情報保護學會論文誌
第16卷 第6號, 2006. 12

FQDN과 개인화 격리 처리를 이용한 정크메일 차단 시스템의 구현 및 평가

김 성 찬[1†], 천 준 호[2‡], 전 문 석[2]

[1](주)유코레일, [2]숭실대학교 컴퓨터학과

An Implementation and Evaluation of Junk Mail Filtering System to use the FQDN Check and personalized Quarantine Process

Sung-Chan Kim[1†], Junho Choun[2‡], Moon-Seog Jun[2]

[1]EUKORAIL Co.,Ltd, [2]Department of Computing, Soongsil Univ.

요 약

초고속 인터넷 망의 확충으로 인터넷을 이용한 정보전달이 보편화 되고, 전자우편은 많은 양의 자료를 빠르고 편리하게 송수신 할 수 있는 가장 보편적인 통신 수단이 되었다. 하지만 정크메일의 수신빈도와 그로 인한 피해가 갈수록 높아져 그 문제가 심각한 수준에 이르게 되었다. 더구나 근래의 정크메일은 시스템을 공격하기 위한 바이러스나 해킹 도구를 전파하는 수단으로 이용 되어 컴퓨터 침해 사고의 심각한 원인으로 지적되고 있다. 따라서 본 연구에서는 실제 상황에서 유입되는 정크메일의 로그 분석을 통하여 그 특징을 분석한 후 FQDN 확인과 개인별 격리처리를 이용한 차단 시스템을 구현 하였고 성능을 평가 하였다.

ABSTRACT

Internet mail has become a common communication method to send and receive an amount of data due to the tremendous high speed Internet service increment. But in other respect, the risk and damage of Junk mail is growing rapidly and nowadays Junk mail delivery problem is becoming more serious, because this is used for an attack or propagation scheme of malicious code. It's a most dangerous dominant cause for computer system accident. This paper shows the Junk mail characteristic which is based on the analysis of mail log in reality and then shows the implementation of the FQDN (Fully Qualified Domain Name) check and personalized classification system and evaluates its performance.

Keywords : *Junk Mail, FQDN(Fully Qualified Domain Name), Classification*

Ⅰ. 서 론

전 세계적인 인터넷 인프라의 확충으로 인터넷 사용자들의 증가와 함께 인터넷을 이용한 자료의 송수신 방법으로 전자우편이 가장 보편적인 통신 수단으로 자리 잡고 있다. 전자우편이 제공하는 저렴하고 편한 방법에 그 사용 또한 급격하게 늘어나고 있지만, 이로 인한 부작용도 심각한 문제가 되고 있다. 그 문제 중의 하나로 우리가 "정크메일"이라 부르는

접수일: 2006년 4월 24일 ; 채택일: 2006년 10월 9일
† 주저자: sckim@mail.eukorail.co.kr
‡ 교신저자: opendr@ssu.ac.kr

것으로 인터넷 메일 사용자들에게는 수신을 원하지 않는 메일을 다량으로 받게 함으로써 사용자들의 시간을 낭비하게 하고 혼란을 주며, 다량의 메일 메시지로 인한 네트워크의 대역폭 손실도 문제가 되고 있다. 근래의 연구보고에 따르면 네트워크에 유입되는 수신 메일의 데이터 크기가 전체 네트워크 통신 트래픽의 10%정도를 차지한다고 한다[1]. 정크메일의 수신 문제는 단순히 원하지 않는 메시지를 수신한다는 문제의 차원을 넘어서, 인터넷 메일 사용의 효용성을 크게 떨어뜨리고, 컴퓨터 시스템에 문제를 발생시키는 악성코드의 전달 매개체로서 그 문제가 심각해지고 있다. 본 연구에서는 "정크메일"의 패턴을 실제 업무에 사용되는 메일서버의 로그 분석을 통하여 그 특징을 연구하고, 이에 대응할 수 있는 효과적인 시스템을 구현 하였다. 그리고 일정기간 실제 사용을 통한 결과를 분석하여 평가하고 기존의 정크메일 차단에 있어 문제가 되어왔던 부분에 대한 방안을 제시하였다. 본 연구의 구성은 다음과 같다. Ⅱ장에서는 본 연구의 기초가 되는 관련연구에 대하여 기술하고, Ⅲ장에서는 본 연구에서 분석한 정크메일 패턴과 구현한 정크메일 차단 방법에 대하여 기술한다. Ⅳ장에서는 구현된 시스템에 대한 사용결과를 분석 평가한 후, Ⅴ장에서 결론을 맺는다.

