国　际　电　信　联　盟

ITU-T

国际电信联盟
电信标准化部门

X.1245

(12/2010)

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

IP多媒体应用中用于反垃圾信息的框架

ITU-T X.1245建议书

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
报文处理系统	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
生物测定安全	X.1080–X.1099
安全应用和服务	
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	X.1140–X.1149
安全协议	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	
计算网络安全	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	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
网络安全信息交换	
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1245建议书

IP多媒体应用中用于反垃圾信息的框架

摘要

ITU-T X.1245建议书提供了IP多媒体应用中用于反垃圾信息的通用框架，如IP电话、即时消息、多媒体会议等应用。框架包括四种反垃圾信息功能，即核心反垃圾信息功能（CASF）、接收方反垃圾信息功能（RASF）、发送方反垃圾信息功能（SASF）和垃圾信息接收功能（SRF）。本建议书描述了每种反IP多媒体垃圾信息功能的功能性和接口。

沿革

版本	建议书	批准日期	研究组	
1.0	ITU-T X.1245	2010-12-17	17	

关键词

反垃圾信息功能、IP多媒体垃圾信息、垃圾信息

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）是国际电信联盟的常设机构，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。

每四年一届的世界电信标准化全会（WTSA）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1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“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或适用性等），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

国际电联提请注意：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、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1245建议书

IP多媒体应用中用于反垃圾信息的框架

1 范围

本建议书提供了反IP多媒体垃圾信息的通用框架。该框架可用于IP多媒体应用中，如IP电话、即时消息、多媒体会议等。框架包括四种反垃圾信息功能，即核心反垃圾信息功能（CASF）、接收方反垃圾信息功能（RASF）、发送方反垃圾信息功能（SASF）和垃圾信息接收功能（SRF）。它描述了每种反IP多媒体垃圾信息功能的功能性和接口。实施本框架的技术方法不在本建议书讨论范围之内。

在应用本建议书所述的反垃圾信息的方法之前，应考虑该方法是否遵循相关法律法规。

2 参考文献

无。

3 定义

3.1 其他文献规定的术语

本建议书使用了以下其他文献规定的术语：

3.1.1 spam 垃圾信息 [b-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。

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

3.2 本建议书中规定的术语

本建议书规定下列术语：

3.2.1 anti-spam functions (ASF) 反垃圾信息功能：一种用于打击IP多媒体应用中垃圾信息的逻辑功能。ASF可以位于如代理服务器、应用服务器等网络要素中。

3.2.2 blacklist 黑名单：通信服务中有关人员或来源的一个身份清单，该清单中的人员或来源不得访问特定的通信资源。

3.2.3 core ASF (CASF) 核心ASF：ASF的一个实例，用于确定和阻断IP多媒体垃圾信息。它还能管理反垃圾信息政策和控制RASF与SASF。

3.2.4 IP Multimedia spam IP多媒体垃圾信息：在IP多媒体应用中未经请求就提供的消息或呼叫，垃圾信息通常具有特定的特性，如容量庞大。为与传统的电子邮件垃圾信息区别开来，IP多媒体垃圾信息指的是在新出现的IP通信方式上的垃圾信息，如即时消息（IM）或经由IP的语音（VoIP）。

3.2.5 recipient-side ASF (RASF) 接收方ASF：ASF的一个实例，用于确定和阻断穿过内部网络边界传送给垃圾信息接收方的IP多媒体垃圾信息。RASF可以位于以下网络要素中，即发往垃圾信息接收方的通信请求作为最后一跳来发送。

3.2.6 sender-side ASF (SASF) 发送方ASF：ASF的一个实例，用于确定和阻断从垃圾信息制造者发往外部网络边界的IP多媒体垃圾信息。SASF可以位于以下网络要素中，即来自垃圾信息制造者的通信请求作为第一跳来发送。

3.2.7 spam recipient 垃圾信息接收方：接收垃圾信息的实体或个人。

3.2.8 spam recipient functions (SRF) 垃圾信息接收功能：一种ASF，用于确定和阻断到达垃圾信息接收方的IP多媒体垃圾信息。SRF可以位于垃圾信息接收方的本地网络或终端中。

3.2.9 whitelist 白名单：通信服务中有关人员或来源的一个身份清单，该清单中的人员或来源是已知的、可信的或得到明确许可的。

4 缩写词和首字母缩略语

本建议书采用以下缩写词和首字母缩略语：

ARS 自动响应系统
ASF 发垃圾信息功能
CA 证书机构
CAS 核心反垃圾信息
CASF 核心反垃圾信息功能
CRL 证书撤销列表
DAC 随意的访问控制
HBAC 基于历史的访问控制
IM 即时消息
IP 网际协议
IPSec 网际协议安全性
L2TP 第二层隧穿协议
MAC 强制的访问控制
MTA 邮件传送代理
NDAC 非随意的访问控制
OTP 一次性口令
PBAC 基于目的的访问控制
PKI 公开密钥基础设施
RAS 接收方反垃圾信息
RASF 接收方反垃圾信息功能
RBAC 基于角色的访问控制
RuBAC 基于规则的访问控制
SAS 发送方反垃圾信息

SASF 发送方反垃圾信息功能
SPF 发送方政策框架
SR 垃圾信息接收
SRF 垃圾信息接收功能
SSL 安全套接字层
TCAC 暂时约束的访问控制
TTP 可信的第三方
TTS 文本至语音
VoIP 通过网际协议传送的语音（IP语音）
VPN 虚拟专用网

5 惯例

功能：在讨论用于打击IP多媒体垃圾信息的框架时，“功能”定义为一个功能集。它用以下符号表示：

功能块：在讨论用于打击IP多媒体垃圾信息的框架时，一个“功能块”定义为一组功能，在本建议书所述的详细程度上，未对其做进一步细分。它用以下符号表示：

6 用于打击IP多媒体垃圾信息的技术方法

IP多媒体垃圾信息可定义为通过IP多媒体应用未经请求而主动发送的消息或呼叫。为区别IP多媒体垃圾信息与传统的电子邮件垃圾信息，IP多媒体垃圾信息指的是借助IP通信方法传送的垃圾信息，如VoIP、即时消息等。IP多媒体垃圾信息通常具备有别于普通IP多媒体应用的特殊特性。通过在适当的IP网络要素上实施反垃圾信息功能，可以利用这些特性来确定和过滤垃圾信息。用于打击IP多媒体垃圾信息的技术方法可分为以下三类：

– 通过对IP多媒体应用的来源进行分析，来打击IP多媒体垃圾信息；
– 通过对IP多媒体应用的特性进行分析，来打击IP多媒体垃圾信息；
– 通过对IP多媒体应用的内容进行分析，来打击IP多媒体垃圾信息。

图1描述了用于打击IP多媒体垃圾信息的三种技术方法以及反垃圾信息技术的例子。

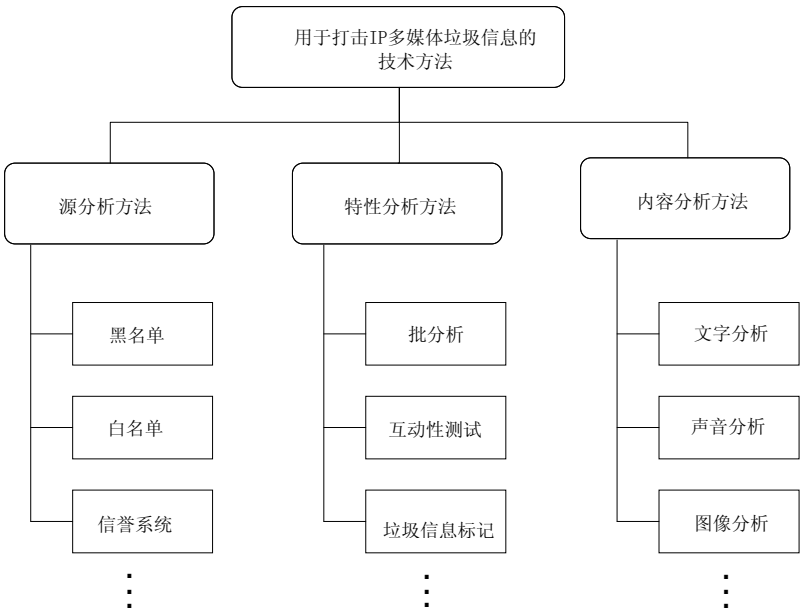

图 1 – 用于打击IP多媒体垃圾信息的技术方法

图1中的许多反垃圾信息技术已在打击电子邮件垃圾信息中得到应用，它们也适用于IP多媒体垃圾信息。用于打击IP多媒体垃圾信息的反垃圾信息技术不限于这些例子。

IP网络上的各种反垃圾信息功能间需要相互交流，以便利用好这些反垃圾信息技术。反垃圾信息实体实施反垃圾信息方法所需的各种功能和接口在以下各节中进行描述。仅用一种反垃圾信息技术无法有效打击IP多媒体垃圾信息。在这种情况下，为了更加有效地过滤垃圾信息，可能需要同时在IP网络中部署应用多种反垃圾信息技术。

