国　际　电　信　联　盟

ITU-T X.1243

(12/2010)

国际电信联盟
电信标准化部门

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

用于打击垃圾信息的互动网关系统

ITU-T X.1243建议书

国际电信联盟

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.1243建议书

用于打击垃圾信息的互动网关系统

摘要

ITU-T X.1243建议书规定了作为一种打击域间垃圾信息的技术方法、用于打击垃圾信息的互动网关系统。网关系统使得不同域之间可以相互通知，并防止垃圾业务量从一个域传送到另一个域。

此外，本建议书规定了网关系统的架构，描述了网关系统基本实体、协议和功能，并提供了发现垃圾信息、信息共享和在网关中打击垃圾信息的具体行动的机制。

沿革

版本	建议书	批准日期	研究组
1.0	ITU-T X.1243	2010-12-17	17

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.1243建议书

用于打击垃圾信息的互动网关系统

1 范围

用于打击垃圾信息的互动网关系统是一种打击各种域间垃圾邮件、垃圾短信等垃圾消息的通用互动机制，可实现不同域之间打击垃圾信息的信息共享并防止发送和接收垃圾信息。本建议书支持打击垃圾信息过滤机制的分集并提供了适应未来技术的灵活性。

在通过本建议书前应考虑是否遵循所有相关国家法律和法规。

2 参考文献

下列ITU-T 建议书和其它参考文献的条款，在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其它参考文献均会得到修订，因此本建议书的使用者应查证是否有可能使用下列建议书或其它参考文献的最新版本。当前有效的ITU-T 建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T X.509] ITU-T X.509 (2000) 建议书| ISO/IEC 9594-8:2001，信息技术 – 开放系统互连 – 号码簿：公共密钥和属性证书框架 。

3 定义

3.1 其它资料规定的术语

本建议书采用了下列其它资料规定的术语：

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

3.2 本建议书确定的术语

本建议书定义了以下术语：

3.2.1 用于打击垃圾信息的互动网关（IGCS）： 用于打击垃圾信息的互动网关是负责发现和阻止垃圾信息的实体。它有一对功能：发送者网关功能（SGF）和接收者网关功能（RGF）。IGCS应与其他端配合，以实现打击垃圾信息的全部功能。

3.2.2 本地打击垃圾信息数据库（local countering spam database）：该术语规定了用于为本地接收者网关功能和发送者网关功能存储垃圾信息、黑名单、打击垃圾信息规则的数据库。

3.2.3 模态（modality）：模态指包含可为人知信息的信息编码。

3.2.4 多模消息（multimodal message）：多模消息指包含不同编码信息的多媒体消息，用于经多种模态进行互动。

3.2.5 接收代理（receiver agent）：接收代理是为消息接收人接收消息的服务器。在电子邮件应用中，POP服务器担当接收代理。

3.2.6 接收者网关功能（receiver gateway function）：接收者网关功能指接收方用于打击垃圾信息，在接收过程中发现和阻止垃圾信息的一种功能。

3.2.7 发送代理（sender agent）：发送代理是为消息发送人发送消息的服务器。在电子邮件应用中，SMTP服务器担当发送代理。

3.2.8 发送者网关功能（sender gateway function）：发送者网关功能指发送方用于打击垃圾信息，在消息发送过程中发现和阻止垃圾信息的一种功能。

3.2.9 打击垃圾信息对等体（spam-countering peer）：在打击垃圾信息过程中，两个IGCS合作确定并阻止垃圾信息，由此一个IGCS是另一个IGCS的打击垃圾信息对等体。

3.2.10 打击垃圾信息对等协议（spam-countering peering protocol）：定义协议，以在打击垃圾信息网关之间交换垃圾信息告警消息和黑名单。

