国　际　电　信　联　盟

ITU-T X.1233

(09/2021)

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 – 打击垃圾信息

打击通过即时消息传播的垃圾邮件的导则

ITU-T X.1233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
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
打击垃圾信息	**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
网页安全（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
网络保卫	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

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1233 建议书

打击通过即时消息传播的垃圾邮件的导则

摘要

ITU-T X.1233建议书规定了即时消息（IM）服务提供商（SP）和用户打击即时消息垃圾邮件（SPIM），以及减少SPIM在网络空间的传播并改善即时消息（IM）用户体验的指导原则。

本建议书分析了在即时消息中生成SPIM的场景，为即时消息服务提供商指定了应对SPIM的技术措施和机制，并为IM用户制定了应对SPIM的导则。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1233	2021-09-03	17	11.1002/1000/14773

关键词

应对垃圾即时消息（SPIM）、导则、IM服务提供商、IM用户。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，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）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/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，这可能并非最新信息，因此特大力提倡他们通过下列ITU-T网址查询相应的可用ITU-T据库：http://www.itu.int/ITU-T/ipr/。

目录

引言

即时消息（IM）应用程序的推广导致即时消息应用（IM）与语音、短消息业务（SMS）和电子邮件一起，成为传播垃圾邮件的重要方式。IM 实时、高效的信息传输，为社交提供了极大便利。然而，此方式亦为垃圾邮件发送者打开了通过即时消息发送垃圾邮件（SPIM）的大门。IM 发送的垃圾广告、色情和其他非法信息（如网络钓鱼信息、病毒、特洛伊木马蠕虫和垃圾邮件散播者软件等）的数量呈指数级增长。这不仅给用户造成骚扰甚至导致经济损失，也严重影响了网络空间的安全。应对 SPIM 已经成为打击垃圾邮件的一个重要因素。

但对于希望在操作或使用即时通信时应对SPIM的服务提供商（SP）和用户，仍然缺乏指导。这意味着应对SPIM的努力尚无有效管理。因此，当务之急是建立相关标准，以指导即时通信运营商和用户的技术和管理措施，防止SPIM。

ITU-T X.1233建议书

打击通过即时消息传播的垃圾邮件的导则

1 范围

本建议书为IM服务提供商（SP）和用户制定了准则，以应对通过即时消息传送的垃圾邮件（SPIM）。这一建议书涵盖了IM垃圾邮件场景、IM SP应对SPIM的技术措施和机制，以及IM用户应对SPIM的应急处置措施等。

2 参考文献

无。

3 定义

3.1 在其他处规定的术语

本建议书使用以下在其它文献中规定的术语：

3.1.1 通过即时消息传播的垃圾邮件（spam over instant messaging）（SPIM）[b-ITU-T X.1244]：以即时消息服务用户为目标的垃圾邮件。

注 – 在本建议书中，没有定义术语“垃圾邮件”。

3.1.2 垃圾邮件散播者（spimmer）[b-ITU-T X.1244]：SPIM的散播者。

3.2 本建议书定义的术语

本建议书定义了以下术语：

3.2.1 即时消息（instant messaging）（IM）：在接近实时的一组参与者之间交换内容。一般来说，内容是短文本消息，尽管情况并非如此。

注 – 基于[b-IETF RFC 3428]。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

IM 即时消息

IP 网际协议

NE 网络运营商

SMS 短消息业务

SPIM 垃圾即时消息

SP 服务提供商

5 惯例

动词“须”表示为符合本建议书的规定而必须严格遵守的要求。

动词“应”和“不应”表明，在几种可能性中，有一种被认为特别合适加以推荐，但没有提及或排除其他可能性；某个行动过程属于优先选项的但不必需；或者（以否定的形式）表示某种可能性或行为不推荐但亦不禁止。

动词“可以”表示允许的可选规定。该术语并不意味着实现必须提供此选项。

6 垃圾即时消息的特征及产生方式

通过SPIM正成为IM服务的主要挑战。SPIM以各种方式影响即时通讯系统的性能，例如内存、中央处理器、存储空间和带宽资源方面的资源浪费，并可能导致诸如蠕虫传播、拒绝服务攻击等重大问题。SPIM方案包括但不限于以下内容，

– 利用自动化手段注册大量账户，用于邪恶目的，如传播SPIM。
– 使用未经账户所有者授权的账户与目标用户建立会话连接，以传播SPIM。
– 缺乏内在安全机制，比如添加好友时缺乏确认机制，造成SPIM病毒可以迅速传播的环境。
– 通过不安全的传递渠道透露消息。黑客可以在即时消息在传送的过程中进行篡改。广告或者恶意代码可能被嵌入消息，将它转变成垃圾即时消息。
– 非法制造商为了商业利益向用户推销SPIM套餐。

7 IM服务提供商应对SPIM的指导原则

7.1 打击SPIM功能的配置

IM SP应在提供IM服务的同时提供打击SPIM的功能。打击SPIM的功能应包括但不限于以下内容：

– 自动用户注册检测和控制；
– 添加好友时的授权控制；
– 消息发送速率检测和限制；
– 基于黑名单的消息筛选；
– 除其他功能外，具有简单反馈机制向IM SP发出收到SPIM的告警。