6.1 来源分析方法

通过分析IP多媒体应用的来源信息，如信誉信息或者来源的垃圾信息散播历史，可以确定来自某处的IP多媒体应用是还是不是垃圾信息。IP地址、域名、电话号码以及用户标识符可用作来源标识符。

基于来源的反垃圾信息技术的例子包括白名单、黑名单、信誉系统等。它们已广泛用于打击电子邮件垃圾信息，并可用于打击IP多媒体垃圾信息。这些技术对IP多媒体垃圾信息的适用性在[b-ITU-T X.1244]中进行描述。不过，来源分析方法存在某些弱点，这些弱点降低了基于来源的反垃圾信息技术的效用，例如，垃圾信息制造者可以尝试进行发送方欺骗或者能够生成许多服务账号。因此，以下方法有望帮助基于来源的反垃圾信息技术更加有效地打击IP多媒体垃圾信息：

– IP多媒体应用来源的强认证；

– 垃圾信息判定政策和相关信息的有效管理。

首先，为了实现高效的垃圾信息过滤，需要高度可靠的IP多媒体应用来源信息，原因是垃圾信息制造者可以力图生成一条弯路，通过设立众多的服务账号或者试图进行发送方欺骗以遮盖发送者是一个垃圾信息制造者，来规避这些反垃圾信息技术。因此，IP多媒体应用来源的强认证有助于提供高度可靠的来源信息。

如上所述，垃圾信息过滤信息（如白名单、黑名单等）以及IP多媒体应用的来源用于确定垃圾信息。因此，需要对垃圾信息过滤信息和垃圾信息判定准则实施有效管理。

该技术的一大优势是，可以在垃圾信息传送给接收方之前阻断它。此外，假定上述因素得以满足，那么是有可能以相比其他反垃圾信息技术较小的代价，来实现对垃圾信息的有效打击的，如内容分析技术、特性分析技术等。

6.2 特性分析方法

6.2.1 基于特性分析的反垃圾信息方法

IP多媒体垃圾信息有许多有别于普通IP多媒体应用的特殊特性。例如，IP多媒体垃圾信息有时以批量信息的形式进行传送，相比普通的IP多媒体应用，其交互活动有限。当某个IP多媒体应用具备一个或多个这种特性时，可以认为它是垃圾信息并将之过滤掉。以下所述是IP多媒体垃圾信息的一些特性，但不限于下面所述的这些特性：

– 批量信息

IP多媒体垃圾信息有时以批量信息的形式进行传送，原因是垃圾信息制造者通常试图一次向许多垃圾信息接收方发送垃圾信息，以便尽可能减少垃圾信息的散播成本。当在短时间内从一个源头向许多目的地传送大量的IP多媒体应用时，该应用可被视为潜在的垃圾信息。

– 有限的交互活动

在许多情况下，IP多媒体垃圾信息仅提供有限的交互活动，原因是垃圾信息制造者倾向于利用机器而不是人工来发送垃圾信息，以降低垃圾信息的散播成本。例如，在即时消息垃圾信息或聊天垃圾信息中，垃圾信息发送方可能不做答复，原因是垃圾信息消息是通过垃圾信息散播机器进行发送的。VoIP垃圾信息 — 电信营销的一种形式，当利用ARS进行发送时，也可能提供有限的交互活动。因此可以通过测试IP多媒体应用的发送方是否提供了交互活动来判定是垃圾信息还是不是垃圾信息。在电子邮件系统中，基于该方法的、最常见的反垃圾信息技术是图灵（Turing）测试和灰名单技术，这两种技术可分别测试发送方和MTA的交互活动。

6.2.2 使用协议信息以打击垃圾信息

当利用特性分析方法来判定垃圾信息时，相比使用内容信息，使用协议信息将更有效。通过分析IP多媒体应用的来源，IP多媒体应用的协议部分可用于判定垃圾信息。在IP多媒体应用内容传送给接收方之前，使用协议信息来判定垃圾信息将花更少的力气，并且相比其他使用内容信息的反垃圾信息技术，它更为有效。以下结果可使该结论更加切实可行：

– 应用提供信息

IP多媒体应用的协议部分承载与IP多媒体应用提供有关的信息，如来源、目的地、发送时间、所用发送协议等。在这些协议部分中，有一部分可用于判定垃圾信息。

– 分析时间选择

在IP多媒体应用内容发送之前发送有关服务开始的协议信息。例如，在VoIP业务中，在呼叫会话开始之前执行信令进程，在信令进程中，要用到协议信息。因此，通过对协议信息进行分析，有可能在垃圾信息传送给接收方之前实现对垃圾信息的判定。

– 加密

尽管IP多媒体应用的内容可以在加密后进行传送，但对协议消息的传送通常不做加密。对IP分组进行加密会使解译分组分析变得非常困难或者变得不可能。因此，相比IP多媒体应用的内容部分，对其协议部分的分析会更容易。

– 媒体类型

IP多媒体应用的协议部分仅使用一种媒体类型；然而，其内容部分有时却体现为难以分析的多媒体形式。

– 传送路径

有时会话或服务开始的协议消息通过网络设备进行传输，如用于即时消息传送的应用服务器以及用于VoIP通信的代理服务器，可以从协议消息中获得有关IP多媒体应用的提供信息。另一方面，内容消息可直接从发送方传送给接收方，而无需通过网络设备来传输。在这种情况下，难以对IP多媒体应用内容进行分析。

6.3 内容分析方法

在内容分析方法中，IP多媒体应用内容分析结果可用于判定垃圾信息。该方法已广泛用于打击电子邮件垃圾信息。相比电子邮件的情况，对IP多媒体应用内容进行分析要困难得多，原因是IP多媒体应用可以是实时的和/或使用多媒体，而电子邮件通常基于文本并且不是实时的。下面所述是在内容分析方法中对有效打击IP多媒体垃圾信息问题所做的一些考虑：

– 内容分析的持续时间

需要在合理的时间内完成对内容的分析，使IP多媒体应用用户能够判定垃圾信息。在实时的IP多媒体应用中，可能无法在应用开始之前实施内容分析。

– 内容分析的精度

为有效实现垃圾信息的判定，IP多媒体应用的内容分析需要达到一定的精度水平。非常先进的声音和图像识别技术将有助于完成此项任务，原因是相比文本分析，对多媒体内容进行分析会很困难。

– 内容的加密

当IP分组做了加密时，对IP多媒体应用内容分析进行解译会变得非常困难或不可能。

– 内容的传送路径

在它通过适当的网络设备进行传输时，如具有内容分析功能的应用服务器或媒体服务器，对IP多媒体应用内容进行分析。

在许多情况下，IP多媒体应用无法满足必要的标准。在实时IP多媒体应用情况下，如VoIP，业务用户看来无法通过内容分析在合理时间内完成对垃圾信息的检测和过滤，原因是只能在呼叫方与被呼叫方之间的通信会话建立起来之后，才有可能对内容进行分析。另一方面，在非实时IP多媒体应用中，如录制的语音消息，可能有充足的时间来对内容进行分析。尽管如此，由于声音和图像识别技术尚不成熟或内容数量不够充分，在获取充分信息以判定垃圾信息方面，内容分析仍可能存在种种困难。当对基于文本的IP多媒体应用内容进行分析时，如即时消息服务和文本消息服务，若内容做了加密或者直接在服务用户之间进行传输而不通过适当的网络设备进行传送以供内容分析时，对垃圾信息的判定也会变得很困难。

7 用于打击IP多媒体垃圾信息的框架

具有反垃圾信息功能的IP网络实体间需要相互交流，以便打击IP多媒体垃圾信息。实施反垃圾信息方法所需的反垃圾信息功能以及反垃圾信息实体间的交流在本节中予以描述。对打击IP多媒体垃圾信息而言，仅用一种反垃圾信息技术可能是不够的。因此，为了更加有效地过滤垃圾信息，可能需要同时在IP网络中实施多种反垃圾信息技术。

本节描述用于打击IP多媒体垃圾信息的框架。它应能方便地扩展至各种各样的技术方法，以便打击各种各样应用和网络中的垃圾信息。框架的设计目的旨在保护用户和网络免遭IP多媒体垃圾信息侵扰。垃圾信息可出现在任何地方，因此，针对各种各样垃圾信息的检测和过滤机制需要通过网络来提供。