3.2.11 用户垃圾信息报告协议（user spam report protocol）：定义协议，用于消息接收者向网关报告垃圾信息。

4 缩写词和首字母缩略语

本建议书采用了下列缩写词和首字母缩略语：

E-mail 电子邮件

FE 功能实体

IGCS 用于打击垃圾信息的互动网关

IM 即时消息

IRC 互联网中继聊天

LscDB 本地打击垃圾信息数据库

POP 邮局协议

RA 接收代理

RBL 实时黑名单

RGF 接收者网关功能

SA 发送代理

SCPP 打击垃圾信息对等协议

SGF 发送者网关功能

SMTP 简单邮件传输协议

WPF 加权参数过滤法则

5 惯例

功能框（Functional block）：在用于打击垃圾信息的互动网关系统中，“功能框”定义为功能集，由下列符号表示：

6 架构

6.1 打击垃圾信息的实体和功能

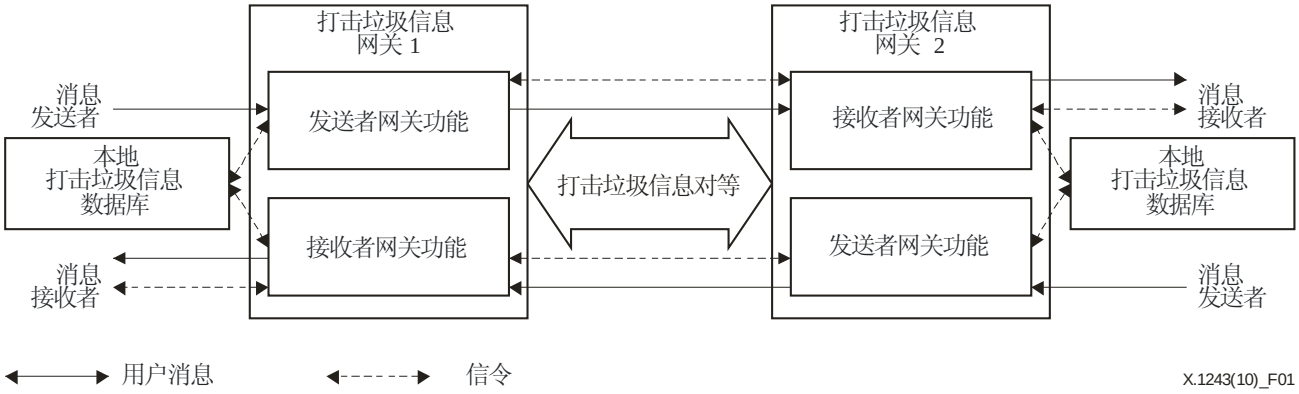

图 1 – 打击垃圾信息互动网关系统的架构

用于打击垃圾信息的互动网关系统（IGCS）

IGCS系统包括打击垃圾信息网关和本地打击垃圾信息数据库。打击垃圾信息网关有两种功能实体：SGF和RGF。这两种功能实体既是决策点，也是规则执行点。SGF用于处理发出的垃圾信息，而RGF用于处理接收的垃圾信息。本地打击垃圾信息数据库（lcsDB）提供了用于垃圾信息识别和打击垃圾信息行动的打击垃圾信息规则。本地打击垃圾信息网关也负责更新lcsDB的打击垃圾信息规则。

RGF和SGF的职责规定如下：

RGF基本上有三种职责：

- 对已知的收到垃圾信息采取打击垃圾信息的行动（阻止、隔离或警告等）；
- 通过接收者垃圾信息报告发现新垃圾信息并更新lcsDB的本地打击垃圾信息规则；
- 发现垃圾信息时，通过发送通知向垃圾信息发送者的SGF通报。

SGF具有两种职责：

- 对已知的发出垃圾信息采取打击垃圾信息的行动（阻止、隔离或警告等）；
- 处理接收者RGF发布的垃圾信息通知并更新lcsDB的本地打击垃圾信息规则。

本地打击垃圾信息数据库（lcsDB）

lcsDB用于存储打击垃圾信息的信息。该信息可进一步分为以下三种类型。

- 垃圾信息识别信息：如垃圾信息的源地址和垃圾信息主题字段（subject field）中的关键字。
- 打击垃圾信息规则：如黑名单和白名单。
- 可疑垃圾信息记录：RGF和SGF报告的可疑垃圾信息样本。

6.2 确定垃圾信息

RGF或SGF根据存储在lcsDB中的垃圾信息识别信息确定已知的垃圾信息。垃圾信息将分为几个等级并作为对应行动进行处理。

6.3 打击垃圾信息行动

一旦确定了垃圾信息，对应的RGF或SGF将根据所确定的垃圾信息等级采取行动。打击垃圾信息行动可包括但又不限于以下内容：

- 垃圾信息告警：RGF/SGF向消息接收者/发送者发送警告；
- 垃圾信息隔离：RGF/SGF将垃圾信息消息隔离并定期向消息接收者/发送者发送隔离摘要；
- 垃圾信息阻止：RGF/SGF阻止垃圾信息消息。

6.4 垃圾信息发现

6.4.1 RGF垃圾信息发现

接收者可向其值守RGF报告反垃圾信息规则。反垃圾信息规则包括但不限于来源/目的地址黑名单、电子邮件主题字段中的关键字等。RGF在lcsDB中更新垃圾信息识别和规则。当一个可疑消息到达时，RGF启动一项评估程序，根据存储在lcsDB中的打击垃圾信息规则判断消息是否为垃圾信息。如果消息判断为垃圾信息，RGF将采取对应的行动。

