인터넷 윤리 확산을 돕는 기술 개발 현황

특집 07

목 차

김 명 주
(서울여자대학교)

1. 인터넷 윤리 확산과 지원 기술과의 개연성

인터넷 윤리 확립과 같은 사회적 새로운 공동 목표를 효과적으로 달성하기 위해서는 구성원 전체에 대한 의식 계도는 물론 새로운 교육 시스템 구비, 미비한 법률 및 제도의 보완 등에 못지 않게 중요한 것이 관련 지원 기술들을 최대한 개발하여 사회의 기반 구조로 보급하는 것이다. 예를 들어, 우리 사회의 가장 심각한 인터넷 역기능으로 1,300여명의 대학생들이 꼽은 1위가 "음란물 제작과 유포"이었는데 이 역기능을 최소화하기 위해서는 음란물을 제작하는 주체에 대한 조사, 처벌 등의 법률적 대비도 필요하지만 이러한 음란물이 실제로 유통되는 경로에 대하여 기술적인 차단막을 개발하여 사회 전반에 걸쳐 설치 운영하게 된다면, 이로 인하여 우리 사회가 지불해야 되는 비용을 가장 빠르면서도 효율적으로 경감시켜주는 방안이 될 수 있을 것이다.

본 본문에서는 인터넷 윤리 확립 차원에서 현실적인 문제로 떠오르는 여러 사안들에 대하여 소프트웨어 개발 등과 같은 기술 지원을 통하여 어떻게 해결할 수 있는지 소개하고자 한다. 영리 목적의 기업체에서 이러한 기술 개발을 통하여 사업을 도모하는 경우도 간혹 있기는 하지만 정보 보호 전문 업체에 의한 정보 보호 전문 기술로 확장되어 그 사업성이 보장되지 않는 한 지속적인 투자가 어렵기 때문에, 인터넷 윤리와 관련된 대부분의 지원 기술은 공공기관이나 정부기관 등에 주관하여 공익을 목적으로 개발되는 것이 보통이다. 본 고에서도 인터넷 윤리 확립 차원에서 다뤄지는 몇 가지 문제를 해결하기 위한 지원 기술들의 현황을 소개하되 국내의 경우 정보통신윤리위원회에서 주도적으로 개발해온 기술들을 중심으로 소개하고자 한다.

2. 이메일 필터링 기술

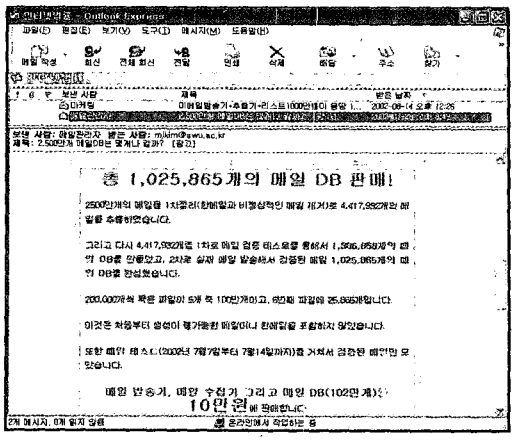
정보 지식 사회의 기반을 형성해온 인터넷이 인류에게 제공해온 다양한 서비스 가운데 가장 큰 파장을 일으킨 것을 꼽는다면 단연 전자우편 서비스를 생각하게 된다. 전자우편 서비스의 핵

심인 전자우편물 즉, 이메일은 전통적인 우편물의 기록성을 제공하면서도 시공의 제한을 극복하는 즉시성, 대다수의 구성원들이 활용하는 대중성마저 충족하고 있어서, 유사 이래 인간이 보유해온 모든 커뮤니케이션 수단 가운데서 가장 영향력 있는 매체로 부각되었다. 메일에 내재된 이러한 능력 때문에 새롭게 부각되는 전자상거래에서는 물론이고 전통적인 상거래에 있어서도 메일은 가장 영향력 있는 광고 매체로 부상되었다. 결국 스팸 메일의 부각은 필연적인 결과인 셈이다. 최근 들어 스팸 메일의 창궐은 다음과 같은 기술적 사회적 근거를 가지고 있다[1].

첫째, 많은 사업자들이 이메일을 통한 광고 효과가 기대보다 크다는 것을 깨달았기 때문이다. 광고 매체로서의 이메일은 가장 막강한 수단으로 부상했는데, IMT Strategy에 의하면 허가된 광고 메일은 DM(Direct Mail)보다 5배, 웹 배너 광고보다 20배 이상의 효과가 있다고 보고되었다. 한 시민단체의 조사에 따르면, 일반인이 수신된 스팸 메일들에 대하여 내용을 보지 않고 삭제하는 경우가 82.6%인 반면, 제목을 본 후 내용까지 읽은 경우는 17.4%나 되는 것으로 밝혀졌는데 이 통계치는 상품 광고를 하려는 사업자에게는 매우 호감이 가는 자료가 아닐 수 없다.

둘째, 스팸 메일 관련 자동화 소프트웨어가 보급되고 있기 때문이다. 스팸 메일을 발송하려면 다량의 이메일주소를 미리 확보하고 있어야 하며, 이들을 대상으로 짧은 시간 안에 모두에게 메일을 동시 전송할 수 있어야 한다. 이 경우, 이메일주소를 확보하는 문제와 자동으로 이메일을 발송하는 문제가 해결되어야 효율성이 올라가는데, 이를 해결해주는 자동 소프트웨어들이 개발되어 아주 저렴하게 배포되는 바람에 현재처럼 스팸 메일이 급증하게 되었다. 이들 소프트웨어를 각각 "이메일주소 자동 추출 소프트웨어", "자동 이메일 발송 소프트웨어"라고 부른다.

