

ITU-T 스팸 대응 기술 국제표준화 동향

박 소 영*, 강 신 각**

요 약

본 고는 ITU-T SG17 Q.5 "Countering spam by technical means"에서의 스팸 대응 기술 표준화 현황을 정리한다. Q.5/17에서의 스팸차단기술 표준화는 주로 이메일 스팸, IP 멀티미디어 스팸, 모바일 단문메시지서비스 스팸을 대상으로 하며, 스팸 차단을 위한 상위 수준의 개요 표준, 기술 프레임워크 표준 및 기술 기법에 대한 표준 개발이 이루어지고 있다.

I. 서 론

스팸(spam)이란 일반적으로 발송자의 재화나 영역의 판매 촉진을 위한 상업적인(commercial) 내용으로 수신자가 원하지 않음에도(unsolicited) 불구하고 불특정 다수에게 대량으로(bulk) 전송되는 메시지를 의미한다. 가장 널리 알려진 형태의 스팸은 이메일(email) 스팸이며, 인스턴트 메시징(instant messaging) 스팸, 유즈넷 뉴스그룹(Usenet newsgroup) 스팸, 블로그(blog) 스팸, 이동전화 메시징 스팸 등 다른 미디어 상에서 발생하는 비슷한 형태의 메시지도 스팸으로 분류될 수 있다. ITU-T 권고 X.1240에서는 스팸을 다음과 같이 정의하고 있다: The meaning of the word "spam" depends on each national perception of privacy and what constitutes spam from the national technological, economic, social and practical perspectives. In particular, its meaning evolves and broadens as technologies develop, providing novel opportunities for misuse of electronic communications. Although there is no globally agreed definition for spam, this term is commonly used to describe unsolicited electronic bulk communications over e-mail or mobile messaging for the purpose of marketing commercial products or services.[1].

스팸은 재화나 서비스를 광고하기 위한 상업적인 목

적으로 주로 이용되어 왔으나, 근래에는 피싱(phishing)과 같이 사기에 이용되거나, 바이러스의 유포에 이용되는 등 스팸으로 인한 피해가 더욱 심각한 상황에 이르렀다. 이에, 여러 국가, 국제기구 및 산업체 등은 다양한 종류의 스팸을 효과적으로 차단하기 위하여 다음과 같이 여러 측면에서의 대응 방안을 모색해 오고 있다.

- 규제(regulation)
- 기술(technology)
- 산업체 활동(industrial action)
- 국제적 협력(international cooperation)
- 교육(education)

이 중에서 본 고에서는 ITU-T를 중심으로 이루어지고 있는 스팸 대응 기술의 국제표준화 동향에 대해서 살펴본다.

II. 개요

2004년 10월 브라질에서 개최된 세계전기통신표준회의(WTSA 2004)에서는 ITU-T에서의 스팸 차단을 위한 기술표준 개발의 필요성을 인정하고, SG17 "Security"를 중심으로 ITU-T 내 관련 연구반(SG, study group)에서 스팸을 차단하기 위한 기술 표준을 개발하도록 지시하는 결의안(Resolution) 52 "Countering and combating spam"을 채택한 바 있다. 이와 같은 결의안의 채택과 한국, 중국 등의 적극적인 표준

본 연구는 지식경제부의 지원을 받는 정보통신표준기술력향상사업의 연구결과로 수행되었습니다.

* 한국전자통신연구원 표준연구센터 (bubble@etri.re.kr)

** 한국전자통신연구원 표준연구센터 (sgkang@etri.re.kr)

기고 활동으로 다양한 종류의 스팸을 차단하기 위한 기술표준의 개발을 주된 목적으로 하는 연구과제인 Q.17 "Countering spam" (현 Q.5 "Countering spam by technical means")가 구성되었다. Q.5/17에서 개발된 혹은 개발 중인 표준권고들 간의 관계성 구조는 [그림 1]과 같다.

