

# 유해콘텐츠 접속 동기에 기초한 기술적 차단 방법의 종합적 제시

조동욱 \*

\* : 충북과학대학교

e-mail: [ducho@ctech.ac.kr](mailto:ducho@ctech.ac.kr)

## A Synthetic Proposal of Technical Blocking Method Based on the Harmful Internet Contents Access

Dong Uk Cho \*

\* : Chungbuk Provincial University of Science & Technology

### 요 약

본 논문은 유해콘텐츠를 접속하는 동기를 통하여 이를 효과적으로 차단하기 위한 전체적 방법에 대한 제시를 행하고자 한다. 이를 위해 첫째, 인터넷 유해 콘텐츠의 접속 동기를 분석한다. 또한 인터넷 유해 콘텐츠를 접속하는데 있어 가장 큰 요소인 스팸메일에 대해 실태 파악 및 분석을 행하고자 한다. 이를 위해 우선적으로 스팸 메일이 증가하는 이유, 스팸메일 발송자가 전자우편을 수집하는 방법 그리고 각종 스팸메일 방지 방안 및 스팸 방지 기술에 대해 기술하고자 한다. 또한 수신측에서 행해지고 있는 스팸메일 차단에 대해 여과를 안 하는 이유 등에 대해 조사함으로써 스팸메일 차단에 대한 연구 방향을 잡기 위한 기초 자료로 삼고자 하며 이를 기초로 이메일을 수집 단계에서부터 차단이 이루어 지게 하기 위한 종합적 차단 방법에 대해 제안하고자 한다.

### 1. 서론

음란 유해 사이트에 대한 사회적인 문제는 이제 더 이상 방치하기에는 심각한 상황이 되어 있는 실정이다. 2003년을 기준으로 보아도 한글로 된 음란사이트가 세계 2위이며 그 증가율은 세계 1위이기 때문에 이에 대한 전반적인 대책이 강구되지 않으면 안 되는 실정이 되었다. 통상 음란물을 접하는 동기는 이메일을 통해 접속하는 경우가 많으므로 이를 차단하는 것이 가장 좋은 방법이라 여겨진다. 본 논문에서는 2003년을 기준으로 했을시 하루 평균 48.7통씩 뿌려지는 스팸메일에 대해 이를 방지하기 위한 종합적, 기술적 방법에 대해 제안하고자 한다. 이를 위해 우선적으로 스팸메일에 대한 실태 파악 및 분석을 행하고자 한다. 또한 현존하는 스팸 메일 방지 기술에 대해 살펴보고 이를 얼마나 효과적으로 사용하고 있는가를 살펴봄으로써 음란물 차단에 대한 전반적인 기술적 해결책을 제안하고자 한다.

### 2. 음란물을 접속하는 동기 분석

음란물을 배포하는 경위를 살펴보면 다음과 같다. 우선 개인 홈페이지에 배너 광고를 이용하는 방법이다.

그 다음이 음란사이트끼리 연대하여 광고하거나 유즈넷을 이용하는 경우이다. 마지막으로 이메일을 이용하여 스팸메일 형태로 배포하는 경우이다. 이중 가장 많이 이용되고 있는 방법이 이메일

을 이용하여 배포하는 경우가 된다. 우선 이메일을 통해 스팸메일로 배포되는 음란사이트 광고가 증가하는 이유에 대해 알아보고자 한다. 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 위변조하는 기술이 등장하여 스팸메일을 받아도 어디에서 메일이 발송되었는지 알 수 없는 경우가 많고, 따라서 어느 곳에 수신 거부나 항의를 해야 할 지 알 수 없는 경우가 다반사이다. 이같은 이유로 스팸메일이 증가하고 있고 또 이를 통해 음란물이 대량으로 유통되고 있는 실정이다. 그러면 음란물들을 발송하기 위해 스팸메일 발송자가 어떻게 전자우편을 수집하게 되는가에 대한 분석이 중요한 자료가 된다. 우선 스팸발송자는 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 이를 나타내었다.

<표1> 스팸 발송자가 전자우편을 수집하는 방법

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

<표1>을 분석해 보면 스팸 발송자는 10~30만원에 구입할 수 있는 전자우편 추출기를 통해 스팸을 발송하는 방법을 쓴다는 것을 확인 할 수 있었다. 따라서 근본적인 차단책중 가장 효과가 있는 것은 이메일 자동 추출기의 작동을 차단할수 있는 차단책임을 알 수 있다.