이메일주소 자동 추출 소프트웨어는 웹 상에서 이메일주소를 자동으로 검색 추출하여 별도의 데이터베이스(DB)를 만드는 것으로 이처럼 구축한 메일주소 DB를 토대로 하여 자동 메일 발송 소프트웨어가 동작하면 가장 강력한 스팸 메일 발생 시스템이 구성된다. 물론 이미 만들어 놓은 메일주소 DB만을 구입해도 자동 메일 발송 소프트웨어만 있으면 스팸 메일 자동 발송이 가능하다. 이러한 소프트웨어들의 판매가격은 수십만 원 이내로 사업자 입장에서는 매우 저렴하기 때문에 더욱 확산되고 있다.



(그림 1) 메일주소 DB 판매 사례

셋째, 사회전반에 걸쳐 IT 인프라가 잘 구현되어가고 있기 때문이다. 시중 PC방은 물론 학교, 가정까지 초고속 인터넷 망이 들어와 있기 때문에 대량의 스팸 메일을 아무 곳에서나 발송할 수 있으며, 스팸 메일의 수신자 폭 역시 매우 넓고 다양하다. 아울러 익명성 보장 및 위·변조와 관련된 IT 세부 기술의 발전으로 말미암아 스팸 메일에 대한 법적 규제를 피해나갈 수 있는 용이한 기법들이 더 많이 출현하고 있다. 예를 들어, 송신자의 메일 주소나 메일 전송 경로와 관련된 헤더정보를 거짓되게 고치는 것은 이제는 매우 쉬운 기술에 속한다. 반면에 국내의 경우 많은 메일서버 관리자들이 자신이 관리하는 메일서버에 대하여 적절한 기술적 조치를 취하지 않음으로

해서 스팸 메일 릴레이 등에 노출되어 국내는 물론 해외로부터 스팸 메일을 발송하는 경유지로 쉽게 이용되고 있는 실정이다.

그렇다고 해서 스팸 메일이 모두 나쁘다고만은 볼 수 없다. 오히려 소비자의 선택과 결정에 도움을 주는 중요한 정보 제공처일 수도 있다. 그러나 음란성 스팸메일이나 사행성 스팸메일은 기성세대는 물론 청소년 이하 어린 연령층에게는 매우 심각한 해악을 끼친다. 불행히도 이들은 자신이 수신한 이메일을 스스로 선별할만한 능력을 충분히 가지고 있지 못하다. 이런 상황에서 수신한 이메일에 대한 여과(필터링) 기술은 매우 효과적인 방패가 될 수 있다.

2.1 이메일 서버 스캐너

가장 근본적인 지원 기술로는 사용자를 대신하여 서버 단에서 이메일 필터링을 해주도록 하는 기술을 생각할 수 있다. 다시 말해서, 메일서버용 핵심 프로그램(UNIX의 Sendmail이나 MS 윈도의 Exchange Server 등)에서 제공하는 기능과 옵션을 이용하여, 수신하는 모든 메일에 대해 수신 허용 여부를 판별하여 결정함으로써 수신자의 스팸 메일 처리 노력을 미리 덜어주려는 대응방안이다. 이 경우, 대개는 수신한 메일의 제목 부분을 살펴보아서, "광고", "섹스", "성인", "ADV:", "ADV:ADLT"" 등과 같은 스팸성 키워드가 있을 경우, 혹은 수신한 메일의 송신주소를 살펴보아서 이미 스패머의 소유로 알려진 메일 주소나 도메인으로부터 전송되어온 메일인 경우, 이를 제거하거나 송신자에게 반송하는 방법을 주로 사용한다. 반면에 이러한 스팸 메일 제거 기능이외에 컴퓨터 바이러스에 감염된 메일까지도 찾아서 제거하기 위하여, 이메일 서버 스캐너(email server scanner)라는 별도의 프로그램을 추가 설치하여 운영한다. 이러한 전통적인 이메일 서버 스캐너로는 procmail[2], inflex[3], IMScanner[4] 등이 있다.

2.2 MUA에서의 필터링 기술

일반 사용자들에게 부담을 전가하는 것이기는 하지만 이메일 서버 스캐너 못지않게 현실적으로 효과를 보는 것은 역시 클라이언트가 직접 자신이 수신한 이메일을 필터링하도록 메일 서비스용 클라이언트 프로그램(MUA, Mail User Agent) 상에 명시하는 기술을 꼽을 수 있다. 여기에는 전통적으로 크게 두 가지 방법이 존재하는데, 이메일 제목에 "광고", "성인물" 등 스팸 메일이 포함하는 단어일 확률이 높은 단어를 미리 지정함으로써 이메일 수신 시에 걸러내도록 하는 필터링 방법과 해당 스팸 메일을 보낸 사람의 주소를 수신거부주소 목록에 등록시킴으로써 나중에 다시 해당 스패머로부터 스팸 메일이 오면 모두 자동으로 반송시킴으로써 스팸 메일 제거라는 귀찮은 작업을 미리 없앨 뿐 아니라 스패머의 메일주소 DB로부터 자신의 주소를 삭제하도록 유도하는 방법이다. 사용자들이 많이 사용하는 메일 서비스용 클라이언트 프로그램인 아웃룩 익스프레스(Outlook Express)에서 이 방법을 적용하려면 다음의 절차를 따른다.

