스팸메일 방지를 위한 제도적 기술적 해결방안에 관한 연구

강장묵* · 유의상** · 이정훈***

The Study about Solution for The Protection of Spam Mails

Jang Mook Kang* · Eui Sang Yoo** · Jung Hoon Lee***

■ Abstract ■

Spam mail is one of the side effect of the development and improvement of the internet that restrains the privacy of the individual on line. However indiscriminate application of Spam mail blocking can also cause significant violation on freedom of doing business to the fluent commercial transactions on line. Therefore this research looks at the exact understanding of the concept of Spam mail and inquiry on its issues. Also it looks at the case studies of its institutional solutions in USA and Europe as well as the advantage and disadvantage of the case studies on its technical solution. Finally, the research inquires into overall prevention of Spam mail, which considers both technical and institutional solution. With this research, limitations of current Spam mail prevention system and technology are pointed out and more effective course of overall Spam mail prevention solution is studied.

Keyword : Spam Mail, Privacy

1. 서 론

2003년 1월, 현재 우리나라의 인터넷 이용인구는 2500만 명을 넘어섰으며, 온라인 주식거래 비중은 67%(일본 3.8%, 대만 7.6%)이고 온라인 쇼핑몰 이용은 31%(미국 32%, 독일 26%)에 이르러 경제협력개발기구(OECD) · 국제전기통신연합(ITU) 등 국제기구에서 벤치마킹 대상(초고속 인터넷 부문)

* 서경대학교 컴퓨터공학과
** 소프트웨어공제조합
*** 고려대학교 정보보호대학원

으로 추천되었다. 그리고 인터넷 이용자 중 월 1회 이상 사용하는 이메일을 가진 사람은 84.4%에 이르고 있다[1]. 그러나 정보화시대의 역기능 중 하나로서 스팸(Spam)메일의 문제가 제기되었고, 오늘날 인터넷상의 네트워크 운영자, 기업 및 여타 조직과 개인사용자들에게 이르기까지 광범위하게 문제를 야기하고 있다. 스팸메일로 인한 문제는 그 규모와 정도가 날로 심각해지고 있으며, 문제의 해결을 위한 여러 다양한 시도와 노력들에도 불구하고 효과적인 해결방안을 찾기가 쉽지 않다.

미국의 경우, 스팸메일로 인한 2002년 총 비용이 89억 달러에 이르렀고, E-Mail 중 30%에 달하는 양이 스팸메일이다[2].

본 연구에서는 스팸메일의 개념을 이해하고, 어떠한 문제들을 유발하고 있는지에 대해 먼저 알아보고, 그러한 문제점들을 해결하기 위해 제도적, 기술적 해결방안을 살펴보았다. 특히, 제도적인 해결방안과 기술적인 해결방안에 대한 사례로 미국과 유럽(EU) 그리고 우리나라 등을 비교 연구하였다. 결론에서는 제도적, 기술적 해결방안의 한계점들을 근간으로 스팸메일에 대한 종합적인 해결방안을 제시하였다.

2. 본 론

스팸 메일은 정보화 사회의 대표적인 역기능으로 헌법이 보장하는 표현의 자유와 개인의 프라이버시보호라는 문제점 등을 유발하였다. 이러한 스팸 메일의 해결방안으로는 크게 제도적(법) 해결방안과 기술적 해결방안으로 나누어 고찰해 볼 수 있다. 본 장에서는 스팸 메일에 대한 정의와 문제점을 전반적으로 살펴보고, 각각의 해결방안이 가지고 있는 장점과 한계점을 함께 고찰해봄으로 종합적인 해결방안의 필요성을 확인하고, 결론에서 제시할 종합적인 해결방안의 도출을 유도하여 보았다.

2.1 스팸메일의 정의

수신자의 의사와 상관없이 일방적으로 전달되는 광고성 전자우편을 뜻하는 용어로는 스팸메일(Spam Mail), 정크메일(Junk Mail), 벌크메일(Bulk Mail), UCE(Unsoilicited Commercial E-Mail) 등이 있다. 이와 같은 다양한 용어 중 본 연구에서는 편의상 스팸메일[3]을 사용한다.

일반적으로 스팸메일은 "발신자가 동의 없이 일방적으로 수신자에게 원치 않는 메시지를 전송한 것"이라고 할 수 있다. 따라서, 발신자의 동의 없이 일방적으로 수신자에게 원치 않는 메시지를 전송한다는 의미에서 "표현의 자유", "정신적 시달림(Nuisance Harassment)", "개인 영역의 침투(Trespass)" 등의 법적 문제가 발생한다. 또한 학자마다 견해차이가 있으나, 스팸메일은 크게 UCE(Unsolicited Commercial E-mail : 원하지 않는 상업적 이메일)와 UBE(Unsolicited Bulk E-mail : 원하지 않는 대량의 이메일)로 구분이 된다. 이러한 일반적 분류와 개념 이해에는 아래의 세 가지 기본적인 특성들이 포함된다.

