

国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.1231

(04/2008)

X系列：数据网、开放系统通信和安全性
电信安全

反垃圾信息技术策略

ITU-T X.1231 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	
业务和设施	X.1-X.19
接口	X.20-X.49
传输、信令和交换	X.50-X.89
网络概貌	X.90-X.149
维护	X.150-X.179
管理安排	X.180-X.199
开放系统互连	
模型和记法	X.200-X.209
服务限定	X.210-X.219
连接式协议规范	X.220-X.229
无连接式协议规范	X.230-X.239
PICS书写形式	X.240-X.259
协议标识	X.260-X.269
安全协议	X.270-X.279
层管理对象	X.280-X.289
一致性测试	X.290-X.299
网间互通	
概述	X.300-X.349
卫星数据传输系统	X.350-X.369
以IP为基础的网络	X.370-X.379
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	
组网	X.600-X.629
效率	X.630-X.639
业务质量	X.640-X.649
命名、寻址和登记	X.650-X.679
抽象句法记法1(ASN.1)	X.680-X.699
OSI 管理	
系统管理协议子集和结构	X.700-X.709
管理通信服务和协议	X.710-X.719
管理信息的结构	X.720-X.729
管理功能	X.730-X.799
安全	X.800-X.849
OSI 应用	
托付、并发和恢复	X.850-X.859
事务处理	X.860-X.879
远程操作	X.880-X.889
ASN.1的一般应用	X.890-X.899
开放分布式处理	X.900-X.999
电信安全	X.1000-

欲了解更详细信息，请查阅 *ITU-T* 建议书目录。

反垃圾信息技术策略

摘要

ITU-T X.1231 建议书强调了反垃圾信息技术策略，其中还包括垃圾信息总的特征和反垃圾信息主要目标。另外，考虑到没有一种方案可独立解决垃圾信息问题，本建议书提出一个列表，以便对可能有效的反垃圾信息技术工具予以评价。

来源

ITU-T 第 17 研究组（2005-2008 年）按照世界电信标准化全会（WTSA）第 1 号决议规定的程序，于 2008 年 4 月 18 日批准了 ITU-T X.1231 建议书。

关键词

反垃圾信息，垃圾信息，技术策略。

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ITU-T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”等其他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他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/>。

© 国际电联 2009

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页码

1	范围	1
2	参考文献	1
3	术语	1
3.1	其它地方定义的术语	1
3.2	本建议书定义的术语	1
4	缩写词和首字母缩略语	2
5	排印惯例	3
6	总体介绍	3
7	总的目标	5
8	技术策略	5
8.1	设备策略	6
8.2	网络策略	7
8.3	业务策略	8
8.4	过滤策略	9
8.5	反馈策略	10
9	系统评估	11
	参考文献.....	12

引言

伴随信息产业的发展，垃圾信息在给普遍用户带来不利影响的同时，也使电信运营商、服务提供商和商业用户遭受巨大利润损失。垃圾信息正在从简单的骚扰成为全球瘟疫。

因此，很有必要发现有效直接的办法来抵制垃圾信息。无论如何，治理垃圾信息有很多方法：立法、培训、国际合作等等，但是，本建议主要关注于技术手段。

反垃圾信息技术策略

1 范围

本建议书强调了反垃圾信息技术策略，其中还包括垃圾信息的总体特性和反垃圾信息的主要目标。另外，考虑到没有单一方案来解决垃圾信息问题，本建议书还提出一个列表，以便对可能有效的反垃圾信息技术工具予以评价。

