論 文
5-4-5

스팸 메일 차단솔루션의 새로운 제어 방식 제안 (The Suggestion of a New Control Method for SPAM Mail Prevention Solution)

김민홍(Min-Hong, Kim)[1] 두창호(Chang-Ho, Doo)[2]

요 약

스팸메일은 최근 전 세계적으로 사회문제가 되고 있으며, 이에 대한 차단 솔루션에 대한 개발 제품이 출시되고 있다. 본 논문은 기존 스팸메일 방지 솔루션을 설치형태에 따른 분류, 장단점 분석과 스팸의 판정법에 따른 분류 고찰하였다. 이에 기존 스팸메일 솔루션의 문제점을 도출하고 현재 적용되지 않은 새로운 필터링 방법인 URL Prefetch 방식을 새롭게 제안하고 이에 따른 방법에 의한 실험을 통한 스팸메일 차단 상승효과를 도출하고, 또한 HTML 유형 방식에 의한 차단방법도 함께 제안한다.

ABSTRACT

SPAM mails become a serious social problem all of the world and the products for SPAM prevention are coming to the market. This study classifies the existing SPAM prevention solutions according to the patterns to be set up and the judging SPAM methods, and analyses the merits and demerits of them. This study also draws problems of the existing SPAM prevention solutions and suggests a new URL Prefetch method, a new filtering method which have been out of use. And it draws synergistic effects of SPAM prevention by this new method and suggests SPAM prevention solution by HTML pattern method

1) 정회원 : 경기대학교 정보과학부 교수
2) 정회원 : 경기대학교 정보과학부
전자계산학과 박사과정

논문접수 : 2004. 3. 30.
심사완료 : 2004. 4. 12.

1. 서론

스팸메일(SPAM mail)은 본인이 원하지 않고 요청하지도 않았음에도 우송되는 전자우편, 즉 원치않은 불청(不請)전자우편을 말한다. 스팸메일은 크게 다른 목적 때문에 전자우편 주소를 제공했음에도 발신자로부터 제공자의 동의없는 전자우편이 우송되는 경우와 전자우편 주소를 제공한 적이 없는 발신자로부터 전자우편이 우송되는 경우로 구분된다.

정보통신부 조사에 따르면 전자우편 주소는 응답자 대다수(94.9%)가 웹 사이트에 제공 경험이 있고, 또 대다수 웹 사이트에서 수집하고 있는 개인정보로서 본래의 제공 목적과 달리 스팸메일 발송에 사용될 소지가 충분한 것으로 알려져 있다.[1] 따라서 스팸메일은 인터넷 이용자라면 누구나 한번쯤 경험하는 가장 일반적인 형태의 정보화 역기능이라고 볼 수 있다. 이러한 스팸메일은 또한 전 세계적으로 사회문제가 되고 있다. 국내에서는 정부와 공공기관이 앞장서 법 정비를 진행하고, 관련 정보를 공지하여 피해를 줄일 수 있도록 하고 있으나, 이것을 통한 효과를 기대하기 힘든 실정이다.

또한 이러한 상황은 미국을 중심으로 한 인터넷 선진국에서는, 스팸 문제가 심각한 상황에 빠져있다. 미국 브라이트 메일 회사에 따르면 (http://brightmail.com), 2004년 2월 현재 동사의 고객이 1개월간 받은 메일의 62%가 스팸 이었다고 보고하고 있다. 또한, 최근 5년 동안 이 문제를 대처하기 위한 비용이 800억 원 정도 들었다고 보고하고 있다.[2]

더구나 대한민국 등은 멀티바이트 문자 코드권 이므로 상용소프트웨어의 수도 적기 때문에 스팸 메일 방지 소프트웨어의 출현이 늦어지고 있어 이에 대한 대비가 절박한 상태이다. 최근 이러한 스팸 메일은 단순히 개인의 문제로만 여겨져 왔던 스팸 메일은 좀 더 악용되어 메일서버, 네트워크를 낭비하고 무엇보다도 최종 사용자의 생산성을 떨어뜨리는 것에 영향을 미치고 있다.

