246建议书的目标是回顾反语音垃圾邮件技术的解决方案，不考虑垃圾邮件制造者身份可靠性的风险。该建议书对语音垃圾邮件进行了概述，总结了用户和电信网络使用的现有反垃圾邮件技术以及它们之间的合作机制。并基于打击垃圾邮件的技术和该合作机制提出了更多技术方案。

修正1引入了来自客户端的反馈机制，接收可能发送到运营商的垃圾邮件呼叫（通过语音、短消息服务（SMS）或多媒体消息服务（MMS））。该修正为电信管理系统和/或客户支持服务接收用户发出的关于呼入的垃圾呼叫、语音或消息（短信/彩信）的通知规定了技术要求，介绍了客户与电话通信网络的运营商/服务提供商就呼入的垃圾呼叫进行交互的场景以及维持此类交互的必要技术措施。这种交互是基于垃圾呼叫被叫方在呼叫完成后立即拨打电信运营商提前提供的反垃圾信息号码。

沿革

版本	建议书	批准日期	研究组	识别码*
1.0	ITU-T X.1246	2015-09-17	17	11.1002/1000/12448
1.1	ITU-T X.1246 (2015) 修正 1	2022-05-20	17	11.1002/1000/14988

关键词

垃圾邮件，语音垃圾邮件

* 读取本建议书时，在浏览器的地址栏键入http://handle.itu.int/及建议书的ID，例如http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）在电信，信息和通讯技术领域是国际电信联盟的常设机构。国际电信联盟电信标准化部门负责研究技术，操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

世界电信标准化大会（WTSA），每四年举行一次，确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第一号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性和适应性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提醒注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适应性不表示意见。

至本建议书截止之日起，国际电联尚未收到实施本建议书可能需要的受专利/软件版权保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新消息，因此特大力提倡他们通过ITU-T网站提供的相应ITU-T数据库进行查询：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1246建议书

电信组织反语音垃圾邮件技术

修正1

编辑性说明：这是一份全文出版物。本修正中的修改内容以与ITU-T X1246建议书（2015）有关的修订标记的形式显示。

1 范围

本建议书对语音垃圾邮件进行了概述，回顾了已有的用于反语音垃圾邮件技术，包括网络端和用户端的技术以及它们之间的合作机制。另外，本建议书也提出了额外的实用性的反垃圾邮件方法，例如信令记录、交互认证、控制措施等。

考虑到网络基础设施的特定特性，本建议书仅着眼于起源于电信网络中电路交换区域的反语音垃圾邮件。源于IP区域的反语音垃圾邮件技术需参见[ITU-T X.1244]和[b-ITU-T X.1245]以及[b-IETF RFC 5039]建议书。预防扮演呼叫者身份的技术不在范围之内。

接受此建议书提出的在使用反垃圾邮件方法前应遵循相关法律法规。

2 参考文献

以下ITU-T建议书和其他本文档中提到的参考文献包含的条款构成了本建议书的条款。在出版时，提及的版本都是有效的。所有建议书和其他参考文献从属于修订版；因此鼓励本建议书的使用者在应用时调查下列建议书和其他参考文献的最新版本。一系列当前有效的ITU-T建议书会定时出版。该建议书不会给出参考文献的单独文件。

[ITU-T X.1240] ITU-T X.1240 (2008)建议书，反电子垃圾邮件技术。

[ITU-T X.1244] ITU-T X.1244 (2008)建议书，全方位打击IP多媒体应用垃圾邮件。

[ITU-T X.1247] ITU-T X.1247 (2016)建议书，打击手机垃圾短信的技术框架。

3 定义

3.1 其他文献规定的术语

本建议书使用的其他处定义的术语如下：

3.1.1 电路交换网络（Circuit-Switched Network） [b-ITU-T M.60]：通过互连传输信道或电信电路为用户在通话或服务期间提供专用链接的网络。

3.1.2 IP网络（IP-Based Network） [b-ITU-T E.370]：使用ISO3层IP协议（OSI 参考模型）的网络。

3.1.3 运营商（Operator） [b-ITU-T M.1400]：负责鉴定和管理电信资源的机构。运营商必须由国家电信管理部门或其代表合法认证。运营商均可以或不可看作贸易伙伴。

3.1.4 报告服务（reporting service） [ITU-T X.1247]：在用户许可情况下，按照国家相关法律法规收集和汇总签约用户有关垃圾信息报告的服务。

3.1.5 短信业务（SMS）（short message service）[b-ITU-T X.1231]：短信业务是使手机、电话和其它短信实体通过完成存储和转发等功能的业务中心传送和接收文本消息的一种消息业务。

3.1.6 短信业务（SMS）垃圾信息（SMS spam） [b-ITU-T X.1242]：通过SMS发送的垃圾邮件。

3.1.7 垃圾信息（spam） [ITU-T X.1240]：“垃圾信息”一词的含义取决于各国根据其国家技术、经济、社会和实际情况对隐私和垃圾信息构成的看法。值得一提的是，随着技术的发展，其含义不断变化并拓宽，为滥用电子通信创造了新的可乘之机。尽管在全球范围内没有有关垃圾信息的一致定义，但该术语一般用来描述为推销商业化产品或服务通过电子邮件或移动消息批量传送的推介性电子通信。

3.1.8 垃圾信息制造者（spammer） [ITU-T X.1240]：制造并发送垃圾信息的实体或个人。

~~**3.1.4 垃圾邮件制造者 Spammer** [b-ITU-T X.1231]：产生和发送垃圾邮件的实体或个人。~~

3.2 本建议书规定的术语

本建议书定义的术语如下：

3.2.1 反垃圾信息号码（anti-spam number）： 由归属/所属服务提供商/电信运营商预先确定的专门的电话号码（该号码可以是全国唯一的，或者每个运营商单独的号码），通过拨打这一号码，用户告知在拨打此反垃圾信息号码之前拨打至其电话号码的呼叫为垃圾呼叫。告知即为拨打了反垃圾信息号码这一事实，用户不应提供任何信息。