6.4.2 SGF垃圾信息发现

SGF垃圾信息发现过程与RGF的发现过程类似。SGF也从接收者的RGF接收垃圾信息通知。SGF评估RGF通知并更新lcsDB中的已验证垃圾信息规则。

6.5 经由打击垃圾信息对等协议的垃圾信息通知

6.5.1 对等发现

当SA试图向RA发送消息时，启动对等发现程序，以在消息传送路径上发现活动的对等IGCS。发现程序可由IGCS中的一个启动。在对等验证的握手程序之后，将建立对等关系。

6.5.2 对等之间的垃圾信息通知

在建立对等关系后，IGCS可通过打击垃圾信息对等协议与其对等体交换垃圾信息通知。因为垃圾信息基本由接收者确定，接收者的RGF负责确定垃圾信息并向发送者的SGF提供垃圾信息的信息。一旦RGF发现了垃圾信息的消息，它将通过垃圾信息通知程序通知发送者的SGF。在收到垃圾信息通知后，SGF应根据本地打击垃圾信息政策决定是否接受。

6.5.3 安全问题

建议将[ITU-T X.509]建议书中的认证机制包括在对等验证的垃圾信息通知程序中。建议通知消息由RGF数字签名。建议只接收来自于可信来源RGF的通知消息。

7 打击垃圾信息过滤技术

7.1 与技术无关的考虑

IGCS应支持打击垃圾信息的技术多样化并提供将现有和未来打击垃圾信息过滤技术进行综合的灵活性。每种过滤技术可根据选择进行实施。为有效地发现垃圾信息消息，IGCS可支持几种过滤技术并将其综合到一个物理网络设备中。过滤技术的具体实施不属于本建议书的范围。本建议书只定义每种过滤技术的接口、数据格式，以确保IGCS对等之间交换打击垃圾信息的信息的互操作性。

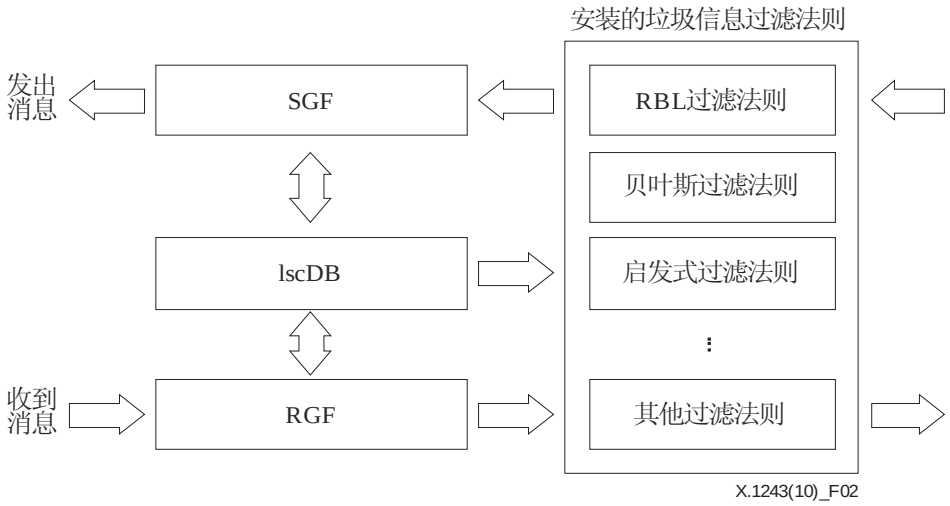

图 2 – 带有多个垃圾信息过滤法则的IGCS

7.2 支持的打击垃圾信息技术

7.2.1 地址清单

实时黑名单（RBL）：RBL由研究垃圾信息并制定其源地址清单的各组织提供。一个打击垃圾信息的系统可订购清单，并通过核查清单判定是否是垃圾信息。

黑名单：黑名单是允许除黑名单以外的所有人进行访问的基本访问控制机制。此外，与RBL一样，名单可不断更新且该方法也受到许多垃圾信息消息并不包含源地址这一事实的影响。一些系统允许用户保留经许可发送者的白名单，但也可能会限制用户从先前未知的来源获得需要的消息。

7.2.2 启发式过滤法则

这些过滤法则基于测试消息中是否存在特定类型的垃圾信息特征的原理，如HTML的排他使用或消息发送对象的类型等。测试通过基于一套已知消息和一套已知为合法的电子邮件的学习过程进行加权。

这些过滤法则存在着以下风险：采用兜售信息技术的消息 – 如HTML中的广告信息将被当作垃圾信息。

该过滤法则可发现一大部分消息且不需要教授或配置。但是，由于它采用了大量的测试，最好更改正在进行的测试的配置以及用来将消息归为垃圾信息的分数。

7.2.3 贝叶斯过滤法则

贝叶斯过滤法则的原理是其打击垃圾信息引擎受训于一套已知的垃圾信息和一套已知合法的消息。在培训过程后，收集垃圾信息消息所用的词汇特征。贝叶斯过滤法则将采用贝叶斯概率计算一条新消息是否是垃圾信息。对于一组过滤法则的情况，学习通常由系统管理员负责。