2.1.1 원하지 않음(unsolicited)

스팸메일에 대한 모든 정의의 핵심적 요소는 이메일 메시지가 원하지 않는 것이어야 한다는 것이다. 일반적으로 당사자들이 사전에 관계를 맺고 있지 않았거나 수신자가 메일의 수신에 동의하지 않

1) 한국인터넷백서, 한국전산원, 2002. p.54.

2) Ferris Networks, Brightmail (ww.brightmail.com) 참조, 89억 달러에 이르는 비용으로는 IT 자원 손실, Help-desk 지원, 생산력 손실 등으로 나누어 분석하였다.

3) 정보통신망 이용촉진 및 정보보호 등에 관한법률 참조 스팸메일이라 함은 다음 각 호의 1에 해당하는 전자우편을 말합니다
가. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 50조 1항의 규정에 의하여 수신자의 거부의사에 반하여 전송되는 영리목적의 광고성 전자우편
나. 수신자의 동의없이 전송되는 영리목적의 광고성 전자우편

은 경우, 그 메일은 원하지 않는 것이라 할 수 있으며, 또한 수신자가 관계의 종료를 위하여 상대방에게 수신거부의사를 통지한 경우(Opt-Out)에도 마찬가지라 할 수 있다.

2.1.2 상업적(Commercial)

이메일 메시지가 발송자의 재화나 용역의 판매 촉진을 위한 상업적인 내용을 담고 있다면 이는 스팸메일로 간주될 수 있다. 그러나 상업성의 판단은 이메일발송자의 실제적인 동기보다는 그 메시지의 내용에 의해 결정되는 것이기 때문에 자동화된 기술적 방법을 이용한다 하더라도 쉬운 문제가 아니다. 따라서 '상업적'에 대한 적절한 법적인 정의가 요구되고 있다.

2.1.3 대량(Bulk)

스팸메일에 대한 가장 현실적인 문제는 메시지의 내용보다도 그 대량성에 있다고 할 수 있다. 최근에는 스팸메일을 여과하거나 차단하기 위한 기술들이 발달함에 따라 발송 방법 또한 매우 다양해졌는데, 동일한 내용의 메시지라도 각각의 메시지에 약간의 특성을 부여하기도 하고, 일정기간 동안 나누어 발송하기도 하기 때문에 기술적인 방법을 통해 스팸메일을 판별해내는 것이 매우 어려워졌다. 그러므로 대량성의 판단을 위한 메시지의 '발송량' 및 '발송기간'에 대한 명확한 기준의 확립이 필요하지만, 현재까지는 어떠한 법률이나 방침에서도 이를 구체화하고 있지 않다.

2.2 스팸메일의 문제점

2.2.1 프라이버시 침해

Privacy란 "Right to be let alone"이라 정의된다. 즉 사생활에 대한 간섭받지 않을 권리라 해석되는데, 사생활의 비밀과 자유의 불가침은 사생활의 내용을 공개 당하지 않을 권리, 자신에 관한 정보를 스스로 관리 통제할 수 있는 권리 등을 내용으로 하는 인격권으로서 오늘날 정보사회가 급속히 진행되면서 그 보호가 절실한 권리이다. 프라이버시권에 대한 개념은 오래 전부터 있었지만 정보화 사회로 진입한 현대에서는 개인 정보에 대한 통제권이라는 보다 적극적인 개념(Self-control on personal information(EU Directive on Privacy Protection 1995)으로 바뀌고 있다. 이 권리의 개념은 미국에서부터 발전해 온 것인데 정보화 사회 진전에 따라 사생활 보호에 대한 권리가 소극적으로 사생활의 평온함을 침해받지 아니하고 사생활의 비밀을 함부로 공개 당하지 아니할 권리에서 나아가 적극적으로 자신에 관한 정보를 관리, 통제할 수 있는 권리를 포함하는 의미로 이해되고 있다. 이는 프라이버시를 침해받지 않을 자유권적 성격뿐만 아니라, 기록된 개인정보가 부정확할 때 당하는 부당함을 사전에 막기 위해 자신의 정보를 확인하고 정정할 수 있는 청구권적 성격도 갖게 된다는 의미이다. 이처럼 개인의 프라이버시권 개념이 능동적이며, 적극적으로 바뀌는 경향은 커뮤니케이션 기술의 발달로 의사소통이 한방향에서 양방향으로 가능해졌기 때문이다. 수신자의 이메일 박스가 개인 고유의 사적 영역이라는 것을 인정하는 추세를 반영한다면, 스팸메일은 수신자가 원하지 않는 메일로서 수신자의 평온한 사생활을 방해하는 것이 되어 사생활의 비밀과 자유에 대한 중대한 침해사유가 될 수 있다. 또한 누구든지 자신의 정보에 대한 관리통제권을 가진다는 측면에서 수신자의 동의 없이 수집되어 전송되므로, 사생활의 비밀의 자유의 침해가 되는 것이다.