Ⅱ. 관련연구

2.1 정크메일 차단 시스템

메일 사용자가 수신을 원하지 않는 정크메일을 완전히 차단하는 방법을 찾아내는 것은 불가능하다. 왜냐하면 정크메일의 정의 자체가 "수신자가 받기를 원하지 않고 요청하지 않았음에도 전송되는 메일"이라는 메일 사용자들의 "정서적인 정의"이기 때문에 정량적인 기준으로 구현된 시스템에서 수신자가 받기를 원하는 메일과 원하지 않는 메일을 일률적으로 판단하는 것이 불가능하기 때문이다. 정크메일 차단 방법은 정크메일에 대한 대응 시점에 따라 〔표 1〕에 나타난 바와 같이 받는 메일 서버 전단에서 차단하거나 받는 메일 서버에서 차단하는 방법, 사용자 메일 클라이언트에서 차단하는 방법이 있다. 현재로서는 다소간의 오탐지율을 인정하면서도 정크메일을 최대한 효율적으로 차단할 수 있는 기술들이 정크메일 차단에 이용되고 있으며 이러한 대부분의 정크메일 분류 방법들은 수신자가 입력하는 룰이나 이미 알고 있는 사전 지식에 기초한 확률적 분포로서 정크메일을 분류 한다든지 정크메일의 특성이 될 수 있는 판단 요소에 점수를 부여하여 정크메일을 판별하는 등의 룰 베이스(Rule Base) 패턴 매치 기반의 컨텍스트 필터링(Context Filtering) 분류 방법이다. 이러한 방법들은 정크메일의 증가에 따른 관리자의 정보 입력 부담이 커지고 룰 베이스(Rule Base) 패턴 매치 연산에 필요한 시스템 자원이 많이 소요된다는 점이 개선 사항으로 지적되고 있다. 다음은 현재 개발되어 사용되는 정크메일 차단 관련 기술 중 베이시안 필터링 기법과 Spam Assassin 방법을 소개한다[2].

〔표 1〕 정크메일 대응시점에 따른 차단 방법

분 류	기 술 정 의
메일서버 전단에서 차단	메일서버 전단의 방화벽 혹은 E-Mail Gateway에서 정크메일을 보내는 서버 혹은 클라이언트의 IP주소 차단, 알려진 도메인에 대한 메일 송신 서버 확인을 통해 정크메일을 차단한다.
MTA에서 차단	메일서버의 MTA(Mail Transfer Agent)에서 제목 또는 내용에 특정단어가 있으면 정크메일로 처리 하는 등의, 정크메일 규칙을 만들어 규칙에 부합한 메일은 정크메일로 처리, 대부분의 Rule Base 정크메일 차단 솔루션이 여기에 해당한다.
MUA에서 차단	메일서버의 MTA에서 일률적으로 적용하는 Rule Base를 개인별 MUA(Mail User Agent)에서 적용하여 정크메일을 차단하는 방법으로 메일을 차단하는 룰은 MUA마다 다르게 적용될 수 있다.

2.2 정크메일 차단 시스템에 사용되는 기술

2.2.1 베이시안 필터링(Bayesian Filtering)

폴 그래햄(Paul Graham)이 2002년 9월에 발표한 "A Plan for Spam"이란 글은 베이시안 필터링에 근거해서 개인마다 다른 정크메일 판별 규칙을 생성하고 이를 이용하여 정크메일을 차단하는 방법에 대해 소개한다. 베이시안 필터링 기술은 미래 상황을 추측할 수 있게 해주는 19세기 토마스 베이시스의 확률론에 근거한 것으로, 전자문서 분류에 많이 사용되는 베이시안 분류방법을 응용한 것이다. 베이시안 분류는 속성 값들이 주어진 목적 값에 조건

부 독립적이라는 가정을 기반으로 한다. 하지만 특정 단어를 선택할 확률보다 선행단어와 연관된 후위단어를 선택할 확률이 더 크다. 이러한 가정에도 불구하고 베이시안 분류는 효율적인 역할을 수행한다. 문서 내에 단어들을 대상으로 확률적인 방법을 적용하여 분류하기 때문에 특정 패턴에 따르지 않는 정크메일을 걸러낼 수 있다. 이는 어떤 사람에게는 정크메일이 될 수 있는 메시지가 다른 사람에게는 유용한 정보가 될 수 있다는 사실에 대해 베이시안 필터링 분류방법은 시간이 지남에 따라 그 효율성이 배가가 되고, 일반적으로 높은 정크메일 차단 율에 아주 적은 오탐지율을 보인다[2][3].

