情 報 保 護 學 會 誌
第17卷 第2號, 2007. 4

스팸메일 현황과 대응에 대한 고찰

권 영 관*, 염 흥 열**

요 약

스팸메일은 이메일이용자들에게 정신적인 피해, 경제적 손실을 주고 있어서, 스팸메일 방지대책이 매우 필요하다. 스팸방지대책의 하나로 스팸블랙리스트에 의한 스팸메일차단방법이 있으며 이메일수신자에게 스팸메일의 수신 양을 줄여주는 효과를 얻을 수 있어, 많은 ISP, 공공기관, 학교, 기업 등에서 이용되고 있다. 그러나 스팸메일 차단에 따른 선의의 이용자가 피해를 입는 경우가 있는 단점이 있다. 본 고에서는 다양한 스팸 대응 기법을 살펴보고, 우선 스팸 대응을 위한 대형 ISP의 사례를 살펴보았다. 우리나라 스팸대응효과는 스팸대응기관 중의 하나인 스팸하우스의 스팸발생 국가순위 등으로 확인한 바, '05.3.14일 현재 스팸발생국가 TOP 10 중에 우리나라는 3위, 스팸발생ISP Top 10중에 코넷망(kornet.net)의 스팸발생순위는 2위를 차지하였는데, '06.9월과 '07.2월의 국가순위는 6위로 개선되었고, 코넷망은 10위권 밖으로 Top 10에 나타나지 않게 되었으며 스팸 발생 건수도 상당량 감소한 것으로 나타나는 등 효과를 발휘하고 있는 것으로 분석되었다. 또한, 본 고에서는 바람직한 스팸 대응 방안을 제시하였다.

Ⅰ. 서 론

이용자에게 도달하는 전체의 이메일 중에서 스팸메일이 50~80%에 이르고 있고, 스팸메일은 이용자에게 정신적인 피해와 함께 생산성 손실, 경제적 손실을 초래하는 것으로 조사 되고 있다. 이러한 스팸메일을 방지하기 위하여 여러 가지 대응기술과 방법들이 단독 또는 복합적으로 사용된다. 효과적인 스팸메일 차단방법 중의 하나인 신뢰도평가시스템의 블랙리스트제한 방법이, 여러 국가의 메일서비스사업자, ISP(Internet Service Provider), 정부기관, 학교 등에서 적용되고 있다. 스팸대응기관들은 그러한 정책을 취하도록 유도하고 있으며 동참하는 ISP들이나 학교, 기업 등의 단체들이 점차 증가하는 추세에 있다.

스팸메일을 차단하기 위한 블랙리스트를 제공하는 기관들은 가능한 한 모든 스팸메일 정보를 수집하여 온라인으로 스팸차단을 원하는 기관이나 단체 등에게 제공하고 있으며, 메일 수신 서버를 운용하는 사업자나, ISP, 기업 등은 블랙리스트를 메일수신서버의 차단정책과 연동하여 스팸메일을 실시간으로 차단하고 있다. 이와 같은 스팸메일차단 방법은 이메일 이용자들의 스팸메일 수신량을 줄여주고, 스팸머들의 활동을 위축시키는 등의 효과가 있어 블랙리스트에 의한 스팸메일차단은 국내·외의 ISP, 정부기관, 학교, 기업 등으로 확산되고 있는 추세이다.

그러나 스팸메일 차단으로 인한 선의의 피해자도 발생하고 있어 이에 대한 대책이 필요하게 되었다. 즉, 스팸블랙리스트관리기관의 블랙리스트에 스팸메일 IP로 등록이 되면 이와 연동된 여러 나라의 ISP, 정부기관, 학교 등에서 메일이 차단되는데, C클래스 등의 IP 대역으로 차단이 이루어진 경우, 그 대역내의 IP를 사용하는 (스패머가 아닌)일반 이용자가 메일을 보내려고 해도 중간에서 차단됨으로 해서 상대방에게 메일이 도착되지 않게 된다.

본고에서는 스팸메일과 스팸차단 기술 및 방법에 대하여 알아보고, 주로 한국에서 발송하고 해외에 서 수신되는 스팸메일의 차단과 스팸메일의 차단으로 인한 일반 이용자들의 피해발생 과정을 알아본다. 이러한 피해를 줄이거나 예방하는 스팸대응활동에 대하여, 대형 ISP의 스팸대응사례를 중심으로 살펴보고 그 운영성과

* 카스정보통신 주식회사 (ceo@castel.co.kr)
** 순천향대학교 (hyyoum@sch.ac.kr)

및 결과를 분석하여 스팸을 억제하거나 줄일 수 있는 방안에 대하여 고찰하고자 한다.

Ⅱ. 스팸메일이란 ?

2.1. 정의

스팸메일이란 "이메일이나 휴대폰 등 정보통신서비스를 이용하는 이용자의 단말기로 본인이 원치 않음에도 불구하고 일방적으로 전송되는 영리목적의 광고성 정보를 말한다."[1] 일반적으로 스팸메일은 꼭 상업적인 목적의 메일만으로 한정하지 않고 본인이 원치 않는 메일은 스팸이라고 볼 수 있으며, UCE(unsolicited commercial e-mail) 또는 UBE(unsolicited bulk e-mail)라고 불리기도 한다.

2.2 스팸 메일 특성[2]

스팸메일은 대표적인 정보화 역기능 중의 하나로서, 대량으로 반복 전송되기 때문에 이를 받는 이용자의 짜증과 불편함을 유발하고 필요한 정보 수신을 방해하며 메일서버의 과부하를 초래하는 등 네트워크자원을 낭비하고 차단을 위한 사회적 비용을 증가 시키게 된다. 스팸메일의 특징을 살펴보면 다음과 같다.

• 원하지 않음(Unwanted) 또는 요청하지 않음(Unsolicited)

스팸메일의 핵심적인 특징으로 수신자가 원하지 않는다는 것이며 스팸의 최종목적지인 수신자입장에서 스팸을 판별하는 가장 기본적인 요소가 된다. 즉 전송자와 수신자간의 사전에 어떤 관계가 없음에도 불구하고 일방적으로 전송되는 것을 말한다.

• 상업성(Commercial)

전송되는 이메일의 목적이 어떤 상업성을 띄고 있다면 스팸을 구성하는 한 요인이 될 수 있으나 수신자가 원하는 상업성 이메일도 있을 수 있으므로 상업성이라는 요소가 스팸을 구성하는 절대적인 기준이 되는 것은 아니다. 다만 영리목적의 상업성 정보는 비영리정보보다 일방적으로 무분별하게 전송되는 경우가 많기 때문에 수신자가 원하지 않는 스팸이 되는 사례가 많다.

〔표 1〕 스팸메일로 인한 피해유형

구 분	1순위	2순위
정신적 피해	21.3%	26.9%
바이러스 감염	18.2%	24%
개인정보 유출	22.1%	13.7%
시간낭비	21.7%	11.7%
정보수신 방해	10.7%	16.1%
경제적 피해	5.7%	7.7%

주 : 중요도 순으로 2개 항목 복수 응답
출처 : 한국정보보호진흥원(2005년 정보보호 실태조사)

• 대량성(Bulk)

스팸의 큰 특징 중 하나가 대량성이라 할 수 있다. 최근 초고속정보통신망 환경을 기반으로 메시지를 대량전송할 수 있는 다양한 응용기술이 발달함에 따라 매우 손쉽게 불특정다수에게 수십만 또는 수백만통의 스팸을 전송할 수 있게 되었다.

• 기타 특징

스팸은 기술적 조작을 통하여 전송자의 신원을 숨기고 반사회적이거나 악의적이고 불쾌한 내용을 포함하여 반복적으로 불특정다수에게 전달된다. 또한 대부분의 스팸은 수신자의 동의 없이 수집되거나 판매된 이메일 주소 등을 이용하여 전달된다.

2.3 스팸메일의 영향[1]

스팸으로 인해 발생하는 가장 큰 문제는 수신자를 성가시고 짜증나게 한다는 정신적인 피해이다. 한국정보보호진흥원의 "2005년 정보보호 실태조사"('05.12월)에 의하면, 스팸메일로 인한 피해 중 인터넷 이용자들이 심각하게 생각하는 피해 유형은 〔표 1〕에서 보는 바와 같이 개인정보 유출(22.1%), 시간낭비(21.7%), 불쾌감·침해 등 정신적 피해(21.3%) 등의 순으로 나타났다.

또한 스팸으로 인한 피해는 스팸을 필터링하는데 근무시간을 낭비하고 생산성 손실을 가져오며, 스팸으로 발생한 각종 문제를 해결하기 위해 추가적인 자원을 투여하는 등 경제적 손실이 초래된다는 점이다.