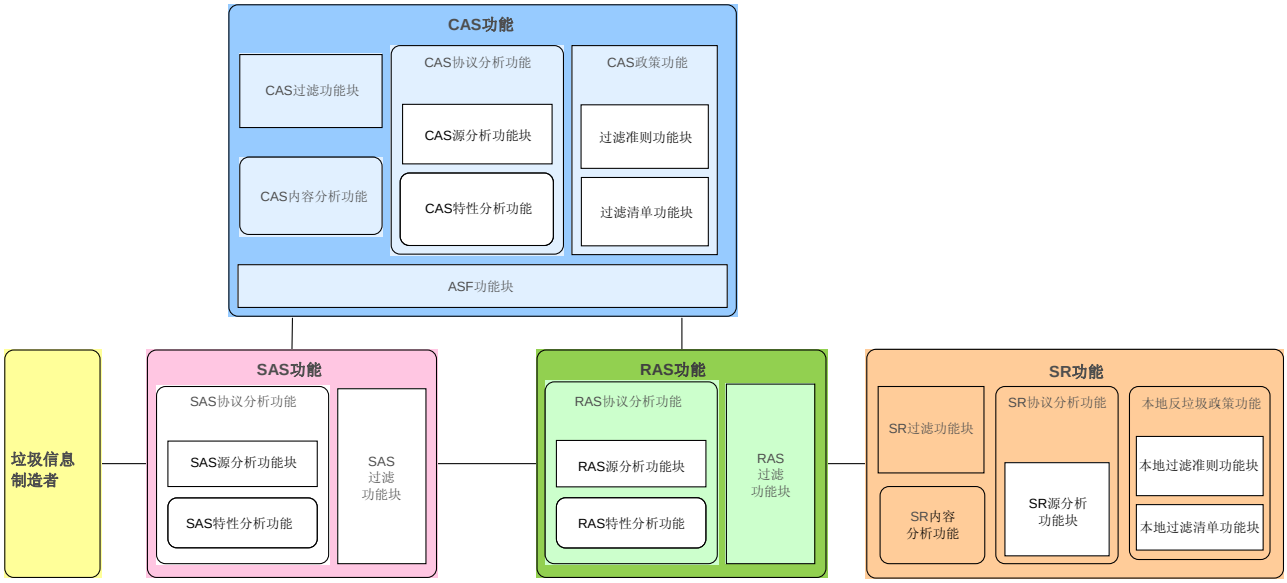

图 2 – 用于打击IP多媒体垃圾信息的框架

用于打击IP多媒体垃圾信息的框架由五个要素构成，如图2所示。以下各节分别描述了各要素的功能和接口。

7.1 垃圾信息制造者

垃圾信息制造者制造并通过网络到处发送垃圾信息。它是垃圾信息的始作俑者。垃圾信息制造者不执行反垃圾信息功能。

7.2 SAS功能

SASF（发送方反垃圾信息功能）是一组反垃圾信息功能，其作用是判定和阻断来自垃圾信息制造者的IP多媒体垃圾信息。SASF可在网络要素上实施，如代理服务器，当中来自垃圾信息制造者的对外通信请求作为最后一跳来发送。SASF与CASF（核心反垃圾信息功能）相互作用，以执行SASF中的反垃圾信息功能。尽管相比实时通信环境中的其他组成部件，SASF的作用可能会弱一些，但在通过网络传播之前，在源头一方阻断垃圾信息将会更有效。

SASF由SAS协议分析功能和用于控制垃圾信息过滤的SAS过滤功能块构成。以下各节描述了SASF可用于打击IP多媒体垃圾信息的各种技术。

7.2.1 SAS过滤功能块

SAS过滤功能块依据SAS协议分析功能的分析结果和反垃圾信息政策，来判定所分析的多媒体应用是垃圾信息还是不是垃圾信息。因此，它需要与CASF以及SASF中的其他反垃圾信息功能或功能块相互交流。

7.2.2 SAS协议分析功能

SAS协议分析功能对收到的IP多媒体应用的协议信息进行分析。它由SAS来源分析功能块以及分别用于分析来源信息和所收到IP多媒体应用特性的SAS特性分析功能构成。

i) SAS来源分析功能块

SASF可依据IP多媒体应用的来源信息来辨别IP多媒体垃圾信息和非垃圾信息的IP多媒体应用。SASF有两个方面的问题与IP多媒体应用的来源有关。一个问题是利用CASF提供的反垃圾信息政策对来源进行过滤，另一个问题是对发送方进行认证。

– 反垃圾信息政策

SASF可以利用IP多媒体数据分组的源地址对垃圾信息进行判定和过滤。不仅利用源地址，而且利用可供SASF使用的其他协议信息，来执行过滤任务。图3描述了SASF中利用来源分析技术打击IP多媒体垃圾信息的各种反垃圾信息功能以及各功能间的相互作用。

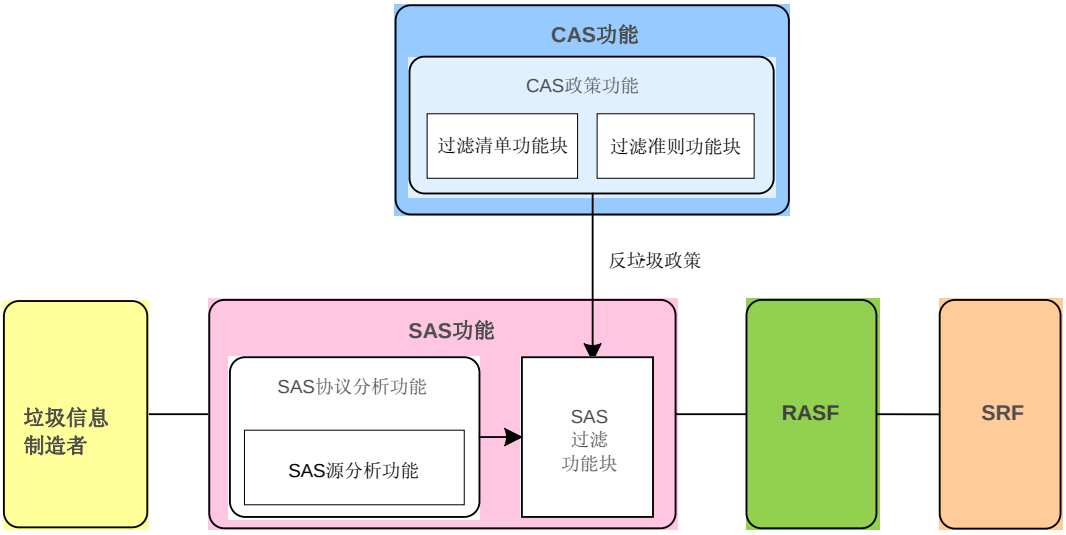

图 3 – 利用SASF中的来源分析功能来打击IP多媒体垃圾信息

SAS过滤功能块可从CAS政策功能处获得反垃圾信息政策。若依据分析结果IP分组被判定为垃圾信息，SAS过滤功能块将对垃圾信息制造者发送的IP分组进行过滤。

– 发送方认证

SASF拥有发送方的认证信息，SASF可以为源通信业务提供用户认证。若需要，SASF可以防止未经授权的实体使用IP多媒体应用。

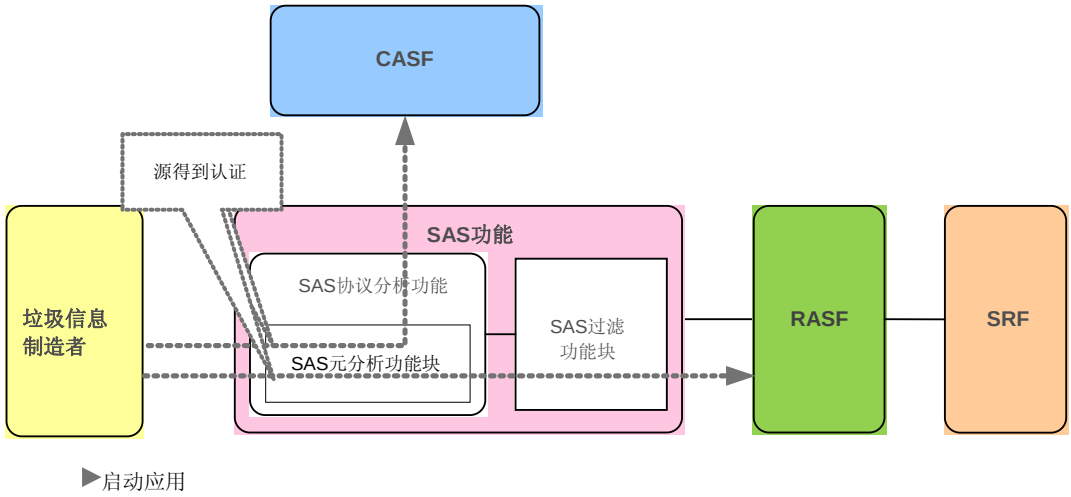

图 4 – SASF来源认证

图4是SASF进行来源认证的图示。SASF的来源分析功能具有认证功能，可在发送给CASF或RASF（接收方反垃圾信息功能）之前对垃圾信息制造者的通信业务进行认证。需要的话，SASF可以放弃无法通过认证的通信业务，只允许将通过认证的通信业务发送给其他ASF。放弃未经授权的通信业务有助于防止力图实施欺骗的垃圾信息制造者。