2.2.2 Spam Assassin

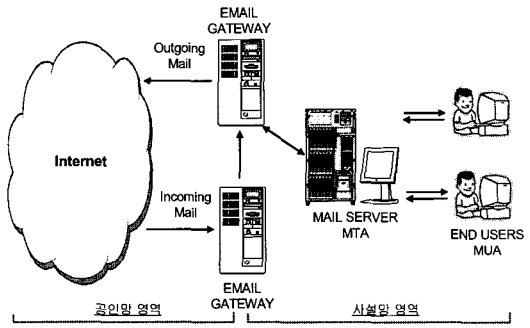
Spam Assassin은 메일에서 정크메일이 가질 수 있는 요소를 분석하여, 각각의 요소에 대해 점수를 주어 모두 합산한 점수가 일정 이상이면 정크메일로 판별하는 방식이다. 점수를 주는 방식에서 정크메일에서 제외될 수 있는 요소는 마이너스 점수를, 정크메일로 판별할 수 있는 요소는 플러스 점수를 주어 일반메일을 정크메일로 판별할 가능성을 줄인다. 메일의 전체 부분에 대해 수행한 결과 값이 5 이상이면 정크메일로 판별하며, 정크메일 판별과정을 메일 헤더에 넣어서 정크메일로 판별된 메일에 대한 자세한 정보를 볼 수 있어 잘못된 룰셋 사용을 방지할 수 있다. 또한 Spam Assassin의 룰셋(Rule Set)은 로컬 네트워크에서 전송된 메일과 외부 네트워크에서 전송된 메일에 대해 각각 다른 값을 부여하여, 로컬 네트워크에서 전송된 메일에 대해 정크메일로 판별될 가능성을 줄이고 있다[4][5].

Ⅲ. FQDN과 개인화 격리 처리를 이용한 정크메일 차단

본 연구는 관련 연구에서 언급된 일반적으로 가장 많이 정크메일 차단 방법으로 사용되는 룰 베이스 패턴 매치 기반의 차단 방법이 과연 실제 상황에서 얼마나 효율적인지에 대한 의문에서 시작 되었다. 이러한 의문점에 대하여 효과적인 대응방안을 연구하기 위해서는 현재 발생하고 있는 정크메일이 어떤 특징을 갖고 있는지 파악하는 것이 중요하며, 파악된 특징에 가장 확실하게 대응할 수 있는 방법을 본 연구에서 찾아내어 제안하였다.

3.1 정크메일 분석

본 연구에서는 정크메일을 분류 할 수 있는 가장 주된 특징을 파악하기 위해 연구자가 소속된 회사의 메일 시스템에 기록된 메일 로그와 메일 사용자에게서 신고 된 정크메일을 분석 하였다. 본 연구에 사용된 기존의 메일 시스템 환경은 [그림 1]과 같다. 실험환경의 메일 시스템은 시스템을 보호하기 위하여 사설 망 안쪽에 위치하며 사설 IP를 사용하고, 인터넷 망으로의 메일 전달과 수신은 [그림 1]에서와 같이 화살표의 방향으로 전달되고 수신된다. 인터넷 망으로부터 메일서버로 전달되는 메일은 우선 1차 E-MAIL GATEWAY를 거치면서 메일에 바이러스가 포함되어 있는지를 검사 받게 되고, 사설 망 안쪽의 사설 IP를 사용하는 메일 서버로 메일을 전달해 주는 두 개의 네트워크 인터페이스를 갖고 있는 리눅스 기반의 센드메일 서버로 메일이 포워드 된다. 이 과정에서 메일 게이트웨이로 유입되는 모든 메일의 바이러스 감염여부와 Black-List, White-List 및 간단한 패턴 매치 룰 베이스(Rule Base)를 이용한 정크메일 차단이 이루어진다.