Ⅲ. 스팸메일 현황

3.1 스팸 발생현황

정보통신부와 한국정보보호진흥원이 발행한 "2007

〔표 2〕 불법 스팸 상담, 신고 접수 현황

[단위 : 건]

구분	2001	2002	2003	2004	2005	2006. 6
신고	254	29,105	78,983	314,474	389,371	377,993
상담	2,669	15,290	19,556	11,854	7,671	22,666
합계	2,923	44,395	98,539	326,328	397,042	400,659

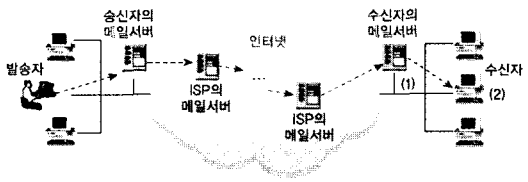
출처 : 2006정보화에 관한 연차보고서, p170

스팸메일 차단솔루션 활용가이드"에 의하면 이용자에게 도달하는 전체 이메일 중 스팸메일이 50~80%에 이르고 있다고 한다. 또한 한국정보보호진흥원의 "2006 스팸동향 및 2007 예측"자료에 의하면 2006년도의 일반이용자 1인당 일평균 이메일 스팸 수신량은 5.3통이며, 2007년에는 대출스팸 등 사회문제 스팸 지속, 국제 스패머의 한국인터넷 인프라 이용, 외국발 한국행 영어 스팸이 증가 될 것으로 전망하고 있다.[3] 정통부는 스팸메일로 인한 국민의 불편을 해소하고 건전한 정보통신 이용환경을 조성하기 위해 한국정보보호진흥원 내에 불법스팸대응센터를 설치하여 운영하고 있는데, 불법스팸 관련 민원상담 및 신고접수건수는 〔표 2〕와 같다.

3.2. 스팸메일의 차단방법[1][4]

메일의 전송경로는 〔그림 1〕과 같으며 메일발송자의 메일은 송신자의 메일 서버와 ISP의 메일서버를 거쳐서 수신 상대방의 메일서버를 통하여 수신자에게 메일이 전달되게 된다. 스팸메일의 차단 방법은, 메일서버를 운영하는 관리자나 개인 이용자가 가장 대중적으로 활용할 수 있는 기술적 대응방안으로 '필터링(filtering)'과 '인증(authentication)'기능이 있다.

스팸메일 차단을 위해, 스팸메일 필터링 또는 정상메일 인증 기능 등을 제공함으로써 정상메일과 스팸메일을 구별할 수 있는 "스팸메일 차단 솔루션"을 이용하는 방법이 있다. 스팸대응기술을 메일전송경로의 어느 단계에서 사용하는가에 따라 솔루션은 '서버용'과 클라이언트용으로 나뉘며, 서버용은 수신자의 메일서버(〔그림 1〕의 (1)) 단계에 설치하며 클라이언트용은 〔그림 1〕의 (2) 단계에 설치한다.



〔그림 1〕 메일 전송 경로

포털사업자 등의 웹메일서비스 이용자의 경우는, 해당 웹메일 서비스업체가 제공하는 다양한 스팸 필터링(서버 단계/이용자 단계)및 인증 서비스를 받을 수 있다. 메일전용 프로그램 이용자 중 별도의 솔루션 구입이 어려운 경우에는, 메일 수신 프로그램에 내장된 기본적인 스팸차단 기능을 본인이 직접 설정함으로써 일정 정도 스팸 차단효과를 거둘 수 있다.

가장 일반적인 스팸메일 차단방법으로는 스팸메일의 제목이나 내용에 존재하는 특정단어나 보낸사람을 이용하여 차단하는 방법이 있으며 대부분의 웹메일이나 메일 클라이언트에서 이를 지원한다. 그러나 이와 같은 방법은 스팸메일이라고 규정지을 수 있는 단어나 보낸사람에 대한 정의가 쉽지 않고 계속적으로 변화하는 스팸메일에는 적용하기 힘든 단점이 있다.

3.3 스팸방지기술[1]

스팸방지기술은 발송지, 통신네트워크, 수신자 컴퓨터 등 여러 수준에서 적용 가능하며 단독으로 사용할 수도 있고 여럿을 조합하여 사용할 수도 있다. 대부분의 스팸방지기술은 이러한 여러 요소를 조합하여 수상한 이메일(스팸)을 구별하는 규칙을 만들어 적용하고 있다.

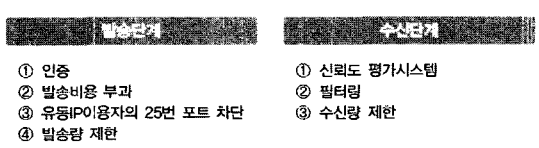
스팸방지기술은 2가지 단계로 구분하여 구현될 수 있는데, 하나는 이메일이 발송되는 발송측에 적용하는 것이며, 다른 하나는 이메일이 수신되는 수신측에 적용할 수 있는 것이다. 〔그림 2〕는 각 단계에서 사용할 수 있는 여러 기술적 대응방법을 나타낸다.

3.3.1. 발송단계 스팸방지기술

1) 인증

인증시스템은 특정 IP 주소의 이메일이 참인지 거짓인지 구분하여 다음 세 가지 중 하나를 알려준다.

• 발송자가 양호함 : 발송자가 특정 IP 주소에서 이



〔그림 2〕 스팸방지기술

메일을 보낸다고 사전에 선언했다.

- 발송자가 양호하지 못함 : 발송자가 특정 IP 주소 목록을 선언했지만 수신중인 이메일의 IP는 이에 포함되어 있지 않다.
- 발송자를 알 수 없음 : 어떻게 처리할지에 대한 정보가 불충분하다.

인증시스템이 특정 IP 주소의 이메일이 참인지 거짓인지 여부를 구분 하려면 이메일을 발송한 도메인 소유자는 자기 도메인에서 발송하는 이메일에 사용하는 IP 주소 목록을 선언해야 한다. 예를 들어 "ABC"라는 메일서버의 IP 주소 목록을 선언했는데 만일 누군가가 목록에 없는 IP 주소에서 접속하면서 "ABC"에서 보냈다고 주장한다면, 이 발송자가 이메일 주소를 위조하고 있다고 의심할 수 있다.

이메일 위조 문제 해결을 위해 지난 수년간 다양한 방안이 나왔으며 이와 같은 인증방법의 개요는 다음과 같다.

① SMTP[1] Authentication

SMTP Authentication은 이메일을 보내는 클라이언트(또는 보내는 이메일 서버)가 누구인지를 판별하기 위하여 이용자 계정과 암호를 이용한다. 인증 과정에서 필요한 이용자 계정과 암호는 일반적인 네트워크를 통해 전송되므로 패킷 가로채기와 같은 해킹 수법에 쉽게 노출된다. 이를 보완하기 위하여 이메일사업자는 SASL(Simple Authentication and Security Layer)[2] 기반의 인증방법을 이용하여 이용자 암호가 네트워크로 전송되는 것을 방지하여 안전성을 향상 시킨다.

② Sender Policy Framework(SPF)

SPF란 이메일주소와 발송서버가 일치하지 않는 이메일을 차단하는 방법이다. 즉 "스팸메일이 아니라는 것을 먼저 증명하지 않으면 무조건 스팸메일로 간주하는 것"이다. SPF는 이메일이 해당 이메일서버에서 정상적으로 발송되었는지를 확인함으로써 스팸메일을 통제할 수 있다. SPF는 도메인 신뢰도 평가시스템(Reputation System)과 연동하여 보다 효과적으로 사용될 수 있다.

③ Sender ID Framework(SIDF)

Sender ID는 Microsoft사에 의해 제안·확장된 형태의 SPF로 발송도메인 인증기능에 발송자 인증기능인 PRA[3] 기능을 추가한 인증기술이다

④ DKIM(Domain Keys Identified Mail)

DKIM은 야후(Yahoo)사와 Cisco사가 공동으로 제안한 이메일 메시지 인증방법이다. 발송도메인은 자신의 이메일서버를 통해 발송되는 이메일을 공개키 방식으로 서명하고 이를 수신서버에서 확인함으로 메시지 전송 및 발송과정의 위·변조를 원천적으로 방지할 수 있는 기술이다.

⑤ PKI 또는 PGP를 통한 인증

PKI(Public Key Infrastructure) 및 PGP(Pretty Good Privacy)는 공개키 방식의 이메일 암호화 및 전자서명 방법이다. PKI는 중앙집중식 인증서 관리를 통해 메시지의 전송과정 및 발송과정의 위·변조를 방지할 수 있는 기술이며, PGP는 이메일이용자간의 공개키 교환을 통해 동일한 효과를 얻을 수 있는 기술이다. 이 두 기술은 현재의 SMTP환경에서 메시지의 암호화, 서명을 통한 메시지의 암호화 및 무결성 보장 등을 위한 방법으로 사용되고 있다.

