스팸 메일 차단 방법론 비교·분석

*김자경, **이광수
숙명여자대학교, 숙명여자대학교
*yewon206@hanmail.net **rhee@cs.sookmyung.ac.kr

An analysis of anti-spam solutions

*Kim Ja Kyung, **Gwangsoo Rhee
Sookmyung Women's University

요약

스팸 메일의 정의와 피해 현황을 살펴보고, 스팸 메일의 제도적·기술적인 규제 방법을 알아본다. 기술적인 규제 방법은 메일 클라이언트/서버 차원의 스팸 방지 방법, ASRG에서 제안한 메일 프로토콜과 헤더를 이용한 스팸 규제 방법, 온라인 우표제를 통한 스팸 규제 방법이 있다. 살펴본 규제 방법들을 분류해보고, 결론과 향후 연구 과제를 제시한다.

제 1 장 스팸 메일 현황

1.1 스팸 메일의 정의

스팸 메일에 대한 일반적 정의를 살펴보면, 스팸 메일은 '발송자의 재화나 용역의 판매 촉진을 위한 상업적(Commercial)인 내용으로 수신자가 원하지 않음에도(Unsolicited) 불구하고 불특정 다수에게 대량(Bulk)으로 전송되는 이메일' 이라고 할 수 있다. 이러한 의미에서 학문적 연구나 공식적 표현은 UBE(Unsolicited Bulk E-mail), UCE(Unsolicited Commercial E-mail), UCBE(Unsolicited Commercial Bulk E-mail)를 사용하고 있다. 그러나 수신자가 원하는지, 원하지 않는지에 대한 판단과 상업성/대량성의 판단 기준이 구체적으로 명확하게 확립되지 않아 스팸 메일에 대한 판별은 쉬운 일이 아니다.

1.2 스팸 메일의 피해 현황

2004년 2월 19일 국내 IT(정보기술)업체들에 따르면 지난해 국내에서 발송된 이메일중 80~90%가 바이러스메일 등을 포함한 스팸 메일로 집계됐다. 이는 스팸 메일 필터링업체인 메시지랩스가 전 세계적 스팸 메일 비율로 밝힌 62.7%보다 훨씬 높은 수준이다. 코넷과 메가패스 등의 메일서버를 운영하는 KT는 지난해의 스팸 메일 양을 집계한 결과 모두 28억 6457만여건의 이메일이 발송됐고 이중 스팸으로 구분돼 발송되기 전에 차단된 메일이 81.4%인 23억3304만여건에 달했다. 데이콤도 지난해 4분기 전체 이메일 가운데 80%를 스팸 메일로 분류해 메일서버에서 차단한 것으로 나타났다. 이러한 상황은 포털업체도 마찬가지다. 야후코리아는 하루 60만통 발송되는 이메일의 10%인 5만4000통만 정상메일로 분류하고 있고, 이메일 발송량이 가장 많은 다음커뮤니케이션도 하루 10% 가량만 정상메일로 분류, 나머지를 차단하고 있다[1]. 이처럼 스팸 메일이 사실상 통제수위를 넘어서면서 바이러스 메일로 인한 피해 등 갖가지 부작용이 발생하고 있어 대책마련을 요구하는 목소리가 커지고 있다.

제 2 장 스팸 메일 대책

2.1 스팸 메일의 제도적인 규제 방법

정통부는 불법 스팸 메일에 대해 과태료를 현행 1000만원에서 최고 3000만원으로 올리고, 법률 체계상 효율적인 스팸 규제를 위해서 현행 스팸 규제에 관한 법률을 단일 법률로 제정할 것을 고려하고 있다. 또한 기존의 '옵트-아웃' 방식에서 벗어나 수신자 사전 동의가 있어야만 스팸 메일을 보낼 수 있는 '옵트-인' 제도의 도입을 검토하고 있으며, 청소년 보호대책으로 청소년 명단을 데이터베이스화해 성인 인증을 강화하고 어린이 전용 도메인의 도입을 추진 중이다.