2.2.1 필터링 기능 활용

아웃룩 익스프레스를 실행한 화면에서 메뉴 [도구(T)] → [메시지 규칙(R)] → [메일(M)]을 선택한다. 이 때, "메시지 규칙" 창이 나타나는데, 여기에서 "새로 만들기(N)"을 선택한다. 새 메시지 규칙 창이 나타나면, [규칙의 조건 선택(C)]에서 제목란에 특정 단어 포함을 체크하고, [규칙의 동작 선택(C)]에서는 삭제하거나 지정된 폴더로 이동을 체크한다. [규칙 설명(D)]에서는 제목란에 특정 단어 포함을 클릭하여, 특정 단어 입력 창에서 차단할 제목에 포함될 단어를 입력하여 추가(A)한 후, 확인을 누르면 된다.

2.2.2 수신거부 기능 활용

아웃룩 익스프레스를 실행한 상태에서 이후에

수신을 거부할 스팸 메일을 선택한다. 메뉴 [메시지(M)] → [보낸 사람을 기준으로 차단(S)]를 선택한다. 만일 현재 어떤 메일주소들이 수신거부에 등록되어 있는지 조회하거나 목록에서 삭제하려면, 메뉴 [도구(T)] → [메시지 규칙(R)] → [차단할 보낸 사람 목록(S)]을 선택한다.

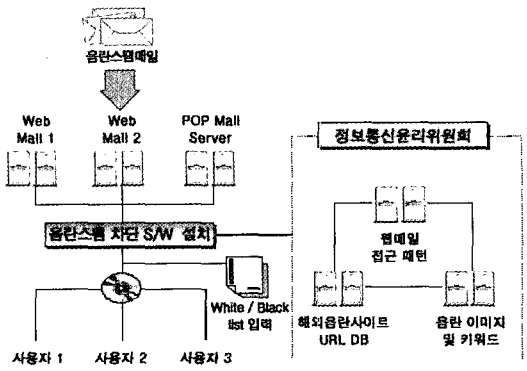
2.3 대표 사례 : 스팸 체커

스팸 체커(SPAM Checker)는 정보통신윤리위원회에서 개발하여 무료 보급하는 음란 스팸 필터링 소프트웨어의 일종이다. 스팸 체커는 음란 사이트 DB, 음란 키워드, 음란 이미지 등을 인식하여 음란 스팸 메일을 차단한다. 국내의 대표적인 웹 메일인 다음(hanmail.net), 네이버(naver.com), 야후(yahoo.co.kr)는 물론 아웃룩 익스프레스(Outlook Express)로 수신되는 음란 스팸메일까지 필터링해준다. 스팸 체커는 다음과 같은 특징을 갖는다.

- 정보통신윤리위원회에서 지속적으로 갱신하고 있는 음란 사이트 DB(해외 포함)와 연동하여 스팸 메일의 연계성을 파악하여 차단한다.
- 수신한 이메일의 제목과 본문에 포함된 문자 정보를 토대로 차단할 뿐 아니라 이메일로 전송되는 이미지 패턴에 대한 음란성 여부를 인식하여 차단할 수 있다. 이를 위해서는 관리자 모드에서 '선별기준' 을 [높은 수준]으로 설정하면 된다.
- 스팸 체커는 기본적으로 음란성 스팸메일을 차단하도록 만들어졌으나, 차단 단어 및 차단 메일주소 목록에 사용자가 원하는 단어 또는 주소를 입력 저장하면, 이메일 수신 허용(White List) 목록과 차단 (Black List) 목록을 개별적으로 설정하여 차단할 수 있게 해준다.
- POP3, IMAP 기반의 일반 MUA뿐만 아니라 주요 웹 메일을 대한 통한 필터링 기능을 제공한다.

(그림 2)는 스팸 체커가 동작하는 모습을 간략하게 보여준다.

스팸 체커는 정보통신윤리위원회 사이트에서 다운로드 받아 설치할 수 있다([5]). 스팸 체커를 설치하면 이메일 필터링에 대한 기준(선별기준)



(그림 2) 스팸 체커 구성도

을 설정할 수 있도록 되어 있는데, 여기에는 크게 낮은 수준, 중간 수준, 높은 수준, 사용자 정의가 제공된다. 낮은 수준을 선택하면 수신되는 메일의 제목과 링크된 URL 주소의 음란성 여부를 판단하여 메일을 차단한다. 중간 수준은 권장 수준으로서 이를 선택하면 수신되는 메일의 제목과 본문내용, 링크된 URL 주소의 음란성 여부를 판단하여 메일을 차단한다. 높은 수준을 선택하면 수신되는 메일의 제목과 본문내용 및 링크된 URL 주소, 그리고 이미지의 음란성 여부를 판단하여 메일을 차단한다. 단, 음란성 이미지의 판별을 위해 다소의 검색시간이 지연될 수 있으며, 음란하지 않은 이미지도 일부 차단될 수 있다. 사용자 정의를 선택하면 수신되는 메일 제목의 단어와 본문내용의 단어가 허용 단어목록에 있을 경우, 또는 발신자가 허용 메일주소에 있을 경우를 제외하고는 모든 메일을 차단한다. 그러나 모든 선별기준에도 불구하고, 메일 내용에 있는 링크된 URL 주소가 음란사이트면 해당 이메일은 무조건 차단된다.