3.2.2 蜜罐技术（Honeypot）： 模拟一个或一组终端检测可疑语音垃圾邮件制造者并辅助验证的软件程序（可能置于终端内），这些系统的输出可用于验证。

3.2.3 交互式用户报告（interactive user report）： 签约用户在电话终端收到包含垃圾信息或本身即是垃圾信息的呼叫后提起的投诉。一般而言，一次报告即为一次拨打至反垃圾信息号码的呼叫（一次呼叫的事实）或通过一条消息将可疑垃圾呼叫转发到反垃圾信息号码。

3.2.~~3~~4 管理实体（Management entity）： 有支配、审计或引导反语音垃圾邮件工作责任的实体。

3.2.5 垃圾呼叫（spam call）： 一般用来推销商业化产品或服务，包含语音、文本或多媒体垃圾消息的电话呼叫。

3.2.6 可疑垃圾呼叫（suspicious spam call）： 被怀疑但未确认为垃圾信息的呼叫。

3.2.~~4~~7 第三方机构（Third party organization）： 可以咨询、辅助或协调反语音垃圾邮件工作的实体。

3.2.~~5~~8 语音垃圾邮件（Voice spam）： 未经请求的，自动拨号的，预先录制的电话记录，通常带有市场产业产品或服务的目的。语音垃圾邮件的内容范围从商品广告到带有攻击性的色情材料。语音垃圾邮件为用户和运营商带来了多种有害影响。

4 缩写和首字母缩略语

本建议书使用的缩写及首字母缩略语如下：

Caller ID 呼叫方标识

CAMEL 移动网络定制应用增强逻辑服务器

CCLTP 呼叫结束时间点

CCOTP 呼叫继续时间点

CDMA 码分多址接入

CDR 呼叫细节记录

CDR_n 始发呼叫细节记录

CDR_{n+1} 从用户返回到其运营商的交互式呼叫细节记录

CLI 呼叫线路标识

CLI_n 始发主叫方到用户的主叫线路标识

CLI_{n+1} 用户向反垃圾信息号码提供反馈时的用户主叫线路标识

COSN 呼叫起始用户号码

COTP 呼叫起始时间点

CRBT 个性化来电彩铃

CS 电路交换

CTSN 呼叫终止用户号码

DMP 设备管理平台

GMSC 网关移动交换中心

GSM 全球移动通信系统

HLR 本地位置寄存器

ID 身份

ISIS 信息共享系统

IMS IP 多媒体子系统

IN 智能网络

INAP 智能网络应用协议

IP 互联网协议

IVR 交互式语音应答

MMS 多媒体消息业务

MSC 移动交换中心

OTAP 无线平台

PSTN 公用电话网

QoS 服务质量

SCP	业务控制点
SIM	用户身份模块
SLETP	信令链路建立时间点
SLRTP	信令链路释放时间点
SMS	短消息业务
SS7	信令系统7号
STP	信令转接点
UMTS	全球移动通信系统
VLR	访客位置寄存器
VMS	语音邮件服务器
VoIP	IP电话

5 惯例

无。

6 语音垃圾邮件概述

语音垃圾邮件是未经请求的、自动拨号的、预先录制的电话呼叫，通常带有市场商业产品和服务的目的。语音垃圾邮件的内容范围从产品广告到攻击性的色情材料，对用户和运营商造成有害的影响。

6.1 语音通信场景

语音通信是电信运营商提供的一项基础服务。最初，语音通信是基于传统的电路交换（CS）网络。随着互联网的发展，它也扩展到基于IP网络的互联网电话（VoIP）。

根据使用的技术可分为如下4种语音通信场景(如图1所示)：

- 场景1：CS-CS：传统移动/固定电路交换语音通信
- 场景2：CS-IP：移动/固定交换电路用户发起，由IP电话用户终止的语音通信
- 场景3：IP-CS：IP电话用户发起，由移动/固定交换电路用户终止的语音通信
- 场景4：IP-IP：IP电话用户间的语音通信。

