
스팸 메일에 대한 현황 분석 및 방지 기술에 대한 고찰

한 길 성 (서원대학교)

차 례

1. 서론
 2. 스팸메일이 증가하는 이유
 3. 메일 서비스 업체별 스팸 방지 기술
 4. 스팸메일에 관한 관련 법규
 5. 스팸메일 차단 방법
 6. 스팸메일 방지 대처 여부
 7. 결론
-

1. 서론

2003년 전반기를 기준으로 한 명당 하루 평균 47건의 스팸메일을 받아 본다는 것은 발송자 입장에서는 비용이 저렴하고 효과가 크다는 점에서 유용한 마케팅 수단이 될 수 있지만, 수신자가 원하지 않는에도 계속 뿌려지는 광고 메일은 더 이상 광고로서의 가치가 없는 사회적 공해에 불과하다[1],[2].

수신자의 의사와 무관하게 지속적이며 대량으로 전송되는 것 그자체가 사회적으로 큰 문제를 야기하고 있으며, 전자우편 이용자, 메일서비스제공사업자(ISP)등에게 유·무형의 큰 피해를 야기하고 있는 실정이다. 우선 전자우편 이용자의 피해는 다음과 같다 할 수 있다.

사이버공간이 자신이 원하지 않은 정보로 채워짐으로써 사생활침해를 야기 할 수 있고

원하지 않은 음란물의 수신으로 인한 정신적 피로 특히, 최근에는 미성년자에 대한 성인 광고 급증으로 사회문제화 될 수 있다. 그리고 개인 정보를 입수한 경로에 대한 불안감이 조성되고 스팸메일 내용 파악 및 삭제에 위한 시간적 낭비가 심하다. 아울러 용량이 한정된 메일박스에 스팸메일이 쌓임으로써 필요한 정보를 받지 못하는 불의의 피해가 발생 등의 문제를 야기한다.

또한 메일서비스제공사업자(ISP)의 피해로는 인터넷 운영의 장애를 야기하며 스팸메일 저장을 위한 하드디스크 용량증가로 비용소요가 크다. 그리고 스팸메일 선별을 위한 인력 소요가 필요하고 수신자들의 항의 및 등록취소 시 처리 비용이 소요된다. 끝으로 신뢰도 저하로 사업상 손실 발생 등을 야기한다 할 수 있다.

본 고에서는 이 같은 스팸메일에 대해 그 증가 이유, 전자우편을 수집하는 방법과 각종 방지책에 대해 살펴보고 이를 규제하기 위한 관계기관의 처벌실적, 스팸메일 여과를 안 하는 이유 등에 조사하여 스팸메일에 대한 정책적, 기술적 입안 시 기초 및 필요한 자료로 사용되고자 한다.

2. 스팸메일이 증가하는 이유

스팸메일이 증가하게 된 것은 전자우편의 대중화와 이를 마케팅에 용이하게 활용할 수 있는 기술 및 솔루션이 결합된 결과라 할 수 있다.

첫째, 전자우편 추출기 등 소위 'Harvesting S/W'가 웹상에 산재해 있는 전자우편 주소를 손쉽게 수집할 수 있게 해주고, 전자우편 발송기는 자체 메일서버가 없는 개인사업자나 영세소호들로 하여금 자신의 PC에서 대량의 광고메일 발송을 가능하도록 해주고 있다. 단 돈 10~30만원만으로 누구나 전자우편과 발송기를 가질 수 있게 되었으며, 수집에서 수천만 건에 이르는 전자우편 주소를 수집, 저장한 DB의 매매, 대여, 복제가 공공연히 성행하고 있는 실정이다.

둘째, 최근에는 발신자 전자우편(E-mail)주소 및 전송경로 등의 헤더정보를 익명으로 하거나 위·변조하는 기술이 등장하여 스팸 메일을 받아도 어디에서 메일이 발송되었는지 알 수 없는 경우가 많고, 따라서 어느 곳에 수신거부나 항의를 해야 할 지 알 수 없는 경우가 다반사이다.