2) 발송비용 부과

개념적으로 스팸 문제를 해결하기 위한 가장 간단한 방법은 전통적인 우편물처럼 각 이메일마다 발송 대가의 지불을 요구하는 것이다. 이는 SMTP의 구조적인 변경에 의하여 구현될 수 있다. 예를 들어 Microsoft사는 이메일 발송에 드는 비용으로써 돈이 아니라 컴퓨터 사용시간으로 지불하는 방법을 제안했다. Microsoft사는 원치 않는 이메일에 대응하기 위하여 메시지 1통을 발송하는 데 소요되는 컴퓨터이용시간을 약 10초까지 늘릴 것을 제안했다. 이런 계획은 평범한 이메일 발송자에게는 아무런 영향을 미치지 않지만, 하루에 수백만 통의

1) 컴퓨터간에 이메일을 전송하기 위한 프로토콜(Simple Mail Transfer Protocol)

2) SASL은 인증서비스와 선택 사항인 보안서비스로 구성되어 있으며, 현재 주요 사용 대상으로 간주하고 있는 프로토콜에는SMTP, POP3(Post Office Protocol Version 3), IMAP (Internet Message Access Protocol) 등이 포함된다.

3) 이메일발송 권한이 허용된 발송측 이메일서버의 IP 주소(Purported Responsible Address)이다.

메시지를 발송하는 자에게는 막대한 컴퓨터 자원이 추가로 필요할 것이므로 스팸발송에 대한 상당한 억제요소로 작용할 것이다.

① Challenge & Response 또는 Bouncing Back
이는 필터링 위주의 스팸 처리방식이 수신서버에 부과하는 부하를 스팸메일 발송자에게 부담시키기 위해 고안된 방법으로써, 내부적으로 화이트리스트와 블랙리스트를 관리한다. 화이트리스트에 등재되어 있지 않은 이용자가 발송한 이메일은 발송자에게 확인메일을 발송하며 이에 응답 메일이 수신되면 해당 발송자의 이메일주소를 화이트리스트에 보관하여 추후에는 이러한 과정 없이 이메일을 사용할 수 있게 하는 방법이다.

② Online Stamp
인가 받은 대량 이메일 발송자는 암호화된 우표를 우표 제공회사로부터 구입하여 모든 발송 메시지에 첨부한다. 참여 ISP는 우표 제공회사가 제공한 우표 필터링 방식으로 우표를 확인하고 통과시킨다. 온라인 우표가 붙은 이메일은 ISP가 구현한 모든 스팸차단 방법을 자동으로 통과하여 수신자의 이메일수신함에 무사히 도착할 수 있다. 온라인 우표 모델은 스패머에게 금전적인 비용을 발생시켜 스팸을 발송하지 못하게 하는 방법으로써, 대량이메일발송자에게 일정량의 비용을 부과하여 스팸발송을 억제하는 방법이다.

③ Graylist
Graylist는 시스템에 처음 접속한 이용자에 대하여 한시적 접속제한을 하며, 일정기간이 지난 뒤 재접속 시도자에 한하여 이메일발송을 허용함으로써, 한 번 발송이 일어난 이용자에 대해서는 지연 없는 이메일발송을 허용해 주는 방법이다. 이는 대부분의 스팸이 이메일발송 시 발생하는 접속지연을 확인하지 않는다는 점에 착안한 것으로써, 소량 고품질의 이메일을 정기적으로 사용하는 이메일환경에 적합한 장치이다.

3) 유동IP이용자의 25번 포트 차단
인터넷을 통과하는 모든 이메일은 이메일 클라이언트와 이메일 서버간 통신 채널인 포트 25번을 사용한다. 포트 25번 차단은 효과적인 스팸방지 대책이다. 즉, 포트 25번을 차단하면 발송자(댁내 가입자, 유동IP 이용자)는 이메일을 보내기 위해 해당 ISP 이메일서버를 이용해야 한다. ISP 이메일서버를 이용하는 이메일은 ISP가 구현한 스팸방지 대응방법(예를 들면 속도제한)을 적용하여 통과 또는 차단할 수 있다. 그러나 포트 25번 차단에는 스팸뿐만 아니라 정상적인 이메일까지 차단하는 문제점이 있다. 이메일 발송을 위해 자신만의 이메일서버를 구동하여 원격지 네트워크의 이메일서버와 통신을 해야 하는 이용자들(예를 들면 웹호스팅 업체)도 있다. ISP는 이런 고객들의 포트 25번을 차단하지 않도록 해야 한다.

4) 발송량 제한
많은 양을 발송하는 이메일서버의 발송량을 제한함으로써 스팸을 줄이는 것으로, 적법한 이용자의 발송을 부적절하게 제한할 수 있기 때문에 발송량 제한은 불충분한 스팸발송 억제방안이다. 일반적으로 제한규칙은 1분, 1시간, 1일 기준으로 설정할 수 있다.

3.3.2. 수신단계 스팸방지기술

1) 신뢰도 평가시스템
신뢰도 평가시스템은 수신측 이메일서버가 발송측 이메일서버의 과거 신뢰도(Reputation)에 근거하여 어떤 것이 스팸이고 스팸이 아닌지를 결정하는 시스템이다. 이 시스템은 이메일 발송자의 IP 혹은 도메인별 이메일사용 이력을 기록함으로써 각 IP 및 도메인별 신뢰도를 평가하여, 스팸발송 등에 악용되는 IP나 도메인으로부터 발송되는 이메일은 수신하지 않을 수 있도록 한다. 즉, 수신허용(화이트)리스트를 유지하고 있으며, 반대로 수신거부(블랙)리스트도 가지고 있다.

① 화이트리스트 허용
발송자가 화이트리스트에 등재되어 있을 경우에 한하여 이메일을 수신하도록 스팸필터규칙을 설정함으로써 대량 스팸을 차단하는 것이다. 화이트리스트와 일치하는 이메일은 수신되고, 화이트리스트에 없는 곳으로부터 수신된 이메일은 삭제 또는 방역폴더에 저장된다. 화이트리스트에 등록된 경우 스팸차단 솔루션을 우회하여 통과시켜 준다.

② 블랙리스트 제한

블랙리스트는 차단하고자하는 이메일주소 목록으로 구성되며, 개인적인 이메일서버소유자에 의해 관리 및 유지될 수 있다. 이메일서버 소유자는 KISA-RBL, MAPS, ORDB 등의 블랙리스트를 선택하여 사용할 수 있다.

- KISA-RBL(Real-time Blocking List) : 한국정보보호진흥원(KISA)에서 무료로 제공하는 실시간 스팸차단리스트이다. 국 내외로부터 스팸정보를 실시간으로 취합하고 이를 다양한 기준에 따라 분석하여 스팸발송에 관련된 것으로 확인된 IP리스트를 생성하여 1시간 단위로 제공한다.
- MAPS(Mail Abuse Prevention System RBL List) : 스팸을 보내거나 릴레이하는 스패머에게 우호적이거나 중립적인 입장을 취하여 스팸에 악용되는 목록이다.
- ORDB(Open-Relay DataBase) : ORDB.org는 확인된 오픈릴레이의IP주소를 제공하는 비영리 기구이다. 오픈릴레이란 발송자를 가리지 않고 이메일을 배달하는 이메일서버를 말한다. 스패머는 이런 서버들을 이용하여 대량의 스팸을 발송하는 등 악용하고 있으므로 차단해야 한다.
- SBL(SpamHaus Block List) : 확인된 스패머의 IP 주소를 제공하는 데이터베이스이다.

2) 필터링

필터링은 가장 흔히 볼 수 있는 스팸방지기술이다. 필터의 가장 큰 장점은 구현이 쉽고, 이용자가 어느 메시지를 스팸으로 간주할 수 있는지를 결정할 수 있다는 점이다. 지능적 필터[4]에서는 이용자의 편지함에 도달하기 전에 특정 메시지를 차단하기 위해서 이용자가 특정 문자나 발송자 주소와 같은 기준을 정해야 한다. 스패머는 이러한 특정문자 차단방법을 우회하고자 철자를 일부러 틀리거나 다른 언어로 표기하는 방법을 사용한다. 이러한 스팸에 대하여 특정문자 차단방법은 효과적으로 대응할 수 없다. 이렇게 특정문자를 우회하는 스팸에 대응하기 위하여 베이지안 필터[5]를 사용하는데 장기간 학습 및 경험이 필요하다. 베이지안 필터는 스팸과 정상 이메일을 구분해야 하는 개인 이용자들이 참조할 수 있도록 전체 메시지에 대한 통계분석을 생성한다. 그런 후에 이 필터는 이용자가 이전에 정당한 이메일이라고 판별한 것과 유사한 메시지만 통과시키는 방법이다. 이러한 베이지안 필터도 우회하는 방법이 있어서 사용에 주의해야 한다.