上述4种语音通信模式和相关技术参见图1。

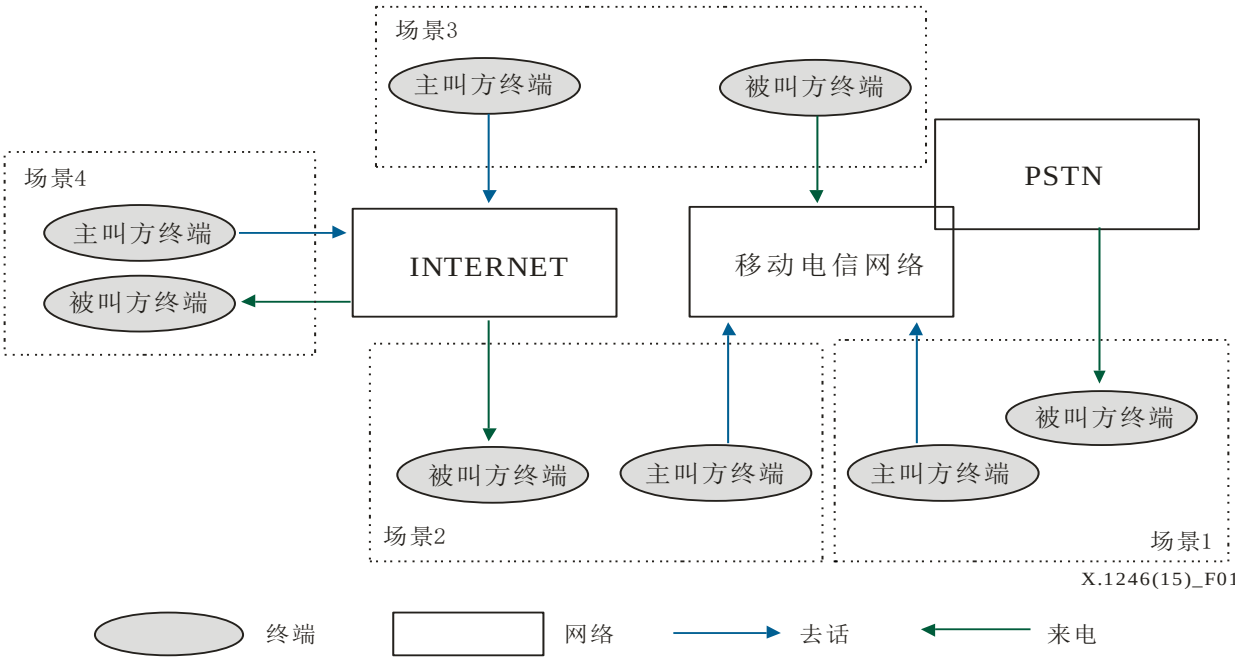


图1 – 电信网络中的语音通信

注 – 图1中的终端包括可接入电路交换网络/IP网络的手机、固定电话、笔记本电脑、PC机等等。一般来说，大多数用户都会信任语音通信的来源。结果，语音垃圾邮件制造者会使用传统电路交换语音通信发起语音垃圾邮件。另外，在场景3和场景4中的反语音垃圾邮件技术在[ITU-T X.1244]中有介绍。因此，本建议书只着眼于场景1 (CS-CS)和场景2(CS-IP)中的反语音垃圾邮件技术。

6.2 语音垃圾邮件特性

语音垃圾邮件可传播内容的范围从商业广告到攻击性的色情材料，会对用户和网络运营商产生有害的影响：

– 语音垃圾邮件包括令人厌烦的、欺诈的或恐吓性的内容

– 用户和运营商要忍受浪费资源

– 用户和运营商在抵制语音垃圾邮件时将花费时间、金钱和精力。

最被广泛认可的语音垃圾邮件的形式被分为以下两类，但不局限于以下两类：

– **类型一（静默电话）**：静默电话的目的是电话营销，通过预先设置的拨号器产生，没有特定的呼叫对象。在此情况下，呼叫可由拨号器终止，被叫方会从电信公司接收到表明电话已掉线的静默音或铃声。术语“废弃呼叫”有相同的意义。通常，这类呼叫期待收到回拨。

– **类型二（骚扰电话）**：这类电话的目的是电话营销，或是带有骚扰、警告、恐吓意图的色情、非法信息、虚假广告等。通常，这类呼叫直到接听不会掉线。

7 反语音垃圾邮件技术

7.1 通用特性

没有一种解决方案可以独自成功。为了减轻语音垃圾邮件的消极影响，有必要实施一系列相关技术的解决方案，应用于6.1节中描述的场景1和场景2，分为网络端技术和用户端技术。

为推荐具体和实用性的技术，需要对电路交换网络的特性有一个比较深的了解，包括网络结构、网络拓扑和信号协议堆栈等。同时也许了解语音服务过程和终端的功能趋势。推荐的技术可被分为网络端技术和用户端技术：

网络端技术对运营商极为重要，即公共交换电话网络（PSTNs）、全球移动电信系统（UMTSs）、全球移动通信系统（GSMs）和码分多址接入（CDMA）网络。与网络端技术相比，用户端技术更灵活并独立。用户反馈是对网络端技术的一项必要的补充。因此，也需要建立两种技术之间的一项有效的合作机制。

7.2 网络端技术

通过向接入网络发送信号发起电话呼叫。为了检测到可疑的语音垃圾邮件制造者，基本方法是收集信令数据，分析并认证。该方法需要全面考虑。通常来说，通话建立阶段包括通信两端的握手。在呼叫建立阶段，呼叫方/被叫方的唯一识别是主叫身份识别（ID）。这将导致以下检测：

1) 任何呼叫处理决策需要在呼叫建立完成之前实时确定。

语音垃圾邮件提出了复杂的技术挑战，因此要剔除它需要有适当的程序与技术手段结合的支持。图2给出了反语音垃圾邮件的基本网络端流程。

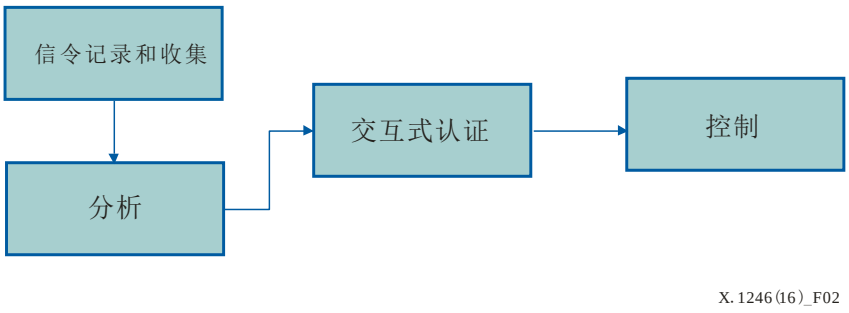


图2 – 反语音垃圾邮件网络端流程

– **信令记录和收集**：实时记录和收集原始信令数据。

– **分析**：确定可疑的语音垃圾邮件制造者并列出他们的号码。

– **交互式认证**：在可以名单中获得直接认证，找出真正的语音垃圾邮件制造者。

– **控制**：为保护正常用户，限制或禁止由认证过程确认的语音垃圾邮件制造者。

用户端流程几乎相同，但在每一部分的措施更简单。在一些案例中交互式认证可以取消。

根据流程，每部分分别对应几种技术。需要注意的是，下面章节讨论的技术中没有一种是可以解决语音垃圾邮件问题的唯一良方。相反，所有的技术是互补的，在同时使用时会更有效。