– 过滤程序

SASF利用来源分析功能对IP多媒体垃圾信息进行过滤的程序如下所述：

1） 传送反垃圾信息政策：SASF从CASF处接收反垃圾信息政策。反垃圾信息政策可以以一个通知或一个请求/答复的方式传送给SASF。

2） 接收IP多媒体应用：SASF接收IP多媒体应用开始信号。

3） 来源认证：SASF对应用来源进行认证。如果认证过程失败，那么SASF拒绝启动来自垃圾信息制造者的请求。

4） 垃圾信息判定和过滤：SASF依据从CASF收到的反垃圾信息政策和请求来源，对收到的IP多媒体应用做出决定。SASF可拒绝或忽略被判定为IP多媒体垃圾信息的通信业务。

ii) SAS特性分析功能

SASF可利用应用的各种特性来辨别垃圾信息，如批量服务。SASF可利用一个门限来对批量信息进行检测。SAS特性分析功能可以包括若干特定的特性分析功能块。各个功能块的功能和接口是一种特定的打击IP多媒体垃圾信息的技术手段，它们不在本建议书讨论范围之内。以下清单是特性的一些例子，SASF可判别之，以便运用反垃圾信息方法。

– 批量信息

SAS特性分析功能能够对来自单个源头的服务请求数量进行分析，并对服务请求的等级进行分析。SAS过滤功能块依据SAS特性分析功能的分析结果以及从CAS过滤准则功能块处接收的反垃圾信息政策，对IP多媒体垃圾信息进行判定。

– 有限的交互活动

尽管对IP多媒体应用来源的交流活动进行测试通常可由CASF来实施，但SASF能够对垃圾信息制造者的业务交流活动进行测试。垃圾信息制造者倾向于使用机器来启动IP多媒体应用，因为它比人工便宜。因此，测试交流活动是辨别IP多媒体垃圾信息的方法之一。

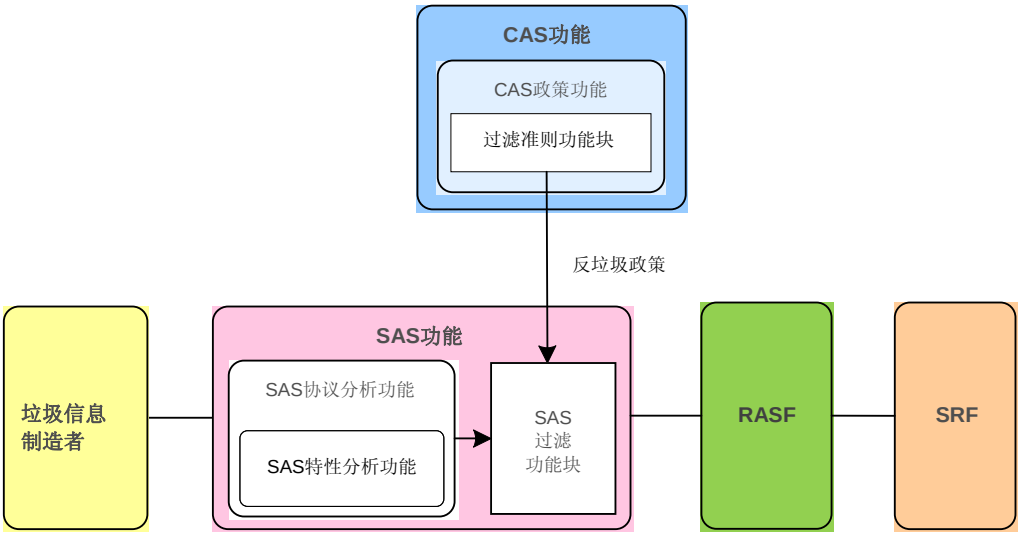

图 5 – 利用SASF中的特性分析功能来打击IP多媒体垃圾信息

SASF利用特性分析技术对IP多媒体垃圾信息进行过滤的程序如下所述：

1) 传送反垃圾信息政策：SAS过滤功能块从CASF处接收有关特性分析的反垃圾信息政策。反垃圾信息政策可以以一个通知或一个请求/答复的方式传送给SASF。

2) 接收IP多媒体应用：SASF接收IP多媒体应用开始信号。

3) 特性分析：SAS特性分析功能从收到的IP多媒体应用中提取与垃圾信息有关的特性。

4) 结果处理：特性分析结果从SAS特性分析功能处发送给SAS过滤功能块。

5) 垃圾信息过滤：SAS过滤功能块依据反垃圾信息政策对垃圾信息进行处理。如果分析结果判定是垃圾信息，那么SASF可拒绝或忽略被判定为IP多媒体垃圾信息的通信业务。

有关IP多媒体垃圾信息的垃圾信息管理政策取决于服务提供商、服务用户、IP多媒体应用、国家规则等。因此，在依据IP多媒体应用特性打击垃圾信息的行动中，SASF和RASF需要与CASF相互作用，以获得有关反垃圾信息政策的信息。

7.3 RAS功能

RASF是一组功能，其作用是判定和阻断传送给垃圾信息接收方的IP多媒体垃圾信息。RASF可在网络要素上实施，如代理服务器，当中发往垃圾信息接收方的对内通信请求作为最后一跳来发送。RASF与CASF相互作用，以执行RASF中的反垃圾信息功能。

CASF和RASF可以在同一时间涵盖垃圾信息制造者和垃圾信息接收方的同一网络设备上执行。不过，设备运行的反垃圾信息功能因通信业务流的不同而不同。也就是说，当通信业务来自设备涵盖的IP多媒体应用用户时，设备的反垃圾信息功能像SASF一样运行，当通信业务发往设备涵盖的IP多媒体应用用户时，设备的反垃圾信息功能像RASF一样运行。

RASF由RAS协议分析功能和用于控制垃圾信息过滤的RAS过滤功能块构成。

尽管出于打击垃圾信息目的，SASF或RASF在技术上可能可以对所传送的通信业务内容进行分析，但在本建议书中，它们不属于内容分析功能，因为内容分析功能还需要满足额外的处理限制条件。当IP多媒体应用不通过CASF进行传送时（这是一种缺省状态），RASF可以将IP多媒体应用传送给CASF，并出于判定垃圾信息目的，请求CASF对IP多媒体应用内容进行分析。

以下各节描述了RASF可用于打击IP多媒体垃圾信息的各种技术。

7.3.1 RAS过滤功能块

RAS过滤功能块依据分析结果和反垃圾信息政策，来判定所分析的IP多媒体应用是否是垃圾信息。因此，它需要与CASF以及RASF中的其他反垃圾信息功能或功能块进行交互。

7.3.2 RAS协议分析功能

RAS协议分析功能对所收到IP多媒体应用的协议信息进行分析。它由RAS来源分析功能块以及分别用于分析来源信息和所收到IP多媒体应用特性的RAS特性分析功能构成。

i) RAS来源分析功能块

RASF可依据IP多媒体应用的来源信息来辨别IP多媒体垃圾信息和非垃圾信息的IP多媒体应用。为了判定垃圾信息，RASF需要描述CASF提供的有关来源的反垃圾信息政策的特性，如黑名单、白名单、信誉记录等。图6描述了利用来源分析技术，打击IP多媒体垃圾信息的各种反垃圾信息功能以及各功能间的相互作用。