이 같은 이유로 스팸메일이 증가하고 있다. 그러면 스팸메일 발송자는 어떻게 전자우편을 수집하게 되는가에 대해 알아보도록 하자.

우선 업무제휴 등을 통해 다른 업체의 회원정보를 제공받는다. 그리고 웹사이트 게시판 등에 공개된 전자우편 주소를 전자우편 추출기나 수작업 등을 통해 수집한다. 또한 전자우편 생성기를 이용하거나 전자우편 주소의 아이디(ID)로 자주 활용되는 영어 단어 등을 무작위로 조합하여 임의의 전자우편 주소를 생성하는 방법이 있다. 그리고 전자우편 주소가 대량으로 저장되어 있는 DB를 구입하거나 타사의 회원정보 DB를 해킹하여 불법적으로 수집하는 등 전자메일 주소 수집 경위는 매우 다양한 형태를 가지고 있다.

아래 <표1>에 이에 대한 백분율을 나타내었다.

<표1> 스팸메일 발송자가 전자우편을 수집하는 방법

수집 방법	백분율
전자 우편 추출기 이용	85%
E-mail DB판매	7%
회원정보 공유	3%
DB 해킹	3%
기타	2%

3. 메일서비스업체별 스팸 방지기술

아래 <표2>에 메일서비스업체별 스팸 방지기술을 나타내었다.

<표2> 메일서비스업체별 스팸 방지기술

서비스업체명	수신거부기능
다음	수신차단주소 지정 :100개 특정 조건 필터링 :발신자 ,수신자, 참조, 제목 단어 등 '스팸메일 걸러내기' 운영(필터링의 일종) -내부기준 및 회원의 스팸신고를 바탕으로 스팸메일 이라 판단된 메일이 수신될 경우 휴지통으로 이동 -4단계의 스팸메일 걸러내기 수준 선택가능 '스팸신고'란 운영
야후	수신차단주소 지정:100개 특정조건 필터링: 발신자, 수신자, 참조, 제목 및 본문 단어 등 '대량편지함'운영(필터링의 일종) - 스팸 성격의 상업성 메일을 대량 편지함으로 자동 분류 스팸 담당자에게 스팸신고 가능
드림위즈	수신차단주소 지정 : 무제한 특정 조건 필터링 : 발신자, 수신자, 참조, 제목 및 본문 단어 등 '스팸신고'란 운영
라이코스	특정 조건 필터링 : 발신자, 수신자, 제목 단어 등 고객센터에서 스팸신고 접수
코리아닷컴	특정 조건 필터링 : 발신자, 수신자, 제목 및 본문 단어
한미르	수신차단주소 지정 :50개 고객센터에서 스팸신고 접수하나 특별한 조치를 취하지는 않음
MSN	수신차단주소 지정 :250개 수신차단도메인 지정: 250개 특정 조건 필터링 :발신자, 수신자, 참조, 제목 단어 등 '광고성 편지 차단' 실시(필터링 일종) -'광고성 편지'혹은 '스팸 메일'로 간주되는 편지를 받은 편지함이 아닌 광고성 편지함으로 보냄 -3단계의 차단 수준 선택 가능 스팸담당자에게 스팸신고 가능

4. 스팸메일에 관한 관련 법규

동법 시행규칙 11조에서는 영리목적의 광고성 전자우편(E-mail)을 전송하는 경우 제목 란과 본문 란에 아래 <표3>과 같은 사항을 표시하도록 의무화 하고 있다.

<표3>광고성 전자우편의 의무 사항

1.광고메일의 제목처음에 “광고”를 반드시 표시해야 합니다.
2.광고메일의 본문에는 메일수신자가 광고메일의 수신을 거부할 수 있도록 수신거부 기능을 설치하고 광고메일 발송자의 업체명 또는 성명과 연락처를 기재하여야 합니다.
3.광고메일 발송자가“광고”문구를 표시하는 경우에는 제목란의 처음에 빈칸 없이“(광고)”라는 문구를 표기하여야 합니다.