이러한 상황에서 본 논문에서는 현재 사용되고 있는 스팸 메일 방지 소프트웨어들의 방식을 설치형태와 스팸메일 판정에 따른 방식들을 고찰함과 동시에 효과적인 스팸 메일 방지를 위한 MTA 형태의 URL Prefetch 방식에 의한 스팸메일 필터링 방식에 대한 새로운 기술을 제안하고자 한다.

2. 기존 스팸 메일 방지 소프트웨어의 고찰

2.1 설치 형태에 따른 스팸 메일 방지 소프트웨어

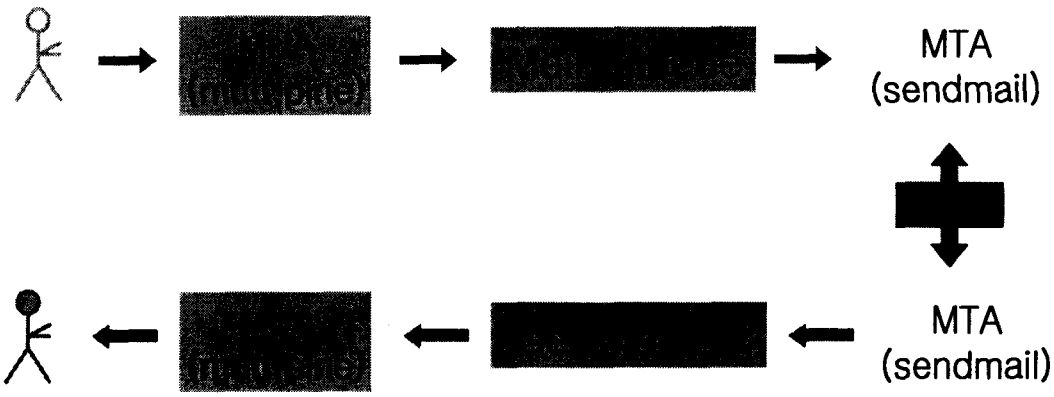
최근 어느 정도는 피해가 큰 미국뿐 아니라 국내에서도 이미 어느 정도의 스팸 메일 방지 소프트웨어가 사용되기 시작하고 있다. 당장 스팸 메일 방지 소프트웨어가 없다면 상당한 기업 생산성 저하를 가져오기 때문일 것이다. 이러한 제품은 바이러스가 전자우편을 통해 배포된다는 특성상, 바이러스 검사 소프트웨어와 합쳐져서 개발, 판매되거나 아니면 독립적으로 벤더들에 의해 판매되는 것들이 있다.

이러한 스팸메일 방지를 위한 기존 소프트웨어를 생각하면, 먼저 설치형태에 따라 2개의 타입으로 분류할 수 있는 것을 알 수 있다.

- MTA(Message Transfer Agent) 형
- MUA(Message User Agent) 형

MTA형 방식은 MTA 레벨, 즉 SMTP 서버 단에서 스팸 메시지를 처리하는 방식으로, 예를들면 각 MTA에서의 ORDB (http://ordb.org)에 기반하는 Blocking 기능이나 TrendMicro사의 InterScan VirusWall 등이 이것으로 분류된다.[3]

이 방식의 경우 메일이 오면 사용자에게 배달하기 전에 서버에 설정된 각종 룰을 기반으로 스팸을 차단하게 되므로 스토리지나, 트래픽 감소에 도움이 된다. 그러나 현재 70% 이상의 시장 점유율을 자랑하고 있는 Sendmail에서 메일 서버를 구성하고 있는 리눅스/유닉



[그림 1] 전자메일 전달과정에서 MTA와 MUA
[Fig. 1] MTA & MUA at E-Mail Transmission Process

스 계열의 대표적인 Mail Transport Agent 로서 높은 성능을 지니고 있으나 끊임없는 버그와 공개적으로 이용이 가능한 서비스라는 점과 root 권한으로 수행된다는 점, 환경설정이 까다롭다는 점 때문에 공격 대상이 되고 있으며 서버에서 동작되기 일방적 규칙 적용 때문에 메일 자체가 정말 스팸일까? 라는 의문과 개인정보의 누출 가능성도 존재하고 있다.