基于贝叶斯概率算法，贝叶斯过滤法则有繁重的系统开销计算且可能在大型打击垃圾信息系统中引入扩展性问题。在小型和高度单一的环境中（如企业或大学网络），这也许是可以接受的。但是，对于主要服务提供商，特别是公共服务提供商，就完全不是这么回事了。

尽管贝叶斯过滤法则用于打击垃圾信息，但当垃圾信息制造者编写其信息时，它有一定的局限性。

7.2.4 多模式过滤

如果IGCS系统要处理多模式过滤，SGF和RGF通过几个功能实体：模态发现功能实体、过滤功能实体和多模消息处理功能实体等其他必要的功能实体分别实施多模式过滤。为支持信息存储和交换，需要定义打击多模垃圾信息的信息数据集。lcsDB将存储包含适当多模消息类型（及主题）以及过滤标准（由用户或运营商输入，或从IGCS对等学习）的打击多模垃圾信息的信息。

如果存在多模元数据的描述且元数据的描述视为值得信赖，多模应用可根据多模内容的元数据描述过滤多模信息。否则，过滤应最好考虑一下功能实体须完成任务的整个多模信息：

- 包含适当多模消息类别和过滤标准的数据库或档案库。数据库或档案库可位于DB接口代理功能实体、多模处理功能实体和多模用户代理相同的场所/范围。在另一种情况下，数据库或档案库可位于与过滤功能实体不同的场所或范围；
- 模态发现功能要素检查发送或接收的多模消息，以确定所包含的模态；
- DB接口代理功能实体在给定的模态和消息类型中从数据库获取过滤标准；
- 过滤功能实体根据过滤标准过滤多模消息。过滤功能实体可完全阻止或部分阻止一个被处理的多模消息的选定多模部分。

图3描述了过滤多模消息的一般架构及必要的功能实体。过滤架构包含模态发现功能实体、过滤功能实体、数据库接口代理功能实体和多模数据库。但是图3显示了通常不执行任何多模过滤任务的多模消息处理功能实体和多模用户代理等其他功能实体。

多模消息处理功能实体处理多模（经过滤的）消息；同步从多模用户代理接收到的多模消息；将多模消息多路复用并向多模用户代理发送。每一种多模用户代理处理模态（因设备而异）输入和/或输出等特定模态。

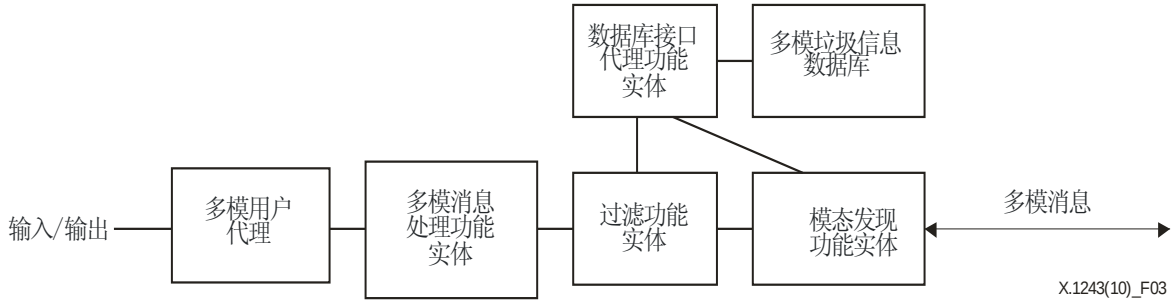

图 3 – 多模过滤架构

图4通过将功能实体映射到接收者网关功能（RGF）详细显示了一般的多模过滤架构。以下步骤描述了功能实体接收多模消息时的程序：

1) RGF接收多模消息

2) 模态发现功能实体识别传送的模态及在接收的多模消息中传送的消息类型。

3) 过滤功能实体可静态配置，所有过滤规则适用于所有潜在的多模消息（即与接收到的多模具体消息无关）；也可动态配置，每条接收到的多模消息各自适用与消息和/或模态有关的规则。

   a) 模态发现功能实体可将确定的模态和消息类型参数提交给数据库接口代理，也可将参数附在接收到的多模消息之后。

   b) 模态发现功能实体将多模消息，或许加上提取的模态和消息类型参数后转给过滤功能实体。

4) 在过滤功能实体尚未根据规则进行配置的情况下，除非数据库接口代理已直接从模态发现功能实体获得了模态和消息类型参数，过滤功能实体将这些参数传递给数据库接口代理。