同时，IM SP须在操作过程中保持打击SPIM的功能。场景应包括但不限于以下内容：

– 维护打击SPIM的数据库，如好友列表和黑名单，以确保其可用性和稳定性；
– 维护用户投诉信息，以提高该信息的准确性；
– 调整打击SPIM功能使用的门限值，例如消息发送速率限制门限值、在将账户添加到黑名单之前可收到的投诉数量的门限值。

7.2 行为监控

IM SP应采取措施监控以下行为，并在检测到异常时生成警报。应监控的行为包括但不限于以下几项：

– 验证失败行为。例如，多个验证请求从同一个网际协议（IP）地址发送。如果存在多次这种行为，则可能是垃圾邮件散播者在窃取账户信息，然后将信息发送给SPIM。此行为应触发警报，并应放弃来自该IP地址的后续验证请求。

– 恶意投诉行为。比如某账户在一定时间内提交大量投诉，无论投诉涉及不同账户还是同一账户，如果投诉数量超过一定门限值，则应触发报警并忽略该账户的投诉，从而提高投诉的准确性。

– 恶意将账户添加到黑名单的行为。例如，如果某些账户将特定账户添加到黑名单，则应检测这些账户是否在可疑账户列表中。如果其中大部分在可疑账户列表中，则应触发警报。在统计某个账户被添加到黑名单的次数时，不应考虑试图将这些账户列数据黑名单的次数，从而提高黑名单的准确性。

7.3 审计和记录

IM SP须取技术措施，审计和记录用户行为及网络安全事件，以打击SPIM。IM服务应审核的记录包括但不限于以下几项：

– 用户行为日志，包括注册行为信息和用户认证信息。例如，IM SP应记录用户的历史行为（例如，超过消息发送速率限制门限值的消息发送行为和恶意投诉行为）。消息发送行为日志应包括但不限于以下信息：发送者的账户信息（例如，IP地址、用户名、发送者是否包括在可疑列表或黑名单列表中）、接收者的账户信息、发送者和接收者之间的关系类型（例如，朋友、非朋友、群组中的朋友成员、群组中的非朋友成员、其他即时消息系统的朋友和电话联系人）。IM服务器提供商应整合对这些信息的分析，以识别可疑或恶意活动。恶意投诉行为日志应包括但不限于以下信息：投诉人的账户信息（如IP地址、用户名，是否包含在可疑名单或黑名单中）、被投诉账户的信息以及某段时间内的投诉数量。如果投诉数量超过门限值，则投诉人账户的投诉将被忽略，从而提高投诉平台的准确性。

– SPIM筛选记录，包括SPIM筛选行为和筛选后的消息。SPIM筛选行为记录应包括但不限于以下信息：受筛选消息的发送账户（例如，IP地址、用户名、是否在可疑列表或黑名单列表中）、正在使用的筛选措施（例如，基于黑名单的筛选程序、发送速率控制或授权控制）。应将筛选后的消息记录下来，以便在筛选错误的情况下重新发送。

7.4 应急响应

IM SP应针对SPIM重大事件制定应急响应计划。

应急响应计划应涵盖的SPIM重大事件应包括但不限于以下情况：

– IM服务器的打击SPIM数据库遭修改、入侵或控制；

– SPIM投诉平台遭修改、入侵或控制；

– 自动注册功能的门限值遭非法修改；

– 针对SPIM的大规模投诉在特定时间内发起。

IM SP应根据实际情况确定每个SPIM事件的类型和级别，并针对每个类型和级别的SPIM事件制定应急响应流程和应急操作指南。

IM SP应建立重大SPIM事件的监控和预警机制，及时发现重大SPIM事件并通知相关人员。

IM服务提供商还应在应急处置后总结SPIM重大事件的原因，评估应急措施的有效性并及时纠正问题。

7.5 风险评估管理

IM SP应对SPIM事件的可能性和严重性进行风险评估。风险管理应置于基本操作活动之下，范围涉及管理评估，安全评估和功能评估。风险评估管理应包括但不限于以下内容。

– IM SP应进行管理评估，包括制定打击SPIM的政策，检查是否有安全合规流程和策略用以降低SPIM风险并应促进政策的实施。IM SP还应根据组织定义的频率或在IM系统或操作环境发生重大变化时，审查并更新当前的风险评估政策和程序。

– IM SP应进行安全评估，评估内容应包括，通过使用标准自动执行漏洞管理流程（例如，列举应用程序缺陷和不正确的配置和格式化清单和测试程序），确定最有可能导致SPIM的原因（例如，密码漏洞、不安全的防火墙设置和特洛伊木马蠕虫），并量化重大SPIM事件的诱发条件。

– IM SP应进行功能评估，其中应包括发现IM系统升级时，IM系统代码中可能存在的不合逻辑的处理和级联错误（例如，自动用户注册、给定时间段内用户发送速率不受限制、缺乏内置安全机制和通过不安全的传递渠道泄露消息）。