그러나 네트워크 및 메일서버를 조직적, 적극적 대응하기 위한 최선의 방법으로 조직 전체적인 정책 반영의 용이하고 전용 SMTP 엔진을 탑재하여, 효율성과 메일서버의 부담을 줄일 수 있기 때문에 아직까지 가장 많이 사용되고 있다.

반면에, MUA형의 방식은 메일서버에서 개인 사용자에게 전달된 메일을 사용자가 읽으려는 순간 개인 사용자가 지정한 룰에 따라 스팸을 차단하게 되므로 개인별 성향에 따른 차단이 가능하다는 것이 가장 큰 특징이다. 정통부에서 배포중인 "음란스팸잡이"
(http://www.spamcop.or.kr/kor_main.jsp)가 이 부류 중에 속한다.[4]

이 MUA 형은 개인적인 설정 가능한 방법으로 개인적으로 메일의 옥석을 가릴 수밖에 없으며 개인의 웹 메일 계정 등도 한꺼번에 처리해야 하고 개개인의 소프트웨어 활용 능력이 중요하다. 그러나 조직적인 관리가 어렵고 네트워크, 메일서버 등의 부하 및 공격에 대해 미온적 대처에 그친다는 단점을 지니고 있다.

이들 방식의 장단점은 [표 1]에서 보는 바와 같으며, 스팸을 차단하고자 하는 상황에 따라, MTA와 MUA 방식이 혼합되어 사용되어야 효과를 극대화할 수 있다.[7]

내용	MTA방식	MUA방식
기존시스템에의 도입용이	릴레이 서버의 설정만 변경하므로 용이함	MUA종류가 많아 어려움 POP3 알림방식의 모델의 경우 동작 시간에 따라 차단율이 차이가 많이남
필터링 책	통일	자유
CPU에 한 부하	높음	낮음
스토리지에 대한 부하	낮음	높음
SPAM판정	통일 룰	개별 룰

[표 1] MTA와 MUA 특징 비교
[Table. 1] The Comparison Character of MTA & MUA

2.2 스팸 메일 메시지 판정에 따른 고찰

다음은 스팸 메일 메시지 판정법으로 스팸 메일 방지 소프트웨어들을 분류를 해 본다.

가. 블랙리스트 / 화이트리스트에 의한 판정

MTA형에서도 MUA형에서도 사용되어, 원천적으로 메일을 받고 싶은 상대와 받고 싶지 않은 상대에 대한 지정을 할 수 있게 한다. 이 규칙은 보통의 경우 모든 다른 룰들의 최상위로 동작을 하며, 성능이나 다른 규칙의 오류률을 보완하기 위한 방식으로 사용된다. 메일 어플라이언스 메이커인 Mirapoint사 (http://www.mirapoint.com)의 . Mos3.3에서는 SMTP세션의 레벨에서도 유저의 메일박스 레벨에서도 이 기능을 사용할 수 있도록 되어 있어, 스팸 대책의 최소한의 기능으로 장착되어 있는 것을 알 수 있다.[5]

나. 중앙관리 스패머 데이터베이스 기반의 판정 MTA형으로 주로 이용되고 있다. MUA형에 실제로 장착되어 있는 예는 없다고 생각된다. 이 방식은 특정 서버에 의존적이지 않고 모든 메일서버가 정보를 공유하는 개념으로 전술한 ORDB와 같은 방식이 포함된다. 이 방식은 데이터는 중앙서버가 관리를 하고 각 서버들이 스패머에 대한 정보를 중앙서버에 DNS나 다른 방법등을 이용해 실시간 정보를 공유하고 있다. 하지만, 이 방식은 자동화 툴에 의해서 특정 서버의 취약점을 검사하고, 취약점이 있는 경우 해당 서버를 스패머 리스트에 올렸다가, 취약점이 해결되면, 요청에 의해서 리스트에서 삭제하는 방식을 채택하고 있어, 관리자의 지속적인 관심이 필요하며, 자신의 서버가 등록이 된지도 모른 채 거부당하게 되는 문제점등을 많이 내포하고 있다. 또한, ADSL과 같이 IP정보가 계속 바뀌는 환경에서는 정보의 정확도를 보장할 수 없어 차단율이나 신뢰도가 많이 떨어진다는 문제점이 있다. 그러면서도 스팸 정보를 공유하고자 하는 수법 자체는 유효한 것이다. 예를들어, AOL 전용 브라우저인 AOL8.0의 "스팸 광고 버튼"과 같이 일정의 규모의 커뮤니티에서 효과를 올리고 있는 것도 있다. AOL에서는 효과가 인정된다고 하여 회사의 웹 메일 서비스에도 그 "스팸 광고 버튼"을 채용하고 있다.