2.2 스팸 메일의 기술적인 규제 방법

스팸 메일의 기술적인 규제 방법으로는 메일 클라이언트에서 차단하는 방법, 메일 서버에서 차단하는 방법, 메일 프로토콜을 사용하는 방법, 온라인 우표제를 이용하는 방법 등이 있다. 클라이언트 차원의 방지는 사용자 측에서 취할 수 있는 형태로 메일을 받아보는 프로그램인 핫메일, 한메일, 아웃룩등에서 제공되는 기능인데, 특정 단어의 필터링, 수신거부 리스트에 등록된 메일 주소에 대한 수신거부 기능이 공통적으로 제공되고 있다. 또한 여러 스팸 메일 차단 프로그램을 이용하는 방법이 있는데, 메일 필터링이 보다 세밀해서 자칫 정보성 메일까지 차단할 우려가 있는 이메일프로그램에서 제공되는 스팸 차단 기능에 비해, 보다 강력한 스팸 메일 차단 효과가 있다. 본 논문을 위해 사용한 스팸 차단 프로그램은 디스패머, 스팸인스펙터, 스팸터미네이터, 스팸 솔터 네 종류인데, 기본적으로 POP3와 IMAP을 지원하고 있다. 디스패머는 팝업 차단 기능, 악의성 있는 단어는 와일드카드로 대체하는 독자적인 특

징을 갖고 있으며, 스팸 인서펙터는 아웃룩 내에 통합되어 아웃룩이 갖고 있는 스팸 메일 차단 기능과 함께 사용할 수 있는데 특정 국가를 차단하는 기능이 포함되어 있다. 스팸 터미네이터는 네가지 프로그램 중 유일하게 웹 메일을 지원하고 있으며 컴퓨터 내의 음란 이미지 검색도 가능하고 인터넷 사용시간을 제어할 수 있는 독자적인 기능이 있다. 스팸 솔터는 송신자, 메일제목, 본문내용, 메일헤더, 특정국가별로 필터를 마련해 가장 강력한 필터링 옵션을 제공한다.

서버 차원의 방지는 메일 서버의 운영자가 취할 수 있는 방법으로 인터넷서비스사업자에게 권리를 부여하여 서버차원의 필터링, 스팸 신고란 운영 등이 있다. 이것은 개인 PC 차원에서 스팸 메일을 걸러내는 것이 아니라 아예 서버 차원에서 스팸 메일을 받지 않도록 하는 기법이다.

ASRG(Anti Spam Research Group)에서 제안하는 스팸 메일 규제 방법들은 기존의 스팸 차단 메일 관련 프로토콜을 수정·보완한 것으로 주로 MIME 헤더와 SMTP 프로토콜을 이용한다[6]. 본 논문에서는 제안된 인터넷 드래프트 문서 중 CRI(Challenge/Response Interworking) 프로토콜과 LMAP(Lightweight MTA Authentication Protocol)을 살펴보겠다. CRI 프로토콜은 '동의에 기반한 통신' 으로 송신자에 대한 인증을 제공하고 의도된 수신자에게 메시지를 전송했는지 확인해준다. SMTP는 이메일의 근원지나 송신자에 대한 인증 과정이 없으나, CRI 프로토콜은 송신자의 이메일 주소를 이용하여 수신자가 보낸 'challenge' 메시지를 받은 송신자만이 응답할 수 있어 송신자 인증과 메시지 인증을 제공한다. MIME 헤더에 송신자의 메일주소, 수신자의 메일주소, C/R 메세지의 타입(challenge, response, informational), C/R 레벨(1-sender, 2-message, 3-turing test), C/R 토큰, C/R 시스템의 신원확인, 송신자가 'challenge' 메세지에 대해 몇 번이나 응답해야만 하는지, 응답했다면 다시 'challenge' 메세지가 올 때까지 화이트 리스트에 얼마나 오래 그 주소가 존재할 것인지 등의 정보가 정의된다. 또한 SMTP의 확장형 프로토콜인 ESMTP를 이용하여 작동할 수 있다. LMAP 역시 이메일 송신자에 대한 인증을 제공하는 프로토콜인데, 인터넷서비스 사업자가 블랙리스트의 IP주소를 공시하면, 수신 MTA는 데이터를 적용해 판단하는 것이다. 따라서 인증된 도메인에서 보낸 메일인지 수신자가 판단할 수 있다. LMAP은 어떤 메일이 인증된 주소에서 온 것인지에 관한 데이터를 분배하기 위해 DNS를 사용한다. 또한 ESMTP의 'MAIL FROM' 커맨드를 수정해서 작동할 수 있다.