① 정적 필터링

정적(Static) 필터링은 가장 기본적인 스팸방지기술로써, 대부분의 이메일 클라이언트와 서비스에 포함되어 있다. 본질적으로 이 방법은 수신 메시지의 다양한 특징에 기반을 둔 미리 정의된 필터링 규칙을 사용하여 이메일 이용자가 수신 메시지를 통제할 수 있는 환경을 제공한다. 필터링 규칙은 수신 이메일의 특성과 이용자의 환경설정 값을 비교하여 만들어진다.

② 적응 필터링

정적 필터링 방법의 가장 큰 단점은 필터링 규칙을 계속 만들어야 한다는 점이다. 스패머는 특정 문자 일치여부 규칙을 속이려고 정적 필터링 규칙을 우회하는 새로운 기법을 끊임없이 개발한다. 따라서 스패머들을 물리치기 위해 끊임없이 필터링 규칙을 재정비해야 하는데 일반 이용자에게는 너무 복잡한 과정이다. 적응(Adaptive) 필터링 방법은 최종 이용자가 수신 이메일의 특징을 분석하여 수작업으로 필터링 규칙을 만드는 대신, 소프트웨어가 수신 이메일의 스팸 여부를 지능적으로 판별하여 필터링 규칙을 자동으로 생성한다. 스팸처리에서 가장 널리 쓰이는 적응 필터링 접근법은 '02년 폴그레이엄(paul Graham)이 제안한 베이지언 필터링 접근법(Bayesian Filtering Approach)이다. 베이지언 필터링은 분석한 분포도를 기준으로 내부 분포도의 매개변수를 추정하는 베이지언 확률법칙을 전제로 한다. 베이지언 접근법의 장점은 특정단어의 출현 빈도수와 같은 일부 증거에 의존하지 않고 이메일 내용 전체를 대상으로 한다

4) 경험, 학습적으로 발전하는 필터(Heuristic filter)

5) 특정 텍스트에서 개별 단어의 출현 빈도를 모두 기록한 뒤, 비슷한 분류의 텍스트를 계속 샘플 자료로 추가시키면서 단어의 연관을 추적하여 임의의 텍스트가 해당 분류에 속하는지 여부를 파악하는 필터(Bayesian filter)

〔표 3〕 개정 정보통신망법 스팸방지가이드라인 요약[2]

구 분	내 용	규 제 내 용	벌칙	위치(P)
불법 스팸메일 이용제한	제50조의4 제1항 제1호	▸ 정보통신서비스제공자는 KISA의 통보를 받은 후 24시간 이내 이용제한 조치 (유동IP 이용자 포함)	1)	14P ~ 15P
		▸ 스팸메가 등록한 모든 서비스를 이용제한할 수 있는 범위 정의 - 모든 서비스가 스팸에 악용되고 있다는 객관적 정황이 있거나 불법에 악용된 특정서비스만 식별할 수 없는 경우		
불법 스팸메일 정보제공	제55조 제1항 및 제2항	▸ 정보통신서비스제공자는 KISA의 통보를 받은 후 48시간 이내 요청정보 제공 (유동IP 이용자 포함)	1천만원 이하 과태료	18P ~ 19P
		▸ 회원관리를 철저히 함으로써 요구시 불법스팸메일의 정확한 정보 제공		
불법스팸을 위한 한자 규제 신설	제67조 제1항	▸ 불법스팸메일와 영업상 이해관계가 있는 자로서 해당 광고행위를 하도록 직·간접적으로 지시하거나 요구, 지원, 선동, 조장, 유도, 공모하는 자로 정의 - 불법스팸메일의 마케팅 실적에 따라 이익을 배분하는 경우 - 불법스팸메일에게 광고를 하게 한 것으로 판단할 수 있는 객관적 정황이 존재하는 경우 - 이용자 관리 소홀로 지속적 불법스팸행위에 자원을 제공하는 경우	3천만원 이하 과태료	57P ~ 59P
기술적 조치 규제 강화	제50조 제6항	▸ 규제대상에 불법스팸메일 신원 또는 출처 은폐를 위한 기술적 조치 추가	1천만원 이하의 벌금 또는 1년 이하의 징역	40P, 46P ~ 47P
불법행위를 위한 스팸규제 신설		▸ 마약, 음란물 관련 등 불법행위를 하기 위한 목적의 스팸발송행위 규제 신설		55P

1) 정보통신망법 상의 처벌규정은 없으나, KISA의 이용자환을 불이행한 경우 통신위원회에서 과징금 부과 가능

출처: 스팸방지가이드라인(안)설명회, p2, 2006.3.3

는 것이다. 베이지안 필터는 스팸메일 집합과 정상메일 집합을 분석하여 스패머들이 사용하는 어휘를 학습한 후에 베이지안 확률을 사용하여 어떤 메시지가 스팸인지 여부를 가려낸다.

3) 수신량 제한

일정한 시간 간격으로 수신측 이메일서버에 도착하는 이메일의 양을 제한하는 것은 간단하지만 효과적인 방법이다. 알려진 신뢰하는 발송측 이메일서버에 좀 더 많은 수신량을 제공함으로써 신뢰도 평가시스템과 상호작용할 수도 있다. 이 방법의 장점은 이메일서버에 수신되는 스팸의 양이 감소될 수 있다는 점이며, 단점은 시급하며 중요한 이메일이 불필요하게 지연될 수 있다는 점이다.

3.3.3. 기타 스팸방지기술

1) 이메일주소 수집 차단기술

스패머가 이메일주소를 홈페이지에서 자동수집하지 못하도록 여러 형태로 변형함으로써 이메일주소를 숨겨놓는 방법이다. 이러한 방법은 Java Script 변환, ASCII Code 변환, CGI SSI 변환, 이메일 주소 이미지화 등을 통해 구현될 수 있다.

2) 이메일주소 자동생성 대응기술

스패머가 이메일주소를 생성하여 이메일을 발송할 때, 존재하지 않는 이메일주소에 대해 '수신자 없음'확인메일을 회신해주지 않도록 설정할 수 있는데 이것을 이메일주소 자동생성 대응기술로 볼 수 있다.

3) 웹메일 자동등록 차단기술

회원가입 단계에서 사람의 육안으로만 식별이 가능한 왜곡된 이미지를 무작위로 제시하여 제한시간 내 입력토록 하는 등의 HIP기술6)을 적용함으로써 자동 프로그램에 의한 무차별적인 계정생성을 제한한다.

3.4 스팸차단 관련 법령

정부는 날로 지능화되는 스팸을 보다 효율적으로 규제하기위하여 2004년 12월에 전화스팸에 수신자가 허락하는 경우에만 광고메일을 보낼 수 있는 Opt-in 규제를 도입한데이어 2005년 12월에 다시 "정보통신망이용촉진 및 정보보호 등에 관한법률"을 개정하여 불법스팸발송을 한 사람에 대한 처벌 등을 신설하였다. 또한, 정보통신서비스제공자에게 불법스팸발송자에 대한 정보제공을 요청할 수 있는 근거를 구체화하고, 정보통신부 및 한국정보보호진흥원의 요청 시 스팸발송자의 정보통신서비스를 즉시 이용제한 할 수 있는 근거를 마련하였다.[5] 그 주요내용은 〔표 3〕과 같다.

3.5 스팸대응 관련기관 및 역할

일반적으로 스팸대응과 관련된 업무를 하는 기관들은 전세계적으로 약 1000여개 이상으로 추정하고 있으며 스팸신고업무기관과 스팸블랙리스트 관리기관으로 나누어 볼 수 있다.

3.5.1. 스팸 신고업무 기관

개인이나 기업 등으로부터 스팸신고를 접수받아 해당스팸메일 관련 ISP에게 스팸 등의 행위를 신고하는

6) 사람의 눈으로만 인식할 수 있는 랜덤코드를 통하여 사람과 자동화 프로그램을 구별(Human Interactive Proof)

업무를 수행하며, Spamcop(미국), Spam-RBL(프랑스), myNet watchman(미국) 등이 활동 중이다. 대표적인 기관으로는 Spamcop(http://www.Spa mcop.net)을 들 수 있는데, 미국에 소재하는 Anti- spam 기관으로 1998년 인터넷 보호를 위한 서비스를 개시하였다.