本建议书会根据各技术的部署位置对其进行介绍和分类，即网络端、用户端技术及合作过程（如图2所示）。

7.2.1 信令记录和收集

为进行分析，信令记录和收集是实时（或类实时）收集呼叫细节记录数据，包括时间相关或电话号码相关数据，例如：

– 呼叫起始时间点（COTP）：呼叫者发起电话呼叫的时间点

– 信令链路建立时间点（SLETP）：呼叫双方建立信号链接的时间点

– 呼叫持续时间点（CCOTP）：呼叫继续并由被呼者接通的时间点

– 呼叫清除时间点（CCLTP）：呼叫结束的时间点

– 信令链路释放时间点（SLRTP）：呼叫结束后释放信号链接的时间点

– 呼叫起始用户号码（COSN）：通常称为呼叫号码，发起呼叫的呼叫方号码

– 呼叫终止用户号码（CTSN）：通常称为被叫号码，接受呼叫的被叫方号码

相同数据尤其是时间相关数据的值在不同收集点的位置会有些许不同。但是在实际中，上述细微差别可以被忽略。

需要注意，被节中使用的信号来自于信令信道，并不来自于服务信道。在信令记录过程中，为了统计和性能诊断，所有收集到的数据几乎已存在于信令管理系统中，因此，出于平衡损耗的考虑，这些数据可以重复利用。

注 – 下面只会列出普通的数据源（基于信令系统7号（SS7），智能网络（IN），IP多媒体子系统（IMS），彩铃（CRBT）语音邮件服务器（VMS）等），尽管有可代替的数据源，例如R2及未接电话警报系统。

7.2.1.1 SS7 信令

SS7信令是可辅助监控语音垃圾邮件的有用来源。为了复制信令信息和参数并记录它们，插入一个信令采集点是有实用性的。信令采集点与信号链路并联，所以信号可以有效地“分束”，即使采集点会消耗一小部分信号功率。在这种情况下，信令点故障不会对信令链路有任何消极影响。

还有另一种采集SS7信令的方法，在两个明确的信令节点之间插入一个隐藏的信令节点。这意味着，为了记录信号，隐藏信令节点会首先将信号分块，然后无差别传输信号。但是，该技术有单点故障的风险。因此需要可靠的故障修复和备份能力。

使用SS7信令记录的巨大优势是它们包含了来自可推理的指示器的细节呼叫数据（见7.2.2节）。但是，如果语音呼叫交换增加，网络扩张，信令采集点的数量需要同步增加，以覆盖所有/大多数信号源，确保监视范围，同时也增加了反垃圾邮件的成本。

建议在核心/本地网络配置信令采集点。为实现全面的采集，这些点会覆盖交换器的所有Mc和Nc接口。此外，为了采集平衡，这些点只需覆盖所有NC接口，如果焦点只集中在国内长途或国际长途，则需覆盖长途/国际信令转接点（STPs）。

注 – 采集信令点属于合理的网元，可通过不同种类的实体元素进行采集。

7.2.1.2 智能网络 (IN)

基于服务控制点（SCP）的方法是为分析移动增强逻辑（CAMEL）或智能网络应用协议（INAP）收集自定义应用。SCP是IN中的关键节点，是决定如何处理电话呼叫的决定因素。

一旦用户签订了IN服务，呼出通话在建立通信链路前会触发SCP，询问被叫用户的访问位置注册（VLR）信息。由于一些运营商青睐于IN服务，很容易收集和记录IN合同用户发起的通话的信令数据。

由于信令采集点会在SCP上或SCP周围，该方法需要比SS7少的信令采集点。无论IN合同用户是否移动，使用该技术都会被轻易监控。

该技术有一项限制。如果IN服务的渗透处于低水平，只有一小部分用户的行为会被监控。但是，可以通过帮助各用户订购IN自定义服务解决这一情况，可保证在呼出电话时都向SCP查询。

该技术受限于普通IN服务流程；因此，只有有限的数据能被手机，例如COTP，SLETP，COSN和CTSN（见7.2.1节）。然而如果引入更复杂的IN服务流程，就还有改善的空间，例如所有的电话信令信号都由SCP转发。

IP多媒体子系统（IMS）技术与上述描述类似，IMS与IN的信令流程相似。

7.2.1.3 个性化来电彩铃 (CRBT)

个性化来电彩铃彩铃是一项一些运营商提供的面向用户的特殊服务。一旦用户订购彩铃服务，其他用户将听到预订的音乐段落，而不是电话铃音。结果，可在彩铃主机中记录和采集信令数据。

该技术受限于服务流程；因此，在服务主机中只能采集有限类型的数据，例如COTP，CCOTP，COSN和CTSN（见7.2.1节），CRBT流程也没有更大的改善空间来采集更多类型的数据。

一旦语音邮件制造者骚扰彩铃用户，制造者将会被监控，因此实现该技术的前提条件是服务的高渗透率。如果现状令人满意，在信令记录和收集上的投资需要相对降低。

7.2.1.4 语音邮件服务器 (VMS)

VMS处理呼叫无应答、呼叫忙、呼叫无限制情况下的电话呼叫。大多数情况下，除非不限制标准，VMS不会回应静默电话。如果垃圾邮件呼叫方打算接通呼叫并直接骚扰被叫方，它会提供主叫方的语音记录，然后通过用户反馈或授权（见7.3.3节）的录音支持交互式认证程序。

与彩铃类似，VMS的服务渗透率和使用率是技术实施的前提条件。

7.2.1.5 蜜罐技术

蜜罐技术用于安装一些连续或随机的电话号码，以吸引语音垃圾邮件制造者。除收集数据之外，蜜罐技术也可以促进分析流程和交互式认证流程。

由于蜜罐技术可由任意呼叫者完成，可以收集一些特定类型的数据，例如COTP，CCOTP，CCLTP，COSN和CTSN（见7.2.1节）。蜜罐会为7.2.2节中介绍的一些分析手段计算或传递数据。