전통적인 이메일 필터링 기술이 완전히 서버 측에서 처리하거나 이와 반대로 완전히 클라이언트에게 위임해왔던 반면 스팸 체커는 어느 정도 중도적인 입장을 취하고 있다. 즉, 음란 사이트에 대한 DB 목록을 가지고 이를 우선적으로 적용하여 필터링한다는 측면에서는 서버 측면의

처리처럼 보인다. 그러나 아웃룩 익스프레스와 같이 수신 허용 목록과 차단 목록을 사용자가 유지하여 이를 적용할 수 있도록 해주는 기능은 클라이언트에게 위임된 필터링 기술처럼 행동하게 해준다.

선별 기준을 높은 수준으로 선택하면 이미지에 대한 음란성도 점검해주지만, false-positive 반응(음란하지 않음에도 불구하고 차단해버림)이나 false-negative 반응(음란함에도 불구하고 차단하지 못함)은 어느 정도 감수해야 하는 형편으로서 보다 높은 정확성을 제공하는 기술 개발이 필요한 실정이다. 또한 음란사이트 DB 목록 역시 항상 변하고 있다는 특성 때문에 완전한 이메일 필터링을 제공해주는 것은 아니다. 그러나 공공기관에서 체계적으로 음란성 스팸 메일을 차단하기 위해 개발하여 보급하는 기술이라는 측면에서는 큰 효과와 의미를 담고 있다.

3. 이메일 계정 자동생성 방지 기술

대량의 스팸 메일 발송은 대량의 송수신 이메일 주소 확보를 전제로 한다. 앞서 소개한 이메일 주소 자동 추출 소프트웨어(스팸봇, spam robot의 준말)는 웹 상에서 이메일주소를 자동으로 검색 추출하여 별도의 데이터베이스를 만들기도 하지만, 스팸 메일을 보내는 송신자용 이메일 계정을 자동으로 대량 생성하는 기능도 함께 제공한다. 이는 스팸 체커와 같은 스팸 메일 차단 소프트웨어가 차단 목록을 중심으로 활동하므로 스패머의 송신 이메일 주소는 쉽사리 차단 목록에 추가된다는 점을 감안하여 스팸봇은 이메일 주소를 자동으로 대량 확보하게 된다. 따라서 스팸봇에 의한 이메일 주소 자동 생성을 막기 위한 기술도 스팸 메일을 억제하도록 하는데 있어서 매우 중요한 역할을 하게 되는데 그 핵심에 HIP(Human Interactive Proof) 기술이 있다([6]). HIP 기술은 회원가입단계에서 인간의 육안으로만 식별이 가능한 왜곡된 이미지를 무작위로 제시하여 제한된 시간 내에 사람으로 하여금 다시 입력하도록 한다. 따라서 자동 프로그램에 의한 무차별적인 계정 생성을 제한할 수 있게 된다.

HIP는 사람은 풀 수 있지만 기계적인 프로그램은 쉽게 풀지 못하는 인지적 단계의 퍼즐을 제공하는 방식이다. 아주 단순한 단어를 무작위로 골라 글자를 약간 훼손시킨 뒤 복잡한 배경 화면 위에 표시하는 Captcha 기술이 그중 가장 대표적이다. 이외에도 새로운 이미지 훼손 모델인 Pessimal Print 기술이나, 게슈탈트 심리학에서 말하는 인간의 이미지 구성능력을 최대한 활용하는 BaffleText 기술 등이 대표적인 HIP 기술로 꼽을 수 있다. 주요 웹 메일에서 새로운 계정을 인가해줄 때 사용하는 HIP 기술에 대한 사례 몇 가지를 보면 아래의 [예]와 같다.

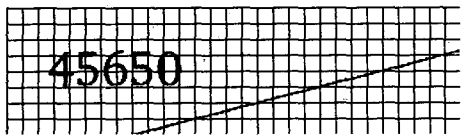
4. 자녀의 PC 사용에 대한 제어 기술

최근 들어 자식을 둔 대부분의 부모가 가장 걱정하는 자녀 문제는 인터넷 게임이다. 자녀들이 시간의 상당 부분을 인터넷 게임에 매달릴 뿐만 아니라 아바타와 같은 게임 소품에 대한 막대한 재정적 지출이 부모에게 큰 걱정을 끼치고 있는 것이 사실이다. 그렇다고 해서 무작정 게임을 말릴 수만은 없는 일이다. 자신의 집안에서 게임하는 행위를 철저하게 봉쇄한다고 자녀가 게임에 대한 욕구를 포기하는 것은 아니다. 오히려 음성화되어 더 큰 화를 불러일으킬 수 있다. 그런 측면에서 게임에 대한 양성화가 필요하되 적절한 제어가 동반되어야 한다. 그러나 자녀와 다른 세대를 살아왔으면 현재에도 바쁘게 살고 있는 부모들에게 있어서 이러한 경계점을 찾는다는 것이 쉽지 않다. 이에 대한 해결책을 기술적으로 시도하려는 노력이 오래 전부터 있었다. 이것의 발상은 백오리피스(BO, Back Orifis)라고 불리는 네트워크 기반 원격 업무 제어 프로그램으로 거슬러 올라갈 수 있다.

[예 1] 한메일

[필수 입력사항]
왼쪽 한글단어를 입력하세요.
입력하신 후 다음 단계로의 이동을 원하시면 다음 단계로 버튼을,
가입취소를 원하시면 가입취소 버튼을 눌러주세요.

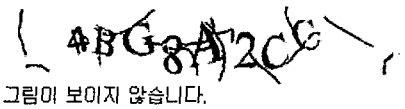
[예 2] 야후코리아



왼쪽 박스안에 보이는 숫자를 그대로 입력하세요.
* 숫자입력 절차는 야후! ID의 자동생성을 방지해줍니다. 이 기술은 카네기멜론 대학의 Captcha프로젝트로 개발되었습니다.