Q.5/17는 중국의 Hongwei Luo(CATR of MIIT)가 라포처(rapporteur), 한국의 윤석용 책임연구원(KISA)이 공동 라포처(associate rapporteur)의 역할을 수행하고 있으며, 한국, 중국, 일본, 독일, 미국, 프랑스 등의 국가에서 권고 개발 작업에 참여하고 있다.

Q.5/17에서 개발되는 권고는 스팸 차단을 위한 상위 수준에서의 기술적 전략을 기술하는 X.1231 "Technical strategies for countering spam"을 기반으로, 이메일 스팸, IP 멀티미디어 스팸, 그리고 이동전화에서의 단문메시지 스팸 차단을 위한 개요, 프레임워크 및 기술방안(technical means)을 정의하는 표준을 개발하고 있다. 더불어, 모든 종류의 스팸 차단을 위하여 공통적으로 적용될 수 있는 게이트웨이 시스템에 관한 표준 및 스팸 위협에 관하여 기술한 부속서(Supplement) 등이 개발되고 있다.

Q.5/17에서 개발되는 모든 권고는 스팸을 차단하기 위한 기술적 방법 외에도 각 국가의 규제 및 정책 측면

과 연관될 수 있다는 판단 하에, 권고 승인 절차는 TAP(traditional approval process)를 따르도록 하고 있다. 즉, 국가별 의견수렴(Determination) 후, 차기 회의에서 국제표준을 승인하는 절차를 따르고 있다.

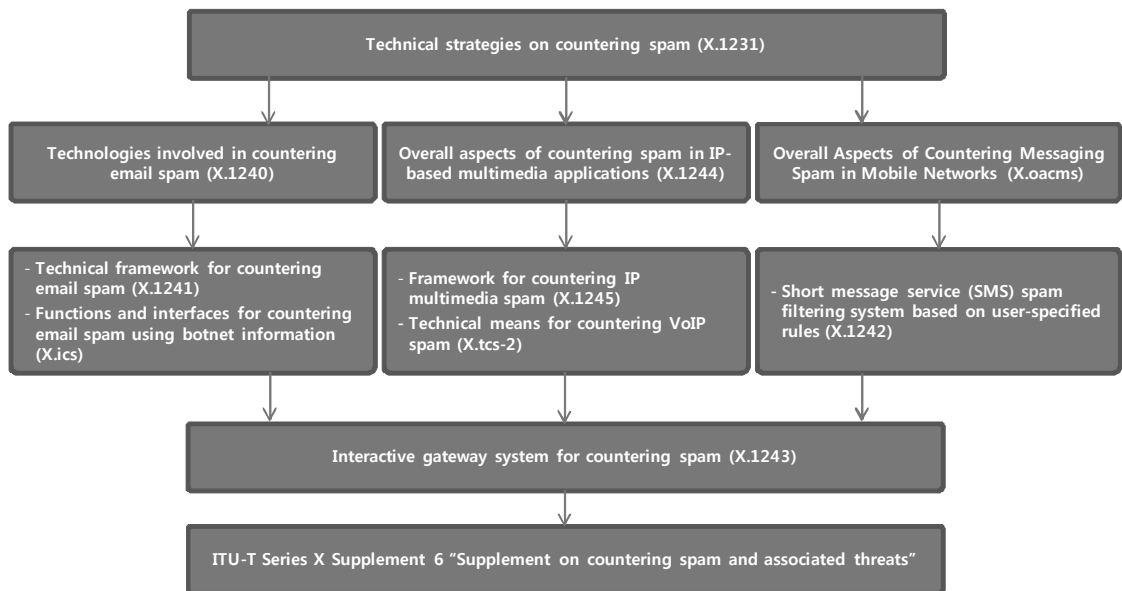
III. 스팸 차단 기술 전략 표준화

Q.5/17에서 개발되는 권고 중 가장 상위 수준에서의 기술전략 및 고려사항을 담고 있는 X.1231 "Technical strategies for countering spam"은 2008년 4월에 최종 승인이 이루어졌다.