7.2.2 分析

为了使用监控系统对反语音垃圾邮件进行分析，收集到的原始数据将会计算并转换成有意义的指标，例如连通率、呼叫释放时间、铃音持续时间等。为了区分语音垃圾邮件制造者和普通用户，需要以特定周期（通常称为时间窗）连续计算这些指标，运营商将给予维护经验调整时间窗的长度。

所有指标会逻辑推理成一个更综合的指标，称为“规则”，可用于分析语音垃圾邮件制造者行为的算法，使其准确性更高。判断语音垃圾邮件制造者的规则模型如图3所示。

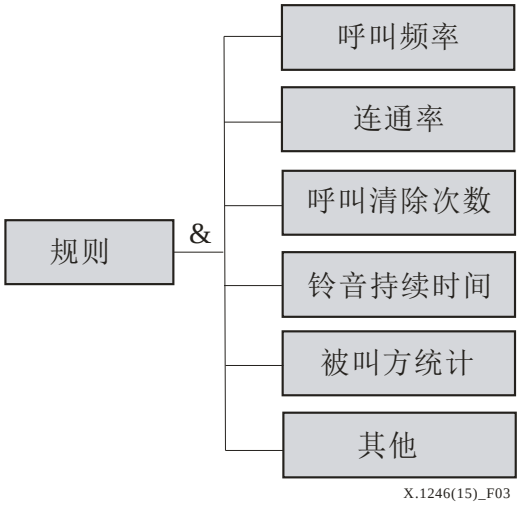


图3 – 规则模型

规则模型是由几个指标的逻辑与操作推断出的。由于数据来源不同，并将收集到一起，不会同时支持所有指标。一个可行的解决办法是设立一个不支持的指标“真”或“1”，并忽视它们。例如，在收集数据并转换成指标后，蜜罐只需铃音持续时间指标来处理所需的分析流程，并将其他指标的值设为“真”或“1”来忽略它们。

规则模型包含的指标及其定义如下所示：

– 呼叫频率：特定周期内的呼叫次数
– 连通率：语音通信或信令链路建立比例
– 呼叫清除次数：主叫方或被叫方主动释放呼叫的次数
– 铃音持续时间：铃音持续的时间
– 被叫方统计：被叫方的统计特性，例如均匀分布，等差数列等。

为了平衡精确度和成本，运营商根据现实服务场景调整指标的阈值。此外，需要针对不同类型的语音垃圾邮件制定具体的规则。

例如，有两种公认的语音垃圾邮件：静默电话和骚扰电话。静默电话（又称废弃呼叫）是由拨号器发起的电话呼叫，没有特定的呼叫对象。在此情况下，呼叫将由拨号器终止，被叫方会接收到电信公司的静默音或指示掉话的铃音。通常这种呼叫期待回拨。骚扰电话是带有骚扰、警告、恐吓意图的色情、非法信息、虚假广告等。通常，这类呼叫直到接听不会掉线。

静默电话和骚扰电话（见6.2节）会在所提规则模型中分别表现出不同的指标特性。对于静默电话垃圾邮件制造者，会表现出更高的呼叫频率或呼叫清除次数，和更低的连通率和铃音持续时间。另一方面，骚扰电话面向特定的被叫方，它倾向于保持更长的铃音持续时间，同时获得更高的连通率。

在一些情况下，一些静默呼叫者会开启“无条件呼叫转移”服务，使用交互式语音应答（IVR）平台告知网络向特定号码无条件转接通话。IVR 平台甚至可以通过铃音向呼叫方发回语音垃圾邮件。这有助于分析审核可疑呼叫者是否开启了“无条件呼叫转移”服务以及目的号码是多少。

事实上，存在更复杂和有效的分析模型用于反语音垃圾邮件，例如与人类社会分析、呼叫计费记录分析等结合的模型。总之，规则模型是发展成更复杂模型的基础。

7.2.3 交互式认证

管理实体或用户服务协议提出需求，在实施一些控制措施前需要查清可疑名单内的呼叫号码。依照要求，有两种可选择的方法实施认证。

第一，电信组织将持续更新可疑名单并将其提交给管理实体，并接受反馈。

第二，如果用户服务协议或管理实体允许，为获得直接认证，运营商可以在可疑名单上进行拨号测试。使用拨号测试的结果，即语音记录文件，经授权的审计职员可以指出记录是否是垃圾邮件。

然而，交互式认证的准确性和质量影响着控制程序。

综上所述，蜜罐可以自己处理交互式认证，也就是说，如果指标的计算结果显示拨出电话是静默电话（见6.2节），蜜罐会回拨以认证；相反，当指标分析确定是骚扰电话，蜜罐会接通电话并记录。

此外，一组静默呼叫者和一个/几个IVR平台的协调会混淆运营商查找语音垃圾邮件真实信号源。有时，IVR平台和静默呼叫者分别从属于不同运营商。例如，接收到垃圾邮件语音记录后，通过请求起始位置注册可以追踪到静默呼叫者和IVR平台之间的潜在联系。

7.2.4 控制

控制是为保护普通用户而约束或禁止/关闭经认证的语音垃圾邮件制造者。下面讨论两种方法。

7.2.4.1 白名单/黑名单

白名单/黑名单，通常被称为大客户列表，生成费时且需要持续更新。白名单/黑名单中每一项的生存周期需要被妥善管理，以保持精确、有效。同时每一项需要在其生命周期内安全管理。

如[ITU-T X.1240]所示，黑名单的质量很大程度上取决于编译器的专业程度。黑名单不可避免会包含误差，这会使接收端阻止一些合法的电话。虽然使用黑名单增加了许多关注，黑名单也是拒绝语音垃圾邮件源和接收者（电话用户）连通的快速解决方法。