[예 3] 핫메일

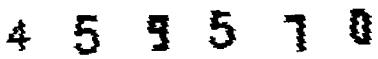
이 그림에 들어 있는 문자를 입력하세요. 이유



그림이 보이지 않습니다.

대소문자를 구분하지 않습니다.

[예 4] 네이버



자동가입 방지를 위하여 상단의 번호를 입력해주세요.

[예 5] 네이트 닷 컴

아래의 파란상자에 나타난 3자리 한글를 입력창에 넣어주시기 바랍니다.
이 절차는 NATE.com ID의 자동생성을 방지해 줍니다.

4.1 백오리피스

백오리피스는 네트워크 상에서 상대방의 컴퓨터를 100% 제어할 수 있도록 해주는 소프트웨어이다. 좋게 표현하면 네트워크 상에서 자원을 원격으로 관리하게 해주는 소프트웨어이지만, 나쁘게 표현하거나 악용하게 되면 무서운 모니터링 및 해킹 프로그램으로 둔갑한다. 백오리피스는 cDc(Cult of the Dead Cow)의 Sir Dystic가 제작한 소프트웨어로서([7]), 정보보호 측면에서는 불법 서버로 구분한다. 그러나 당사자는 백오리피스를 윈도우 운영체제 관리자 도구라고 스스로 평가한다. 1998년 BO 1.2가 공개된 후 2000년초에는 BO2k가 소스 코드와 함께 공개되었다.

백오리피스(BO2k)는 서버(BO2k.exe)와 클라이언트(BO2kgui.exe, BO2kcgf.exc)라는 두 개의 모듈이 연동하여 동작한다. 서버는 상대방 컴퓨터에 설치되는 것이며, 클라이언트는 관리자 또는 해커가 다루는 모듈이다. 백오리피스(BO2k)는 다음과 같은 주요 기능을 제공한다.

- 서버 시스템의 강제 종료와 부팅
- 서버 시스템의 암호 정보, 시스템 정보 유출
- 서버 시스템의 레지스트리 값 조회 및 변경
- 서버 시스템의 사용자의 키 입력 추적
- 메시지 송신
- 네트워크 트래픽 방향 재조정
- 서버 시스템 내 공유 파일(폴더) 생성/삭제
- 서버 시스템의 프로세스 신규 실행 및 중단
- 서버 시스템의 동영상 캡쳐 및 실행

이러한 막강한 네트워크 제어 기능들을 제공하는 백오리피스로 인하여 많은 네트워크 기반 모니터링 소프트웨어들이 출현하게 되었다. 회사에서 근무하는 부모가 집에서 게임하고 있는 아

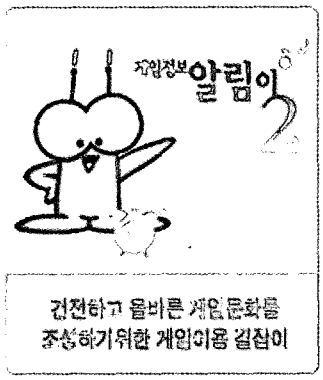
이의 컴퓨터에 대하여 모니터링하고 심지어 제어까지 할 수 있는 소프트웨어들이 다수 등장하였는데 이들의 기술적 배경은 역시 백오리피스를 그 뿌리로 두고 있다.

4.2 게임정보알림이

게임정보알림이는 관리자가 설치하되 사용자들의 게임 행태를 모니터링 및 조정할 수 있도록 정보통신윤리위원회에서 개발하여 무료로 배포하는 프로그램이다([8]).

게임정보알리미의 관리자는 게임 이용 연령 및 게임 내용을 고려하여 게임의 신호 등 색상을 정할 수 있고 게임사용자의 게임 이용 범위 레벨을 설정할 수 있으며, 게임 사용자는 자신에게 부여된 레벨에 따라 해당 색상의 게임을 즐길 수 있다. 게임의 이용 및 결제 서비스 등의 내용에 따라 게임을 적색, 황색, 녹색으로 분류하는데, 적색 게임은 청소년이 사용하기에 부적합하므로 관리자가 각별히 주의할 필요가 있으며, 황색 게임은 청소년이 이용하는데 있어서 관리자의 관심이 좀더 필요한 게임이라 할 수 있다. 그리고 녹색 게임은 누구나 이용할 수 있는 건전한 게임을 나타낸다. 이처럼 게임을 분류한 후, 게임의 이용 및 결제 서비스 등의 내용에 따라 관리자가 게임사용자의 게임 이용범위를 설정할 수 있다. 게임 이용 범위의 레벨은 모두 1, 2, 3으로 구분된다. 레벨 1은 게임사용자가 적색, 황색, 녹색 게임 모두를 이용할 수 있는 수준이며, 레벨 2는 게임 사용자가 황색, 녹색 게임을 이용할 수 있는 수준이고, 레벨 3은 게임사용자가 녹색 게임만을 이용할 수 있도록 해준다.

게임 사용자는 게임을 할 때, 매번 게임정보알림이에 로그인하는 것을 권장된다. 게임 사용자가 게임정보알림이에 로그인을 하지 않고 게임을 이용할 경우에는, 관리자가 환경설정에서 기본적으로 설정한 '게임이용 범위' 레벨대로 게임의 이용이 제한된다.