다. SMTP 세션 특성에 기반 한 판정

이것은 스팸 세션의 동향에 기반 한 판정인데, 이것도 MTA형에서 이용되는 수법이다. 원리적으로 MUA에서의 실제 장착은 할 수 없다. 이 방식은 대규모 메일서버에서 많이 이용되는 방식이다. DoS 아답터 등과 같은 호스트로부터의 과도한 SMTP접속요구를 검출하여 접속제한을 거는 등의 방법으로 SPAM 송신을 슬로 다운시켜, 메일서버의 기능을 유지하는 것에 주안을 두고 있는 것이 많다. DEEPSoft사의 WBlock에서도 [그림2]과 같은 기능을 실제로 장착하고 있다.

[그림 2] 과도한 메일발송으로 서버 응답 지연
[Fig. 2] A Server Response Delay at Excessively E-Mail Sending

라. 메일 컨텐츠에 의한 판정

컨텐츠에 의한 판정은, 웹 프락시에 있어서의 컨텐츠 필터링과 똑같이, 메일내용을 체크하는 것이다. MTA형에서도 MUA형에서도 이용된다. 그렇지만 이 컨텐츠 필터링에는 기술적, 사회적문제가 많다.

MUA형의 경우, 완전히 메일을 받은 다음에 처리하기 때문에 메일서버 자체의 부하는 전혀 경감되지 않고 메일서버는 스팸의 피해를 직접 받는 것이 되어 버린다. 또, 컨텐츠 체크를 위한 방식으로 메일헤더정보를 해석하는 것 이외에 특정 문구의 패턴 매칭 정보를 해석, 출현 비율의 비교에 의한 스팸 메시지를 판정을 하는 것(예를들면, SpamAssassin

http://spamassassin.org)이 있지만, 그 판정은 완전하지 않다. 메일이라고 하는 미디어의 성격상, 불완전한 필터링이 사회적으로 용서되지 않는 경우도 많고, 잘못하여 필터링 했을 때의 보상조치가 필요하다. MTA방식도 문제를 내포하고 있는데, MTA방식에서는 필터링할 때, IP와 같은 세션 정보만을 이용하여 필터링할 경우, 메일본문전체를 수신하지 않는 경우도 있고, 필터된 메일을 유저에게 제공하지 못하는 점이 문제가 된다. 오검출을 적게 하기 위해서 통계에 기반 한 좀더 상세한 베이지안 필터링을 실시하는 등의 노력에 의해 정밀도는 향상되어 오고 있다. 베이지안 필터링의 효과에 대해서는, 2003 SPAM Conference 자료가 상세하게 나와 있다.

http://spamconference.org/proceedings2003.html

그렇지만 완전하게 처리하지 못하는 것은 간단하게 추정할 수 있다.

메일의 컨텐츠 필터링에는 사회적인 문제도 많고, 기업 네트워크에서는 MTA형의 컨텐츠 필터링이 가능하지만 국립조직이나 ISP에 있어서는 법적근거가 없다면 대응은 어렵다. 원래 유저에게 있어서의 스팸은 한 가지 모양이 아니다.

3. 기존 솔루션의 문제점

위 스팸 방지 솔루션을 고찰을 통해 현재 사용되고 있는 스팸 방지솔루션에서는 여러 가지 문제가 다음과 같이 나타내고 있다.

■ 사용자의 MUA 종류를 모두 지원하는 것이 불가하며, " 음란 스팸잡이"의 모델의 경우 효과가 떨어지게 된다.

■ 사용자가 필터룰의 관리 및 교육의 부재

이런 이유로 인해 MUA의 모델은 사용자에 의한 선택이 되어야 하며, 기관이나 단체에서 선택할 수 있는 방법은 현재로서는MTA 방식이 가장 타당하다. 하지만, MTA 방식의 도입의 경우 다음의 문제가 예상된다.