일일 백만 건 이상의 스팸, 해킹 관련 불편사항을 접수하여 해당 ISP에 신고하는 활동을 하고 있으며 SCBL (SpamCop Block List) DB관리 및 서비스를 제공하고 있다.

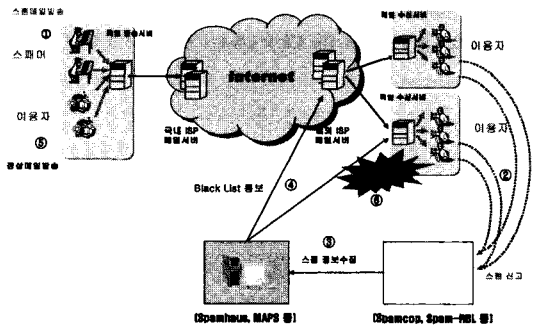
3.5.2. 스팸 블랙리스트 관리기관

스팸신고 업무기관의 자료 등을 수집하여 스팸송신 블랙리스트를 작성 등록 관리하며, ISP의 메일수신서버와 블랙리스트 관리기관의 DB를 실시간 연동하여 제공함으로서 스팸성 메일 수신을 차단되게 한다. 이러한 활동을 하는 기관으로는 Spamhaus(영국), MAPS(미국) 등을 들 수 있다.

- Spamhaus(http://www.spamhaus.org)는 영국에 소재하며 전 세계적으로 스팸방지를 목적으로 운영되는 단체로서, 1998년 설립되어 18명의 지원봉사자로 운영되고 있는 것으로 알려져 있다. SBL(The Spamhaus Block List), XBL(Expolits Block List), PBL(The Policy Block List)의 Block List DB를 운영한다. 이 단체가 제공하는 DB자료는 주요 ISP, 기업, 대학, 정부 등에서 사용되고 있다.[6]
- MAPS(http://www.mail-abuse.com)는 미국에 소재하며, 스팸방지 기술 개발을 목적으로1996년에 설립되어 초기에는 비영리로 운영하였고 2000년부터 서비스를 유료화하여 전세계 약 2000여개 기업과 ISP에게 RBL(Realtime Blackhole List)서비스를 제공하고 있다.
- 국내에서의 대표적인 스팸업무기관으로는 한국정보보호진흥원(KISA)을 들 수 있으며 KISA의 불법스팸대응센터(http://www.spamcop.or.kr)에서 불법스팸신고 및 처리 업무를 수행하고 있다.

Ⅳ. 스팸메일 대응 사례 및 분석

앞에서 살펴본 바와 같이 스팸은 이용자에게 시간적인 낭비와 경제적인 피해를 발생시키므로 스팸대응기관이나 ISP들이 스팸을 방지하거나 감소시킬 수 있는 방법들을 연구하고 개발하여 적용시키고 있다. 본장에서는 스팸메일 차단 업무의 흐름을 살펴보고, 스팸메일차단으로 인한 선의의 피해자가 발생하는 경우와 이에 대한 이용자의 불편을 최소화 할 수 있는 대처방안을 알아본다.



〔그림 3〕 스팸메일 차단 업무처리 과정도

4.1 스팸메일 차단 업무흐름

인터넷을 이용하는 메일전송은 국내의 메일전송경로와 해외의 메일전송경로가 크게 다르지 않으며 스팸메일차단 과정도 유사하다. 스팸메일차단 조치에 따른 선의의 이용자가 피해를 입는 경우가 있는데, 국내에서의 이용자의 피해 해소는 비교적 빠르고 쉽게 처리되나, 외국에서의 한국발 스팸메일 차단조치에 대한 스팸차단이 해제되기 까지는 많은 노력과 시간이 필요하게 된다. 따라서 한국에서 발송되는 스팸메일에 대한 해외에서의 메일수신서버차단과정을 중점적으로 살펴보기로 한다.

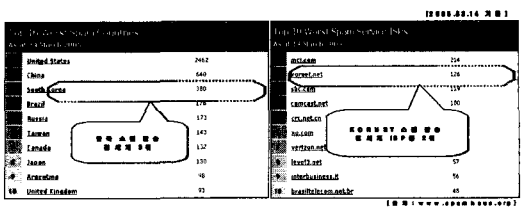
스팸메일 차단업무 처리과정도는 〔그림 3〕과 같으며 스팸메일의 차단과정은 다음과 같다.

① 스패머가 불특정 다수의 이용자에게 스팸메일을 발송하게 되면,

② 스팸을 받은 이용자는 Spamcop이나 Spam-RBL 등의 스팸신고업무를 하는 기관에 스팸신고를 한다.

③ 스팸신고업무기관은 스팸메일 발송자의 IP주소를 Spamhaus나 MAPS 등의 블랙리스트 관리기관에 통보한다.

④ 블랙리스트관리기관은 ISP, 기업, 대학, 정부 등에 블랙리스트를 통보한다. 블랙리스트 DB는 On-line으로 연동되어 바로 적용될 수 있으며, 블랙리스트 차단목록에 의해 해당되는 메일은 차단된다.



〔그림 4〕 10대 스팸발생 국가 및 ISP 현황

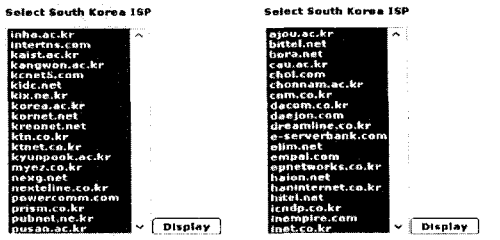
이때 유동IP대역내의 IP들에 의해 스팸메일이 발생되거나, 스팸을 발생하는 개별IP들이 여럿인 때는 C클래스나 B클래스의 IP대역을 차단하기도 한다. 가장 심각한 경우는 스팸메일을 전달하는 메일서버 IP를 차단하는 것이다.

⑤ 스팸메일들로 인해 C클래스 또는 B 클래스의 IP 대역이 차단된 경우 등에, 같은 IP대역의 IP를 사용하는 일반 메일이용자의 정상적인 이메일도 수신메일서버 측에서 차단(⑥)이 되어 수신자가 메일을 받지 못하게 되므로 선의의 피해자가 발생한다.

4.2 스팸 발생 및 차단 현황 사례

전세계적으로 스패머리스트나 스팸차단블랙리스트 DB를 유지하고 배포하는 기관은 많으나, 스팸하우스(Spamhaus) 처럼 국가별, ISP(사업자)별 순위를 공표하고 통계화하는 기관은 유일하다. 스팸메일 차단의 필요성이 커지면서 더욱 많은 ISP 및 메일서버 운용자들에게 SBL을 사용하도록 권유되고, 채택되어 가고 있다. 스팸하우스는 "Top10 worst spam countries(2007 2월 현재는 The 10 Worst Spam Origin Countries), Top 10 Spam service ISP's, The 10 Worst ROKSO[7] Spammers"의 리스트를 제공하고 있다. 따라서 스팸하우스의 SBL(Spamhaus Block List) 예를 적용하여 살펴보기로 한다.

〔그림 4〕에서 보는바와 같이 2005년 3월 14일 현재 우리나라는 스팸발생건수 380건으로 전세계의 스팸발생국가 SBL 3위에 올라 있으며, 코넷망(kornet.net)은 126건의 스팸발생을 기록하여 전세계 스팸발생ISP의 SBL 2위로 표시되고 있다. 코넷망에서의 스팸발생건수는 한국 스팸발생 건수의 약33%를 점유하고 있어 국가



출처 : http://www.spamhaus.org/sbl/isp_list.lasso

〔그림 5〕 대한민국의 스팸발생 ISP들 예시

순위에 큰 영향을 미치고 있는 것으로 나타났다.

또한 스팸하우스 홈페이지에서, 〔그림 5〕의 예시 화면에 나타나는 바와 같이 각 국가별로 스팸을 발생시킨 ISP의 목록을 확인 할 수 있으며 해당 ISP를 선택하면 스팸발생건수와 스팸발생 IP를 확인할 수 있다. 해당 스팸발생 IP들은 SBL에 등재되어 스팸 메일 차단에 사용된다.