(그림 3) 게임정보알림이

관리자가 청소년에게 유해한 게임을 발견하여 이를 게임목록에 추가하고자 할 경우에는 '게임관리' 메뉴의 '추가' 버튼을 클릭한다. '추가하기' 창이 열리면, 추가하고자 하는 게임의 게임명, 게임파일명 등의 정보를 입력하고 게임의 신호등 색상을 설정한 후, 추가 버튼을 누르면 게임목록 DB에 해당 게임이 추가된다. 게임을 추가한 후에는 컴퓨터를 재부팅하도록 되어 있다. 물론 게임정보알림이의 게임목록 DB에 해당 게임이 포함되어 있지 않거나, 게임의 특성이 변할 경우에 일부 게임의 필터링이 이루어지지 않을 수 있다. 이 부분은 지속적으로 변하는 부분이므로 100% 완벽한 필터링을 기대하기는 어렵다. 그러나 게임정보알림이를 통하여 게임에 대하여 소외된 부모가 상당한 필터링 정보를 얻을 수 있을 뿐 아니라 이를 토대로 자녀들의 게임 활동을 모니터링하고 제어할 수 있다는 점에서 부모 측면의 부담을 상당 부분 덜어준 기술로 평가된다. 물론 부모와 자식 간에 게임정보알림이와 같은 소프트웨어 사용에 대한 합의 내지 협의가 선행되어야 그 효과를 볼 수 있을 것이다.

4.3 PC 사용 원격 제어 기술

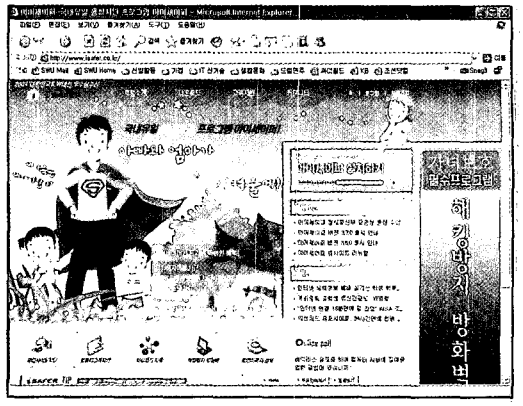
게임정보알림이의 기능과 유사하면서도 좀더 광범위하게 자녀들의 PC 행태를 원격으로 모니

터링할 수 있는 상용 소프트웨어 및 해당 사이트들이 국내에서도 개발되어 보급 중에 있다. 대표적인 사이트로 텔레키퍼([9])와 아이세이퍼([10])를 꼽을 수 있다.

텔레키퍼의 경우, 자녀의 컴퓨터 사용 행태와 사용 통계를 모니터링할 수 있으며(현재의 화면 보기, 실행 중인 프로그램 보기, 실행 중인 게임 보기, 방문한 유해사이트 목록보기, 인터넷 서핑 및 게임 시간 통계), 자녀의 컴퓨터 사용에 대한 제어를 설정할 수 있다(게임 차단, 유해 사이트 차단, 컴퓨터 사용시간 제한, PC 사용허가).

(그림 4) 텔레키퍼 사이트

아이세이퍼의 경우 역시, 텔레키퍼와 유사한 기능을 보이고 있다. 아이세이퍼는 인터넷 상의 유해정보를 담고 있는 사이트와 이미지 및 유해단어를 차단하는 기능을 지원하며, 매일매일 기하급수적으로 늘어나는 인터넷 유해사이트의 목록을 업데이트하여 유해사이트의 접속을 막아준다. 유해사이트로 등록된 사이트가 아니어도 관리자가 차단 목록과 단어를 지정하여 운영할 수도 있다. 컴퓨터, 프로그램 및 인터넷 사용에 대해 조건부 허가 기능을 제공하며, 일부 악성코드 발견 및 치료, 개인 방화벽의 기능도 제공해 준다.



(그림 5) 아이세이퍼 사이트

이러한 PC 사용 원격 모니터링 및 제어 기술은 자녀의 나이가 어릴수록 어느 정도 큰 효과를 볼 수 있다. 반면에 자녀의 나이가 높을수록 이러한 감시 기술은 그 효력이 크지 못하며 자녀들의 PC 사용 행태를 부모의 의도대로 변화시키는데 있어서 근본적인 해결책이라고는 보기 힘들다. 그러나 부모와 자식이라는 특별한 관계가 상당한 제어력을 가질 수 있는 환경 하에서 이 기술은 자녀에 대한 상당한 바람막이 역할을 해줄 수 있다.

5. 불건전 사이트 신고 기술

정보통신윤리위원회 산하 불법 청소년 유해정보신고센터가 운영하는 사이트로 "인터넷 119"가 있다. 인터넷119에서는 음란, 명예훼손, 자살, 폭탄, 엽기, 도박 사이트 등 각종 유해정보에 대해 신고 접수를 받아 심의를 통해 해당 내용 삭제, 이용해지, 경고 등의 시정을 요구한다. 아울러 시작페이지 변경, 음란 팝업창, 성인 사이트 피해 사기 등 각종 민원 상담을 통해 피해상황을 파악하여 피해경보를 발령한다. 이 인터넷119에서 불건전 사이트에 대한 신고를 신속하게 할 수 있도록 도와주는 소프트웨어를 개발하여 배포하고 있는데 바로 "인터넷 파랑새"이다([11]).

(그림 6) 인터넷 파랑새

인터넷파랑새는 신고화면 바로가기, 증거자료 캡쳐, 신고자 자동설정 등의 서비스를 제공하는 자동신고 프로그램으로, 편리하고 신속하게 불법·유해정보를 신고할 수 있도록 도와준다.