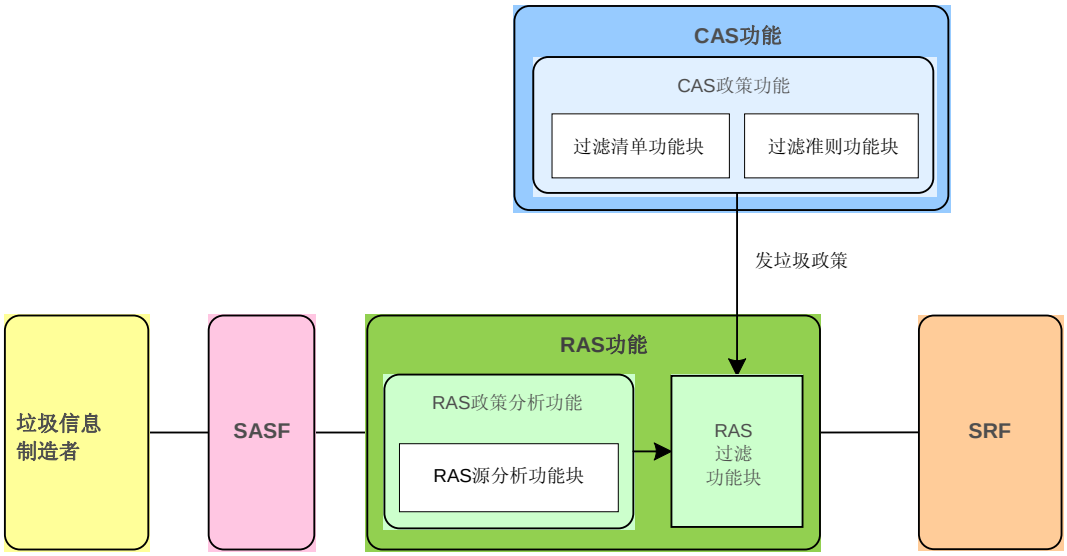

图 6 – 基于来源分析打击IP多媒体垃圾信息

RASF依据IP多媒体应用的来源信息，判定某个IP多媒体应用是垃圾信息还是不是垃圾信息，并依据结果做出相应处理。为了有效实施基于来源的反垃圾信息技术，需要高度可靠的来源信息，因此，假定RASF从SASF处接收的IP多媒体应用是值得信任的，也就是说，是经过认证的。RASF根据CASF提供的垃圾信息过滤准则或垃圾信息过滤清单来判定IP多媒体垃圾信息。CASF负责维护过滤清单和过滤准则，以支持RASF、SASF或CASF自身对垃圾信息做出判定。RASF利用来源分析方法对垃圾信息进行判定和过滤的程序如下所述：

1) 从CASF传送反垃圾信息政策：RASF从CASF处接收反垃圾信息政策。反垃圾信息政策可以以一个通知或一个请求/答复的方式传送给RASF。

2) 接收IP多媒体应用：RASF接收IP多媒体应用，并检查IP多媒体应用的来源。

3) 垃圾信息判定和过滤：RASF依据来源信息和在前一阶段中接收的反垃圾信息管理政策对收到的IP多媒体应用做出决定。依据服务提供商或服务用户的反垃圾信息政策，RASF可拒绝或忽略被判定为IP多媒体垃圾信息的通信业务。

当RASF依据黑名单或白名单对垃圾信息进行判定时，可使用来自CASF的过滤清单。当RASF依据信誉记录对垃圾信息进行判定时，可使用过滤准则，如门限信誉记录，以此来判定某个IP多媒体应用是否为垃圾信息。

ii) RAS特性分析功能

RASF可以通过使用IP多媒体应用检查垃圾信息是否具有IP多媒体垃圾信息的各种特性。RAS特性分析功能可包括若干特定的特性分析功能块。用于打击IP多媒体垃圾信息的技术手段不在本建议书讨论范围之内。

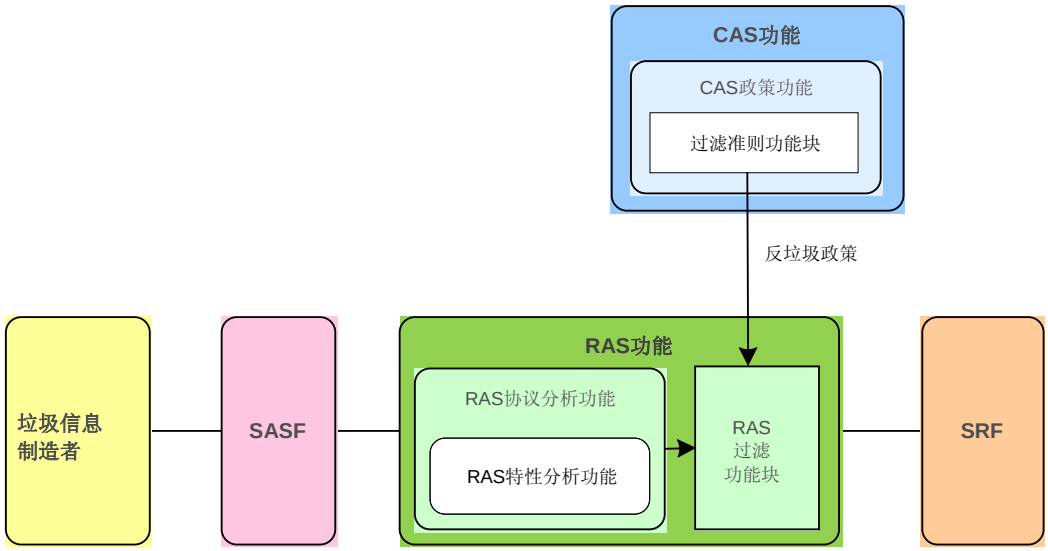

图 7 – 基于特性分析打击IP多媒体垃圾信息

图7描述了RASF中利用特性分析技术打击IP多媒体垃圾信息的各种反垃圾信息功能以及各功能间的相互作用。RASF利用特性分析技术对IP多媒体垃圾信息进行判定的程序如下所述：

1) 传送反垃圾信息政策：RAS从CASF处接收有关特性分析的反垃圾信息政策。反垃圾信息政策可以以一个通知或一个请求/答复的方式传送给RASF。

2) 接收IP多媒体应用：RASF接收IP多媒体应用开始信号。

3) 特性分析：RAS特性分析功能从收到的IP多媒体应用中提取与垃圾信息有关的特性。

4) 结果处理：RAS特性分析功能将分析结果提供给RAS过滤功能块。

5) 垃圾信息过滤：RAS过滤功能块依据反垃圾信息政策对垃圾信息进行处理。如果分析结果判定是垃圾信息，那么RASF可拒绝或忽略被判定为IP多媒体垃圾信息的通信业务。

7.4 CAS功能

CASF能够对反垃圾信息政策实施管理，并对RASF和SASF实施控制。当依照IP多媒体应用类型提供IP多媒体应用时，如果垃圾信息制造者与垃圾信息接收方之间存在一条IP分组路径，它还能够对IP多媒体应用的来源或特性进行分析，以判定和过滤垃圾信息。CASF具有CAS协议分析功能、CAS内容分析功能、CAS过滤功能块、CAS反垃圾信息政策功能以及ASF控制功能块。本节描述了CASF中用于打击IP多媒体垃圾信息的各个实体的功能性和相互作用。

7.4.1 CAS过滤功能块

CAS过滤功能块依据分析结果和反垃圾信息政策，来判定所分析的IP多媒体应用是垃圾信息还是不是垃圾信息。因此，它需要与CASF中的其他反垃圾信息功能或功能块进行相互交流。

7.4.2 CAS协议分析功能

CAS协议分析功能对收到的IP多媒体应用的协议信息进行分析。它由CAS来源分析功能块以及分别用于分析来源信息和所收到IP多媒体应用特性的CAS特性分析功能构成。

i) CAS来源分析功能块

当在CASF驻留其中的网络组成部件控制下提供IP多媒体应用时，例如，在应用服务器控制下，用户登录即时消息传送服务或登录VoIP服务，CASF可以作为一个可能的功能实体，通过来源分析来判定垃圾信息。图8描述了CASF中利用来源分析技术打击IP多媒体垃圾信息的各种反垃圾信息功能以及各功能间的相互作用。

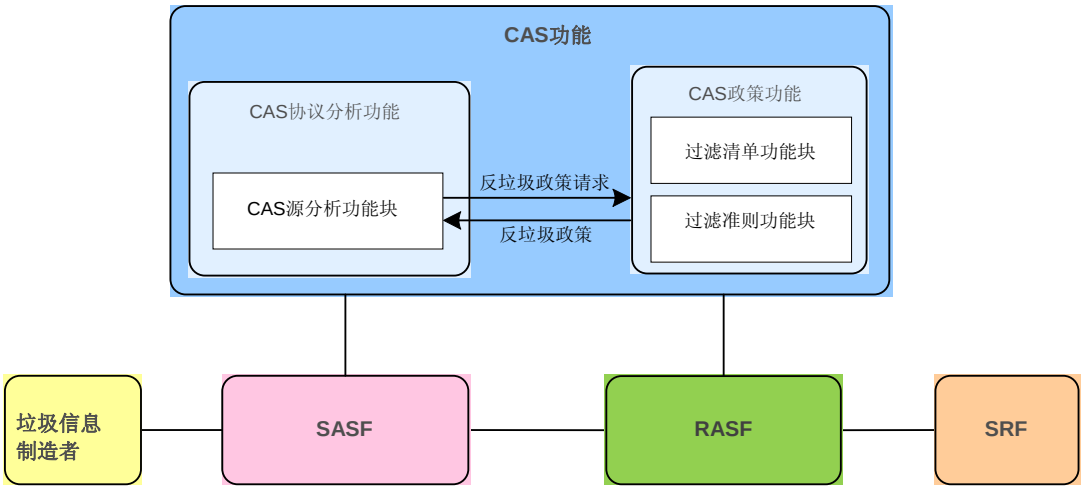

图 8 – 基于来源分析打击IP多媒体垃圾信息

下面描述了一个可能的打击IP多媒体垃圾信息的程序，它基于CASF中IP多媒体应用的来源信息：

1) 认证：用户若想使用某个IP多媒体应用（如即时消息传送服务），那么需要通过某个网络组成部件对用户进行认证，如具备CASF的某个应用服务器。

2) 接收IP多媒体应用：用户向CASF发送一个有关IP消息传送的请求，CAS来源分析功能块检查用户来源。

3) 获取反垃圾信息政策：CAS来源分析功能块从CAS政策功能处请求并接收反垃圾信息政策。

4) 垃圾信息判定和过滤：CASF依据来源信息和在之前阶段中接收的反垃圾信息政策，对收到的IP多媒体应用做出决定。CASF可拒绝或忽略被判定为IP多媒体垃圾信息的通信业务，当通信业务被确定为垃圾信息时，将依据服务提供商或服务用户的反垃圾信息政策做相应处理。