[그림 1] 메일로그 수집에 사용된 기존의 메일 송수신 시스템 환경

리눅스 기반의 센드메일 서버는 외부 인터넷 망에서 내부 사설망으로 전달되는 메일과 내부 사설망에서 외부 인터넷 망으로 발송되는 메일을 전달하는 기능을 담당하고 있으며, 리눅스에서 제공하는 IP TABLE 패킷 필터링[6]을 이용하여 [그림 3]과 같이 E-MAIL GATEWAY와 메일 서버 간에 25번 포트를 이용한 통신만 허용 되도록 설정 되어있다. 메일 시스템에서의 메일 패킷의 흐름을 통제하는 것은 메일 시스템을 외부 위협으로부터 보호하고 메

일에 편승해서 침투해 오는 악의적이고 공격적인 코드를 차단하는데 반드시 필요하다. 메일이 유입되는 입구와 발송되는 출구의 길목에 메일의 정상 유무를 검사할 수 있도록 하기위한 것이다. [그림 2]와 같이 리눅스 상에서 구현한 IP TABLE은 패킷 필터링 도구로서 Source와 Destination의 각 네트워크 인터페이스별로 원하는 데이터 패킷과 서비스를 Accept 혹은 Deny 하도록 하는 일종의 패킷 필터링 방화벽이다[7].

```
#Define Policy to receive e-mail from ns.eukorail.co.kr (Antivirus wall)
iptables -A INPUT  -s $VIRUSW -d $EGATE -i eth1 -p tcp --dport 25 -j ACCEPT
iptables -A OUTPUT -s $EGATE -d $VIRUSW -o eth1 -p tcp --sport 25 -j ACCEPT

# Define Policy to receive and send with Lotus Notes
iptables -A OUTPUT -s $EG_INT -d $LOTUS -o eth0 -p tcp --dport 25 -j ACCEPT
iptables -A INPUT  -s $LOTUS -d $EG_INT -i eth0 -p tcp --sport 25 -j ACCEPT

iptables -A INPUT  -s $LOTUS -d $EG_INT -i eth0 -p tcp --dport 25 -j ACCEPT
iptables -A OUTPUT -s $EG_INT -d $LOTUS -o eth0 -p tcp --sport 25 -j ACCEPT

# Policy to send e-mail to anybody to Internet (From Lotus Notes)
iptables -A OUTPUT -s $EGATE -o eth1 -p tcp --dport 25 -j ACCEPT
iptables -A INPUT -d $EGATE -i eth1 -p tcp --sport 25 -j ACCEPT
```

[그림 2] 메일 패킷 통제를 위한 IP TABLE 구성

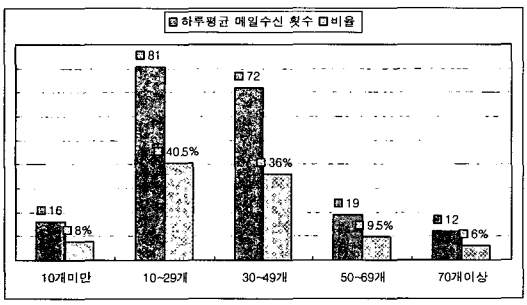
[그림 2]에서 구현한 IP TABLE은 바이러스를 검사하는 Incoming E-Mail Gateway와 실제 사용 메일 서버인 로터스 노츠 도미노 서버사이에서 메일을 릴레이 해주고 인터넷 영역으로 메일을 발송해주는 역할을 하는 E-Mail Gateway 사이의 메일 흐름을 단방향으로 진행하도록 하고, 로터스 노츠 도미노 서버와 E-Mail Gateway 상의 메일 패킷은 양방향으로 진행 하도록 구현하였다. 이와 같은 Source와 Destination간의 SMTP 서비스만 허용되도록 패킷의 흐름을 구현함으로써 외부 공격자로 부터의 메일 릴레이 공격과 같은 해킹 시도를 차단하도록 설계 하였다. [그림 1]과 같이 실제 서비스 메일 시스템을 사설망에 두고, 수신 메일 서버와 발송 메일 서버를 이원화 하여 메일 패킷을 정해진 보안 장비를 경유해서만 통과하도록 흐름을 통제하여 운영함으로써 시스템 공격을 원천적으로 차단하고 메일에 첨부되어 들어오는 악성 코드 및 바이러스로부터 메일 시스템을 보호 할 수 있다[8]. 기존의 메일 시스템에 정크메일을 차단하기 위한 효과적인 방법을 추가하기 위하여, 3개월의 조사기간 동안 수신 된 메일에 대한 로그와 메일 사용자에서 신고 된 정크메일의 로그 정보를 분석하여 몇 가지 중요 특징을 파악하였다.