本建议书描述总体技术策略而并未提出任何特定类型垃圾信息的技术策略。另外，本建议书给出了一个建立高效有效反垃圾信息的等级体系架构模型。模型包括如下方面：

- 设备策略；
- 网络策略；
- 业务策略；
- 过滤策略；
- 反馈策略。

事实上，本建议书提供了主管部门根据国家法律和政策认定不正确的对抗多种垃圾信息的技术策略。

2 参考文献

无。

3 定义

3.1 其它地方定义的术语

本建议使用如下其它地方定义的术语：

3.1.1 认证 [b-ITU- T X.811]：为实体宣称身份提供确认。

3.1.2 IP电话 [b-ITU- T Q-Sup.49]：IP电话指直接连接(如通过以太网接口或xDSL线)到IP网络的终端（例如，专门的语音终端或者多用途个人计算机）。

3.1.3 短消息实体（SME） [b-ITU-T Q.1742.3]：写短消息或者解短消息的实体。SME可以处于或不处于宿主归属寄存器（HLR）、短消息中心（MC），访问归属寄存器（VLR）、移动台（MS）或者移动交换中心（MSC）之中，可以或无法进行区分。

3.2 本建议书定义的术语

本建议书定义如下术语：

3.2.1 即时消息（IM）：即时消息指用户之间接近实时的消息传送。这些消息通常（但不要求）很短。IM经常用于会话模式，即，消息来回传送的速度很快，足以使参与方保持交互式会话。

3.2.2 IP多媒体垃圾信息：IP多媒体垃圾信息指基于实时IP多媒体应用的未请求消息或呼叫。与传统垃圾电子邮件不同，IP多媒体垃圾信息通常指最近基于IP通信（例如即时消息、呈现业务、基于IP语音等等）出现的垃圾信息。垃圾互联网电话（SPIT）、语音垃圾信息或VolP垃圾信息（VAM）和垃圾即时消息（SPIM）是现在特定IP多媒体垃圾信息的名称。

3.2.3 模式：模式指包含人类可以感知信息的信息编码。例如，模式信息包括用于人机接口的文本、图形、语音、视频和触觉信息。多模式信息可以来自于或者目标是多模式设备，例如用于声音输入的麦克风、触觉输入的笔、图片/文本输出的屏幕、触觉反馈的震动设备或者用于视觉障碍的盲文输入设备。

3.2.4 多模式消息：多模式消息指用于多模态交互设备交互编码信息的多模式消息。

3.2.5 多媒体消息业务（MMS）：多媒体消息业务是在短信业务之后，基于移动通信网、无线网或者固定网提供的可以传送包括文本、图形、音频、视频等多媒体消息的一种消息业务。

3.2.6 短信业务（SMS）：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。

3.2.7 垃圾信息制造者：垃圾信息制造者指制造并发送垃圾信息的实体或个人。

4 缩写词和首字母缩略语

本建议书使用如下缩写词和首字母缩略语：

DDoS	分布式拒绝服务（Distributed Denial of Service）
DoS	拒绝服务（Denial of Service）
Email	电子邮件（Electronic Mail）
HLR	宿主归属寄存器（Home Location Register）
IM	即时消息（Instant Messaging）
IP	互联网协议（Internet Protocol）
MC	短消息中心（Message Centre）
MMS	多媒体消息处理业务（Multimedia Messaging Service）
MS	移动电台（Mobile Station）
MSC	移动交换中心（Mobile Switching Centre）
PSTN	公众电话交换网（Public Switched Telephone Network）
SME	短消息实体（Short Message Entity）
SMS	短信业务（Short Message Service）
SMTP	简单邮件传送协议（Simple Mail Transfer Protocol）
SPIM	基于互联网消息的垃圾信息（Spam over Internet Messaging）

SPIT	基于互联网电话的垃圾信息（Spam over Internet Telephony）
VAM	语言垃圾信息或VoIP垃圾信息（Voice Spam or VoIP Spam）
VLR	访问归属寄存器（Visitor Location Register）
VoIP	基于IP的话音（Voice over IP）

5 排印惯例

无。

6 总体介绍

垃圾信息是发送方通过计算机、手机、固定电话等终端向受信方发送的、通常为非请求、不必要和有害的电子信息。垃圾信息可能采用电子邮件、移动消息业务、IP多媒体或者其它电子形式传播。事实上，垃圾信息的含义通常取决于国家、组织或者个人的理解。特别是垃圾信息的含义是随着可能扩展垃圾信息生成方式的信息通信技术的发展而扩展。通常具有如下特征：