ii) CAS特性分析功能

当在CASF某个网络实体控制下来提供IP多媒体应用时，CASF可以作为一个特性分析点，用于打击垃圾信息。CASF分析IP多媒体应用是否具有垃圾信息的各种特性，并利用反垃圾信息政策中的过滤准则来判定它是垃圾信息还是不是垃圾信息。图9显示了CASF中用于打击IP多媒体垃圾信息的特性分析方法的总体结构和接口。

CASF政策功能拥有过滤准则功能块，它包含用于判定IP多媒体垃圾信息所需的垃圾信息过滤准则，并向SASF或RASF提供这种准则，以支持它们对垃圾信息做出判定。例如，当IP多媒体应用为批量信息形式时，当CAS特性分析功能试图判定垃圾信息时，CASF过滤准则功能块可以提供数量准则，用于判定IP多媒体应用的数量水平，以判定它是否为IP多媒体垃圾信息。

图9描述了CASF中利用特性分析技术打击IP多媒体垃圾信息的各种反垃圾信息功能以及各功能间的相互作用。

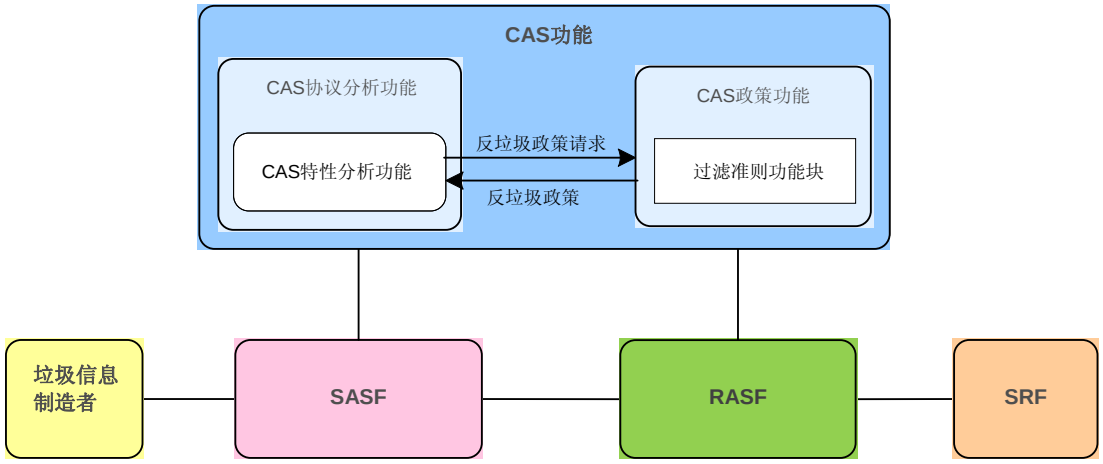

图 9 – 基于特性分析打击IP多媒体垃圾信息

下面描述了CASF中用于打击IP多媒体垃圾信息的特性分析程序：

1) 垃圾信息特性分析：当在CASF所属的网络实体控制下，一个IP多媒体应用试图进行连接时，CASF分析其是否具有垃圾信息特性，如是否是批量信息、交互活动是否有限等。

2) 获取反垃圾信息政策：特性分析功能请求有关反垃圾信息政策的CAS政策功能，政策与用于垃圾信息过滤的特性分析有关。反垃圾信息政策块向CAS特性分析功能发送所请求的信息。

3) 垃圾信息判定和过滤：CAS特性分析功能依据特性分析功能的分析结果和收到的反垃圾信息政策，对IP多媒体应用是垃圾信息还是不是垃圾信息做出决定。

7.4.3 CAS内容分析功能

CASF拥有CAS内容分析功能。当IP多媒体应用通过CASF驻留其中的网络设备（如应用服务器或媒体服务器）传送给接收方时，这些功能可对IP多媒体应用的内容进行分析，以判定它是否为垃圾信息。

在使用IP多媒体应用的协议信息（如垃圾信息的来源信息或特性）判定垃圾信息时，任何CASF、SASF或RASF都可作为分析者。而另一方面，如果利用内容分析判定垃圾信息，传输IP多媒体应用内容的CASF便是一个合理的内容分析功能实体点，可使用基于内容的反垃圾信息技术打击IP多媒体垃圾信息。

图10描述了CASF中利用内容分析技术打击IP多媒体垃圾信息的各种反垃圾信息功能以及各功能间的相互作用。

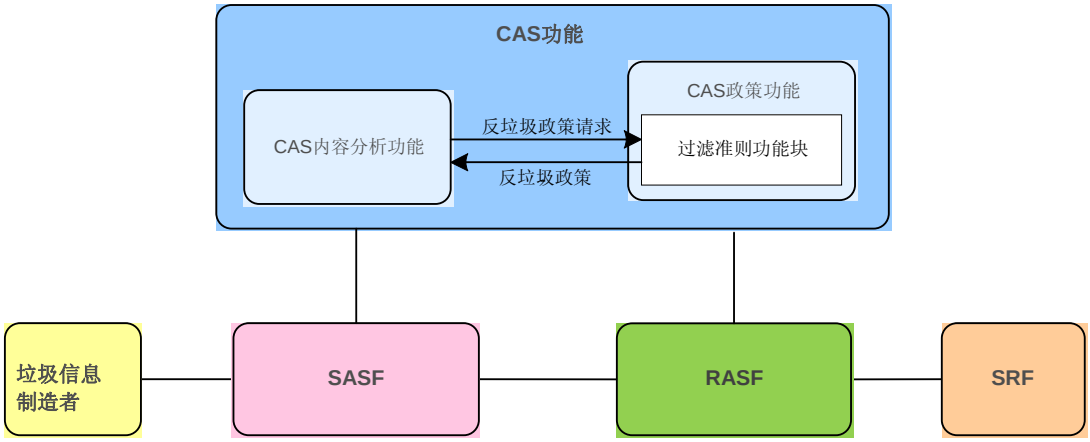

图 10 – 基于内容分析打击IP多媒体垃圾信息

下面描述了CASF中用于打击IP多媒体垃圾信息的内容分析程序：

1) 接收IP多媒体应用：IP多媒体应用内容达到CASF。

2) 内容分析：CAS分析功能对IP应用内容进行分析。

3) 获取反垃圾信息政策：CASF请求有关反垃圾信息政策的CAS政策功能，并从过滤准则功能块处接收政策。

4) 垃圾信息判定和过滤：CASF依据分析结果和反垃圾信息政策，对IP多媒体应用是垃圾信息还是不是垃圾信息做出决定。

如第6节所述，内容分析方法的适用性可能受限于IP多媒体应用的特性，如IP多媒体应用是实时的或不是实时的、是多媒体的或不是多媒体的、IP多媒体应用的内容是经过加密的或未经加密的。

7.4.4 CAS政策功能

CAS政策功能负责维护用于打击IP多媒体垃圾信息的反垃圾信息政策，由过滤准则功能块和过滤清单功能块构成。

i) 过滤准则功能块

过滤准则功能块负责维护用于判定IP多媒体垃圾信息的反垃圾信息过滤准则。根据部署的反垃圾信息技术，可以使用各种各样类型的过滤准则。例如，在对批量信息进行分析过程中，从一个源头一次可发送的IP多媒体应用门限数量就可以作为一条过滤准则。过滤准则的创建和管理机制不在本建议书讨论范围之内。

ii) 过滤清单功能块

过滤清单功能块负责管理利用来源分析技术来判定IP多媒体垃圾信息的过滤清单。根据部署的反垃圾信息技术，可以使用各种各样类型的垃圾信息过滤清单。例如，黑名单、白名单和信誉记录都可用作过滤清单。过滤清单或可以是许多服务用户同享的公共清单，或可以是亲自管理的个人清单，抑或是两者兼有。过滤清单的创建和管理机制不在本建议书讨论范围之内。