2.2.2 인터넷 자원의 불필요한 소모

이메일 서비스 제공자인 Hotmail이나 Brightmail과 같은 제3자와 서비스의 통계에 따르면, 현재 인터넷 상에서 왕래되고 있는 이메일 중 약 30~40% 정도가 스팸메일[4]이라고 하며, 이는 점차적으로 계속 증가할 것이라고 한다. 이러한 막대한

4) http://www.brightmail.com/pressreleases/020403_sos_whitepaper.html, 2003, "Of these 40 billion messages processed by Brightmail's system each month, 41% are filtered as spam"이라고 화이트페이퍼를 통해 언급.

양의 스팸으로 인하여 ISPs나 중계서버는 물론, 일반 개인 사용자들의 네트워크 대역폭, 메모리, 저장용량 등의 인터넷 네트워크 자원들은 불필요하게 소모되고 있는 것이다. 인터넷 자원의 불필요한 소모량을 정확하게 파악한다는 것은 사실 어려운 일이지만, 인터넷 사용자나 시스템의 운영자가 스팸메일을 보고, 지우고, 여과하고, 방지하는데 불필요한 시간과 비용을 소비할 수밖에 없다는 점만으로도 스팸메일으로 인한 피해는 인정될 수 있을 것이다.

2.2.3 제 3자의 피해와 표현의 자유

스팸메일은 수신자에게 커다란 불만을 야기하게 되므로, 스팸 메일발송자들은 그 메시지의 머리말에 허위의 반송 이메일 주소를 기재하거나 본문에 허위의 수신거부 주소를 기재한다. 또한 허위 주소 등으로 인하여, 실제로는 스팸 발송자와 전혀 관련이 없는 사이트임에도 불구하고, 스팸메일에 기재된 제이메일 주소나 웹 사이트 기록만으로 스팸 메일 수신자로부터의 불만이나 고의적인 서비스방해 공격 등을 받는 선의의 피해자가 발생하도록 유도하기도 한다.

이와 같은 심각한 스팸메일의 피해로 인하여, 강력한 스팸메일 여과(Filtering) 및 차단(Blocking) 기술 적용 그리고 법률 입안 등으로 정상적인 상거래를 위축시키고 건전한 상거래를 위한 합법적인 이메일 직접 마케팅 등의 선의의 기업들이 가져야 할 표현의 자유가 침해당할 수도 있다.

2.2.4 기타 간접적 · 비경제적 손실

스팸메일은 간접적, 비경제적인 측면에서도 다양한 손실을 야기하고 있다. 우선 대부분의 스팸메일은 그 메시지의 내용이 매우 불건전하기 때문에 특히 그러한 메시지가 청소년에게 발송이 된 경우, 수신자의 불만이나 정신적 피해가 훨씬 더 커지게 된다[5]. 그리고 일반 이용자들이 스팸메일로 인해 인터넷 상의 모든 광고를 회의적으로 받아들이게 될 수도 있으므로 합법적인 광고주들 또한 피해를 입을 수 있으며, 스팸메일 발송자들에게 개인정보가 유출될 것 등을 우려한 이용자들로 인해 전자상거래가 위축될 수 있다. 또한 스팸메일을 막기 위한 여러 대응책들로 인하여 정상적인 상거래를 하는 기업의 표현의 자유 등 많은 합법적인 일반 이용자들이 피해를 입을 수도 있다.

2.3 스팸메일에 대한 제도적/법적 해결방안

2.3.1 사회적 규범과 시장 원리 그리고 코드

Lawrence Lessig교수는 "Code and Other Laws of Cyberspace"에서 규범, 코드, 법, 시장 등이 상호 유기적으로 관련되어, 가상 세계(CyberSpace)를 통제해 나갈 것으로 예상하였다. 그 중 스팸 메일에 대한 규제로 도덕적인 규범(사회적 비판 등)으로 인한 접근 방법으로 네티켓(Netiquette)의 원칙들을 살펴볼 수 있다. 하지만, 막연하게 적용되어오던 규범의 한계로 인하여, 사업자들의 자율규제만을 기대할 수는 없다. 따라서 규범, 시장원리[6], 코드간의 유기적인 선순환적 관계를 극대화할 수 있는 제도적 뒷받침이 절실해 졌다.

2.3.2 스팸메일에 대한 법률적 해결방안

(1) 미 국

미국은 스팸메일에 대한 적극적인 법률 제정 및 방안 마련을 위해 꾸준한 노력을 계속하여 왔다.