包含用户号码或号码段的黑名单通常部署在网关移动交换中心（GMSC），SCP，交换器和其他网络实体中。通常，相同运营商网络的黑名单可以部署在SCP，交换器或其他网络实体中，然而其他运营商网络的黑名单可以部署在GMSC中，其黑，名单容量太小无法存储大量号码。为了解决这个问题，可在GMSC后使用隐藏信令节点（见7.2.1.1节）。

白名单需要与授权数据库相互作用，这些数据库用来维护已确定合法的呼叫者，排除与语音垃圾邮件制造者有相同性质的非计划内合法呼叫者。这些呼叫者可能是呼叫中心，通知服务，反馈/数据收集服务，例如定期付款提醒，管理实体发起方案的反馈，宣传计划，紧急-/灾难-方案计划等。

7.2.4.2 回溯机制

该机制能追溯到语音垃圾邮件制造者的真实物理位置。必要时可以标记处语音垃圾邮件制造者的准确位置或地址。

根据现有技术，运营商可以基于移动交换中心（MSC）提供的信息定位语音垃圾邮件制造者的真实位置；然而，该技术只能定位到近似的区域。更精确的位置需要由运营商的位置信息服务提供，例如辅助全球定位服务。

7.3 用户端技术

用户端技术是对网络端技术的有效补充。反馈措施可以提供具体的语音垃圾邮件制造者信息（如下所述），这对运营商是特别重要的反馈。用户端技术需要一些智能移动电话特性的辅助，对这些的支持可能与制造商不同。

7.3.1 白名单/黑名单

用户可以使用电话内的连接控制特性来阻挡特殊号码或黑名单内标记的号码，同时会允许被标记为白名单的特殊号码（有用户设定或有一些移动应用同步）接通。

当与网络端同步时，该技术基于白名单/黑名单工作，然而由于用户可以管理自己的名单，用户端通常服从于个人喜好。

7.3.2 呼叫延时

呼叫延时是特别为静默电话工作的信令级别技术（见6.2节）。

在主叫方和被叫方之间的信令链路建立后，铃音会从链路周期性地产生。会产生一些静默电话，用户会接收到静默音或指示掉话的短暂持续铃音。

由于智能手机的支持，用户在终端（用户端）可以阻止静默电话。由于用户可以在信令层为每个来电设置铃音持续时间的阈值，如果铃音持续时间小于阈值，静默电话可能会被遗漏。然而，呼叫记录会保存在移动电话的通话记录中，如果忽略了短铃音正常通话，用户可以仔细检查。

7.3.3 反馈

在接收到语音垃圾邮件后，用户可以向运营商提供反馈，指明语音垃圾邮件号码和其他具体信息。反馈渠道包括发短信、打电话、发邮件或向运营商客户服务部（或其他等同部门）的官方网站投诉。所有渠道都需要为用户反馈提供方便的程序。方便使用的渠道可由终端模块或用户身份模块（SIM）卡、或网络中设备管理平台（DMP）、无线平台（OTAP）等平台建立。

此外，一旦运营商服务部门收到反馈，授权审查员需核实反馈信息的真实性和有效性，并在进一步行动前申请类似的交互式认证程序。

7.4 合作机制

为了反语音垃圾邮件，运营商会与管理实体、其他运营商或用户合作，建立一些相应的合作和通信模式。

运营商可以建立或支持一个信息共享系统（ISS）。这个特殊系统可以覆盖与其他机构的基本语音垃圾邮件信息交换，包括可疑/认证垃圾邮件呼叫方名单，语音垃圾邮件分类、反垃圾邮件技术等。

管理实体会考虑ISS的实施和信息交换机制的建立，甚至组织运营商正是会议，及共享最新信息的第三方组织。

用户在网络端可以向服务器上传或下载黑名单，实现共享。然而，运营商需要有一个认证机制来判别个人黑名单中的某项是否是真正的语音垃圾邮件制造者。运营商需要为上传和下载黑名单提供一个接口。该机制应与用户反馈相互作用。同时，管理实体需要审计更新的数据，以避免不适当的信息。

为了落实信息共享机制，运营商需要循环向管理实体提交已查清的黑名单，并替换管理实体已确定的黑名单。

另外，管理实体将结合所有从各运营商收到的黑名单并申请适当的行动和程序。此外，管理实体将承担更多责任，例如在源头抑制语音垃圾邮件，同时保证运营商履行其职责。

7.5 解决方案

没有一项解决方案可以完全独立成功执行。为了有效抵制语音垃圾邮件，网络端和用户端技术在每一流程将协同应用。

为了达到高准确度，有必要在信令记录程序将多种数据源整合在一起。然而，一项综合数据源的成本是极高的。

需考虑以下情况。

首先，为了保证反语音垃圾邮件的有效性，SS7信令可能是单一的选择，因为比起其他数据源，它覆盖了所有信令链路以获得最有用的数据（如7.2.1节所述）。

另一方面，基于IN、CRBT或VMS的数据采集系统是成本平衡的，前提是运营商已经开展IN，CRBT或VMS服务。然而，CRBT或IN网络的数据源不会覆盖7.2.1节中讨论的所有特定数据。因此，这些服务的数据源是互补的。

7.2.2节提出的模型是易用并低成本的，也通常用于反语音垃圾邮件。为了提高分析的准确性，可以采用更多复杂的规则模型和算法。例如，呼叫释放原因编码的统计和拒绝呼叫编码的统计大大减少了可疑名单。

然而，综合的规则模型或算法会导致高度的系统复杂度和长耗时程序，反过来会增加整个反语音垃圾邮件的延时，最后降低用户满意度。考虑这些，适当规则模式或算法的选择对运营商是有重大意义的。