4.3 스팸차단의 영향

스팸블랙리스트관리 기관의 블랙리스트에 등재되어 수신메일서버에서의 해당메일이 차단되면 정상적인 메일을 보내더라도 메일을 전달할 수 없게 된다. 예를 들어 스팸하우스 SBL에 포함되면 해외의 많은 국가 및 ISP에 의해 메일전송이 차단되는 결과를 가져오며, 국내 메일사용자의 서비스가 안 되는 등 선의의 피해자가 발생한다. 특히나 B클래스 또는 C클래스의 IP가 차단되면 그 대역내의 정상적인 이용자들도 메일이 차단되어, 즉 스팸블랙리스트관리기관인 스팸하우스의 블랙리스트(SBL)에 스팸메일 IP로 등록이 되면 이와 연동된 여러 나라의 ISP, 정부기관, 학교 등에서 메일이 차단되는데, 유동IP대역이나 C클래스 등의 IP 대역으로 차단이 이루어진 경우, 그 대역내의 IP를 사용하는 (스패머가 아닌)일반 이용자가 메일을 보내려고 해도 중간에서 차단됨으로 해서 상대방에게 메일이 도착되지 않게 된다. 이렇게 차단된 일반이용자의 메일은 IP가 차단되지 않은 국내나 해외의 다른 곳의 수신측에는 메일이 잘 전송되므로, 본인의 메일을 수신하지 못한 것을 나중에 알게 됨으로써 피해가 발생하기도하고, 차단이 해제되기 전 까지는 개인적으로나 사업적으로 꼭 필요한 상

7) ROKSO : Spamhaus' Register Of Known Spam Operations

대방에게 메일을 전송하지 못해서 생기는 피해나 불편사항이 발생하게 된다.

스팸하우스 등의 스팸대응기관에서 강력한 스팸메일 차단을 위해 메일서버IP를 차단하는 사례도 있는데, 이는 해당ISP에서의 스팸메일 발생이 계속되거나 발생량이 계속적으로 증가하는 때에 주로 취하는 조치로 추정된다. 메일서버 IP가 차단된 경우는 해당ISP의 모든 이용자의 메일서비스가 안 되는 등 피해규모가 매우 커지게 된다.

스팸메일차단의 효과를 높이기 위해 국제 블랙리스트기관에서 배포된 IP대역을 ISP또는 특정 회사 등에서 적용함으로써 이용자에게 전달되는 스팸메일을 차단하는데, 이와 같은 차단정책에 의해, 선의의 이용자들도 IP 대역의 Blocking에 의한 메일, 또는 인터넷 전체가 안 되는 경우가 상당량 발생하고 있다. 또한 스팸하우스의 Top 10리스트에 포함이 되면 스팸발생상위국 및 스팸발생상위 ISP로 인식됨으로 인한 이미지 손상과 함께 업무협력 등에 영향을 받게 된다.

4.4 스팸메일 대응 활동

4.4.1 스팸메일 대응 과정

스팸메일에 대한 대응 업무사례의 하나로 해외의 스팸메일차단에 대하여 ISP의 스팸메일차단 해제를 위한 대응사항을 중점적으로 살펴보면 다음과 같다.

ISP의 스팸대응부서에서의 평상시 스팸대응은 Spamcop, KISA 등으로부터 스팸정보를 수집하여, 해당 ISP망을 이용하여 스팸메일이 발송되지 않도록 하는 활동을 하며, 스팸대응기관들과 스팸정보를 공유하는 등의 협력체계를 확보한다.

① 스팸대응기관 등으로부터 수집된 스팸관련 정보를 분석하여 스팸메일이 발송되지 않도록 스팸차단정책에 반영한다.

② 스팸관련 정보 분석 등의 결과를 활용하여 또는 일반이용자가 발송한 메일이, 메일 수신측에서의 차단 등으로 전달되지 않는 경우가 발생하는 등의 사유로 불편사항이 접수되면,

③ 해당 스팸메일의 추적 조사 등을 통하여 스패머나 관련 고객을 찾아 경고 또는 해당 IP의 차단하는 등의 조치를 취한다.

④ 스팸발생의 차단이나 억제조치를 취한 후에는 스팸하우스 등에 해당 IP를 스팸블랙리스트에서 삭제해 줄 것을 요청한다. 스팸대응 및 차단조치기관들은 해당IP로부터 더 이상 스팸이 수신되지 않거나 문제가 없다고 판단되면 블랙리스트에서 삭제하는 조치를 취한다.

⑤ 스팸차단블랙리스트에서 해당IP를 삭제한 DB를 제공하면 메일수신서버의 차단이 해제되어 해당 고객의 메일이 수신자에게 전달될 수 있게 된다.

4.4.2 스팸메일 대응 및 조치

ISP들의 스팸대응부서는 스팸하우스, 스팸캅, KISA 등의 스팸대응유관기관들과 긴밀한 협력체계를 확보하여 스팸정보를 공유하고, 스팸메일차단정책에 반영하는 등의 활동을 한다. 보다 효율적이고 효과적으로 스팸메일에 대응하기위하여 스팸메일 관련 정보를 체계적으로 분석, 관리하는 스팸대응시스템을 구축 운용하는 ISP도 있다. 즉 스팸관련사항들에 대한 접수 및 응신업무를 자동화 하여 수작업에 의한 업무처리를 최소화함으로써 스팸메일 대응에 큰 효과를 얻을 수 있다. 자동화 시스템에 의한 처리가 안 되는 사항은 스팸대응부서의 운용자가 처리하며, 우선처리대상자를 선정하여(불편사항이 계속적으로 발생하는 이용자, 주요기업이나 단체 등) 처리하거나, 해당고객에 대한 원격 기술지원 조치 등으로 메일이용자의 불편사항을 해소할 수 있다.

ISP들은 스팸메일에 대한 신고접수 및 처리사항을 분석하고, 스팸대응기관의 블랙리스트를 연계한 차단정책을 마련하여 적용함으로서 신속하고 적절한 스팸메일 차단과 스팸메일감소 효과를 얻을 수 있다. 특히 스팸을 대량으로 전송하는 스패머와 많은 이용자들로부터 중복 신고 접수되는 스팸행위자를 끝까지 추적하여 적절한 조치를 취함으로써 스팸발생을 상당량 줄일 수 있다고 본다.

스팸메일을 차단하기 위한 블랙리스트를 제공하는 기관들은 가능한 한 모든 스팸메일 정보를 수집하여 온라인으로 스팸차단을 원하는 기관이나 단체들에게 제공하고 있으며, 메일 수신 서버를 운용하는 사업자나, ISP, 단체 등은 블랙리스트를 메일수신서버의 차단정책과 연동하여 스팸메일을 실시간으로 차단하고 있다. 이러한 스팸대응기관들의 스팸메일차단이 이메일 이용자들의 스팸메일 수신 양을 줄여주고, 스팸머들의 활동을 위축시키는 등의 효과를 나타낼 수 있다.

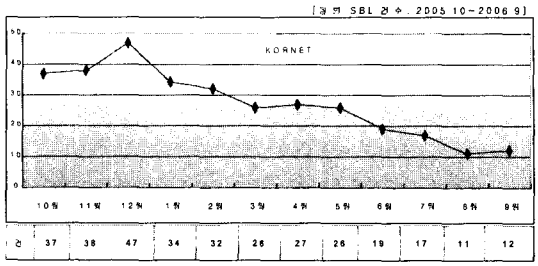
따라서 스팸대응부서에서는 스팸메일차단 조치와 함께 스팸차단으로 인한 일반이용자의 피해를 줄이는 방향으로 스팸대응을 하여야 한다고 본다. 그 방안중의 하나는 고질스패머를 찾아내어 스팸발생원을 차단하는 것으로 상당한 효과가 있는 반면에 많은 노력과 시간이 필요한 경우가 대부분이다. 또한 해킹 등으로 선의의 이용자의 IP가 도용되거나 선의의 이용자 시스템을 이용하여 스팸이 발생되는 경우가 있어 해당 가입자에 대하여 안내, 경고, 스팸억제를 위한 기술지원 또는 해당IP 차단 등의 조치가 필요할 경우도 있다. 메일서버의 차단 정책적용에 있어 일반적인 방법(패턴필터링, 베이지안 필터링, URL chaser[8], 바이러스필터링 등)들의 적용과 함께, 국제 스팸기관의 블랙리스트의 IP와 연계한 차단 정책이 효과적이다. 특히 스팸차단정책의 적용에 있어서도 그 동안의 스팸대응 분석 자료와 스팸대응기관들의 스팸정보를 분석하여 가장 많은 스팸메일 발생IP들을 우선순위화하여 적용한다면 스팸발생IP 전체를 차단하는 것보다, 소요되는 자원이나 노력면에서 상당한 효과를 얻을 수 있을 것이다.