---

5) http://www.brightmail.com/press/state_of_spam.pdf, 2003, "The State of Spam(Impact & Solutions)", Brightmail, January 2003, p.9 중에서 "Unsafe for Children and Offensive to Adults"장에서 상세하게 피해 정도를 설명하고 있으며, 특히 스팸메일 중 포르노그라피 관련 메일이 18%를 차지하며, 증가되는 추세라고 분석하였다.

6) 가입자 수가 많은 ISPs 서비스를 이용할 경우, "온라인 우표제"를 실시하여 네트워크효과로 비용이 0(Zero)에 가까울 수 있는 점, 스팸메일로 인한 측정하기 어려운 비용(스트레스 유발 등)이 있는 점, 정크 메일 발송자가 부담해야 할 발송비용의 상당부분이 ISPs와 수신자의 통신망 이용 증가비로 전이되는 현상 등은 본 연구의 범위를 벗어나므로 구체적으로 다루지 않겠다.

〈표 2-1〉 미국의 스팸메일 관련 법규[7]

년 도	기구 및 법률 명칭	비 고
2001	요청하지 않은 상업적 전자우편법(Unsolicited Commercial Electronic Mail Act of 2001)	• 107차 의회 본 회의에서 발효. • 수신 거부 의사 후에는 스팸메일 전송을 금지. • 반송주소(Return-Address), 사후수신여부(Opt-Out)를 결정하는 내용을 메일 안에 반드시 명시. • 허위 발신자 주소, 거짓광고 등에는 형법(Criminal Code)에 의거하여 처벌가능 • ISP의 선의의 의도로서 스팸메일 차단시 법적 책임 묻지 않음.
1998	Washington State의 정크 메일 방지법 (Junk E-Mail Law)	• Rep. Roger Bush에 의해 소개. • Unpermitted or misleading electronic mail-Prohibition. • Unpermitted or misleading electronic mail-Violation of consumer protection act. • ISPs가 합리적으로 고려하여 스팸메일이라 판단하여 메시지를 차단한 경우라 할지라도 선한 뜻이라면 면책함. • 버지니아주 등 다양한 스팸메일 관련 법규가 있음.
1997	네티즌보호법 (Netizens Protection Act)	• The Communications Act (1934)를 수정하여, 전자메일에 의한 광고까지 포함하였었음. • 뉴저지의 Mr Smith 에 의해 언급 후, 의회에 제출하였으나 입법되지 못함.
1986	컴퓨터사기와 오용금지법 (Computer Fraud and Abuse Act)	• 1994, 1996년 수정. • 개인의 허가 없이 고의적으로 타인의 컴퓨터에 접속하여 손해를 가하거나 정보를 습득하는 것을 금지. • 스팸 발송자에 대한 적용가능.

하지만, 각 주간의 관할권 문제와 표현의 자유(강력한 스팸메일 방지법안으로 인한 선의의 피해 발생에 대한 우려) 등의 여러 문제점으로 1997년의 네티즌 보호법 등 주요 법안이 입법되지 못하였다. 또한 각 주별로 마련한 주법에서도 상충되는 부분이 있다. 하지만, 최근 우리나라의 "정보통신망 이용촉진 및 정보보호 등에 관한 법률"에 미국의 적극적인 입법 노력은 상당부분 영향을 주어 왔다.

(2) EU

<표 2-2>를 살펴보면, EU 연합은 1995년 "The European Union Directive 95/46/EC" 제정과 1997년 "Directive 97/66/EC of The European Parliament and of the Council of 15 December 1997"을 통하여 정보통신부문에 있어서 개인의 정보처리 및 프라이버시보호에 관한 지침을 마련하였다[8]. 하지만, 스팸메일에 관한 지침은 포함되지 않았다. 그러나 2002년 개정지침(2002/58/EC)에서는 Soft Opt-In 방식의 미국보다 엄격하게 적용(미국, Opt-Out)되는 스팸메일 지침을 발표하였다[9]. 아래 <표 2-3>은 Opt-In, Soft Opt-In, Opt-Out에 대한 비교 설명이다.

7) Junk E-mail Law 중 "The law specifically permits Internet Service Providers to block messages which they reasonably feel are in violation. It also exempts them from liability for any good faith effort they make to block these messages"라 함. "http://www.mcnichol.com/spam.htm", 2003.

8) "CyberSpace의 법과 기술", 고려대학교 CIST 정보보호 정책연구회, 북카페, 2003. 1., pp.470-771.

9) http://www.cdt.org/privacy/guide/protect/privacy-memo.pdf 2003년 2월 9일 방문 확인. "EU Directive on Privacy Protection in the Electronic Communications Sector", October 2002를 살펴보면, "On unsolicited marketing messages or "spamming", the new directive adopts an "opt-in" approach, which meams that users must give prior permission before being sent unsolicited electronic communications for marketing purposes." 에서 기본적으로 Opt-In을 근본으로 하지만, 아래와 같은 예외조항을 둔 소프트 Opt-In을 채택했다. "However, the directive allows merchants to use e-mail addresses collected from customers under an "opt-out" rule".