이 권고는 스팸을 차단하기 위한 기술적인 전략을 제시하고 스팸의 일반적인 특성 및 스팸을 차단하는 목적 등에 관하여 기술한다. 더불어, 하나의 솔루션만으로는 스팸을 효과적으로 차단하기 어렵다는 것을 인정하고 스팸을 차단하기 위한 효과적인 방법을 평가하기 위한 체크리스트를 제공한다[3].

IV. 이메일 스팸 차단 기술 표준화

이메일 스팸 차단 기술과 관련된 권고로는 이메일 스팸을 차단하기 위한 기법들에 대하여 소개하는 X.1240 "Technologies involved in countering e-mail spam",



(그림 1) Structure of Q.5/17 Recommendations (2)

이메일 스팸을 차단하기 위한 기술 프레임워크를 정의하는 X.1241 “Technical framework for countering email spam”의 개발이 완료되었고, 봇넷(botnet) 정보를 이용한 이메일 스팸 차단 기법을 소개하는 권고초안 X.ics “Functions & interfaces for countering email spam using botnet information”이 개발 중에 있다.

X.1240 “Technologies involved in countering e-mail spam”은 Q.5/17의 설립 초기부터 개발이 이루어진 권고로, 2008년 4월에 최종 승인이 이루어졌다. X.1240은 이메일 스팸 차단 솔루션을 개발하고자 하는 이용자에게 가이드와 정보를 주기 위한 목적으로 개발된 권고로, 이메일 스팸의 기본적인 개념, 특성 및 영향, 이메일 스팸 차단을 위한 기술에 대하여 소개한다. 또한, 이메일 스팸 차단 솔루션, 이메일 스팸 차단을 위한 여러 표준기구 및 관련 기구들의 활동에 대해서 기술한다. 이 권고는 이메일 스팸 차단을 위한 프레임워크 및 기술기법 표준을 개발하는 데 있어 기반(baseline) 표준으로 활용될 수 있다[1].

X.1241 “Technical framework for countering email spam”은 이메일 스팸 차단을 위한 기술 프레임워크를 제안하는 권고로 2008년 4월에 최종 승인이 이루어졌다. 이 프레임워크는 스팸 차단을 실행하는 도메인 구조를 제안하고, 그 내부의 주요 모듈에 대한 기능을 정의한다. 이 프레임워크의 핵심은 서로 다른 이메일 서버 간에 이메일 스팸에 관한 정보를 공유하는 메커니즘을 가진다는 것이다. 따라서 이 권고에서 제안하는 프레임워크에 따라 설계된 시스템은 상호연동을 통하여 스팸 차단 효과를 향상시킬 수 있을 것으로 기술되고 있다[4].

X.ics “Functions & interfaces for countering email spam using botnet information”는 봇넷 정보를 이용하여 이메일 스팸을 차단하기 위한 기능 및 인터페이스를 정의하는 권고초안으로, 한국인터넷진흥원(KISA) 임채태 팀장(책임연구원)이 에디터를 맡아 개발을 진행하고 있다. 이 권고초안에서는 봇넷에 의해 전달되는 이메일 스팸을 차단하기 위한 일반적인 구조를 제안하고, 그 구조에서 요구되는 기능 및 인터페이스에 대하여 기술한다. 이 권고는 X.1243에서 정의하는 스팸 차단 게이트웨이 시스템에 부합한다고 밝히고 있다[5]. 최근 X.ics의 개발이 지연됨에 따라, 권고 개발을 위한 보다 적극적인 기고 활동이 촉구되고 있다.

V. IP 멀티미디어 스팸 차단 기술 표준화

ITU-T Q.5/17이 처음 설립되었을 때는 이메일 스팸 차단 기술표준을 개발하는 데에 초점을 두고 있었으나, SPIT(spam over Internet telephony), SPIM(spam over instant messaging) 등 다양한 IP 멀티미디어 응용 상에서의 스팸이 새로운 위협으로 떠오르는 것을 인정하고 IP 멀티미디어 스팸의 차단을 위한 기술표준 개발을 병행하기로 하였다.