메일 클라이언트나 서버 차원의 차단은 스팸을 거절하는 사람들의 개입이 필요했으나, 온라인 우표제는 송신자 지불 체계로 스패머들에게 스팸의 비용을 부담시킴으로써 스패머의 부담을 가중시킨다. 스팸을 받음으로써 초래되는 불편함보다 우편 요금을 지불하는 불편함이 덜하다는 생각에서 출발하였는데, 우리나라에선 온라인 우표제와 관련한 많은 논란이 있어왔다. 실제로 온라인 우표제를 시행하고 있는 다음커뮤니케이션의 경우, 온라인 우표제 때문에 다음 메일 주소로는 가입이 안 되는 곳이 많아 가입 회원들의 불편함이 초래되고 있다. 온라인 우표제는 이용 요금을 부과하는 방법에 따라 크게 '금전성 우표' 와 '작업성 우표' 두 가지 방식이 있다[7, 8]. 본 논문에서 살펴볼 '금전성 우표' 의 예는 www.mail-net.com/spam 에서 제안한 E-Postage Fees를 살펴볼 것이고, '작업성 우표' 의 예로 마이크로소프트사의 Penny Black Project를 살펴볼 것이다. 먼저 E-Postage Fees는 온라인 우표에 대해 금전상의 우편 요금을 부과하자는 것이다. 우표 요금의 결정은 수신자에게 있고, 지불된 요금을 받게 되는 사람도 수신자가 된다. 이때 이메일 주소의 리스트가 필요한데, 각 이메일 주소에 대한 우표 요금을 수신자가 결정하는 것으로 자신의 친구나 호의적인 도메인에 대해서는 요금을 무료로 결정할 수 있다. 작동 과정을 보면, 메일 헤더의 FROM 주소를 검사해서 수신자가 제시한 우표 요금에 부합할 경우엔 메시지를 받게 되고, 요금에 미달한 경우에 발신자는 'Insufficient E-Postage' 라는 통보를 받게 된다. 이때 우표 요금은 어음교환소를 통해 지불하게 된다. '금전성 우표' 의 경우 전자 지불의 한 형태이기 때문에 세계적인 소액 전자 지불 시스템에 대해 그 기반 구조를 세우는 일이 우선시되고 이것은 큰 부담이 아닐 수 없다. 따라서 이메일 시스템에 대한 전체적인 변화가 요구된다는데 '금전성 우표' 의 문제점이 있다. '작업성 우표' 는 금전이 지불되지 않는 우표를 의미한다. '작업성 우표' 는 돈을 주고 우표를 사는 대신, 약 10초 정도 걸리는 수학 문제를 풀어 우표를 충전하는 방식이다. 즉 스패머들이 스팸을 보내려면 스팸을 보내기에 충분한 양의 우표를 충전하기 위해 더 많은 머신을 구입해야 할 것이고 결국 스팸 메일을 보내는 것을 포기할 수 밖에 없을 것이라는 생각이다. 마이크로소프트의 Penny Black Project의 경우 이 작업성 우표를 풀기는 어렵지만 증명하기는 쉬운 수학적인 퍼즐로 비유한다. 우표를 여러 개 발생시킬수록 소요되는 요금으로는 CPU 사이클, 메모리 사이클, 튜링 테스트 등이 있다.

제 3 장 스팸 규제 방법 분류

앞에서 살펴본 여러 스팸 규제 방법들을 사용되는 목적에 따라 분류할 수 있다. 제시된 방법들을 집단간 동의여부에 따라, 적용되는 범위에 따라 분류해본다. 또한 보다 다양한 계층의 욕구를 충족시켜 줄 수 있는 종합적인 방법을 생각해본다.