■ 사용자의 반발

■ 관리자의 지속적인 관심과 관리 필요

개인의 메일이 감시되고 중앙에서 통제된다는 것은 개인의 인권침해에 해당될 수 있으며, 관리자가 전체 시스템의 이상유무와 필터의 추가 관리에 의해서만 새로운 유형의 스팸에 대응할 수 있다. 현재의 방식은 추가 비용이 너무 많이 요구되며, 시간이 지남에 따라, 솔루션 도입에 대한 효과를 기대하기가 점점 힘들어지는 문제점이 있다.

4. MTA형 SPAM 필터에의 요구점

이상에서 서술한 MTA형에서 문제가 되는 것은 아래와 같은 요구점이다.

■ 상세한 SPAM 룰에 대해서 사용자가 자유로이 설정이 가능한가?

■ 기존 시스템에 영향을 주지 않고 도입가능한가?

■ 대량의 SPAM처리에 견딜 수 있는 충분한 성능이 있는가?

상세한 필터설정을 사용자가 할 수 없다면 실제로 운영은 어렵다. 화이트리스트/블랙리스트의 설정이 가능한 것은 많지만 상세한 필터링 룰을 기술할 수 있는 것은 적다.

또, 시스템 도입으로 인한 업무를 최소화할 수 있는 환경이 제공되어야 한다. 만약, 새로운 시스템도입으로 인해 사용자의 설정 변경등의 요구가 필요하게 되면 효과를 기대하기가 힘들 것이다.

스팸의 특성상 단시간에 집약적으로 트래픽이 집중되었다가 사라지는 점을 고려할 때, 최고 메일처리량에 대한 요구가 많이 증가되었고, 이 값은 평균적인 처리 값과 많이 차이가 있어 점점 SMTP의 성능이 중요한 이슈가 되고 있다. 더욱이, 최근에 바이러스 중에는 스팸성을 지닌 것이 발견되고 있는데, 이들은 바이

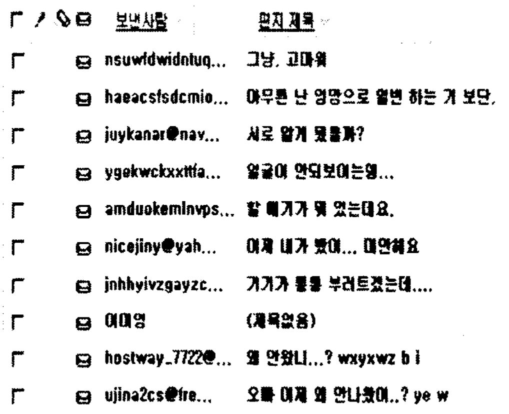
러스내부에 메일 엔진을 탑재한 채로, 불특정 메일서버에 대한 DDoS 공격을 감행하고 있어, SMTP의 성능은 이제 필수적인 확인사항이 되고 있다.

이상의 세 가지 조건을 충족하는 것으로 디프소프트사의 WBlock (http://www.deepsoft..co.kr)이라는 제품이 있다.

5. 새로운 필터링 방식의 제안

현재 필터링기술이 진화함에 따라 스패머의 송신술도 진화하고 있기 때문에 항상 새로운 필터링 방식을 생각하지 않으면 안된다.

현재, 스패머(SPAMMER)의 수법은 점점 교묘화되고 있다. 2003 Spam Conference 중에서 Paul Graham이 지적한대로 지인을 가장한 메일과 업무의 연락을 가장한 메일이 가장 대책이 어렵다. 제목에 "그냥 고마워"등과 같이 써있는 SPAM메일이 가장 늘어나고 있다. 또 [그림3]에 실제로 나에게 도착한SPAM메일을 보여주었는데, 이 샘플들은 기본적인 제목의 필터를 가지고는 정상메일과 구분할 수 있는 방법이 없다.