电子性：垃圾信息一般通过开放的通信网络，尤其是互联网进行发送，不同于邮寄、纸质广告、直销等传统方式。垃圾信息通常便宜、方便并且容易伪装。

推介性：垃圾信息通常包含广告、欺诈信息或病毒等。

另外，垃圾信息通常还具有以下全部或部分特点：

批量且重复发送：垃圾消息和垃圾电子邮件往往采用无目的批量发送的形式，同时实时垃圾通信总是重复发起。但垃圾信息制造者除了接受者的通信地址（例如电子邮件地址、接收者的电话号码）以外并不知道其它信息。

未经所有者同意而使用其地址：垃圾信息制造者通常使用未经接收者明确同意而收集的地址发送垃圾信息。事实上，一些软件程序可通过网络收集通信地址或自动生成通信地址。

隐藏或者错误的消息来源：垃圾信息通常通过错误消息头或者隐藏来源的方式来伪造信源。垃圾信息制造者通常使用非授权第三方服务器（并不验证信息源信息）。

难以阻止：由于存在大量的消息，故此很难检测垃圾信息。通常难以阻止垃圾信息，而且容易导致错报和漏报。

策略是独立于技术的，但是仍值得评价技术因素：在权限内什么通信媒体容易被误用导致垃圾信息问题，那些不可能被误用。通常垃圾信息使用的通信媒介如下：

电子邮件

当前，由于传输电子邮件的电子邮件协议和基础通信架构（例如互联网）的薄弱性，垃圾邮件成为各种垃圾信息中威胁最大的。简单邮件传输协议（SMTP）是电子邮件传输中最普遍使用的协议。SMTP为每一封电子邮件定义了信封和信头。信封包含接收者的地址并且

接收者不能看到。在发送过程中，作为消息从发送者发送到接收者的目的地址。通常，在发送过程中，这个包含在信封中的目的地址被拷贝到接收者可以看到的电子邮件头。垃圾信息制造者通常使用两种SMTP认证过程的缺陷：

- 无需认证，因此用户可以隐藏和伪造他们地址。
- 绝大多数电子邮件中的信封和信头的字段可以伪造。

另外，发送电子邮件的成本很低，但是它们的负面影响通常很大。

移动消息业务

移动消息最大的优点就是方便、高效、低成本和容易使用。但是如今，用户在享受移动消息优点的同时还面临移动垃圾消息。移动垃圾消息通常指通过SMS或MMS发送的未请求消息。根据当前统计，最主要的垃圾短信类型有：

- 业务订购欺骗；
- 广告信息；
- 非法欺骗；
- 色情信息。

这些类型消息通常带有欺骗性和虚假性，也被称作欺骗消息。

应注意到，伴随移动电子邮件业务的出现通过移动设备接收电子邮件已非常普遍，而这更易于被垃圾信息制造者利用。

IP多媒体

伴随IP多媒体的发展，垃圾信息概念开始扩展到IP多媒体范围，例如垃圾即时消息、垃圾IP电话、垃圾呈现业务、垃圾博客、垃圾新闻消息、垃圾在线游戏等。在一些特定环境出现了通过各类媒体传送的垃圾信息的专业术语，例如：SPIM（垃圾即时消息）、SPIT（垃圾IP电话）等等。另外，作为新的多媒体业务，多模式交互也被垃圾信息影响，单一的多媒体垃圾信息可能多次出现在用户接口。例如垃圾信息网络消息可能导致播放有着相同或者不同内容的垃圾语音片断、垃圾视频片断或者在屏幕上播放垃圾文本。但多模式增加了面对垃圾多媒体的可能，因此，对于多模式交互的垃圾多模式问题将会越来越普遍。

SPIM：即时消息是互联网中快速发展的一种方便、实时和便宜的通信方式。通常用于私人通信。同时，即时消息应用正在越来越多地应用于企业。但是不幸的是，越来越多的非法信息，例如病毒、有害代码等等正在通过即时消息传播，通常被称作SPIM。虽然SPIM在整个垃圾信息的比例很小，但是发展却非常快速。