또한 이에 대한 관련 법규 내역을 아래 <표4>와 <표5>에 나타내었다.

<표4>정보통신망 이용촉진 및 정보 보호 등에 관한 법률

제50조(광고성 정보전송의 제한) ①누구든지 수신자의 명시적인 수신거부의사에 반하는 영리 목적의 광고성 정보를 전송하여서는 아니된다. ②제1항의 규정에 의한 영리목적의 광고성 정보를 전자우편(E-mail)으로 전송하고자 하는 자는 정보통신부령이 정하는 바에 의하여 다음 각호의 사항을 전자우편(E-mail)에 명시하여야 한다. 1.전송목적 및 주요내용 2.전송자의 명칭 및 연락처 등 3.수신거부의 의사표시에 관한 사항 제55조 ③정보통신부장관은 이 법에 위반한 정보통신서비스제공자등에 대하여 필요한 시정조치를 명할 수 있다.
제67조(과태료) ①다음 각호의 1에 해당하는 자는 500만원 이하의 과태료에 처한다. 15.제50조제1항의 규정을 위반하여 영리목적의 정보를 전송한 자. 19. 제55조제3항의 규정에 의한 시정조치 명령을 이행하지 아니한 자

<표5>정보통신망 이용 촉진 및 정보 보호 등에 관한 법률 시행 규칙

제11조(영리목적의 광고성 전자우편의 명시방법)

①영리목적의 광고성 전자우편(E-mail)을 전송하고자 하는 자는 법 제50조제2항의 규정에 의하여 전자우편(E-mail)의 제목란 및 본문란에 다음 각호의 사항을 수신자가 쉽게 알 수 있도록 각각 명시하여야 한다.

- 1.전자우편(E-mail)의 제목란: “광고”라는 문구와 전자우편(E-mail)의본문란의 주요내용
- 2.전자우편(E-mail)의 본문란: “수신자가 수신거부의 의사표시를 할 수 있는 용이한 방법과 전송자의 명칭 및 연락처(전화번호 또는 전자우편(E-mail) 주소)

②전자우편(E-mail)의 제목란에 제1항제1호의 내용을 명시하는 경우에는 처음에 “광고”라는 문구를 표시하고, 이어서 전자우편의 본문란의 주요내용을 표시하여야 한다.

또한 정보통신부에서는 최근 해외로 무분별하게 전송되는 한글 스팸메일 차단을 위해 OECD와 EU등 국제기구와 협의, 광고와 스팸메일에 의무적으로 @표시를 하도록 하고 이를 국제 표준으로 할 계획임을 밝혔다[3].

정통부는 이에 앞서 지난 6월부터 영리목적의 광고나 음란 E-mail를 반드시 표시토록 하는 한편 영어로 된 수신거부 안내표시도 병기토록 했다. 이를 위반할 경우 2년 이하의 징역이나 1천만원 이하의 벌금이 부과된다.

5. 스팸메일 차단방법

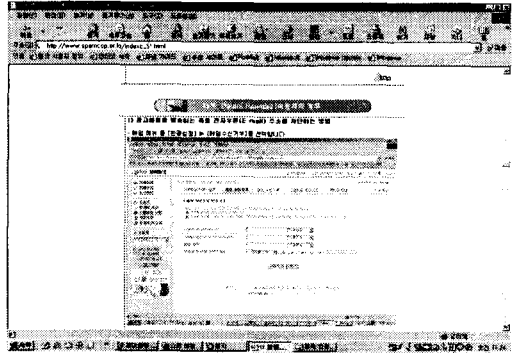
5.1 광고메일수신자

(1) 필터링에 의한 방법

□ 광고메일을 발송하는 특정 메일의 주소를 차단하는 방법

메일 메뉴 중 [환경설정][메일수신거부]를 선택한다.