X.1244 “Overall aspects of countering spam in IP-based multimedia applications”는 한국의 제안으로 Q.5/17의 IP 멀티미디어 스팸 차단 표준 시리즈 중 제일 먼저 제안된 권고로 2008년 9월에 최종 승인이 이루어졌다. X.1244에서는 타 권고에서의 스팸 정의를 참고하여 IP 멀티미디어 스팸을 다음과 같이 정의하고 있다. IP 멀티미디어 스팸은 IP 멀티미디어 응용 상에서 발생하는 원하지 않는 형태의 메시지 또는 호를 말한다. 기존 이메일 스팸과 구분하여, IP 멀티미디어 스팸은 인스턴트 메시징, 프레즌스, 또는 VoIP(voice over IP) 서비스와 같이 IP 상에서 새롭게 등장하는 전기통신 방식에서 생성되는 스팸을 지칭한다 (unsolicited messages or calls through IP multimedia applications. To distinguish this from traditional e-mail spam, IP multimedia spam denotes spam on newly emerging telecommunication methods over IP, such as instant messaging (IM), presence, or voice over IP (VoIP) services.)([6].

X.1244는 다음과 같은 내용을 포함한다.

- IP 멀티미디어 스팸의 기본 개념, 특성 및 스팸 차단을 위한 기술 이슈 현황
- IP 멀티미디어 응용 스팸을 특성에 따라 분류하고 각 그룹에 속하는 스팸이 가지는 특성 정의
- IP 멀티미디어 스팸을 유발할 수 있는 다양한 보안 위협 정의
- 기 개발된 이메일 스팸 차단 기법 및 IP 멀티미디어 스팸에의 적용성 분석
- IP 멀티미디어 스팸 차단을 위한 고려사항

X.1245 “Framework for countering spam in IP-based multimedia applications”은 X.1244에서 정의하는 IP

멀티미디어 스팸에 대한 대응 프레임워크를 제안하는 표준으로 한국 주도 하에 2010년 12월에 최종 승인이 이루어졌다. X.1245는 IP 텔레포니, 인스턴트 메시징, 멀티미디어 컨퍼런스 등 다양한 IP 멀티미디어 응용 상에서 발생하는 스팸 차단을 위한 일반적인 구조를 제안한다. 여기에서 제안하는 스팸 차단 프레임워크는 4개의 스팸차단 기능으로 구성되어 있다. 중앙 스팸차단 기능(core anti-spam functions; CASF), 착신측 스팸차단 기능(recipient-side anti-spam functions; RASF), 발신측 스팸차단 기능(sender-side anti-spam functions; SASF), 그리고 착신자 기능(spam recipient functions; SRF)이 그것이다. 이 권고는 IP 멀티미디어 스팸을 차단하는 데 있어 이들 기능의 역할, 절차 및 인터페이스에 대하여 기술한다[7].

IP 멀티미디어 스팸을 차단하기 위한 구체적인 기술 기법을 제안하는 권고 중 하나로, VoIP 스팸 차단 기법을 제안하는 X.tcs-2 “Real-time blocking list (RBL)-based framework for countering VoIP spam”가 개발되고 있으며, 한국인터넷진흥원(KISA) 윤석용 책임연구원이 에디터를 맡아 개발을 주도하고 있다. 이 권고 초안은 리스트 기반의 이메일 스팸 차단 기법을 응용한 RBL(real-time blocking list) 기반의 VoIP 스팸 차단 프레임워크를 제공한다. 이 프레임워크는 다음의 4가지 기능 요소를 포함한다; VoIP 스팸 차단 시스템(VoIP spam prevention system; VSPPS), VoIP 스팸 차단 정책 서버(VoIP spam prevention policy server; VSPPS), VoIP 스팸 차단을 위한 RBL 센터 시스템(RBL centre system for VoIP spam prevention; VSP-RBL), 이용자 명성 시스템(user reputation system; URS). 권고 초안에서는 이들 기능 요소의 역할, 동작 절차 및 인터페이스 등에 대하여 기술한다. 이 권고 초안은 IP 멀티미디어 스팸 차단 기술 권고 시리즈 중 하나로서 개발되고 있으며, 따라서 X.1244 및 X.1245의 내용에 부합한다고 밝히고 있다[8]. 이 권고 초안은 2011년 4월에 제네바에서 개최되는 ITU-T SG17 회의에서 determination을 추진할 예정이며, 금번 회의에서 determination이 이루어질 경우 2011년 8월에 제네바에서 개최되는 SG17 회의에서 최종승인(decision)이 추진될 예정이다.