5) 数据库接口代理功能实体查询多模数据库，以获得对应的多模和消息标准。数据库接口代理功能实体将这些值编辑成具体规则并将这些规则提供给过滤功能实体。

6) 过滤功能实体适用可用的规则并过滤收到的多模消息。取决于规则和政策设定的不同，多模消息或被允许通过，或完全阻止或部分阻止，后者中多模消息中仅有部分模态被阻止。

7) 过滤功能实体将过滤后的多模消息传递给多模消息处理功能实体，或许加上一些过滤结果（即用于登录或安全警告的信息）。

8) 多模消息处理功能实体处理收到的（经过滤的）多模消息。功能实体同步从不同输入多模用户代理收到的输入，将多模消息发送到其模态组件并将这些与模态相关的部分传递给输出模态用户代理。

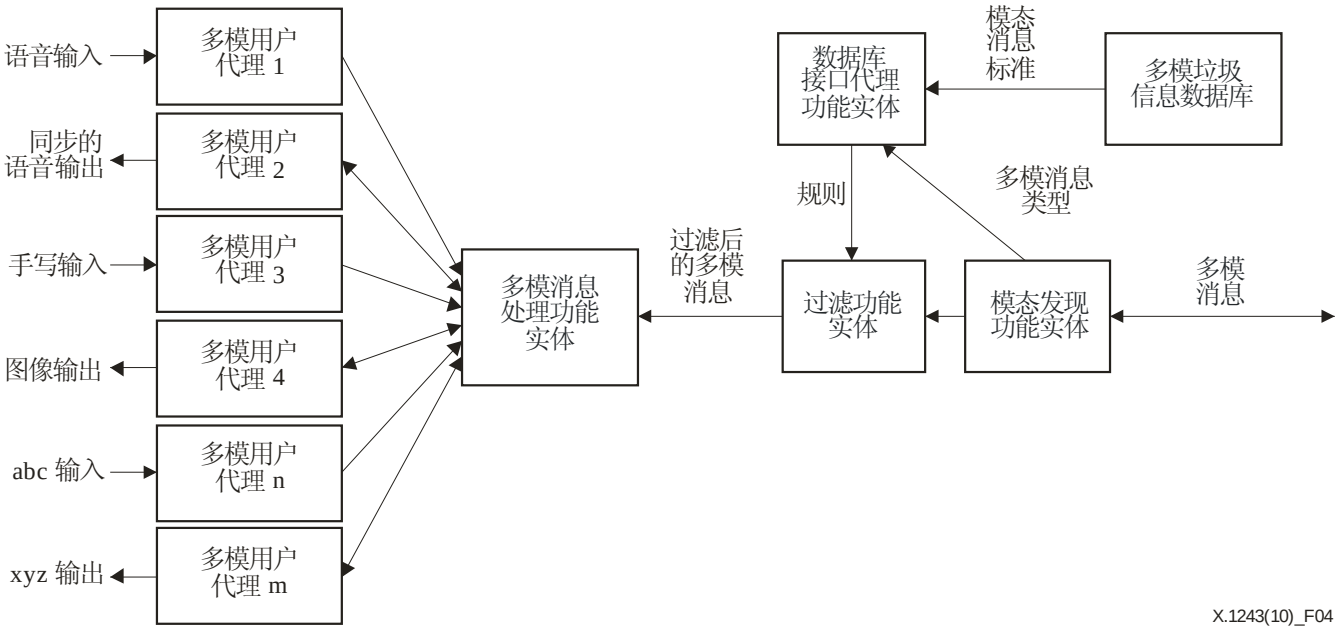

图 4 – 接收者网关功能（RGF）中的多模过滤

说明 – 图4描述了各种多模用户代理。RGF可能不需要所有的多模用户代理同时出现。

7.2.5 控制垃圾信息过滤法则（Damp spam filter）

控制垃圾信息过滤法则用于控制消息接收的速度。对于控制垃圾信息过滤器而言，一个重要的输入参数是垃圾信息控制系数。该系数是一种针对可疑消息的量度，它控制着消息的接收速度。当收到高度可疑的消息时，系数相应地提高且控制垃圾信息过滤法则将降低接收可疑电子邮件的速度。该参数通常由体验或声望数据库等外部垃圾信息系统产生。控制垃圾信息过滤器也可影响电子邮件回复延迟、传输窗口大小和控制周期等。

7.2.6 电子邮件标题过滤法则（Email header filter）

电子邮件标题过滤法则（EHF）监控SMTP转换并确保它遵循相关的协议。它可用于识别不符协议之处及伪造的电子邮件标题。为重建SMTP会话并追踪协议状态，EHF可要求封包整理碎片、TCP流汇编等。EHF以协议等级分析为重点，它提供了关于改善垃圾信息整体识别准确率的额外信息。EHF通常整合在许多商业反垃圾信息系统以及一些开源反垃圾信息系统中。