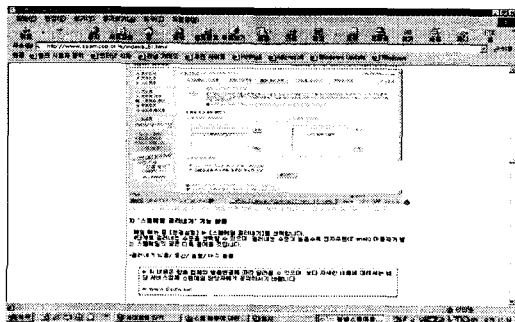
택한다.



□ 광고메일에서 주로 사용되는 특정단어를 통한 스팸메일 차단방법

-메일 메뉴 중 [환경설정][메일 자동분류][만들기]를 선택한다.

-제목이나 본문의 특정단어, 예컨대(광고나 성인광고, 홍보 CD, 포르노등의 단어가 차단되도록 설정을 해 놓으면 해당 단어가 들어있는 메일은 수신 시 자동 삭제되거나 원하는 폴더로 자동 수신된다.



-마찬가지 원리로 외국으로부터 전송되는 광고메일에 대해서는 제목란에 AD: 및 ADV:ADLT라는 단어는 차단되도록 설정해 놓을 수 있다.

□ 스팸메일 걸러내기 가능 활용

-메일 메뉴 중 [환경설정][스팸메일 걸러내기]를 선택한다.

-4단계로 걸러내는 수준을 선택할 수 있으며 걸러내는 수준이 높을수록 전자우편 이용자

가 받는 스팸메일의 양은 더욱 줄어드는 것이다.

이때 4단계는 낮음/중간/높음/아주 높음/등으로 구성되어 있다.

(2) 스팸메일 발송자에게 수신 거부하는 방법

- * 수신거부 메뉴가 별도로 설치되어 있는 경우 그것을 선택하여 수신거부 한다.
- * 수신거부의사를 전달한 전자우편 주소가 기재되어 있는 경우 그 주소로 수신거부 메일을 전송한다.

(3) 메일 내용 안에 수신방법이 안내되어 있지 않은 경우

수신한 광고메일의 호신이나 답장기능을 활용하여 발송자 전자 우편주소로 수신거부 메일을 발송한다.

5.2 메일서버 관리자

(1) 제목에 “ADV” 표시메일 수신차단 방법

제목에서의 패턴에 의한 스팸메일 처리는 한글로 제목을 다는 경우에 인코딩/디코딩이 고려되어야 하므로 그다지 큰 효과를 발휘할 수는 없으나 메일로 유포되는 바이러스와 같이 특정한 제목을 가지는 경우와 해외에서 들어오는 메일들의 경우에 있어서 그 효과를 볼 수 있다.

이러한 패턴의 처리는 메일이 들어올 때의 메일헤더 정보에 기반하여 처리를 하는 것으로서 패턴은 다음과 같다.

```
HSubject:$>check_subD{ADVMail}"We don't accept Advertisement Mail!"
Scheck_subR<ADV$*>#$error$:550${ADVMail}
```

하나씩 떼어서 설명하면, H헤더의 Subject 제목부분을 검사하게 되는 것으로서 이 부분에 ADV라는 문자열이 있게 되면 메일을 거부하게 된다.

(2) 스팸메일 발송자에게 전자우편주소의 실제 사용여부를 알려주지 않는 방법

스패머들이 사용하는 소프트웨어의 경우 특정메일서버로 사용자 아이디에 대한 쿼리를 보내 사용자의 존재유무를 알아 낼 수 있도록 하는 경우가 있다.

```
vrfy george
```

```
250georg@myhost.domain.co.kr
```

```
vrfy georgel
```

```
550georgel User unknown
```