SPIT：目前已发现的一些垃圾信息问题包括与IP网络相关的问题及其它更复杂的威胁，例如误传、窃听、VoIP拒绝服务攻击、包注入和不必要消息（VoIP垃圾信息和SPIT）。后者主要由于VoIP发送语音消息成本低廉而产生，最终导致了和垃圾邮件类似的情况：大量的不必要语音邮件可以在几秒钟内发遍世界。

垃圾信息发展

垃圾信息不限于以上选择。随着越来越多信息通信技术和应用的出现，垃圾信息也会无处不在。此外，如提出的反垃圾信息方案无效，任何通信技术和应用都可能成为垃圾信息的媒介。

7 总的目标

本条的目的是描述反垃圾信息的最终目标。重点是要达到什么目标而不是具体的实现步骤。

反垃圾信息的目标如下：

- 验证实体是否有权在认证和/或授权以后发送消息和发起通信。
- 保护合法用户发送的消息或者发起的通信的地址和/或其它重要信息不被隐藏或者伪装
- 在信息传送过程中保护隐私。
- 所有实体对其自身的信息传送或者转发行为负责。
- 保护电信网络，防止非授权访问或者操作，以保证有效和高效接入。
- 提供信源的必要信息，以确保未来可追溯性。
- 保护业务设备不受病毒和非授权接入的侵害，以确保可用性。
- 垃圾信息过滤，如果必要，可以存储到特定设备，用于追溯和取证分析
- 提供反馈平台，不仅支持准确有效的信息报告，还支持国际合作和立法等等
- 采用众所周知的国际协议，用于反垃圾信息的适当信息共享和分发。

另外，以上目标的实现基于特定的环境。

8 技术策略

反垃圾信息需要多个方面来进行，包括：行业技术、行业自律、国际合作、立法、反馈和培训。在这些方面中，技术对保证其它方面实施至关重要。本建议书主要侧重于一般的反垃圾信息策略。

为便于分析，有必要首先对业务进行分类。根据业务传输方式，业务可以划分为存储转发业务和实时通信类业务。存储转发类包括电子邮件业务、移动消息业务、多媒体消息业务等等。实时通信类业务包括IP电话、IP传真等等。不同业务中反垃圾信息方式有很大不同。因此，有必要根据一般技术策略对具体业务进行详细分析。

为了有效反垃圾信息，建议实施包括不同部分的等级模式。另外，实施方面越多，越有效果。图1显示反垃圾信息的等级结构，具体如下：

过滤策略	反馈策略
业务策略	
设备策略	网络策略

图1 – 反垃圾信息的等级结构

该等级结构中中共有五个部分，可以分为三个层面：基础设施层面，业务层面和应用层面。设备策略和网络策略属于基础设施层面，是等级结构的基础。其实施有助于为上层技术策略建立安全和可靠的基础。另外，设备策略和网络策略相互影响。安全网络需要安全设备，同时安全设备需要合理的网络。业务策略属于业务层面，它是五个部分中最重要的部分，因为其直接负责提供业务。最后过滤需求和反馈需求属于应用层面，在反垃圾信息过程中最贴近用户；同时又相互影响。图2显示各部分之间的关系：