7.2.7 加权参数过滤法则（WPF）

加权参数过滤法则（WPF）通过分析多参数发现垃圾信息。参数基于统计信息，包括电子邮件会话数量、目标服务器数量、电子邮件尝试次数、发送邮件的期间、发送邮件的速率、尝试邮件和成功发送邮件比率等等。每一个参数都有配置的门限和配置的加权值。此外，整套加权值（可通过提前数次实验进行证明）也是必要的。对于每个电子邮件，规则中所有的参数都将被检查。只有通过配置门限的参数才会被加权。如果参数的总和超过预设的门限，则WPF可从普通邮件中将垃圾电子邮件识别出来。

8 打击垃圾信息对等协议的进程

8.1 对等发现

对等发现进程在两个IGCS之间建立对等关系。该进程在一个IGCS试图沿着消息交付路径发现一个合法的IGCS时被启动。当一个RGF发现一个可疑的垃圾信息消息时，对等发现进程开始。

建议对等发现消息包括以下信息：

- 初始IGCS的RGF/SGF的地址列表：源地址（即源IP地址和端口对）。为防止出现单点失效，IGCS可综合多个RGF和SGF，用于冗余。地址列表可包括初始IGCS所有RGF/SGF的地址
- IGCS对方的地址：IGCS@{对方代理的地址}
- 垃圾信息的来源地：垃圾信息发送者的地址
- WELL_KNOWN, USER_REPORTED or OTHER可疑垃圾信息的类型：WELL_KNOWN（众所周知）、USER_REPORTED（用户报告）或OTHER（其他）
- 所附的可疑垃圾信息：后附的可疑垃圾信息。

当发送了对等发现消息后，初始IGCS将启动一个计时器。如果在设定的截止期限内未收到回复的消息，初始IGCS将无法发现一个对等的IGCS。对等发现回复消息可包含以下信息：

- 回复IGCS的RGF/SGF的地址列表。
- 可疑垃圾信息的确认：确认可疑垃圾信息是否被回复IGCS视为垃圾信息。

8.2 对等设定

在时间期限终止前，如果初始IGCS收到了对等发现回复消息，它可开始建立对等关系。此过程有两个主要行动：

- IGCS更新对等列表：将对方IGCS的地址列表增加到对等列表中。
- 支持的垃圾信息过滤法则的名单：每个IGCS中可支持的垃圾信息过滤法则。

8.3 打击垃圾信息消息的交换

在对等设定程序之后，IGCS开始打击垃圾信息消息的交换。在此过程中，两个对等IGCS交换共同支持的垃圾信息过滤法则的信息。每个IGCS根据交换的消息相应地更新其lcsDB。

8.4 对等释放

如果在一段时间内未发现垃圾信息，一个IGCS可通过发送一条对等释放消息来终止对等关系。在收到对等释放消息后，IGCS将根据规则移除或重复使用相关的对等信息。

9 打击垃圾信息网关系统的实施模式

9.1 组合模式（Integrated model）

9.1.1 模式描述

在组合模式中，IGCS综合在由一个RA和一个SA组成的消息系统中。每个系统有一个网关（一个RGF和一个SGF）以及一个lcsDB。如在电子邮件系统中，一个RA可以是一个POP3服务器，而一个SA可以是一个SMTP服务器。一个RGF/SGF可作为提供POP3和SMTP服务的组合服务器而予以实施。对于电子邮件系统，也需要一个lcsDB来提供打击垃圾信息的规则。图5显示了一个组合模式。

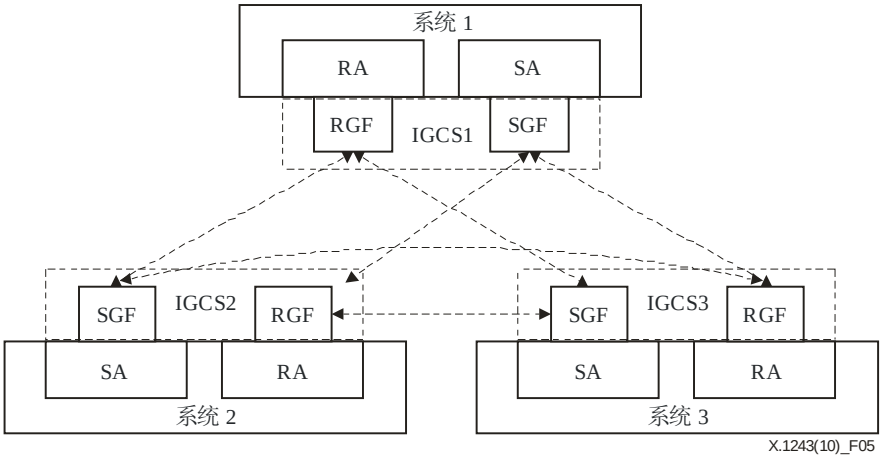

图5 – IGCS组合模式

9.1.2 使用案例

组合模式适合客户端/服务器（client/server）模式，其中一个服务器负责发送/接收许多客户的消息。在这种情况下，服务器作为打击垃圾信息活动的一个决策点和规则执行点。