과 같이 사용자의 유무를 확인할 수 있도록 하는 명령어를 서버의 SMTP 연결 상태에서 계속적으로 던짐으로써 유효한 사용자의 리스트를 알아낼 수 있는 것이다. 그러므로 아래와 같이 sendmail.cf에 설정하도록 하여 이러한 명령어를 무용화 시킬 수 있도록 한다.

```
# privacy flags privacyOptions =
```

```
authwarnings, novrfy, noexpn
```

```
@스팸스나이퍼(http://www.spamsniper.co.kr)
```

:가상의 이메일 주소를 생성해서 이메일을 대신 받아 주는 서비스이다.

```
@메일 워셔(http://www.mailwasher.ent)
```

:mailwasher는 외국 S/W인데, 메일을 받을 때 제목만 불러와 확인해서 필요 없는 메일은 바로 삭제할 수 있도록 해주는 프로그램이다.

6. 스팸메일 방지 대처 여부

스팸메일로 인해 피해를 입지 않기 위해

스팸메일 차단 소프트웨어를 사용하거나 그와 유사한 조치를 취하고 있는 사람은 조사 대상의 14.5%에 불과하였다. 이는 스팸메일로 인한 피해 가능성에 대하여 우려하고 있는 네티즌 비율에 비하면 아주 적은 수치이다. 특히 스팸메일로 인한 피해 방지 대처여부에 관한 조사에서는 인구특성에 관계없이 거의 모두 특별한 대책을 세우지 않은 것으로 분석돼 주의가 요망된다. 그러나 인터넷 활용정도 측면에서는 활용 정도가 많을수록 조치를 취하는 비율이 높아지고 있다.

<표6> 인터넷 활용정도 측면에 따른 스팸메일 피해 방지 대처율

인터넷 활용 정도	조치비율	비 조치 비율
인터넷 검색이 가능한 정도 (308명)	10.4	89.6
인터넷과 컴퓨터 응용프로그램 이용가능(1391명)	14.7	85.3
프로그램을 만들 수 있는 정도(241명)	15.8	84.2
대형 시스템을 운영할 수 있는 정도(60명)	26.7	73.3

또한 아래 <표7>에 스팸메일 방지 대처를 안하는 이유에 대해 설문조사를 하였는데 이의 결과를 나타내었다.

<표7> 스팸메일 방지 대처를 안하는 이유

방지 대처 안하는 이유	백분율
몰라서 안함	10%
귀찮아서 안함	57%
안되는 것 같아서 안함	16%
필요한 부분이 있어서 신경 안쓰임	10%
스팸이 오는게 기분 좋다	7%

7. 결론

본고에서는 스팸메일의 피해, 그 증가 이유, 스팸 방지 기술과 관련 법규 그리고 스팸메일 방지 대처 여부에 대해 분석하고 이에 대한 조사를 수행하였다. 그 결과 의외로 스팸메일 방지 대처를 안 하는 사람이 많았으며 광고성 메일에 대한 처벌을 강화해야 한다는 의견이 상당히 높았다. 이 같은 조사 결과를 바탕으로 보다 효과적인 정책적, 기술적 방법 등이 공론화되어 인터넷이 유용한 수단은 될지언정 더 이상 이로 말미암은 피해는 극소화 할수 있는 다각도의 정책 시행이 이루어져야 하리라 여겨진다.

참고문헌

- [1] <http://www.spamcop.or.kr>
- [2] 네이버 뉴스, '스팸메일의 무분별한 확산을 막기 위해 전쟁' 불법스팸 메일 단속을 대폭 강화, 10월 18일
- [3] 조선닷컴, '스팸메일에 @표시' 국제 표준화 추진, 2003년 10월 12일

저자 소개

● 한길성(Kil-Sung Han)



1972년 : 공군사관학교 전자공학과 (공학사)

1977년 : 서울대학교 전자공학과 (공학사)

1981년 : 서울대학교 대학원 전자공학과 (공학석사)

1996년 : 충북대학교 대학원 컴퓨터공학과 (공학박사)

1997년 ~ 현재 : 서울대학교 정보통신공학과 교수

<주관심분야> : ATM, 인터넷 역기능, 영상공학