〈표 2-2〉 EU의 스팸메일 관련 지침

년도	기구 및 법률 명칭	비 고
1997	Directive 97/66/EC	• Directive 97/66/EC of The European Parliament and of the Council of 15 December 1997 • 기존의 Directive 95/46/EC를 보완(1997년 12월 15일) • 전화, 디지털TV, 디지털이동네트워크 등 정보통신부문(Telecommunication services)에 대한 세부 규칙으로 전환
2002	Directive 2002/58/EC	• Directive 2002/58/EC of The European Parliament And of The Council of 12 July 2002 • 기존지침(Directive 97/66/EC) 폐지 • 2002/58/EC 채택(2002년 7월 12일) • 스팸 메일에 관한 규제 강화 • 전자우편(Electronic Mail)을 통해 다이렉트 마케팅 할 경우, 규제 방식을 Opt-Out 방식에서 Soft Opt-In 방식으로 변경 • 다이렉트 마케팅의 목적으로 자동발신 시스템, 팩스에서 전자우편까지 가입자의 사전동의를 받도록 확대 규제

〈표 2-3〉 스팸메일 규제 방식

규제 방식	설 명	비 고
Opt-In	• 개인정보처리이용권이 명시적으로 인정되지 않는 한, 개인정보의 처리 및 이용이 금지되는 방식 • 개인정보처리이용권은 법률의 규정, 정보주체의 동의에 의해서 인정될 수 있음	
Soft Opt-In	• Opt-In 방식을 기본으로 하여 예외규정을 허용하는 엄격하지 않은 Opt-In 방식	EU
Opt-Out	• 기업 또는 정부가 특정한 개인정보를 처리하는 것을 부인하는 권리를 정보주체에게 주는 방식. 정보주체가 제 3자의 정보처리에 대해 명시적인 거부를 하지 않는 한, 제 3자의 개인정보처리권이 인정되는 방식	미국, 한국

2.3.3 제도적 해결방안의 한계

제도적 해결방안으로는 크게 소극적인 전통적인 규범이나 비공식적인 통제방안과 적극적인 법률적 통제방안으로 나누어 살펴볼 수 있다.

첫째, 사회적 압력이나 자율규제와 같은 비공식적 이고 소극적인 대응노력들은 강제성의 결여로 큰 효과를 얻고 있지 못하다.

둘째, 스팸메일에 대한 적극적인 대응 방식인 법률적인 해결책은 우회기술의 급속한 발전에 따른 법적 장치 마련의 시차, 강제성에 따른 문제, 관할권 등 사이버 공간에서의 특수성 등에 기인하여 한계에 노출되어 있다. 특히 새로운 기술과 사회현상에 대한 다양한 견해들로 인한 구체적이고 실질적인 구속력을 가지는 법률 제정의 어려움, 스팸메일의 기술적 특성으로 야기되는 관할권 문제 그리고 각 국의 상이한 이해관계로 인한 국제적 통일성 결여 등에 있어서 취약성을 드러내고 있다.

2.4 스팸메일에 대한 기술적 해결방안

2.4.1 스팸메일에 대한 여과(Filtering)기술

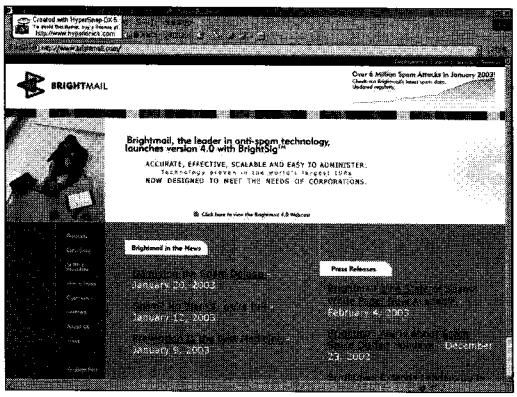
최근 스팸메일 관련 Software[10]의 대부분이 최종사용자 단계에서의 여과(Filtering)기술을 사용하고 있다. 특히, Microsoft Outlook나 MS-outlook Express와 같은 이메일 클라이언트 소프트웨어들

10) 국내 사용 제품으로는 컴트루테크놀로지사의 "클린스팸"(http://www.cleanspam.co.kr), 테라스테크놀로지사의 "Mail Watcher"(www.spamfree.co.kr), 쓰리알소프트사의 "Spambreaker"(http://www.spambreaker.com), 지란지교소프트사의 "Spam Sniper"(http://spamsniper.co.kr), 아이돌피아사의 "E-mail Safer"(http://www.yespam.com), 와우프리사의 "Spambuster"(http://www.spambuster.co.kr) 등이 있다.