VI. 메시징 스팸 차단 기술 표준화

Q.5/17에서는 이메일 스팸 및 IP 멀티미디어 스팸과

더불어, 이동전화 단문메시지서비스(short message service; SMS) 상에서 발생하는 스팸을 차단하기 위한 권고의 개발이 진행되고 있다.

X.1240 및 X.1244와 마찬가지로 상위 수준에서 모바일 네트워크에서의 메시징 스팸 차단 기술에 관한 개요 표준으로 X.oacms “Overall aspects of countering messaging spam in mobile networks”가 개발되고 있다. 이 표준은 2010년 4월 제네바에서 개최된 SG17 회의에 새로운 표준화 항목(new work item)으로 제안되어 동의가 이루어졌으며, 중국의 Linlin Zhang(MIT)이 에디터를 맡아 개발을 주도하고 있다. 이 권고 초안은 메시징 스팸의 현황, 메시징 서비스의 분류 및 특성, 메시징 스팸의 종류 등 메시징 스팸의 전반적인 사항을 제공하지만, 단문메시지서비스 및 멀티미디어메시지서비스(multi-media message service; MMS) 스팸만을 권고 초안의 범위로 한다. 이 외에도 본 권고 초안에서는 메시징 스팸 차단을 위한 여러 표준화기구에서의 활동 내용, 메시징 스팸 차단 기술 및 메커니즘의 소개와 비교 분석 결과를 소개하고, 모바일 네트워크에서 메시징 스팸을 차단하기 위한 새로운 솔루션을 제안하는 것을 목적으로 한다[9].

X.1242 “Short message service (SMS) spam filtering system based on user-specified rules”는 이용자 규칙 기반의 SMS 스팸 차단 기법을 제공하는 권고로, 중국의 주도적인 참여 하에 2009년 2월에 최종 승인이 이루어졌다. 이 권고는 이용자별로 설정된 규칙에 기반을 두어 SMS 스팸을 필터링하는 시스템의 구현을 위하여 개발되었다. 이 권고는 SMS 스팸 필터링 시스템의 구조, SMS 스팸 필터링 기능, 이용자의 서비스 관리 방법, 관련된 통신 프로토콜 및 SMS 기능을 가지는 단말에 대한 기본 기능 요구사항에 대하여 기술하고 있다[10].

VII. 스팸 차단 기법 표준화

앞에서 이메일 스팸, IP 멀티미디어 스팸, SMS 스팸 차단을 위한 기술 고려사항 및 프레임워크 등을 제공하는 권고 및 권고 초안을 소개하였다. Q.5/17에서는 이와 같이 특정 형태의 스팸을 차단하기 위한 기술뿐만 아니라 모든 종류의 스팸을 대상으로 하는 권고 개발이 이루어지고 있으며, 이런 표준화 활동의 일환으로 X.1243 “Interactive gateway system for countering spam”의

개발이 2010년 12월에 완료되었다.

이 권고는 다양한 종류의 스팸을 차단하기 위한 상호 작용 게이트웨이 시스템을 정의한다. 이 게이트웨이 시스템은 착신자의 게이트웨이가 발신자의 게이트웨이로 스팸 통지(spam notification)를 할 수 있도록 함으로써 스팸 트래픽이 네트워크를 통해 전달되는 것을 막는다. 이 권고는 이와 같은 스팸 차단 게이트웨이 시스템의 구조를 정의하고, 시스템 내의 기본 구성요소, 프로토콜 및 기능에 대하여 기술하며, 스팸 발견, 스팸 차단 정보 공유, 그리고 게이트웨이 시스템의 스팸 차단 동작에 대한 메커니즘을 제공한다[11].