건전한 정보화 사회를 구성하는데 있어서 불건전 정보에 대한 신고정신이 중요한 기능을 담당하고 있음을 인식할 때, 인터넷 파랑새는 사이버시대 시민정신의 한 축을 담당할 수 있는 기술로 평가할 수 있다.

6. 인터넷 내용 등급 서비스 기술

인터넷내용등급서비스란 정보제공자가 자신의 정보내용을 객관적 평가를 거친 등급기준으로 분류하여 이용 가능한 등급정보를 표시하면, 정보이용자 및 청소년 보호자가 해당 정보내용을 선별 또는 차단해주는 소프트웨어를 사용하여 해당 정보내용을 기존의 영화등급이나 도서관의 분류된 자료처럼 참고할 수 있도록 하는 서비스이다. 즉, 정보제공자가 정보내용을 일정기준에 따라 등급을 표시해 두면 인터넷 사용자가 자신의 연령이나 수준에 맞게 정보를 선택할 수 있는 방식이다. 현재 주요 선진국들은 청소년 보호를 목적으로 인터넷내용등급서비스를 도입하여 자국의 문화적 특성을 고려한 등급서비스를 제공하고 있다.

6.1 인터넷내용등급서비스의 국내외 동향

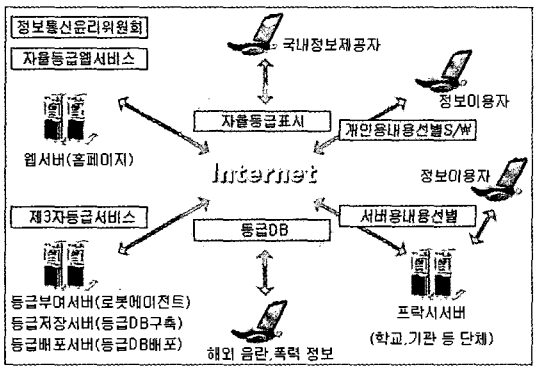
인터넷 기반이 튼튼하고 시장규모가 가장 큰 미국, 캐나다 등의 경우는 ICRA(RSACi), SafeSurf, Netshepard 등 복수의 내용등급체계와 지역기반의 다양한 상업적 등급서비스가 존재한다. 북미는 전반적으로 민간기업 중심의 자율적인 등급서비스들이 시장에서 경쟁하는 형태이다. 이러한 시장 중심의 인터넷등급서비스 모델은 이용자의 선택권을 극대화할 수 있으며, 인터넷 내용에 대한 외부적 검열의 가능성을 배제할 수 있다는 점에서 많은 장점을 지니고 있다. 미국 등 북미의 경우는 대부분의 인터넷 컨텐츠가 자국 내에 존재하고 있어 관련 기업의 자율정화 능력이 높다.

미국과는 달리 대부분의 유해 컨텐츠가 외국의 서버를 경유하여 민간 기업의 자율정화 능력이 상대적으로 떨어지고, 인터넷 관련 시장의 규모가 협소하여 인터넷내용등급서비스의 상업적 이윤 창출이 어려운 그 외 국가들은 공공부문의 지원을 통해 이루어지고 있다. 국내에서는 정보통신윤리위원회가 인터넷상의 음란·폭력 정보 등의 불건전정보로부터 청소년을 보호하고 성인의 볼 권리를 보장하기 위해 한국적 문화가치 및 국제 호환성 등을 고려하여 인터넷내용등급서비스(SafeNet)를 개발·도입하여 2001년 9월부터 시행하고 있다.

6.2 SafeNet

SafeNet은 국제적인 기준을 기반으로 국내 실정에 맞게 만들어졌다. 현재 5개 범주에 5등급(0등급에서 4등급)을 분류기준으로 하고 있다. SafeNet은 현재 국제적으로 시행되고 있는 RSACi([12]), ICRA([13]), Safety-Online(일본 ENC)의 등급기준과의 호환성도 고려하여 설정되었다. 따라서 인터넷내용등급서비스의 내용선별 소프트웨어를 이용할 경우 호환성이 보장된다. 정보통신윤리위원회는 인터넷내용등급서비스의 투명성, 객관성 및 전문성 확보를 위해 각 계각층의 주요인사들로 구성된 등급전문위원회를 운영하고 있다. 정보통신윤리위원회의 인터

넷내용등급서비스는 인터넷 정보에 대한 이용자 중심의 자율규제라는 큰 틀 속에서 국내 정보에 대한 자율등급서비스와 해외 음란·폭력 정보 등에 대한 제3자등급서비스를 실시하고 있다. 자율등급서비스는 국내 정보제공자가 노출, 성행위, 폭력, 언어, 기타 등 5개 범주 5단계(0~4등급)의 등급기준에 따라 자율적으로 등급을 표시하면, 정보통신윤리위원회가 보급한 내용선별 소프트웨어에 의해 정보이용자가 인터넷 정보를 선별하여 이용할 수 있도록 하는 것이다. 또한 제3자등급서비스는 해외의 음란·폭력물 등을 중심으로 등급DB을 구축하여 정보이용자에게 제공하는 것을 의미한다. 이같이 SafeNet은 자율등급서비스와 제3자등급서비스를 가능하게 해주는 인터넷내용등급시스템이다.