코넷망을 운영하는 대형 ISP인 KT는 스팸메일 발생을 줄이고, 스팸메일로 인한 고객 불편사항을 해소하기 위한 스팸대응센터를 운용하고 있다. KT스팸대응센터는 블랙리스트 IP대역에 대한 해제조치와 스팸메일 발송 IP에 대한 주기적인 분석과 점검 등 적극적인 스팸메일 방지활동을 하여 스팸진원지라는 오명을 벗어나고 있다.[7][8]

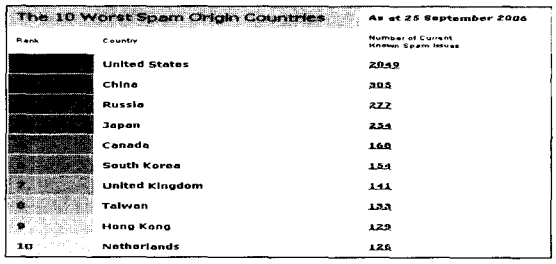
4.5 스팸대응활동 결과

스팸대응활동의 결과는 그 효과나 영향이 여러 형태로 나타날 수 있는데, 스팸하우스의 SBL현황 사례를 위주로 분석해 본다. [그림 7]은 스팸하우스에서 공표한, 코넷망의 IP로 스팸을 발생시킨 SBL 현황으로, 2005년 10월부터 2006년 9월까지의 기준일 평균스팸 발생건수를 그래프로 나타낸 것이다. 스팸메일 발생에 따른 SBL 등록은 스팸메일차단으로 이어지며, 그 건수는 점차 감소하는 추세를 보이고 있다.

보편적으로 선의의 피해를 해소하기 위한 해당IP를 스팸하우스에, SBL의 목록에서 삭제하도록 요청을 하여도 즉시 반영이 안 되는 경우가 많다. 특히 단독IP가 아닌 C클래스나 B클래스 단위로 차단된 경우에는 그 대역의 모든 IP가 스팸을 보내지 않는다는 신뢰를 얻기 전에는 SBL에서 삭제되기가 쉽지 않기 때문이다.

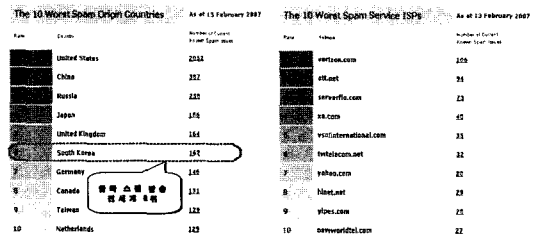


[그림 7] 월별 스팸하우스 SBL 건수



(출처:http://www.spamhaus.org/statistics/countries.lasso)

[그림 8] 스팸하우스의 국가별 SBL 순위

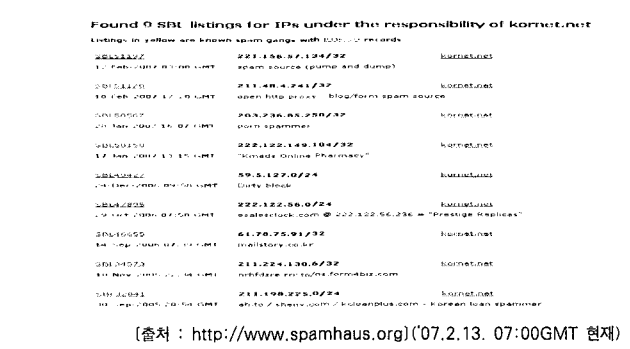


(출처 : http://www.spamhaus.org)

[그림 9] 스팸하우스의 국가별, ISP별 SBL 순위

2006년 9월 25일 현재의 국가별 스팸하우스 SBL 순위는 [그림 8]과 같으며, 미국 2049건(1위), 중국 305건(2위), 러시아 277건(3위), 일본 254건(4위), 캐나다 168건 (5위), 한국은 154건(6위)을 나타냈다. 국가별 SBL 순위는 인터넷사용 인구에 비례하는 경향이 있는데. 상

8) 스팸메일내의 URL을 해당 site를 검사하여 스팸일 경우 차단하는 방법으로 URL을 분석하여 해당 site까지 확인하여야 하므로 다소 성능에 지연을 가져올 수 있다.


Found 9 SBL listings for IPs under the responsibility of kornet.net

Listings in yellow are known spam gangs with [illegible] records

[illegible]	221.158.97.134/32	kornet.net
	spam source (pump and dump)	
[illegible]	211.48.4.241/32	kornet.net
	open http proxy - blog/form spam source	
[illegible]	203.236.65.230/32	kornet.net
	porn spammer	
[illegible]	222.122.149.104/32	kornet.net
	"Xmas Online Pharmacy"	
[illegible]	59.5.127.0/24	kornet.net
	Dutty block	
[illegible]	222.122.56.0/24	kornet.net
	ezaleclock.com @ 222.122.56.236 = "Prestige Replicas"	
[illegible]	61.78.75.91/32	kornet.net
	mailstory.co.kr	
[illegible]	211.224.130.6/32	kornet.net
	mhfdare.re.to/ml.formabiz.com	
[illegible]	211.198.225.0/24	kornet.net
	gb.to / shens.com / kloanplus.com - Korean loan spammer	

〔출처 : http://www.spamhaus.org〕('07.2.13. 07:00GMT 현재)

〔그림 10〕 스팸하우스의 Kornet.net의 SBL 등록 내역

대적으로 그 규모가 작은 대만이나 홍콩이 10위권에 올라 있는 것은 많은 중국의 해커 및 스패머들의 활동장소로 활용되고 있는 것으로 추정된다.

코넷망에 대한 스팸하우스 SBL 순위는 KT스팸대응센터의 적극적인 스팸대응활동으로 인해 '06년 9월 현재 10위권 밖의 순위를 유지하고 있으며 그 발생량도 줄여가고 있다. 코넷이 국가순위에 차지하는 비율은 8%(12건) 정도이다. '07.2.13일 현재의 스팸하우스 SBL순위를 살펴보면 [그림 9]에서 보는바와 같이 한국의 국가별 순위는 '06.9.25일의 순위와 같은 6위를 나타내고 있으며 스팸발생건수는 154건에서 164건으로 약간 증가되었다. '05.3.14일과 비교해보면, 한국의 SBL 순위는 3위(2005.3.14.현재)에서 6위로 크게 개선되었으며, 코넷망의 SBL순위는 2위(126건)에서 10위권 밖의 순위를 유지하고 있는 것으로 나타났고, 코넷망이 한국의 국가순위에 미치는 영향은 33%정도(126건)에서 8%정도(12건, '06.9.25), 6%정도(9건,'07.2.13)로 감소하였다.

이와 같은 결과에서 알수 있는바와 같이 해외로의 메일전송량이 많은 코넷망의 스팸대응활동이 스팸발생건수를 줄이고 결과적으로는 스팸하우스의 SBL 국가순위를 낮추어 우리나라의 스팸에 대한 이미지를 개선하는 효과를 거두었다고 본다. 그러나 '06.9.25일과 '07.2.13일의 스팸하우스의 SBL 순위를 비교해보면, 국가순위에 큰 영향을 미쳤던 코넷망의 스팸발생건수의 점유율은 7.8%에서 5.6%로 감소하였음에도, 한국의 스팸발생건수는 154건에서 162건으로 5%정도 증가하였고 국가순위는 같은 6위를 나타내고 있다.

이상의 결과에 의해서, 코넷망을 운용하는 ISP인 KT 스팸대응센터의 적극적인 스팸대응활동이 스팸발생을 감소시키고 스팸에 대한 우리나라의 이미지를 개선하는 효과를 얻고 있음을 알 수 있으며, 코넷망의 스팸발생은 줄었는데 오히려 우리나라의 스팸발생건수는 증가하는 현상이 나타나 메일서비스 사업자나 타 ISP, 학교 등에서도 적극적인 스팸메일대응활동을 전개한다면 우리나라의 스팸발생건수를 크게 줄이고 나아가 스팸발생국의 오명을 떨쳐 버릴 수 있다고 본다.

V. 결 론

스팸메일은 지식정보화시대 역기능 중의 하나로서 이용자 등에게 정신적, 경제적 피해를 가져오게 되어 스팸메일을 억제하거나 차단하는 스팸메일방지대책이 필요하다. 가장효과적인 방법은 스팸메일을 발생시키지 않는 것이나, 이메일은 단순한 텍스트뿐 만아니라 다양한 형태의 멀티미디어 자료 전송까지 손쉽게 전송할 수 있고 전송비용이 거의 들지 않는 경제적 장점 등으로 인하여, 이메일을 저비용고효율의 마케팅 툴로 이용하는 스패머들이 늘고 있어 스팸메일도 첨차 증가하는 추세에 있다. 스팸메일의 차단은 발송단계에서 차단하는 경우와 수신단계에서 차단하는 방법을 들 수 있는데, 발송단계에서의 차단방법은 메일서비스 사업자나 ISP 등의 스팸차단정책을 우회하거나 스팸으로 인지하기 어려운 경우 등으로 스팸메일이 발송될 수 있다. 따라서 수신단계에서 또 다시 차단하면 이메일 이용자의 스팸메일 수신을 줄일 수 있어 효과적이다.