〈표 2-4〉 여과(Filtering)기술의 적용 위치별 분류

여 과 위 치	대 상	비 고
최종사용자 (End-User)	Microsoft Outlook, MS-outlook Express 등 이메일 클라이언트 S/W 등	최종사용자의 비용 소요
ISPs, 대리 서비스 (Collaborative filtering by third parties)	ISPs, Brightmail(www.brightmail.com), Hotmail(www.hotmail.com), 등과 같은 메일 서비스 회사 등	IP 실명제, 스팸 신고 등을 통하여 서버에서 차단

과 연동하여 효과적으로 스팸메일을 차단하고 있다. 또한 최신의 온라인 업데이트를 통한 최신의 스팸 유형(pattern)이 반영된 온라인필터를 실시간으로 제공하여 사용자의 편의성을 높인 제품들이 많다. 이러한 기술들은 메시지의 머리말이나 전체 내용에 근거하거나 블랙리스트, 스팸기록보관소(archives)를 통해 스팸메일을 걸러낼 수 있고, 반대로 모든 메일들 중에서 적합한 것으로 확인된 것만을 선택하여 수령하게 할 수도 있다. 여과기술은 <표 2-4>과 같이 크게 여과기술이 적용되는 위치별로 최종사용자와 ISPs 또는 제3자 대리 서비스 등으로 분류할 수 있다.



[그림 2-1] http://www.brightmail.com

2.4.2 스팸메일에 대한 차단(Blocking) 기술

여과기술은 일단 메시지를 받기 위해 수신서버나 메일 클라이언트에 메시지가 수신되어지기 때문에, 네트웍 대역폭과 저장 공간 차지 등의 한정된 자원을 소모한다는 한계를 가지고 있다. 따라서, 메일 서버나 메일 클라이언트에서 스팸의 전송을 거부하는 것이 가능하도록 하는 몇 가지 기술적 차단방안들이 개발되어 왔다. 최근 ISPs 또는 메일 서버 회사에서 메일 수신거부 기능을 이용하여 해당 주소를 등록해 놓으면, 등록된 주소에서 오는 메일을 사용자에게 수신되지 않고 보낸 사람에게로 반송되게 되는 서비스 등으로 스팸메일에 대한 차단 기술이 활용되고 있다.

또한 반송 메시지를 보내지 않고 특정 인터넷 호스트에서 발송되는 이메일 또는 그 밖의 자료전달을 거부하는 블랙리스트라 불리는 DB를 통하여, 스팸 발송자들의 접속이 잦은 인터넷 호스트를 DB 위에 블랙리스트를 올려, 수신 서버의 운영자가 메시지의 전송을 확인하고 거부하는데 이용하도록 하는 것이다.

2.4.3 스팸메일에 대한 수신사후거부방식 (Opt-Out)

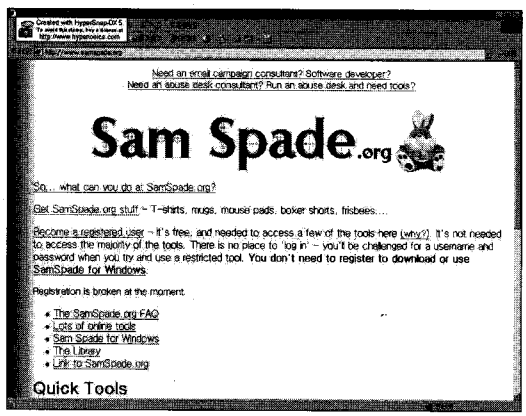
표현의 자유를 보호한다는 측면에서 스팸 메일 규제 방식으로는 수신사전승인(Opt-In) 방식보다 수신사후거부(Opt-Out) 방식이 보다 적합한 보호방식이다. 수신사후거부방식(Opt-Out)은 스팸메일을 수신 받은 후, 답장 또는 기타의 방법을 통해 스팸발송자에게 스팸메일 발송의 금지와 메일링 리스트 목록에서 자신의 이메일 주소를 삭제해 달라는 Opt-Out을 요구한다. 그러나 이러한 개별적 Opt-Out은 잠재적 스팸발송자의 수가 워낙 많기 때문에 스팸메일의 억제에는 그다지 효율적이지 못하며, 다수의 스팸메일이 Opt-Out 버튼을 상징적으로 둘 뿐 지키지 않는 다는 문제점을 가지고 있다. 따라서 이를 보완하기 위한 방안으로 범세계적인 Global Opt-Out제도의 도입[11], 네티켓, Opt-

11) David E. Sorkin, "Technical and Legal Ap-

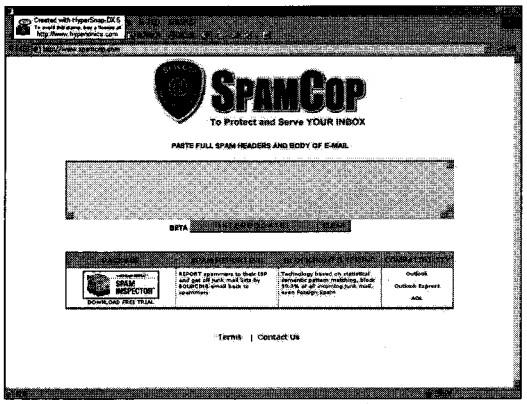
Out의 자동화 툴(Tool)을 이용한 적극적 대응 기술 등이 요구되어진다.