7.4.5 ASF控制功能块

ASF控制功能块与SASF和RASF相互作用，以支持它们判定和过滤垃圾信息。它从CAS政策功能处向RASF和SASF传送反垃圾信息政策。

7.5 SR功能

垃圾信息接收方是IP多媒体垃圾信息的终点。如果没有垃圾信息打击机制，那么用户将受到IP多媒体信息的侵袭和破坏。

垃圾信息接收方拥有SR（垃圾信息接收）功能，以保护其自身免受IP多媒体垃圾信息侵扰。用户可设定反垃圾信息政策或者从服务提供商处接收这种政策，以过滤IP多媒体垃圾信息。SR功能由SR协议分析功能、SR内容分析功能、SR过滤功能块和本地反垃圾信息政策功能构成。本节描述垃圾信息接收方用于打击垃圾信息的各种功能以及各反垃圾信息功能间的相互作用。

7.5.1 SR协议分析功能

SR协议分析功能拥有SR来源分析功能块，它依据发送方信息对垃圾信息做出判定。尽管可能对CASF、SASF和RASF上的垃圾信息进行过滤，但在直接连接的IP多媒体应用情况中，可以用SRF的反垃圾信息功能和反垃圾信息政策来打击IP多媒体垃圾信息。

垃圾信息接收方可以定义一个本地过滤清单和本地过滤准则，或者可以从其他反垃圾信息功能处接收这种清单，如CASF。用于定义反垃圾信息政策的特定机制不在本建议书讨论范围之内。图11描述了SRF中利用来源分析技术打击IP多媒体垃圾信息的各种反垃圾信息功能以及各功能间的相互作用。

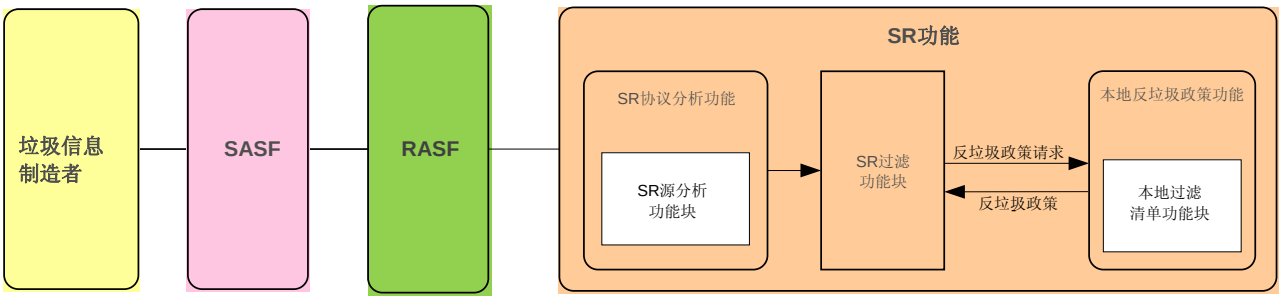

图 11 – 利用垃圾信息接收方中的来源分析功能来打击IP多媒体信息

下面描述了一个可能的打击IP多媒体垃圾信息的程序，它基于垃圾信息接收方中IP多媒体应用的来源信息：

1) 接收IP多媒体应用：SRF接收IP多媒体应用开始信号，并检查IP应用的来源。

2) 获取反垃圾信息政策：SR协议分析功能从本地反垃圾信息政策功能处请求并接收反垃圾信息政策。

3) 垃圾信息判定和过滤：SR过滤功能块依据反垃圾信息政策和来源分析结果，对收到的IP多媒体应用做出决定。垃圾信息接收方可拒绝或忽略被判定为IP多媒体垃圾信息的通信业务。

垃圾信息接收功能可利用特性分析从技术角度辨别垃圾信息。然而，由于SR协议分析功能在具有高度可变性的用户组控制之下，依赖垃圾信息接收方来执行高级的垃圾信息打击功能（如特性分析方法）存在风险，因此，SR协议分析功能没有特性分析功能块。

7.5.2 SR内容分析功能

垃圾信息接收方有可能依据内容分析结果来打击垃圾信息。垃圾信息接收方可以维护其自身的、用户特定的内容分析机制，或者从服务提供商处接收机制。内容分析的反垃圾信息政策置于本地反垃圾信息政策功能中，作为本地过滤准则功能块的一部分。图12描述了SRF中利用内容分析技术打击IP多媒体垃圾信息的各种反垃圾信息功能以及各功能间的相互作用。

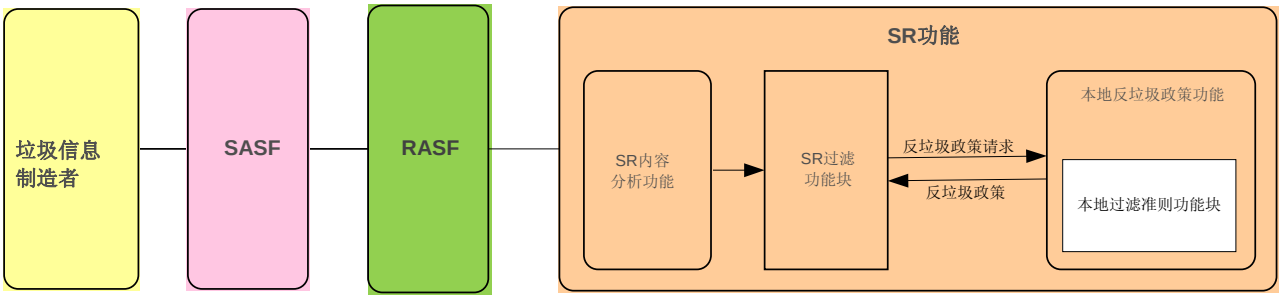

图 12 – 利用垃圾信息接收方中的内容分析功能来打击IP多媒体信息

垃圾信息接收方利用内容分析技术对IP多媒体垃圾信息进行过滤的程序如下所述：

1) 接收IP多媒体应用：SRF接收IP多媒体应用开始信号。SR内容分析功能为判定垃圾信息而执行内容分析。

2) 获取反垃圾信息政策：内容分析结果传送给SR过滤功能块。SR过滤功能块从本地反垃圾信息政策功能处请求并接收反垃圾信息政策。

3) 垃圾信息判定和过滤：SR过滤功能块依据反垃圾信息政策和内容分析结果，对收到的IP多媒体应用做出决定。垃圾信息接收方可拒绝或忽略被判定为IP多媒体垃圾信息的通信业务。