(그림 7) SafeNet

6.2.1 자율등급서비스

정보제공자가 자율적으로 자신이 제공하는 정보에 대해 HTML 문서 내부에 META 태그를 이용하여(PICS label을 사용) 등급표시를 하면, 정보이용자는 등급 표시된 정보의 PICS를 인식하는 웹브라우저 혹은 내용선별 소프트웨어를 통해 적정 등급수준을 정하여 인터넷내용등급서비스를 제공받게 된다. 정보통신윤리위원회는 정보제공자가 손쉽게 자기 자신이 제공하는 정보에 대해 PICS의 방법에 의한 자율등급표시를 할 수 있도록 인터넷내용등급서비스 홈페이지([14])의 등급표시페이지에서 웹서비스를 제공하고 있다.

6.2.2 제3자등급서비스

제3자등급서비스는 정보이용자에게 제3의 기관에 의해 부여된 등급 데이터베이스를 배포하는 레이블 뷰로 서버(Label Bureau Server)를 이용하여 등급서비스를 제공받을 수 있는 방식이다. 정보이용자가 레이블 뷰로 서버를 인식할 수 있는 내용선별 소프트웨어 등을 이용할 경우, 정보제공자가 등급표시(PICS Label)를 하지 않았더라도 인터넷내용등급서비스를 이용할 수 있다.

6.2.3 자율등급 표시방법

항목		내용
〈META http-equive= "PICS-Label"		〈meta〉 태그의 성격을 알려줌
PICS-1.1		인터넷내용선별 체계 기술규격에 관한 버전 정보
〈service url〉		관련기관의 서비스 URL명
labels 레이블이 적용되는 문서에 대한 정보, 레이블 자체의 정보, 기타 정보를 제공	l	labels의 약자
	gen true	generic boolean : 이 옵션이 true로 설정 되면 for quoted URL을 접두어로 시작한다는 모든 URL에 동일한 기준으로 적용함
	for	for "정보제공자의 자율등급표시 URL명"은 등급기준에 의한 등급표시가 적용된다는 URL
ratings (〈category〉〈value〉)		등급기준 표시값으로 r (n 1 s 2 v 1 l 2 i 0 h 0)으로 표시함 • 노출 = n, 성행위 = s, 폭력 = v, 언어 = l • 마약사용조장, 무기사용조장, 도박 = i • 음주조장, 흡연조장 = h ※ n, s, v, i는 해당 0~4등급수준으로 표기, i, h는 0 혹은1(없음 0, 있음 1)로 표기함

다음은 정보제공자의 자율등급표시 사례를 보여준다.

```
〈META http-equiv="PICS-label" content= '(PICS-1.1
"http://www.safenet.ne.kr/rating.html" l gen true[false] for
"정보제공자 자율등급표시 URL 명" r (n 1 s 1 v 2 l 3 i 0 h 1))'〉
```

위와 같이 자율등급표시가 완료되면, 정보제공자의 전자문서 소소의 헤더(header) 내부에 '붙이기' 하면 된다. 단, 사이트와 디렉토리 단위일 경우는 디폴트 페이지, 페이지 단위일 경우에는

디폴트와 해당 페이지에 모두 표시하는 것이 바람직하다.

7. 결 론

본 논문에서는 인터넷 윤리 확산에 기여할 수 있는 IT 기술 특히 소프트웨어 기술에 대한 현주소를 살펴보았다. 이메일 필터링 기술, 이메일 계정 자동생성 방지 기술, 자녀의 PC 사용에 대한 제어 기술, 불건전 사이트 신고 기술, 인터넷 내용 등급 서비스 기술 등 5가지 주요 영역에서 제시된 기술들은 현실적으로 인터넷 윤리 확산을 돕는 기술로 평가될 수 있다. 그러나 대부분의 첨단 기술이 그렇듯이 인터넷 관련 기술의 빠른 발전과 사회에서의 급격한 확산은 이러한 지원 기술들의 완벽함을 처음부터 기대할 수 없게 만들어 왔다. 그럼에도 불구하고 현실적으로는 큰 효과를 입증해주고 있기 때문에, 기술 개발과 보급 측면에서 인터넷 윤리를 확산하고자 하는 이러한 연구 접근 방법은 앞으로도 더욱 강조되어야 할 것이다.

참고문헌

[1] 김명주, "급증하는 스팸메일에 대한 다양한 대응 방안", 인터넷 법률, 13권, pp.24-80, 법무부, 2002. 8. 1.

[2] http://www.procmail.org/

[3] http://pldaniels.com/inflex/

[4] Myuhng-Joo Kim et al., "IMScanner: An Advanced Mail Server Scanner Filtering E-mails Infected with Known or Unknown Virus", ICIS (2nd International Conference on Computer and Information Science), 2002. 8. 8.

[5] http://spam.icec.or.kr

[6] http://www.aladdin.cs.cmu.edu/hips/

[7] http://www.cultdeadcow.com

[8] http://www.icec.or.kr/front/discuss

[9] http://www.telekeeper.com

[10] http://www.isafer.co.kr

[11] http://www.internet119.or.kr/i-bluebird

[12] http://www.rsac.org/

[13] http://www.icra.org/

[14] http://www.safenet.ne.kr

저자약력

김 명 주

1982년 3월~1986년2월 서울대학교 컴퓨터공학과 공학사
1986년 3월~1988년2월 서울대학교 대학원 컴퓨터공학과 석사
1988년 3월~1993년8월 서울대학교 대학원 컴퓨터공학과 박사
1993년 9월~1995년8월 컴퓨터신기술 공동연구소 특별연구원
2003년 2월~2004년2월 미국 펜실바니아대학교(UPenn) 객원연구원
1995년 9월- 현재 서울여자대학교 정보보호학전공 교수
관심분야 : 정보 보안, USN, 의료정보, 콘텐츠 보안