2.4.4 스팸메일에 대한 기타 기술

스팸 발송자는 허위의 답신 이메일 주소, 허위의 Opt-Out 버튼, 허위의 웹 페이지 URL 기재 등을 통하여 발신자의 위치와 정보를 은닉하려 한다. 따라서, 스팸메일 발송자에 대한 위치추적(URL)과 신고(Reporting) 그리고 보복(Retaliation) 등의 기술적 대응으로 스팸메일을 방지할 수 있다. 스팸메일을 수신한 인터넷 사용자들의 스팸의 추적과 신고를 돕기 위한 서비스나 수단들도 이용할 수도 있는데, 사용자가 이메일에 담겨져 있는 주소나 관련정보들을 판독할 수 있도록 도와주는 유틸리티들을 모아 둔 웹 사이트인 SamSpade[12], 자동적으로 스팸 메시지의 머리말을 분석하여 사용자 대신 관련 당사자에게 불만의 메시지가 가도록 하는 웹 기반의 서비스인 Spamcop 등이 있다.



[그림 2-2] http://www.samspade.org



[그림 2-3] http://www.spamcop.com

2.4.5 기술적 해결방안의 한계

스팸메일에 대한 소극적인 대응 기술로는 여과(Filtering)기술과 차단(Blocking)기술 그리고 Opt-Out 등이 있다. 그리고 적극적인 대응 기술로는 스팸메일에 대한 신고(Reporting)와 기술적 보복(Retaliation : IP추적 후 공격하는 방법 등) 등이 있다.

첫째 소극적인 기술인 웹 클라이언트 기반의 여과(Filtering)기술과 수신서버나 중계서버의 운영자, 또는 제3자에 의한 공동여과 등과 같은 여과기술은, 스팸 판별 전에 각각의 스팸메일을 서버로부터 다운로드받아야 하고 수신에 따른 네트웍 대역폭 및 서버 저장용량 차지 등의 문제점까지 막을 수는 없다. 따라서 여과장치가 제 역할을 한다 하더라도 이미 ISPs나 중계서버 또는 수신 서버에 발생한 손해까지 해결할 수는 없는 것이므로 스팸문제에 대한 근본적인 해결책이 될 수 없다. 또한 스팸발송자가 도메인이나 머리말을 거짓으로 기재하는 경우, 필터링 효과를 발휘할 수 없다. 이와 비교하여 차단기술은 좀 더 효과적인 측면이 있으나 막대한 비용이 소요되며, 원천 봉쇄에 따른 표현의 자유 등 제반 문제점에 노출되어 있다. Opt-out의 경우, 많은 국가로부터 시도되고 있으나, 스팸메일의 경우 이메일 주소, 웹 페이지의 URL(Uniform Resource Locator), Opt-Out에 관한 안내문 등을 기재하지 않거나 유효하지 않는 경우가 많다. 이는 이메일 주소 수집 도구(Tool)들의 강력함과 발송비

proaches to Unsolicited Electronic Mail," U of San Francisco Law Review, Vol.35, 2001.

12) 사이트가 제공하는 도구(Tools)로는 "The address digger," "Obfuscated URLs," "The safe web browser," "Reverse DNS," "Traceroute," "Whois," "Rwhois", "Whois," "Dejanews author search," "USPIS," "Blackhole list check," "IP whois" 등이 있다. "http://samspade.org/t/refer?i = on" 2003.

용이 들지 않는 점 등 경제적인 요인과 함께 작용하여, 비용 대비 성과 측면에서 스팸메일 발송이라는 우회기술들의 적용이 보다 효과적이기 때문이다. 따라서 법적인 강제성과 도덕적인 규범 의식(네티켓, 사이버 윤리 등)이 체계적이고 효과적으로 자리 잡지 않는 한 기술적인 방지 대책이 가진 한계점은 너무나 큰 것이 사실이다.

둘째 스팸메일에 대한 적극적인 대응책의 하나라 할 수 있는 신고나 보복행위는 스팸 발송자추적의 어려움, 보복 행위라는 도의적 부담 그리고 스팸 메일 발송지를 발견하고서도 관할권 문제 등으로 인한 처벌 가능성 등 많은 문제점에 노출되어 있다.