### 3. 메일서비스업체별 스팸 방지기술

무작의적으로 뿌려지는 스팸을 방지하기 위해 메일서비스 업체별로 스팸방지를 행하고 있는 것이 현 실정이다. 이를 아래 <표2>에 나타내었다.

<표2> 메일서비스업체별 스팸 방지기술

서비스 업체명	수신 거부 기능
다음	수신차단주소 지정 :100개 특정 조건 필터링 :발신자 ,수신자, 참조, 제목 단어 등 '스팸메일 걸러내기' 운영(필터링의 일종) -내부기준 및 회원의 스팸신고들 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
코리아 닷컴	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

위의 표에서 알수 있듯이 메일 서비스를 제공하는 포털들마다 나름대로 그 방지책을 강구하고 있다는 것을 확인할수 있다. 그러나 후에도 언급하겠지만 방지기술이 나와도 이를 일반인들이 사용 안한다는 것이 문제가 될 수 있다.

### 3. 스팸메일에 관한 관련 법규

음란물등의 유통을 방지하기 위해 당국에서는 스팸에 대한 규제 법규가 당연히 있다. 이의 주요 내용은 동법 시행규칙 11조에서는 영리목적의 광고성 전자우편(E-mail)을 전송하는 경우 제목란과 본문란에 아래 <표3>과 같은 사항을 표시하도록 의무화 하고 있다.

<표3> 광고성 전자우편의 의무 사항

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

또한 당국에서는 최근 해외로 무분별하게 전송되는 한글 스팸메일 차단을 위해 OECD와 EU등 국제기구와 협의, 광고와 스팸메일에 의무적으로 @표시를 하도록 하고 이를 국제 표준으로 할 계획임을 밝혔다[1]. 정통부는 이에 앞서 지난 6월부터 영리목적의 광고나 음란 이메일을 반드시 표시토록 하는 한편 영어로 된 수신거부 안내표시도 병기토록 했다. 이를 위반할 경우 2년 이하의 징역이나 1천만원 이하의 벌금이 부과된다. 그러나 실제 이를 위반하여 스팸을 발송한자에 대한 처벌은 극히 미약한 것으로 파악되고 있으며 따라서 법 규제가 강하게 시행되지 않는 점을 이용하여 무작위로 스팸이 발송되고 있는것도 현 실정이다. 결국 법 집행의 미약을 근거로 음란물에 대한 스팸메일이 증가하고 있으며 이용자가 이를 차단하기 위해서 차단 단어를 적어나도 교묘히

이를 피하는 용어를 선택하여 씌으로써 실제 음란물의 배포를 막기에는 어려운 것이 현 실정이다.

#### 4. 음란 스팸메일 차단방법

##### 4.1 광고메일수신자에 의한 차단

###### (1) 필터링에 의한 방법

- 광고메일을 발송하는 특정 메일의 주소를 차단하는 방법
- 광고메일에서 주로 사용되는 특정단어를 통한 스팸메일 차단방법
- 스팸메일 걸러내기 기능 활용  
-4단계로 음란스팸등을 걸러내는 수준을 선택할 수 있으며 걸러내는 수준이 높을수록 전자우편 이용자가 받는 스팸메일의 양은 더욱 줄어들게 된다. 이때 4단계는 낮음/중간/높음/아주 높음/등으로 구성되어 있다.

###### (2) 스팸메일 발송자에게 수신 거부하는 방법

이는 수신거부 메뉴가 별도로 설치되어 있는 경우 그것을 선택하여 수신거부 하거나 수신거부의사를 전달한 전자우편 주소가 기재 되어 있는 경우 그 주소로 수신거부 메일을 전송한다.

###### (3) 메일 내용 안에 수신방법이 안내되어 있지 않은 경우

수신한 광고메일의 호신이나 답장기능을 활용하여 발송자 전자우편주소로 수신거부메일을 발송한다.

##### 4.2 메일서버 관리자에 의한 차단

###### (1) 제목에 "ADV" 표시메일 수신차단 방법

제목에서의 패턴에 의한 스팸메일 처리는 한글로 제목로 된 경우에 인코딩/디코딩이 고려되어야 하므로 그다지 큰 효과를 발휘 할 수는 없으나 메일로 유포되는 바이러스와 같이 특정한 제목을 가지는 경우와 해외에서 들어오는 메일들의 경우에 있어서 그 효과를 볼수 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 Subject제목부분을 검사하게 되는 것으로서 이 부분에 ADV라는 문자열이 있게 되면 메일을 거부하게 된다.