[그림 3]은 하루 평균 수신되는 메일의 수를 전체 메일 사용자수에 대비해 비율로 표시한 그림이다. 하루 평균 10개에서 50개 정도의 메일을 수신하는 사용자가 전체 메일 사용자중 약 71%정도를 차지하고 있음을 알 수 있다. 그림 4는 전체 수신 메일 수 중 정크메일이 차지하는 비율을 나타낸 그림으로 정크메일의 수신 비율을 수식 (1)에 의하여 계산하였다[4,9,10].

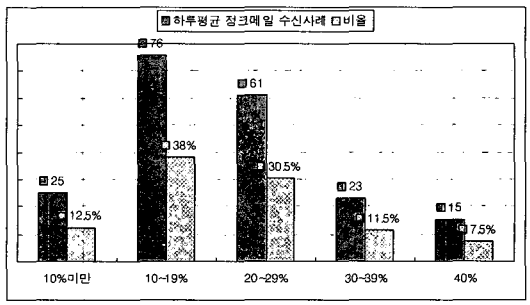
정크메일의 수신율 =(1 계정당 수신되는 정크메일 수 / 1 계정당 수신되는 전체 전자 메일 수) × 100 (1)

정크메일 수신 비율 조사 결과 수신되는 메일 중 약 10%~30%가 정크메일인 사용자가 전체 메일 사용자중 약 61% 정도임을 알 수 있다. 실험 환경의 메일시스템에 메일이 도착하게 되면, 먼저 E-MAIL GATEWAY에 메일이 수신되고 어디서 발송된 메일인지 메일로그를 남기게 된다. 조사기간 동안 수신된 정크메일의 특성을 결정하기 위하여, 수신된 정크메일의 로그를 분석하여 보았다.

[그림 5]는 메일 사용자들의 메일 클라이언트에



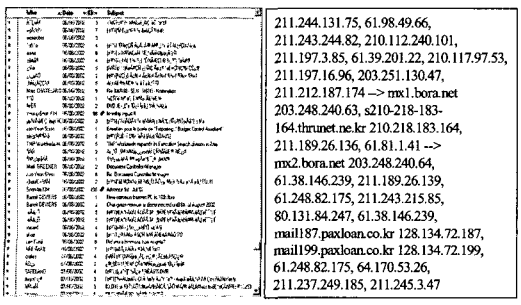
[그림 3] 하루 평균 수신되는 전자메일 수



[그림 4] 전제 수신 메일 중 정크메일 수신비율

수신된 정크메일의 모습을 보여주고 있다. 수신된 정크메일의 메일 헤더를 보면 메일이 지나온 전송 경로를 볼 수 있는데, 정크메일은 최초 발신자의 IP 추적을 피하기 위해서 정상적인 기능을 하는 메일 서버로서 확인 되지 않은 여러 곳의 메일 릴레이 시스템을 거쳐 전송되었음을 알 수 있다. 보다 자세한 분석을 위해서 메일 데이터의 헤더를 분석하면 그림 6과 같으며 이것은 정크메일 패킷의 헤더를 분석한 결과이다. 메일 패킷의 헤더를 분석해 보면 먼저 눈에 띄는 정보가 메일을 어디에서 보냈는가 하는 "From" 구문인데, 조사기간 동안에 수신된 정크메일의 일부를 표본 추출하여 분석한 결과 "From" 구문에서 추출한 도메인과 IP 주소가 정상적으로 도메인 관리 기관에 등록된 도메인으로부터 발송되는 메일은 단 한 개도 없었다. [그림 7]의 예에서 메일 발신 도메인은 "mx15.mx.voyager.net"이고 이 도메인의 IP 주소는 "216.93.66.102" 이지만, 실제로 도메인 관리기관에 도메인 검색 명령어인 "dig"나 "nslookup"을 이용해 "216.93.66.102"의 IP 주소를 검색해 보면, 메일 발신지의 도메인 정보나 도메인의 메일 교환 레코드 정보인 "MX" 레코드 정보를 찾을 수 없다. 이는 정크메일의 정의인 "본인이 원하지도 않고 요청하지도 않았음에도 전송되는 송신자가 불명확한 메일"과도 일치하는 것으로, 정크메일을 보내는 송신자는 대량의 메일을 인터넷상의 불특정 공인 IP에 대용량의 수신자 정보를 갖고 있는 데이터베이스를 이용한 발신전용 메일서버를 통하여 메일을 발송하기 때문에 발생하는 현상이다[11,12]. 대부분의 정크메일 차단 방법에서는 특정 IP에서 발생하는 똑 같은 형태의 메일 트래픽이 어느 기준이상 발생하면, IP 차단 리스트에 등록시켜 메일 수신을 거부하거나 다량으로 유입되는 정크메일의 패턴을 정크메일 차단 소프트웨어에서 일정기간 학습을 통해 정크메일 차단 룰에 등록시켜 차단한다[13]. 아니면 관리자가 직접 차단 리스트에 입력하여 정크메일을 차단하고 있다. 하지만 유동 IP를 이용하여 대량의 정크메일을 보내면서 지속적으로 IP를 바꾸거나 여러 경로를 거치게 하면, IP 추적을 통한 차단은 사실상 무용지물이 되며, 다양한 패턴의 정크메일을 정크메일 차단 소프트웨어에서 학습을 통해 인지하려면, 정크메일 차단 시스템에 소요되는 하드웨어적인 비용이 증가하여 효율적인 차단 시스템을 구성하기 어렵다[3,14,15].