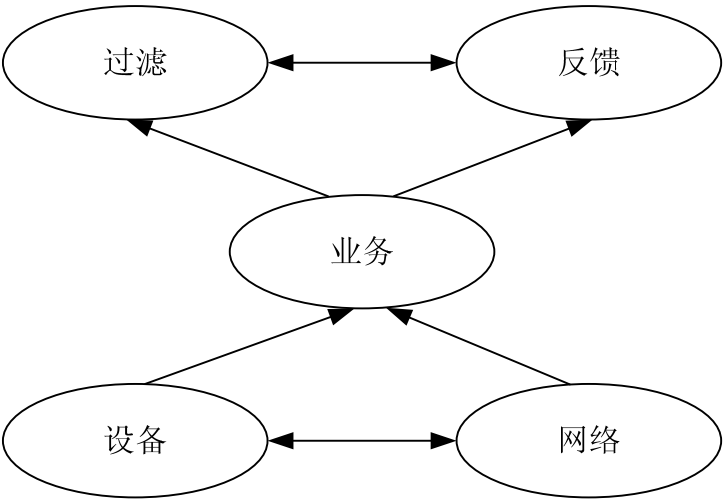


图2 – 不同部分之间关系图

此外，推荐使用众所周知的国际协议来满足这些策略。一旦所有策略得到满足，成本相对所保护的本身的价值可能非常高。因此，根据应用情况来定制策略就变得非常重要。另外，打击垃圾信息的方法应该运作用户定制。由于存在大量的策略组合方式，所以希望有一些描述文件可以覆盖大部分的业务。通过行业和研究型组织进行标准化有利于解决方案和产品的复用。同时，反垃圾信息的技术解决方安可以尽快以较低的成本实施。

8.1 设备策略

设备是反垃圾信息等级架构的基础；因此，设备保护对反垃圾信息至关重要。

8.1.1 增强相关设备的软件安全

垃圾信息制造者可以使用有明显漏洞的第三方计算机资源和网络资源来发送垃圾信息。这些资源变成牺牲品，也可以叫做botnets或者僵尸计算机。垃圾信息制造者可以远程控制这些牺牲品来发送垃圾信息。安装安全操作系统和应用软件并及时升级防病毒软件来防止设备免受病毒侵害非常有效。

8.1.2 提供不同管理角色

由于业务系统的重要性，业务系统需要提供分级用户管理。分级用户支持包括如下管理角色：用户管理角色、系统管理角色和审计管理角色。用户管理角色用于管理管理员、操作员和审计员的配置；系统管理角色用于维护和操作设备；审计管理角色用于审计操作日志和系统日志。另外，根据不同业务需要，系统可能提供一些特殊的管理角色。

8.1.3 提供完整的操作日志和系统日志

为了保证系统的正常运行，系统须提供完整的操作日志和系统日志。

操作日志用来提供操作历史，所有登录和操作事件均应记录。操作日志至少应包括如下字段：操作者姓名、操作时间、操作命令、是否成功。

系统日志主要记录系统运行状态信息，主要包括性能信息、故障信息等对不同系统或不同业务，系统日志内容可能不同。

然而，操作日志和系统日志不仅仅可以服务于系统维护，同时也可协助管理员确保系统程序无破坏性活动。

8.1.4 提高终端的安全性和灵活性

终端是最重要的最终用户设备，总是垃圾信息的直接受害者。因为不同终端有不同功能，故此只能提出总策略。包括但不限于下列各项：

- 支持认证和授权，特别是智能终端；
- 支持黑名单和/或白名单；
- 提供反病毒软件（特别为智能终端）。

8.2 网络策略

类似于设备需求，网络安全也是反垃圾信息的基础。通过正确的网络拓扑和安全设备（例如防火墙、安全路由器、安全网络等等）的实施，垃圾信息会大大减少。

8.2.1 隔离业务网和互联网

业务通常都是基于开放IP技术，所以各种业务网络面临着来自互联网上的威胁。

需提供如下功能：

- 保护业务网络免受来自互联网的攻击，例如DoS、DDoS攻击。业务网络通常非常重要并且可以被管理员远程控制。由于互联网对每个人来说都是开放的，故此业务网络必要可以抵抗来自互联网的威胁。通常，防火墙和其它安全设备被用于保护业务网络免受这些威胁。

- 在控制平面保护协议信令免受非法侵入。这点对VoIP特别重要，PSTN一般安全和可靠，但是互联网并不安全可靠。因此，VoIP网关最好可以阻止非法协议信令以便获得和PSTN一样的安全级别。

8.2.2 提供冗余和备份机制来保持业务网的稳定性

业务设备和网络非常重要，故此需要提供冗余设备和备份路由。另外，冗余和备份机制必须实用、有效且具有合理成本。

8.3 业务策略

由于业务直接满足用户需求，因此业务策略是等级模型中最重要的部分。但业务种类繁多，且具有不同的功能和漏洞。因此不同业务的反垃圾信息业务策略也有所不同。但不同业务有相同的反垃圾信息一般业务策略，如下所示：