###### (2) 음란 스팸메일 발송자에게 전자우편주소의 실제 사용여부를 알려주지 않는 방법

스팸머들이 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 george1
550george1 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.net>)

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

#### 5. 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 높은 것으로 파악되고 있다.

<표4> 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 <표5>에 스팸메일 방지 대처를 안하는 이유에 대해 나타내었다.

<표5> 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 안 쓰임	10%
스팸이 오는게 기분 좋다	7%

#### 6. 기술적으로 음란 콘텐츠를 차단하기 위한 종합적 문제 해결 방안 제시

지금까지의 스팸에 대한 현황 분석을 통해 다음과 같은 결론에 도달하여 향후 연구 방향 검토를 위해 다음과 같은 크게 3개로 나누어 종합적 고찰을 행하고자 한다.

첫째, <표4>의 설문조사 결과에서 알수 있듯이 일반인들이 수신측에서 음란물을 차단하기 위해 스팸메일을 차단할수 있는 기술이 있음에도 불구하고 이를 사용 안한다는 것 이다. 심지어 <표5>에서 알수 있듯이 귀찮아서 스팸 방지대처를 안한다고 하는 응답이 약 60%에 달하는 것은 연구 방향을 향후 어떻게 설정해야 하는지 디레마에 빠지게 하는 결과이다. 어떻게 기술을 개발해야 귀찮아서 안한다는 응답이 없도록 할것인가가 향후 연구의 첫째 관건이 된다.

둘째, 수신측에서의 스팸 차단과 더불어 이메일 자동 추출기의 기능을 차단하는 방법이 활성화 되어야 하리라 여겨진다. 지금도 다음사이트에서는 이를 시행하고 있는데 [2] 이는 다음사이트 가입 회원에 대해서만 혜택을 볼수 있는 단점이 존재한다. 범용적인 이메일 추출기 기능 방지 툴이 개발되어야 하며 이를 메일 서버에 모두 설치하도록 해야 한다. 우선적으로 일반 사용자(즉, 정상 사용자)의 불편을 최소화 할수 있는 이메일 자동 추출기 차단 알고리즘이 개발이 시급한 실정이다.

셋째, 내용 기반 음란 유해 콘텐츠 차단 툴이 효과적으로 개발되어야 한다. 현존하는 목록기반 방법과 단어 기반 방법만으로는 음란 유해 콘텐츠가 차단이 안되므로 이를 극복하기 위한 내용 기반 음란 콘텐츠 차단 방법이 개발되어야 한다. 이상과 같이 언급한 세가지 사항이 동시에 행해져야 음란 콘텐츠의 무분별한 배포와 유통으로부터 청소년을 효과적으로 보호할수 있으리라 여겨진다.

## 7. 결론

본 연구에서는 효과적인 음란 유해 콘텐츠의 기술적 차단 방법에 대해 전반적인 제안을 행하였다. 이를 위해 음란물을 음란 스팸에 대한 전반적 고찰과 분석을 시행하였다. 우선적으로 스팸의 증가 이유, 스팸 방지 기술과 관련 법규 그리고 스팸메일 방지 대처 여부에 대해 조사하였다. 그 결과 의외로 스팸메일 방지 대처를 안하는 사람이 많은 것으로 분석되었다. 또한 음란 스팸과 음란 콘텐츠를 기술적으로 차단하기 위한 종합적 방법도 제안하였다. 향후 이메일 자동 추출기의 차단 방법에 대한 개발 그리고 수신측에서의 차단에 대해 귀찮아서 안 쓴다는 문제를 개선키 위한 연구, 내용 기반 음란 콘텐츠 차단등에 대한 연구가 지속적으로 행해져야 하리라 여겨진다.

## 참고문헌

[1] 조선닷컴, ‘스팸메일에 @표시’ 국제 표준화 추진, 2003년 10월 12일

[2] <http://www.daum.net/> "전자 우편 발송 체계"

[3] <http://www.captcha.net/> "The Captcha Project"

[4] 한국정보보호진흥원 불법스팸대응센터, "이메일 주소 추출 방지"