– IM SP应定期开展风险评估，或在必要时审查和更新其风险评估政策。风险评估应包括三个相互关联的组成部分：管理、安全和功能评估。例如，管理和安全评估应与一般风险评估一起进行，功能评估应在IM系统升级之前、期间进行或两者兼用。与此同时，IM SP应修复组织定义的响应时间中的合法缺陷，或者实施控制以防止垃圾邮件散播者利用该漏洞。

7.6 安全保护措施

IM SP应采取安全保护措施打击SPIM。安全保护措施应包括但不限于以下内容。

– IM SP应部署反分布式拒绝服务攻击措施，以保护黑名单库、投诉平台、安全监控和审计方法并提高打击SPIM功能的可用性。

– IM SP应部署防病毒、防木马和防蠕虫措施，以防止服务器被垃圾邮件散播者感染和控制，垃圾邮件散播者会先修改打击SPIM的配置或禁用打击SPIM的功能，然后再发送SPIM。

– IM SP应在IM系统的网络边界、系统和应用程序中实施多种访问控制方法，以防止垃圾邮件散播者进行未经授权的访问。垃圾邮件散播者会先修改打击SPIM的配置或禁用打击SPIM的功能，然后再发送SPIM。

– IM SP应部署入侵检测和保护方法，以检测网络攻击，并防止IM系统遭垃圾邮件散播者入侵，垃圾邮件散播者会先修改打击SPIM的配置或禁用打击SPIM的功能，然后再发送SPIM。

8 IM用户功能支持打击SPIM

IM用户应有可能配置IM客户端，以防止在使用IM系统时出现SPIM。该配置应包括但不限于以下内容。IM用户应可能：

– 使用验证确认机制，包括验证请求的确认和添加组确认，以确保用户批准所有操作。

– 可以通过设置配置，禁止接收来自未授权用户的消息或文件。

– 及时配置黑名单，并且禁止接收来自可疑账户的消息或文件。

– 使用强密码并定期更改，以防止账户被盗并用于发送SPIM。

– 监控特权功能的执行，同时禁用并更改已实施的可能导致SPIM设置（例如，接受陌生人的身份验证请求）。

9 服务提供商/网络运营商应对SPIM的导则

服务提供商或网络运营商（SP/NE）可通过建立统一的SPIM投诉平台、建立统一的黑名单数据库，防范SPIM、测试并验证IM系统的打击SPIM功能，为IM SP提供SPIM检测服务，帮助打击SPIM。这其中包括但不限于以下内容。

– SP/NE应为多种IM服务建立统一的投诉平台。投诉平台可以接受用户关于SPIM发送账户的投诉，并根据不同的IM服务对投诉进行分类。当针对某个IM账号的投诉用户数量达到一定数量后，该IM账号的详细信息会被送交对应的IM服务黑名单数据库。

– 服务提供商/网络实体应为多个IM服务建立统一的黑名单数据库。黑名单数据库与网络中各IM服务的黑名单数据库同步。黑名单有两个来源，包括在数据库中的账户如下：

  • 通过上述投诉平台纳入投诉针对的账户；

  • 通过SPIM检测服务检测到的SPIM发送账户。

– 服务提供商/网络实体应为IM SP提供定期拨号测试验证服务，防止IM系统中的打击SPIM功能因黑客攻击而关闭。如果验证后没有开启相应功能，SP/NE可以向IM SP发送报警。拨号测试验证功能包括但不限于以下内容，以模拟：

  • 自动注册行为，并验证IM系统是否能够识别和阻止自动注册；

  • 某账户在某一时间单位内发送多条消息（消息数量超过IM系统设置的门限值），验证IM系统是否能够检测并丢弃该账户后续发送的消息；

  • 黑名单账户发送消息，验证IM系统是否可以丢弃该账户发送的消息；

  • 恶意投诉，验证IM系统是否能够识别并丢弃这些恶意投诉。

– 服务提供商/网络实体可以为IM SP提供SPIM检测服务。他们应与每个IM SP签署服务水平协议，其中应包括保护用户隐私的保密条款。检测SPIM SP/NE的过程如下：

  • 在网络关键节点部署检测系统，在IM SP授权下检测IM报文包头；

  • 分析IM账户发送多条IM消息的行为。如果IM账户在一定时间范围内发送的消息数量超过一定门限值，则可以确定该账户正在发送SPIM；

  • 直接丢弃上述账户发送的IM；

  • 将上述账户纳入黑名单数据库。

通过SP/NE提供的SPIM检测服务，可以在边缘附近找到并丢弃SPIM，既节省了网络带宽，又避免了IM服务器资源的消耗。

参考文献

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications*.

[b-IETF RFC 3428] IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging*. https://tools.ietf.org/html/rfc3428

ITU-T 建议书系列

系列 A	ITU-T 工作的组织
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	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
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，以及相关联的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
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	用于电信系统的语言和一般软件问题

瑞士印刷
2021年，日内瓦