8.3.1 支持认证

当实体（用户或者设备）使用业务时，业务系统应支持严格的认证。一方面，严格的认证可阻止非法实体使用业务。另一方面，准确的认证记录可用于追溯。

如今由于实施了认证和实名制，一些国家已在移动网络方面取得了诸多成就。

8.3.2 支持可配置转发地址

业务设备应关闭开放转发和采用限制转发。设备应支持可配置转发地址列表。它们仅仅转发来自允许地址的消息。相反，来自其它地址的消息将被屏蔽。

8.3.3 支持严格消息格式

对于特定消息，特别是商业消息，需要制定严格的消息格式。这样，业务系统就可以具备足够信息来处理这些消息。

8.3.4 符合国际标准

为了加强互连互通和互操作能力，要求通信协议符合国际标准。

8.3.5 提高垃圾信息的可追溯性

一方面，业务系统在实体接入时应对其进行标识和认证，并获取实体准确的源信息，把相应信息记录到数据库。另一方面，业务系统应根据数据库中的记录提供审计功能用于追溯。

8.3.6 支持信息流控制

系统管理员可以限制通信带宽或者每个特定时间段内发送消息的数量。

8.3.7 提供统计功能

统计信息可以使系统管理员清晰地了解到系统当前状态，例如流量信息或者访问者信息。

8.4 过滤策略

过滤是最通用的反垃圾信息技术。过滤的最大优势就是实施起来简单而灵活。

8.4.1 支持垃圾信息过滤

通常，有两种过滤方式：基于地址过滤和基于内容过滤（包括基于关键词过滤）

基于地址的过滤可用于存储转发业务和实时业务。对于存储转发业务，基于地址的过滤根据信息源地址过滤信息和电子邮件。它可以有效防止业务系统发送或转发垃圾消息和电子邮件。对于实时业务，基于地址的过滤根据主叫电话号码或地址阻止呼叫。一般而言，基于地址的过滤是非常有效和方便的打击垃圾信息的方式。

基于内容的过滤也可用于存储转发业务和实时业务。对于存储转发业务，基于内容的过滤按内容或关键词过滤消息和电子邮件。对于实时业务，基于内容的过滤根据内容切断通信。理论上，与基于地址的过滤相比，基于内容的过滤更加合理。但是，基于内容的过滤总是消耗大量资源。其准确度与分析算法密切相关。

任何一种过滤方法都不可能过滤所有垃圾信息。因此，最好同时使用两种方法。此外，业务设备应支持病毒过滤。

8.4.2 提供垃圾信息过滤的备份/记录机制

对于存储转发类业务，业务设备应自动备份垃圾信息。对于实时通信类业务，业务设备应自动记录垃圾信息摘要。并进行存储可以用于日后查询。

8.4.3 垃圾信息过滤性能要求

对于垃圾信息过滤，性能指标至关重要。误报率和漏报率是评价垃圾信息过滤性能的最重要的因素。误报是指没有反例时检测出反例，漏报是指有反例却未检测出反例的情况。因此，误报率是反例被误报为正例的比例。漏报率是正例被误报为反例的比例。表1是垃圾信息过滤结果：

表1 – 垃圾信息过滤结果

		实际情况	
		正例	反例
测试结果	检测出的正例	A	B
	检测出的反例	C	D
注 – 正例是垃圾信息，反例为非垃圾信息。			

测试样本总数为T。

$$T = A+B+C+D$$

误报数是B。

漏报数是C。

误报率 = $B / (B + D)$ 。

漏报率 = $C / (A + C)$ 。

误报率和漏报率是紧密相关的。通常误报率越大，漏报率越小。然而，哪个数值更重要取决于实际环境。在商业事务中，提高漏报率比误报率更加重要。

8.4.4 提供简单灵活的过滤配置

面对大量多变的垃圾信息，最好提供简单灵活的过滤配置，例如友好界面、可选配置方式等等。另外，通用过滤规则可以划分到可以存储到不同数据库和存储器的过滤库。如有必要，这样的过滤库可以容易地选择和使用。