3. 결 론

스팸메일의 제도적 방안과 기술적 방안에서 노출된 여러 가지 한계를 극복하기 위해서는 종합적인 대응 방안이 요구되어 진다.

첫째, 스팸메일의 명확한 정의와 범위에 대한 합의가 국제적으로 이루어져야 한다. 따라서, 스팸메일에 대한 국제적 기준을 근거로 국제적인 차원에서의 대책마련에 초석을 마련해야 한다. 이는 스팸메일이 관할권의 문제로 해결에 어려움을 가지고 있기 때문이다.

둘째, 스팸메일에 대한 정확한 정의를 바탕으로 기술과 제도적 해결방안 중 적극적인 방안(법 제정, 추적 및 신고 그리고 보복 등)을 중심으로 종합적인 대응전략을 마련해야 한다. 일예로 기술적인 스팸메일 발신지 추적 후, 항의 메일 자동 발송 및 기술적 보복 조치에 대한 일정수준의 정도를 개인의 자기 방어 차원에서의 인정을 허용하는 법제 마련 등을 고려해 볼 수 있을 것이다.

셋째, 스팸메일에 대한 기술과 제도적 해결 방안 중 소극적인 대응 방안인 필터링 및 블록킹 기술과 규범 및 시장원리 그리고 네티켓 등에 대한 상호 보완적인 대응 전략을 추진해야 한다. 특히, 현재의 스팸메일 발송의 비용이 ISPs 사업자나 소비자에게 전가되는 구조적인 문제점을 해결할 수 있는 메일우표제 등의 기술적인 부분에 대한 접근과 꾸준한 교육을 통한 사이버 윤리의 정착 그리고 새로운 기술에 대한 즉각적인 대응을 구현할 수 있는 기술과 법률적 전문가들로 구성된 협의체 등을 마련하여, 다각적인 측면에서의 스팸메일 방지 전략을 구사하여야 한다.

참 고 문 헌

[1] "한국인터넷백서", 한국전산원, 2002, p.54.

[2] "CyberSpace의 법과 기술", 고려대학교 CIST 정보보호 정책연구회, 북카페, 2003, pp.470-771.

[3] "인터넷상의 스팸메일 법적 규제 정비방향", 유의선, 2002.

[4] "Technical and Legal Approaches to Unsolicited Electronic Mail," David E. Sorkin, U of San Francisco Law Review, Vol. 5, 2001.

[5] "EU Directive on Privacy Protection in the Electronic Communications Sector," October, 2002

[6] "The State of Spam(Impact & Solutions)," Brightmail, January 2003, p.9.

[7] http://samspade.org/t/refer?i = on, 2003.

[8] http://www.cdt.org/privacy/guide/protect/privacy-memo.pdf, 2003.

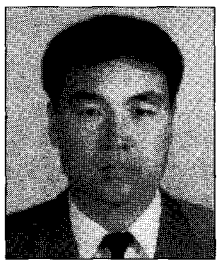
[9] http://www.brightmail.com/pressreleases/020403_sos_whitepaper.html, 2003.

[10] "http://www.mcnichol.com/spam.htm," 2003.

◈ 저 자 소 개 ◈

강 장 묵 (wseoul@bcline.com)

고려대학교 일반대학원에서 석사, 고려대학교 정보보호전문대학원에서 공학박사과정으로 재학중이며, 현재 서경대학교 컴퓨터공학과 겸임 교수와 (주)슈퍼테크놀러지 기술연구소 연구 소장으로 재직하고 있다. 연구관심분야로는 정보보호 중 정보보호기술의 전략적 활용, 스테가노그라피, 정보전, 프라이버시 등이며, 한국 SI 학회, 한국정보보호학회 등 국내 학술지에 발표하였다.



유 의 상 (yes@ksfc.or.kr)

고려대학교 경제학과 졸업, 중앙대 국제대학원 석사, 고려대학교 정보보호대학원에서 공학박사과정으로 재학중이며, 현재 정보통신부 정부출연기관 소프트웨어공제조합 총무팀장으로 재직하고 있다. 주요연구관심분야로는 CMM, 정보보호관련 컨설팅 및 지적재산권 등이며, 한국SI학회, 한국디자인학회 등 국내학술지에 논문을 발표하였다.

이 정 훈 (hoon@kisa.or.kr)

인하대학교 법정대학에서 학사, 연세대학교 행정대학원에서 일반행정으로 석사(1988), 고려대학교 정보보호대학원에서 정보보호학과 박사과정으로 재학중이며, 현재 한국정보보호진흥원 정보보호산업지원센터 센터장으로 재직하고 있다. 연구 관심분야로는 해킹바이러스, 전자서명, 개인정보보호, 정보보호산업정책 등에 관한 정책분야이며, OSIA 기술발표회 등에 국내 정보통신산업정책을 발표하였다.