每个国家的交互式认证程序是不同的。因此，管理实体会基于国情协助制定适当的认证程序。

基于早先规定的控制程序，需要更好地结合用户端和网络端方法以降低语音垃圾邮件的危害。运营商的客户服务部门在控制程序和满足用户需求上需扮演重要角色。

附件A

打击垃圾呼叫的交互式措施和技术措施

（本附件是本建议书不可或缺的一部分）

摘要

本附件概述了旨在打击垃圾呼叫的流程，并提出了在接到垃圾呼叫后立即拨打号码/（电信运营商专门分配的）号码来打击此类垃圾呼叫的技术基础。在该框架内，决定运营商必须提供专门的反垃圾信息号码和为这些号码提供不同级别的呼叫细节记录处理功能。此外，本附件提供了信息共享机制，以便在运营商间交互的框架内打击垃圾信息。

本附件提供了打击垃圾信息的技术基础，即签约用户在接到垃圾呼叫后立即通过短时呼叫反垃圾信息号码来告知运营商。

本附件适用于语音呼叫业务、短消息业务（SMS）和多媒体消息业务（MMS）。

签约用户与电信运营商/服务提供商互动的交互式报告服务场景，以打击电话终端收到的垃圾呼叫

[ITU-T X.1247]介绍了用于处理垃圾消息的用户反馈机制和用户报告的概念。

ITU-T X.1246建议书介绍了不同的交互验证和垃圾信息处理机制。

此处介绍的交互式机制补充并扩展了本建议书（ITU-T X.1246）和[ITU-T X.1247]主要部份的现行程序。垃圾呼叫的签约用户/被叫方与电信运营商/服务提供商之间的建议的交互在于这样的事实：用户向该电信运营商/服务提供商的专门反垃圾信息号码进行短时呼叫或将收到的垃圾消息转发到该号码。

A.1 交互式反馈场景/算法/使用案例

通过CDR/CLI细节的自动处理，利用呼叫反垃圾信息号码的事实来确定垃圾呼叫的场景包括以下步骤：

1) 被叫方/客户/签约用户收到来话呼叫，将其识别/定义为垃圾呼叫或可疑垃圾呼叫（语音垃圾信息、垃圾短信或垃圾彩信）。

2) 关于该呼叫（以及任何其他呼叫）的CDR/CLI存储在电信运营商的电信管理系统（或其他一个系统/多个系统）中。此CDRn/CLIn包含主叫方标识符（垃圾呼叫的可能来源）、被叫方标识符（垃圾呼叫被叫方）、呼叫时间。

3) 在完成本次呼叫后，被叫方/客户/签约用户立即/尽快拨打其归属/所属服务提供商/电信运营商预先确定的专门的反垃圾信息号码（取决于国家监管，该号码可以是全国唯一的，或者每个运营商单独的号码），即作为交互式用户报告拨打反垃圾信息号码。

4) 本次呼叫的CDRn+1/CLIn+1也保存在运营商的电信管理系统中。

5) 运营商接收到用户拨打至反垃圾信息号码的呼叫，捕获所有技术信息CDRn+1（CDR和CLI，细节程度各不相同），自动查找可能的垃圾呼叫的签约用户/被叫方在拨打反垃圾信息号码之前收到的最后一个呼入的CDRn呼叫，并开始收集有关可能的来自垃圾呼叫侧的信息（可能与其他运营商/监管机构交换此信息）。

6) 如果拨至反垃圾信息号码的呼叫是单一和/或错拨的，则无需采取进一步的步骤。

7) 如果可能的垃圾呼叫的多个被叫方向反垃圾信息号码进行了多次呼叫，且在每种情况下，CDR处理系统将确定相同主叫号码或在签约用户/用户呼入反垃圾信息号码之前

收到的最后来话呼叫的CLIn，这将更有可能检测到垃圾呼叫的真正来源以帮助找到垃圾信息制造者。

8) 可以选择性为CDR处理系统设置各种门限值，杜绝误报。

A.2 技术要求

A.2.1 为了接收被叫方的反馈呼叫，电信运营商/服务提供商需设置一个专门的反垃圾信息号码。

A.2.2 为了处理大量的反馈呼叫，电信运营商/服务提供商的电信管理系统需拥有基于整体形成的CDR和更为详细的CLI细节接收和处理这些呼叫的能力。

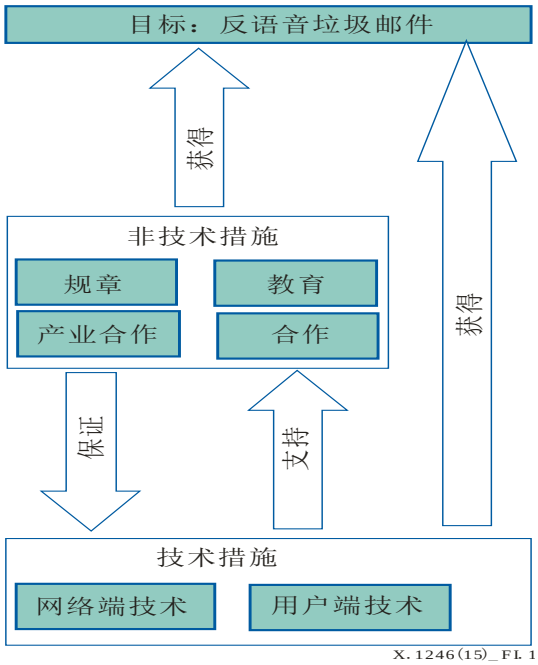
A.2.3 电信管理系统需具备针对报告服务的服务质量（QoS）统计数据。

附录 I

反语音垃圾邮件综合措施

（本附录不是本建议书的组成部分）

由于反语音垃圾邮件不是一个简单的技术问题，需应用多种处理方法，如图I.1所示：



图I.1 – 反语音垃圾邮件结构

– 相关规章有助于保护用户和运营商不受语音垃圾邮件影响。
– 产业合作是必须的，所以产业合作伙伴需对多种技术进行开发和实施。
– 合作可以帮助运营商和管理实体共享有效采纳法规和技术开发的信息。
– 对用户的教育是重要的，可使其遭受语音垃圾邮件的经济损失最小化。