3.1 집단간 동의 여부에 따른 분류

메일 클라이언트에서 스팸 메일을 차단하는 방법은 개인의 기호에 맞게 필터링을 구성하면 되므로 집단간의 동의는 필요없다. 메일 서버에서 차단하는 경우도 마찬가지이다. 메일 서버의 운영자가 서버 차원에서 보다 적극적으로 메일을 통제하면 된다. 그러나 메일 프로토콜이나 온라인 우표제의 경우는 적용하기에 앞서 집단간의 동의가 우선적으로 필요하다. 또한 기존에 존재하는 시스템의 기반 구조를 수정하고, 송신자를 인증하기 위해 필요한 정보를 수집하는 과정도 요구된다.

3.2 적용 범위에 따른 분류

개인용으로 스팸 방지를 위해서는 메일 클라이언트 차원에서 이메일 프로그램의 스팸 차단 기능을 사용하거나, 보다 정확한 필터링을 위해 앞에서 소개된 여러 스팸 차단 프로그램을 사용할 수 있다. 기업이나 단체에서 사용하기 적합한 스팸 방지 방법은 메일 서버 차원에서 스팸 메일을 규제해 주는 것이다. 이러한 서버 차원의 규제 방법은 메일 서버에 들어오는 스팸뿐만이 아니라, 바이러스 감염으로 인해 외부로 바이러스가 유포될 위험이 있는 나가는 메일에 대해서도 스팸 여부를 판별해 주는 것도 요구된다. 이런 아웃바운드 방식이 적용되면, 이용자수가 많은 기업이나 단체에서 바이러스 확산 방지에 기여할 수 있다. 또한 사용자가 일일이 스팸 메일을 관리하는 시간과 불편함을 줄일 수 있다는 장점이 있다.

3.3 종합적인 대안 제시

과거 개인 PC차원에서 스팸 메일을 방지하는 방법이 많이 사용되었다면, 지금은 아예 서버 차원에서 스팸 메일을 방지하여 PC에 도달하지 못하도록 하는 방법이 점점 더 많이 사용되고 있다. 그러나 이메일 서비스제공업체들은 서버 차원의 필터링 외에도 개인 사용자가 이용할 수 있는 필터링 기법도 동시에 제공해야한다. 비교적 다양한 계층의 욕구를 만족시켜 주는 스팸 방지 방법으로는 온라인 우표제를 들 수 있을 것이다. 개인부터 기업체, 이메일서비스제공업체에게까지 적용되어 사용할 수 있고 수신자의 개입이 비교적 덜해 스팸 메일을 받음으로써 초래되는 불편함이 다른 방법에 비해 덜하다. 그러나 온라인 우표제가 정착하기 위해서는 제도적인 방법들이 우선적으로 요구된다. 다자간 협력 체계를 구축하여 블랙리스트나 스패머에 대한 추적 정보를 서로 공유하여 송신자에 대한 인증이 효과적으로 제공되어야 한다. 송신자 인증 기술은 기술적인 스팸 규제 방법의 핵심일 것이다. 이메일 발신자의 신뢰성을 측정하는 송신자 인증 방법은 모든 기술적인 스팸 규제 방법에 공통적으로 필요한 부분이기 때문이다.

제 4 장 결론 및 향후 연구 과제

스팸 메일은 광고성 메일, 음란성 메일, 바이러스 유포뿐만이 아니라 사이버 범죄에까지 악용되고 있다. 이러한 스팸 메일을 근절하기 위해서는 앞에서 살펴본 여러 가지 차단 방법과 더불어 메일 사용자 개개인의 자발적인 자정 노력과 정부 차원의 제도적인 규제가 필요할 것이다.

참고문헌 :

[1] 스팸 메일의 피해현황,
유상욱기자 파이낸셜뉴스 2004/2/19일자
[2] De-Spammer,
http://www.spinnerbaker.com/despamr.htm
[3] Spam Inspector, http://www.giantcompany.com
[4] Spam Terminator, http://www.spamterminator.co.kr
[5] Spam Sorter, http://www.spamsorter.com
[6] Anti Spam Research Group, http://asrg.sp.am
[7] 금전성 우표, http://www.mail-net.com/spam/#details
[8] 작업성 우표,
http://www.research.microsoft.com/research/sv/PennyBlack/