스팸 대응기관들은 스팸메일 수신을 줄이고 더 나아가 스팸메일의 발생을 억제하기 위하여 스팸블랙리스트를 ISP, 학교, 정부기관, 특정기업 등에 제공하고, 블랙리스트를 현행화하는 등의 관리를 하고 있다. 스팸블랙리스트에 의한 스팸메일 차단 방법을 채택하는 ISP, 학교, 기업 등이 늘어나면서 스팸차단 효과도 커지고 있다. 그러나 스팸메일 차단에 따른 선의의 이용자가 피해를 입는 경우가 발생하므로, ISP, 학교, 기업 등에서는 스팸발생을 억제하기 위한 차단정책 적용과 함께 선의의 피해자가 발생하지 않도록, 차단된 스팸메일의 IP가 스팸블랙리스트에서 삭제되기 위한 조치가 필요하다.

이러한 필요성에 의해 활동을 시작한 KT스팸대응센터의 적극적인 스팸대응결과로 나타난바와 같이 스팸대응 활동초기 ('05.3.14일 기준)와 '07.2.13.현재의 수준을 비교해보면, 한국의 SBL순위는 3위에서 6위로 개선되었으며, 코넷망의 SBL순위는 2위에서 10위권 밖의 순위를 유지하고 있는 것으로 나타났다. 대응초기에 "Top

10 worst service ISP's"에 2위를 나타낸 코넷망은, 한국의 스팸발생건수 380건 중에 126건으로 33%정도였으나, '07.2.13일 현재는 한국스팸발생건수 162건 중 코넷망은 9건으로 6%정도로 크게 개선되었다. 또한 코넷망에서의 스팸발생건수는 126건에서 9건으로 대응초기의 7%수준으로 감소하였다. 따라서 KT스팸대응센터의 적극적인 스팸대응활동이, 메일전송량 등 인터넷 트래픽이 매우 큰 코넷망의 스팸발생건수를 줄이고 결과적으로는 스팸하우스의 SBL 국가순위를 낮추어 우리나라의 스팸대응에 대한 이미지를 개선하였다고 볼 수 있다.

그러나 국제인터넷에 가장 넓은 대역을 확보하고 있고, 대 규모의 가입자들이 이메일을 이용하는 코넷망의 스팸메일 건수의 감소 및 전체스팸발생건수에 대한 점유율이 감소('06년9월 : 7.8%에서 '07년2월 : 5.6%로)한 것과는 달리 전체 스팸발생건수는 증가하는 현상을 나타내었다. 이는 코넷망에서 감소한 스팸발생건수보다 더 많은 스팸메일이 발생하고 있는 것으로 메일서비스 사업자, 타 ISP, 학교 등에서도 적극적인 스팸대응활동을 한다면 스팸메일을 줄이고 국가의 이미지 향상에 크게 기여할 수 있을 것으로 생각한다. 스팸메일을 줄이는 효과적인 차단정책이나 감소방안들이 적용되어도 스패머들은 이를 우회하는 등의 새로운 방법들을 찾아내어 끊임없이 스팸메일을 발송하고 있으므로 이에 대한 대응도 지속적으로 효과적인 방법을 찾아내는 꾸준한 노력의 운영이 필요하다.

스팸메일을 줄이기 위하여 한국정보보호진흥원은 일반이용자가 알아야할 사항과, 웹사이트/메일서버관리자가 알아야할 사항, 광고성정보전송자가 준수해야할 사항, 스팸방지 관리 감독의 의무사항 등의 스팸방지수칙, 스팸메일 차단방법 등을 공지하고 있다. 이러한 권고와 방법들을 실천하는 스팸메일 감소방안을 메일 이용자들이 준수하고, 메일서비스 제공자들이 적용·운영한다면 스팸메일감소에 상당한 효과를 얻을 수 있을 것이다. 그러나 스패머들은 스팸메일 발송을 계속적으로 시도하여 스팸메일을 발송할 것이므로, 메일서비스를 제공하는 ISP등이 메일서비스 단계에서 차단하는 등의 대응을 한다면 스팸메일 감소에 더욱 큰 효과를 발휘할 수 있을 것이다.

스팸메일에 대한 대응에는 여러 형태의 방법들이 있겠으나 다음과 같은 방법들이 효과적인 바람직한 대응방법이 될 것으로 본다.

스팸메일의 생산을 방지하거나 줄이기 위해서는 스팸메일의 발송을 차단함이 효과적일 것이며, 메일의 발송량을 제한하거나 발송비용을 부과하는 방법을 적용한다든지 발송단계에서 스패머 블랙리스트에 의한 차단정책 적용 등을 들 수 있다. 또한 메일발송전에 웜바이러스 등의 감염여부를 확인하여 차단정책을 적용한다든지 해킹 등에 의해 선량한 이용자의 PC 또는 서버가 전문 스패머의 스팸발송매개체가 되지 않도록 보안대책이 강구됨이 바람직하다. ISP, 학교, 기업체, 정부기관 등은 네트워크에 스팸차단시스템을 설치하여 적절한 스팸차단정책을 적용·운영하면 스팸메일차단 효과를 더욱 높일 수 있을 것이다. 발송단계에서의 차단이 이루어지지 않거나 차단방법들을 회피하여 발송되는 스팸메일에 대해서는 수신단계에서 차단하여야 하는데, 메일서버의 스팸차단정책에 스팸대응기관들의 스팸메일블랙리스트에 의한 차단정책을 포함하는 방법이 신속하고 효과적인 대응에 도움이 될 것이다.

이와 같은 방법들과 함께 메일서버, 스팸차단시스템 등의 운영결과와 스팸메일 블랙리스트에 의한 차단IP 등에 대한 주기적인 분석을 통하여, 중복적이고 고질적인 스패머나 스팸을 다량으로 발송하는 IP들에 대한 우선순위(TOP10, TOP 50, TOP100 등)를 정하여, 집중적으로 스팸발송 IP를 추적하고 경고, 차단 등의 적절한 조치를 취함으로서 스팸발송을 억제하거나 스팸메일의 차단에 효과적일 것이라 생각한다.

참고문헌

[1] MIC, KISA, "2007스팸메일 차단 솔루션활용 가이드", 정보통신부, 정보보호진흥원, http://www.kisa.or.kr/kisa/spam/*2007스팸메일차단가이드.pdf*, pp 8, pp 14~15, pp 18~19, pp 64~78, Jan 2007.

[2] MIC, KISA, *스팸방지가이드라인(안)설명회*, 정보통신부, 정보보호진흥원, pp4~5, pp2, 2006.3.3.

[3] http://www.kisa.or.kr/06년 *스팸현황 및 07년 예측.pdf*

[4] URL빈도분석을 이용한 스팸메일 차단 방법, *정보보호학회논문지* 제14권 제6호, 2004.12.

[5] 대한민국정부, *2006정보화에 관한 연차보고서*, pp 170~171, 대한민국정부, http://www.mic.go.kr, 2006.11.22.

〔6〕 http://www.spamhaus.org
〔7〕 "KT, 하나로 스팸진원지아니야", *서울신문*, 17면, 2005.7.17.
〔8〕 "한국스팸발송 세계3위 오명", *국민일보*, 14면, 2005. 7.17.

< 著 者 紹 介>

권 영 관 (Young-Kwan Kwon)
종신회원
1986년 2월 : 서울산업대학교 전자공학과 졸업(학사)
1990년 9월 : 연세대학교 공학대학원 전자공학과 졸업(석사)
1982년 1월~2000년 3월 : 한국통신, KT 부장, 국장
2000년 3월~2005년 4월 : KT 중앙데이터통신국장, 인터넷기술담당(상무)
2005년 4월~2006년 12월 : KT Linkus 신사업추진본부장
2007년 1월~현재 카스정보통신 주식회사 사장
2002년 1월~현재 : 한국정보통신기술사협회 부회장
2002년 1월~현재 : 한국인터넷기반진흥협회 이사
현재 : 정보통신기술사, CISSP
<관심분야> 네트워크보안, 망관리 및 보안관제, Security Service

염 흥 열 (Heung-Youl Youm)
종신회원
1981년 2월 : 한양대학교 전자공학과 졸업(학사)
1983년 2월 : 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월 : 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사, 현 총무이사
2004년 1월~현재 : 한국인터넷정보학회 이사, 논문지 편집위원
2004년 1월~현재 : OSIA 이사
2003년 9월~2004년 3월 : ITU-T SG17/Q10, Associate Rapporteur
2004년 3월~현재 : ITU-T SG17/Q9 Rapporteur
2006년 11월~현재 : 정통부 정책자문단 정보보호 PM
<관심분야> 네트워크보안, 전자상거래보안, 공개키 기반구조, 부호이론, 이동통신보안