9.2 域模式（Domain based model）

9.2.1 模式描述

在域模式中，IGCS作为具有多个用于负载平衡要求的多个SA和RA的消息传送代理。SGF/RGF分布在一个域中可有几种情况。每种SGF/RGF情况负责一个域中的几个SA/RA并负责打击本地域和域间垃圾信息消息。

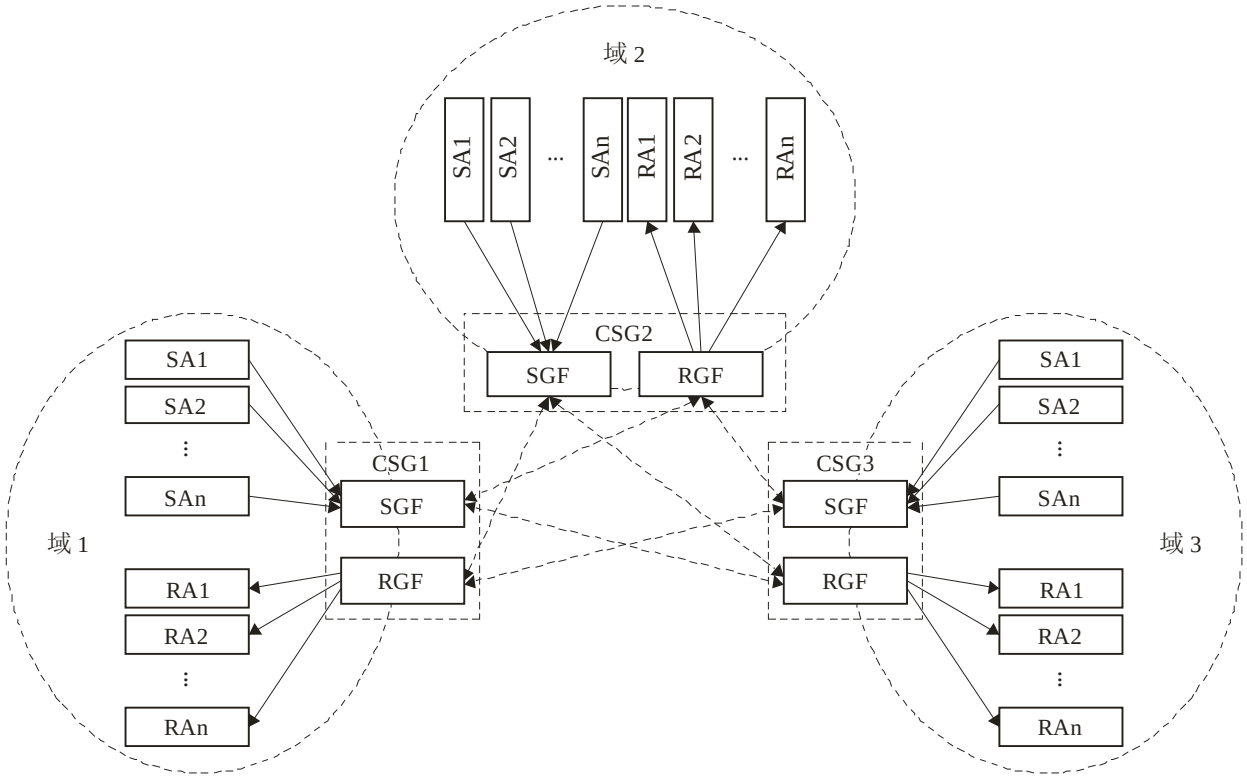

图6 – 域模式

9.2.2 使用案例

域模式可用于基于域的打击垃圾信息用途并特别适合端到端通信系统，例如许多流行的即时消息应用：IRC等。对于端到端模式，用户端系统自身就同时是RA和SA。管理大量带有组合IGCS模式的用户端RA和SA将非常困难。但是，域模式可通过分布方式解决问题。

9.3 旁路部署模式（Bypass deployment model）

9.3.1 模式描述

在无线网络中，IGCS也可通过无线接入点进行部署。无线接入点绕过所有发给IGCS的消息。IGCS根据保存在本地数据库（lscDB）中的规则对收到消息进行判断并将正常消息注入到无线网络中。