7.5.3 SR过滤功能块

SR过滤功能块依据分析结果和反垃圾信息政策，来判定所分析的IP多媒体应用是还是不是垃圾信息。因此，它需要与SRF中的其他反垃圾信息功能或功能块进行相互交流。

7.5.4 本地反垃圾信息政策功能

本地反垃圾信息政策功能用于维护用户特定的反垃圾信息政策，以打击IP多媒体垃圾信息。这些功能由本地过滤准则功能块和本地过滤清单功能块构成。

i) 本地过滤准则功能块

本地过滤准则功能块用于维护用户特定的反垃圾信息过滤准则，以判定IP多媒体垃圾信息。过滤准则类型取决于SRF支持的反垃圾信息功能。

ii) 本地过滤清单功能块

本地过滤清单功能块用于管理用户特定的过滤清单，以便依据来源分析来判定IP多媒体垃圾信息。清单类型取决于SRF支持的来源分析功能性。

7.6 框架中的各参考点

本节定义框架中各要素之间的参考点。图13显示了框架中的各参考点。

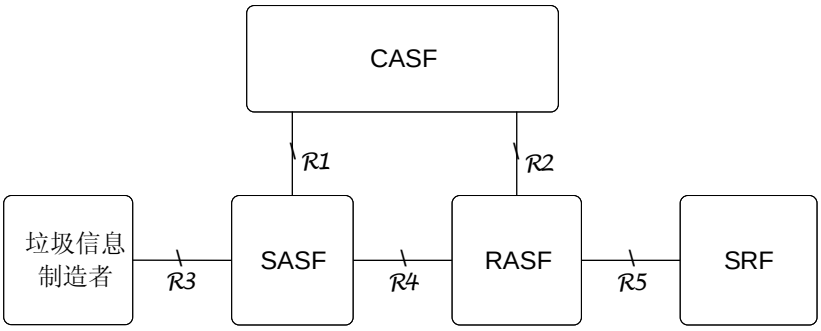

图 13 – 反垃圾信息框架中的各参考点

7.6.1 参考点R1

R1位于CASF与SASF之间，用于获得从CASF到SASF的过滤政策。CASF通过R1来控制SASF。

7.6.2 参考点R2

R2位于CASF与RASF之间，用于获得从CASF到RASF的过滤政策。CASF通过R2来控制RASF。

7.6.3 参考点R3

R3位于垃圾信息制造者与SASF之间，用在IP多媒体应用协议和/或数据传输业务中。

7.6.4 参考点R4

R4位于SASF与RASF之间，用在IP多媒体应用协议和/或数据传输业务中。

7.6.5 参考点R5

R5位于RASF与垃圾信息接收方之间，用在IP多媒体应用协议和/或数据传输业务中。

附录一

通过增加垃圾信息散播难度反击垃圾信息

（本附录不是本建议书的组成部分）

增加垃圾信息散播难度可以作为打击IP多媒体垃圾信息的技术方法之一。不过，该方法与其他直接确定和过滤垃圾信息的方法略有不同。增加垃圾信息散播难度有助于间接减少垃圾信息的数量，但这一方法需要付出工作和时间，成本较高。减少垃圾信息数量的一种途径是提高垃圾信息制造者制造和发送垃圾信息的成本和工作量，从而增加垃圾信息的散播难度。垃圾信息制造者散播垃圾信息的成本由以下几部分构成：监管费用（包括非法垃圾信息预期罚款）、支付给服务提供商或网络提供商的IP多媒体应用使用费和垃圾信息传送费（即交互活动测试费）等。可用以下方法来增大垃圾信息的散播难度：

– 使IP地址获取具有难度：增大收集有关垃圾信息散播目标信息（如IP地址和IP多媒体应用服务账号）的工作量，加大垃圾信息制造者发送IP垃圾信息的难度。

– 支付系统：对IP多媒体垃圾信息收费将有助于减少垃圾信息的数量。不过，对可能的垃圾信息（如批量的IP消息）采用支付系统不是一个技术问题。

– 防止批量信息传送：考虑到许多时候垃圾信息是以批量信息形式传送的，因此，防止批量信息传送将有助于减少垃圾信息的数量。

– 交互活动测试：对垃圾信息制造者的交互活动进行测试可提高垃圾信息散播费用。不过，这一做法可能产生副作用，因为它也可能对正常的IP多媒体应用用户造成干扰。

通过增大垃圾信息散播难度打击垃圾信息的方法不限于以上各例子所述。

在交互活动测试中，CASF可充当测试者的角色。在防止批量信息传送方法中，CASF、SASF或RASF可确定批量性，即特定数量水平，以及具有批量性的IP多媒体应用块。在CASF控制下，收取批量信息通信或消息费也是一种可能的增大垃圾信息散播难度的方法。

SASF或RASF有时会对协议信息进行分析，但它通常不会采取额外的措施来增大垃圾信息的散播难度，如防止批量信息传送的控制措施、支付管理或交互活动测试。简而言之，SASF或RASF将采取某些措施来支持CASF处理垃圾信息，CASF将在增大垃圾信息散播难度中发挥主要作用。

附录二

在框架使用过程中有关安全性与实用性方面的考虑

（本附录不是本建议书的组成部分）

II.1 安全性方面考虑

以下所述是用于打击IP多媒体垃圾信息的安全性方面的考虑：

– 认证

认证是一个过程，在此过程中，一个实体，不论是垃圾信息接收方还是CASF，通过出示除真正用户外他人难以伪造的证书以确认其身份。

为了确定IP多媒体应用消息的发送方，有必要对用户进行认证，它将有助于阻断众多欺骗性攻击类型的垃圾信息。无法实施适当的用户认证将便不能追踪垃圾信息制造者，原因是垃圾信息制造者可以通过欺骗性攻击来伪造其IP地址。

可以通过许多方法来实现认证。一些认证方法，如简单的口令认证，可以很方便地进行实现，但它们一般都比较脆弱和原始。其他的认证方法，如安全套接字层（SSL）、IPSec、安全外壳、Kerberos，将更复杂并需要更多的时间来实现和维护，但它们可提供强劲的和可靠的认证。

其他的新兴技术，如密码签名方法，将证明是一种更好的解决方案。不过，有关发送者认证的、最常用的和目前可用的方法依然是经典的发送者政策框架（SPF）、域密钥。

– 访问控制

访问控制是一种实现并实施授权政策的方法。访问控制可授予一项用户许可，允许某个用户执行或禁止某个用户执行有关垃圾信息接收的行为和ASF，如某项安全政策所规定的那样。

通常在认证建立后应用访问控制。访问控制一般分为任意的访问控制（DAC）和非任意的访问控制（NDAC）。在DAC中，对象所有者规定谁可访问对象或规定各项政策。除了DAC，所有的访问控制政策都归类为NDAC。在NDAC中，政策是不由用户规定的各规则。强制的访问控制（MAC）、基于角色的访问控制（RBAC）、基于目的的访问控制（PBAC）、基于历史的访问控制（HBAC）、暂时约束的访问控制（TCAC）和基于规则的访问控制（RuBAC）是有关NDAC的一些例子。

– 机密性

机密性指的是用于确保只有经过授权的用户才可进行安全通信的各种机制。有两种主要的机制来为以电子形式传送的信息提供机密性：加密或者通过安全的基础设施进行传输 — 例如，通过虚拟专用网络（VPN）或其他的加密链路。

IPSec是用在大多数VPN中以便通过互联网建立安全连接的协议。IPSec是一种得到广泛认可的、有关安全传输的标准，它很灵活，并比其他一些加密方法便宜。IPSec提供了强劲的加密、完整性和认证功能，它对需要通过互联网安全地进行数据传输的组织机构而言尤为有用。

第二层隧穿协议（L2TP）是一种用于支持VPN的隧穿协议。它对点对点协议（PPP）内的某个特定网络层协议进行封装以实现对PPP帧的密码保护以及对隧穿协议内的数据进行封装。

– 数据完整性

完整性指的是当信息在垃圾信息接收方与垃圾信息制造者之间传送时无法对之进行修改。没有适当的保护，垃圾信息制造者能够对IP多媒体消息的内容进行修改或扰乱。

通过使用由密码散列函数生成的消息摘要，系统管理员可以检测到对消息所做的非授权修改。散列函数也可与其他标准的密码方法相结合来对数据源进行验证。当散列算法与密码相结合时，它们产生特殊的消息摘要，用于确认数据源。

当使用数字签名来支持数据完整性时，可要求公开密钥基础设施（PKI）对加密密钥实施管理。PKI密切跟踪公开加密密钥对用户和组织机构的分配和回收情况。

作为数字签名和PKI的一种可选方案，可用秘密密码来提供数据完整性。秘密密钥应用比较简单，在该应用中，只使用一个密钥，为了实现加密和解密功能，发送方和接收方都必须持有密钥。秘密密钥系统得到广泛应用，但其遇到的困难是如何安全地实现对秘密密钥的分发。

– 不可否认性

不可否认性指的是一种方法，利用它，消息的发送方或通信业务的发起方之后无法否认曾经进行过通信业务。

通过捆绑法律文件以及捆绑以下有关服务器管理的安全机制和可信过程来实现不可否认性：SSL、质疑响应OTP令牌、安全散列和审计日志。

用于实现不可否认性的一种常用方法是利用数字签名，它可认为是在电子数据处理中替代传统签名的最佳可选方案之一。为了实现数字签名，需要一个可信的第三方（TTP）或PKI。TTP或PKI至少可以支持一个负责发放数字证书和证书回收清单（CRL）的认证机构（CA），以检查已撤销证书的情况。

II.2 实用性方面考虑

框架的主要目标之一是确保尽可能减少对业务的负面影响。显然，采取反垃圾信息措施对个人和业务产生积极的效果，并达成公司的需求。

以下实用性方面的考虑基于处理操作。它们是实施反垃圾信息系统的指导原则，并为潜在的供应商提供高层信息。

– 提供高精度和高性能；
– 可部署于互联网周边；
– 与流行的IP多媒体应用系统进行集成；
– 运行于可选的客户服务器平台：UNIX、Windows等；
– 对输入和输出的IP多媒体垃圾信息进行过滤；
– 灵活匹配组织机构的政策与优先级；
– 用户能够建立单独的或特定的过滤器；
– 允许最终用户管理其自身的IP多媒体应用垃圾信息文件夹，并设定简单的优先级；

– 白名单和黑名单管理功能；
– 通过低至用户层的业务费用分层管理，实现对内容的过滤，包括增加服务器方的内容过滤功能。

参考资料

[b-ITU-T X.1240] ITU-T X.1240建议书（2008），《用于打击垃圾电子邮件的技术》。

[b-ITU-T X.1244] ITU-T X.1244建议书（2008），《打击IP多媒体应用中垃圾信息的概述》。

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2011年，日内瓦