8.4.5 尽量降低过滤成本

应在垃圾信息占用大量资源之前尽早过滤垃圾信息。因此在传输开始时就应过滤垃圾信息，而不应遗留给后面的业务设备。

8.4.6 支持黑名单与白名单

有两种类型的基于地址的过滤：可接受发送者的白名单和可疑垃圾信息制造者的黑名单。

黑名单是基于垃圾制造者的列表，包括机器名称，IP地址、MAC地址或其它类电子地址。过滤系统可按照黑名单过滤消息或阻止通信。

白名单是基于可接受发送者的列表。工作机制与黑名单类似，只是白名单是可接受的地址清单。

事实上，黑名单/白名单方法通常太不成熟以至于不能为大多数用户接收。但是，此类方法非常简单并且不需要太多资源。为了提高过滤有效性，过滤设备必须支持黑名单与白名单，特别要支持黑名单来对抗垃圾信息。

8.4.7 支持过滤多模式消息

对于多模式消息有如下需求

- 支持完全过滤特定多模式消息
- 支持过滤特定多模式消息附件和在一个多媒体消息内的部分多模式内容
- 支持入口（接收）和出口（发送）的多模式消息过滤

8.5 反馈策略

最终用户是最终的垃圾信息接收者、潜在的病毒和欺骗消息的可能受害者。最终用户的参与有助于有效高效地抵抗垃圾信息。因此，在制定反垃圾信息方案时应考虑到最终用户的反馈。但最终用户对反馈机制的参与应出于自愿。

8.5.1 提供垃圾信息反馈平台

应向受垃圾信息影响的个人提供申诉手段。作为垃圾信息接收者，自然人的权利需得到立法保护。因此，必须为他们提供申诉渠道。需要建立这样的机制来支持这个目标，包括给权利机关汇报这些垃圾信息情况。这样的反馈处理程序需要透明、高效和有效。反馈平台就可以起到这种作用。

8.5.2 对反馈共享提供标准格式

反馈平台需采用标准记录格式来记录反馈信息。因此，不同运营商和实体可以共享反馈信息。通过共享的反馈，可以获得垃圾信息制造者的主要地址，可将其放到黑名单中。

9 系统评估

为了有效评估反垃圾信息的技术或者系统的有效性，需要考虑如下因素：

- 误报率
- 漏报率
- 成本：反垃圾信息方法应能灵活提供定制解决方案。由于存储大量的可能策略组合，建议提供大量轮廓来覆盖大范围的业务。
- 当前系统的互操作性：反垃圾信息的前提是保证现有系统的正常操作，即，实施反垃圾信息方案不能影响现有系统的运行。
- 符合国际标准：技术解决方案一定要基于开放国际标准以便获得全球互连互通和扩展。另外，标准化有利于解决方案和原件的复用。这有助于快速以较低成本引入新的反垃圾信息解决方案和技术。

以上方面是评估反垃圾信息措施的一般性标准。在实际业务网络中，还需要考虑其它具体问题。

参考文献

- [b-ITU-T Q.1742.3] Recommendation ITU-T Q.1742.3 (2004), *IMT-2000 references (approved as of 30 June 2003) to ANSI-41 evolved core network with cdma2000 access network*.
- [b-ITU-T Q-Sup.49] Recommendation ITU-T Q-series Recommendations – Supplement 49 (2004), *Technical Report TRQ.2840: Signalling requirements to support IP telephony*.
- [b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- [b-ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.
- [b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*.
<<http://www.ietf.org/rfc/rfc2505.txt>>
- [b-IETF RFC 2554] IETF RFC 2554 (1999), *SMTP Service Extension for Authentication*.
<<http://www.ietf.org/rfc/rfc2554.txt>>
- [b-IETF RFC 2635] IETF RFC 2635 (1999), *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)*.
<<http://www.ietf.org/rfc/rfc2635.txt>>
- [b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol*.
<<http://www.ietf.org/rfc/rfc2821.txt>>
- [b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions*.
<<http://www.ietf.org/rfc/rfc3685.txt>>

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、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其他组件的结构、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	电信系统使用的语言和一般性软件情况