9.3.2 使用案例

旁路部署模式可用于无线网络中。可在垃圾信息进入无线网络前将其过滤，以便降低最终用户因传送垃圾信息流量而产生的不必要费用。

附录一

SCPP消息定义的示例

（本附录不构成本建议书的不可或缺部分）

以下列出了一个用ASN.1语言定义的SCPP消息示例，并经过了ASN.1编译程序的检查：

```
SCPP-MESSAGES {itu-t(0) recommendation(0) x(24) igscs(1243)
asn1-module(0) scpp-messages(1)}
DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

-- SCPP Message body definition
SCPP-PDU ::= SEQUENCE {
     sourceAddress        IGCS-Address,
     destAddress          IGCS-Address,
     igcs-message-body    CHOICE {
               peerDiscovery   PeerDiscoveryDEF,
               peerSetup       PeerSetupDEF,
               dataExchange    DataExchangeDEF,
               peerKeepAlive   PeerKeepAliveDEF,
               peerRelease     PeerReleaseDEF},
     nonStandardData      OCTET STRING OPTIONAL,
     ...
}

-- PeerDiscovery Message definition
PeerDiscoveryDEF::=SEQUENCE {
     setupRequest    BOOLEAN,
     igcsSignature   IGCS-Signature
}

-- PeerSetup Message definition
PeerSetupDEF::=SEQUENCE {
     setupResponse        BOOLEAN,
     sgfList              SEQUENCE OF IGCS-Address,
     rgfList              SEQUENCE OF IGCS-Address,
     supportedFilters     SupportedSpamFilters,
     igcsSignature        IGCS-Signature
}

-- Countering Spam Data Exchange Message definition
DataExchangeDEF::=SEQUENCE {
     csData               SET OF SpamFilterData,
     ...
}

-- Peer Keep Alive Message definition
PeerKeepAliveDEF::=SEQUENCE {
     sgfUpdates      GF-Updates,
     rgfUpdates      GF-Updates,
     filtersUpdates  SupportedSpamFilters
}
-- Peer Release Message definition
PeerReleaseDEF::=SEQUENCE {
     peerRelease     ENUMERATED{request(0), confirm(1)},
     nonStandardData OCTET STRING OPTIONAL,
     ...
}
```

```
-- IGCS supported addresses, include IGCS,SGF,RGF address definition
-- Support IP address, Email ID and other types of address
IGCS-Address::=CHOICE{
     ipAddress
     SEQUENCE { ip OCTET STRING(SIZE(4)),
                port INTEGER(0..65535) },
                ip6Address
                SEQUENCE { ip OCTET STRING(SIZE(16)),
                           port INTEGER(0..65535) },

     emailAddress         IA5String(SIZE(1..512)),
     nonStandardAddress   OCTET STRING,
     ...
}

-- Signature data for authentication
IGCS-Signature::=SEQUENCE {
     igcsID          INTEGER(0..65535),
     signatureData   OCTET STRING,
     ...
}

-- RGF/SGF status update information
GF-Updates::=SEQUENCE {
     gateType        ENUMERATED {sgf(0),rgf(1)},
     gateAdd         IGCS-Address,
     gateRemove      IGCS-Address
}

-- IGCS Supported Spam filters and related data

SupportedSpamFilters::= SEQUENCE {
     supportedFilter SEQUENCE OF SpamFilters

}

SpamFilters::=SEQUENCE{
     filterID        INTEGER(0..128),
     filterName      IA5String(SIZE(1..512))
}

SpamFilterData::=SEQUENCE {
     filterID        INTEGER(0..128),
     filterData      OCTET STRING,
     ...
}

END
```

参考文献

[b-ITU-T X.680] Recommendation ITU-T X.680 (2008) | ISO/IEC 8824-1:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*

[b-ITU-T X.681] Recommendation ITU-T X.681 (2008) | ISO/IEC 8824-2:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification.*

[b-ITU-T X.682] Recommendation ITU-T X.682 (2008) | ISO/IEC 8824-3:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification.*

[b-ITU-T X.683] Recommendation ITU-T X.683 (2008) | ISO/IEC 8824-4:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.*

[b-ITU-T X.1231] Recommendation ITU-T X.1231 (2008), *Technical strategies for countering spam.*

[b-ITU-T X.1240] Recommendation ITU-T X.1240 (2008), *Technologies involved in countering e-mail spam.*

[b-ITU-T X.1241] Recommendation ITU-T X.1241 (2008), *Technical framework for countering e-mail spam.*

[b-IETF RFC 1869] IETF RFC 1869 (1995), *SMTP Service Extensions*.

[b-IETF RFC 1939] IETF RFC 1939 (1996), *Post Office Protocol – Version 3*.

[b-IETF RFC 2060] IETF RFC 2060 (1996), *Internet Message Access Protocol – Version 4rev1*.

[b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*.

[b-IETF RFC 2635] IETF RFC 2635 (1999), *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*).*

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol*.

[b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format*.

[b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions.*

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