附录 II

交互式认证的建议解决方案

（本附录不是本建议书的组成部分）

一般而言，每次交互式认证意味着一次可疑呼叫号码的拨号，在接通前记录回拨铃音，以及接通后的语音，然后审计内容以核实是否为语音垃圾邮件。如果所有这些步骤都由手动完成，这将耗费运营商相当多的人力。因此，为平衡成本，需要采用一项最优的措施。

交互式认证可以对拨号记录集中操作，并半自动审计分布在网络每个角落的语音垃圾邮件制造者的语音证据。

这种集中式方法自动同时执行拨号和记录工作，仅允许审计员成功审计去除白噪声和其他无用回拨铃音的语音证据。

附录 III

反语音垃圾邮件政策建议

（本附录不是本建议书的组成部分）

语音垃圾邮件是用于广告、诈骗和骚扰等的危险工具，会发生在日常通信中。为了有效抵制语音垃圾邮件，需要考虑各参与团体各方面的不同措施，尽管本建议书介绍了不同种类的技术。它们是用户（或订阅者），运营商，管理实体和第三方机构。因此，本附录描述了反语音垃圾邮件涉及到的几方面内容。

III.1 用户

用户是语音垃圾邮件通信链的最终受害者，他们对于拦截垃圾邮件有很大的需求。因此，用户需要在反垃圾邮件整个过程中采取一些措施。下面提出了基于变化情况的一些建议：

– 用户需在自己的设备，例如智能手机上安装反垃圾邮件应用。为了有效防护，反垃圾邮件应用必须是最新的，

– 用户一旦接收到语音垃圾邮件，需向电信运营商或第三方机构反馈所有语音垃圾邮件的细节信息。

– 用户需要更有意识地注意日常通信，保护个人信息不泄露给垃圾邮件制造者。

III.2 运营商

运营商是整个反语音垃圾邮件过程中的重要环节。由于语音垃圾邮件会严重降低用户 满意率，导致网络资源的浪费，运营商需要检测到语音垃圾邮件，保护其网络并提供更好的服务。

– 运营商需要监控整个通信网络，检测导致反常信令传输或流量模式的潜在语音垃圾邮件。

– 运营商需要向自己市场分布或销售渠道内可能成为语音垃圾邮件目标的所有设备预先安装最新版本的反垃圾邮件应用。对于第三方销售渠道，运营商需要保证所有设备受最新应用保护。

– 运营商需要提供培训活动，并鼓励用户向第三方机构提供详细的语音垃圾邮件制造者信息反馈，这种反馈可通过激励项目操作。

– 运营商需要与管理实体和第三方机构构成联盟，以加大反语音垃圾邮件的力度。

III.3 管理部门和第三方机构

管理实体和第三方机构可以直接监督或引导运营商，甚至提供必要的支持。

– 管理实体和第三方机构需要培训或向用户和运营商提供反语音垃圾邮件的培训活动。

– 管理实体和第三方机构需要引导更多的语音垃圾邮件研究趋势，并针对语音垃圾邮件的最新模式争取找到更有效的抑制措施和技术。

– 管理实体和第三方机构需要疏通广告和促销渠道，使现有语音通信环境正常化，或调节特许广告拨号系统。
– 管理实体和第三方机构需要与运营商甚至用户共享最新的黑名单；该黑名单需要在运营商和用户的支持下管理。
– 管理实体需提供加强反语音垃圾邮件力度的环境，以保护用户的权益。

参考文献

[b-ITU-T E.370] ITU-T E.370 (2001)建议书，公共电路交换国际电信网络与IP网络互连的服务准则。

[b-ITU-T M.60] ITU-T M.60 (1993)建议书，维护术语和定义。

[b-ITU-T M.1400] ITU-T M.1400 (2013)建议书，运营商网络互连名称。

[b-ITU-T X.1231] ITU-T X.1231 (2008)建议书，反垃圾邮件技术策略。

[b-ITU-T X.1242] ITU-T X.1242 (2009)建议书，基于用户指定规则的短消息业务（SMS）垃圾信息过滤系统

[b-ITU-T X.1245] ITU-T X.1245 (2010)建议书，IP多媒体应用反垃圾邮件框架。

[b-ITU-T Y.1001] ITU-T Y.1001 (2000)建议书，IP 框架 – 聚合电信网络和IP网络技术的框架。

[b-IETF RFC 5039] IETF RFC 5039 (2008)，会话发起协议(SIP)和垃圾邮件。

ITU-T 系列建议书

系列 A	ITU-T 工作安排
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	整体网络运营、电话业务、服务运营和人为因素
系列 F	非电话电信服务
系列 G	传输系统和媒体、数字系统和网络
系列 H	视听和多媒体系统
系列 I	综合服务数字网络
系列 J	有线电视网络和电视的传播，合理的计划和其他多媒体信号
系列 K	干扰防护
系列 L	环境和信息通信技术、气候变化、电子垃圾、能源效率；结构、安装和电缆保护以及外部设备的其他因素
系列 M	电信管理、包括电信管理网和网络维护
系列 N	维护：国际广播节目和电视传输电路
系列 O	测量设备说明书
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关的测量和测试
系列 R	电报传输
系列 S	终端服务终端设备
系列 T	远程信息处理服务终端
系列 U	电报交换
系列 V	电话网络之上的数据通信
系列 X	**数据网络、开放系统通信和安全**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	电信系统的语言和通用软件方面

瑞士印刷
2022年，日内瓦