[그림 3] 제목으로 필터링이 어려운 스팸 샘플
[FIg. 3] The Sample of SPAM E-mail a Difficulty Filtering using a Title

이런 종류의 스팸을 차단하기 위해서 URL Prefetch방식에 의한 필터링을 새롭게 제안한다. 스패머의 목적은 메일을 읽게 해서 광고효과를 높이는 것에 있는데, HTML이나 각종첨부파일을 이용한 스팸은 기존기술로 대처가능하다. 그러나 최근의 스팸 메일은 본문의 내용이 링크로만 구성되어 있거나, 그림으로 구성되어 있어 경우가 많다. 메일자체에서 내용을 보여 주기보다 URL을 클릭 하도록 유도하여 웹 사이트에서 홍보효과를 보기 위한 전략이다. 이런 종류의 스팸을 대처하기 위한 방식이 URL Prefetch방식이다. URL Prefetch 방식은 다음과 같이 3가지 과정으로 이루어 진다.

1) 메일본문내의 URL 추출과정

2) Prefetch Agent를 통한 URL 방문 및 확인 과정

3) URL 주소 자체나 URL 컨텐츠에 대한 스팸 판정

Prefetch Agent의 결과는 캐쉬를 이용하여 일정기간 재사용할 수 있다. 이 방식을 이용하면 2 차, 3차에 걸친 URL 속임 기능도 대처가 가능하게 된다. 실제 사이트에서 본 기술을 적용하여 확인한 결과 [그림 4]와 같이 7% 이상의 스팸차단율 상승효과를 확인할 수 있었다. 그림에서 패턴필터부분이 URL Prefetch에 해당하는 부분이다.

구분	13~14	14~15	15~16	16~17	17~18	18~19	19~20	20~21	21~22	22~23	23~24	계	비율
합계	5109	8083	5456	5519	5602	6686	10329	8081	7572	7136	6499	302207	100
헤더정보	0	0	0	0	0	0	0	0	0	0	0	0	0
동량제한	0	0	0	0	0	0	0	0	0	0	0	0	0
첨부파일	0	0	0	0	0	0	0	0	0	0	0	0	0
동일문건	0	0	0	0	0	0	0	0	0	0	0	0	0
패턴필터	499	554	456	539	1207	1317	921	3617	2626	1660	3112	23629	7,818
메시지필터링	4610	5529	5000	4980	4485	5381	9408	4464	4946	5476	5377	278578	92,181
메일제목	2146	2394	2430	2346	2249	2808	4103	2526	2543	2519	2304	102757	34,002
메일본문	787	842	597	647	491	599	567	276	324	512	390	11531	3,946
본문URL	749	1062	991	917	778	923	931	729	1035	1335	1443	18873	6,245
메일헤더	928	1231	932	1170	957	1051	3807	931	1034	1110	1240	145317	48,085

[그림 4] URL Prefetch의 실험 결과

[Fig 4] Result Test of URL Prefetch

또 다른 방식으로는 HTML 유형 방식이 있다. 위의 URL Prefetch는 시스템 부하나 반응속도가 느린 반면, 이 방식은 기계가 생성하거나, 비정상적은 HTML의 유형을 분석하여 차단하는 방법이다. 예를 들어, [표 2]와 같이 HTML 태그로만 구성되어 있는 메일이나, HTML태그로 사용 불가한 태그를 포함한 경우를 분석하여 차단하는 방법이 가능하다.

```
<html>
<head>
<title>Untitled Document</title>
<meta http-equiv="Content-Type"
content="text/html;
charset=euc-kr">
</head>
<body leftmargin="0" topmargin="0"
marginwidth="0"
 marginheight="0">
<iframe src="http://lm1.ez.ro" name="2"
frameborder="0"
 width="420" height="650"
scrolling="no"></iframe>
</body>
</html>
```

[표 2] 태그들로만 구성된 스팸 샘플
[Table. 2] SPAM Sample a Component Tags.