앞서 소개된 권고 외에도 스팸 차단을 위한 여러 국가 및 표준화기구에서의 관련 활동에 대한 정보를 제공하는 ITU-T X.1240 series - Supplement on countering spam and associated threats가 2009년 9월에 개발된 바 있다. 이 부속서는 스팸에 효과적으로 대응하기 위해서 효과적인 규제, 기술, 서비스 이용자 및 사업자의 교육 등 다양한 측면에서의 접근법이 적용될 필요가 있다고 언급하고 있다[12].

VIII. 결론

사업적인 목적의 내용을 담은 이메일 스팸이 대부분이었던 과거와는 달리, 근래에 발생하는 스팸은 이용하는 미디어가 다양해짐에 따라 기술적으로 차단이 어려울 뿐만 아니라, 스팸의 목적이 변질됨에 따라 스팸으로 인한 피해가 더욱 심각해지고 있다. 이에 따라 서비스 제공업자, 기술 개발자 등 관련 주체들은 하나의 스팸 차단 기술이나 솔루션만을 통해서도 효과적으로 스팸을 차단할 수 없다는 것에 인식을 같이하고 있다. 이에 따라 개별 스팸 차단 기술에 대한 권고 개발과 함께, 이러한 기술의 복합적인 도입과 상호작용에 대한 기술 검토 또한 함께 이루어지는 것이 바람직한 것으로 판단된다. 더불어 Q.5/17 설립 초기에 논의되었던 연구항목의 역할을 다시 상기하여 피싱 등과 같이 서비스 이용자에게 막대한 피해를 주는 사기성 스팸 대응을 위한 권고 개발을 진행할 지에 대한 검토가 필요한 것으로 생각된다.

참고문헌

- [1] ITU-T Recommendation X.1240 "*Technologies involved in countering e-mail spam*", April 2008.
- [2] ITU-T TD 1440 Rev.3, "Report of Q.5/17", Dec. 2010.
- [3] ITU-T Recommendation X.1231 "*Technical strategies for countering spam*", April 2008.
- [4] ITU-T Recommendation X.1241 "*Technical framework for countering email spam*", April 2008.
- [5] ITU-T TD 1280 "Proposal for revised draft text for X.ics : Functions & interfaces for countering email spam using botnet information", January 2011.
- [6] ITU-T Recommendation X.1244 "*Overall aspects of countering spam in IP-based multimedia applications*", September 2008.
- [7] ITU-T Recommendation X.1245 "*Framework for countering spam in IP-based multimedia applications*", December 2010.
- [8] ITU-T TD 1424,"Proposal for the 4th revised text on ITU-T draft Recommendation X.tcs-2: Real-time blocking list (RBL)-based framework for countering VoIP spam", December 2010.
- [9] ITU-T TD 1464 Rev.2 "Updated text of X.oacms: Overall aspects of countering messaging spam in mobile networks", December 2010.
- [10] ITU-T Recommendation X.1242 "*Short message service (SMS) spam filtering system based on user-specified rules*", February 2009.
- [11] ITU-T Recommendation X.1243 "*Interactive gateway system for countering spam*", December 2010.
- [12] ITU-T X.1240 series Supplement "*Supplement on countering spam and associated threats*", September 2009.

〈著者紹介〉

사 진

박 소 영 (Soyoung Park)

1999년 2월: KAIST 산업공학과 졸업
 2001년 2월: KAIST 산업공학과 석사
 2001년 1월~현재: 한국전자통신연
 구원 선임연구원
 관심분야: 통신비밀보호, 스팸대응,
 감청정책

**강 신 각 (Shingak Kang)**

1984년 2월: 충남대학교 전자공학과
 졸업
 1987년 8월: 충남대학교 전자공학과
 석사
 1998년 2월: 충남대학교 전자공학과
 박사
 1984년 3월~현재: 한국전자통신연
 구원 표준연구센터 팀장(책임연구원)
 관심분야: VoIP, IPTV, 멀티캐스트,
 통신비밀