6. 결론 및 향후과제

최근에 이슈가 되고 있는 스팸성 바이러스의 경우 바이러스를 내포한 메일이 다량으로 발송이 시도되어, 특정 서버의 서비스나 네트웍 트래픽을 갑자기 증가시킨다. 이 문제는 개인의 문제에서 사회적인 생산성 저하 문제로 부각되고 있어 스팸성 바이러스를 MTA에서 사전 차단하고자 하는 움직임이 나타나고 있다. 그러나, MTA에서 모든 트래픽을 처리할 수가 없기 때문에 트래픽 제어 기능이 포함되어야 한다. 이러한 기능은 단위 시간 내에 과도한 접속이나 스팸 혹은 바이러스로 판단되는 메일이 계속 유입될 경우 일시적인 접속을 거부함으로써 가능해 진다. 이것은 블랙 리스트와는 달리 한시적인 차단을 함으로써 정상적인 트래픽이 계속 차단될 수 있는 문제점을 보완할 수 있으며, ADSL이 보편화된 우리나라 실정에 맞는 새로운 차단 방식이다. 앞으로의 문제로는 컴퓨터 바이러스나 해커와 마찬가지로 스패머의 방식은 점차 진보하고 있다. 이러한 진보에 대응하기 위해서는 법제의 개편뿐 아니라, 스팸 패턴 분석, AI 기법 도입, 스팸 정보에 대한 정보 공유등이 함께 이루어져야 할 것이다.

참고 문헌

[1] 정보통신부,"정보화역기능 실태조사 보고서", 2000.12

[2] http://brightmail.com/

[3] http://ordb.org

[4] http://www.spamcop.or.kr/kor_main.jsp

[5] http://www.mirapoint.com/

[6] http://spamassassin.org/

[7] 2003 Spam Conference Proceedings(2003) http://spamconference.org/proceedings2003.html

[8] Douglas E. Comer, "Internetworking with TCP/IP, Vol 1 : Principles, Protocols, and Architecture", Prentice-Hall, Inc., 1995.

[9] Marshall Brain, "Motif Programming", Digital Press, 1991.

[10] Matthijs van Doorn, Anton Eliëns, "Integrating applications and the World-Wide Web", Proceedings of Third International World- Wide Web Conference, Vol. 27, No. 6, pp. 1105-1110, 1995.

[11] Moore, K., "MIME(Multipurpose Internet Mail Extensions) : Part Two : Message Header Extensions for Non-ASCII Text", RFC 1522, Univ. of Tennessee, 1993.

[12] Nathaniel S. Borenstein, "Metamail", Bell Communications Research, Inc. (Bellcore), 1991.

[13] J. Myers, "IMAP4 Authentication Mechanisms", RFC1731, 1994.

[14] Jonathan B. Postel, "Simple Mail Transfer Protocol", RFC 821, 1982.

[15] David H. Crocker, "Standard for the format of ARPA Internet Text Messages", RFC 822, 1982.

[16] IAN S. GRAHAM, "The HTML Sourcebook", John Wiley & Sons, Inc., 1995.

[17] Borenstein N. & Ned Freed, "MIME(Multipurpose Internet Mail Extensions) : Part One : Mechanisms for Specifying and Describing the Format of Internet Message Bodies", RFC 1521, Bellcore, Innosoft, 1993.

[18] Moore, K., "MIME(Multipurpose Internet Mail Extensions) : Part Two : Message Header Extensions for Non-ASCII Text", RFC 1522, Univ. of Tennessee, 1993.

[19] David H. Crocker, "Standard for the format of ARPA Internet Text Messages", RFC 822, 1982.

[20] Jonathan B. Postel, "Simple Mail Transfer Protocol", RFC 821, 1982.

[21] M. Crispin, "Internet Message Access Protocol-Version 4", RFC1730, 1994.

[22] M. Crispin, "Distributed Electronic Mail Models in IMAP4", RFC1733, 1994.

김 민 홍

1965 한양대학교 공학사
1976 고려대학교 경영대학원 경영학 석사
1996 아주대학교 대학원 공학박사
1981~현재 경기대학교 정보과학부 교수
관심분야 : 시스템프로그래밍 운영체제

두 창 호

1988년 경기대학교 수학과 졸업(이학사)
1996년 경희대학교 산업정보대학원 전자계산학과 공학석사
1997년- 현재 동남보건대학 웹컨텐츠개발과 조교수
2000년-현재 경기대학교 정보과학부 전자계산학과 박사과정
관심분야 : 시스템 프로그래밍 분산처리, 운영체제