본 연구에서는 정크메일의 발신지 정보의 IP 주소 혹은 경유된 메일 릴레이 시스템이 정식 도메인으로서 역할을 하지 않고 도메인 영역의 메일 교환 레코드인 "MX" 레코드를 갖고 있지 않다는 것에 착안하여 메일이 인터넷 영역에서 도착하게 되면, 1차 정크메일 차단 시스템에서 메일의 헤더부분에 포함된 발신자의 IP 주소를 역으로 검색하여, FQDN (Fully Qualified Domain Name)인지 아닌지를 판별한 후, 정상적인 도메인에서 보내는 메일로 판별된 경우 메일 전송을 허락하고 그렇지 않은 경우 송신자에게 반송시켜 송신자 등록 절차를 거쳐 메일 전송을 허가 받도록 시스템을 구성하여 1차 정크메일 차단 시스템을 구현 하였다. 정크메일 발신 서버의 경우 최초 발신자 IP 추적을 피하기 위하여 [그림 6]과 같이 여러 곳의 메일 서버를 거치면서 릴레이 되어 전달되는 경우도 있지만 아무리 여러 곳의 발신 전용 릴레이 서버를 거치더라도, 메일 릴레이 서버에서 발송되는 메일은 정상적인 도메인을 사용하지 않기 때문에 FQDN확인에서 차단되도록 한 것이다. 하지만 정상 도메인에서 발송된 전자 우편일지라도 정상 도메인 시스템에 도메인 스푸핑 공격과 같은 문제가 발생하여 정크메일 발송 서버로 이용될 수 있는 가능성도 있으며, 정상 도메인에서 발송한 메일이라



211.244.131.75, 61.98.49.66,
211.243.244.82, 210.112.240.101,
211.197.3.85, 61.39.201.22, 210.117.97.53,
211.197.16.96, 203.251.130.47,
211.212.187.174 --> mx1.bora.net
203.248.240.63, s210-218-183-164.thrunet.ne.kr 210.218.183.164,
211.189.26.136, 61.81.1.41 --> mx2.bora.net 203.248.240.64,
61.38.146.239, 211.189.26.139,
61.248.82.175, 211.243.215.85,
80.131.84.247, 61.38.146.239,
mail187.paxloan.co.kr 128.134.72.187,
mail199.paxloan.co.kr 128.134.72.199,
61.248.82.175, 64.170.53.26,
211.237.249.185, 211.245.3.47

[그림 5] 수신된 정크메일과 전송경로 추적

```
from mx15.mx.voyager.net (mx15.mx.voyager.net [216.93.66.102])
with ESMTP id iA10WZ103220 ; Tue, 1 Jun 2004 09:32:36 +0900"

Field Name: Received
Data Type: Text List
Data Length: 119 bytes
Seq Num: 1
Dup Item ID: 3
Field Flags:
```

[그림 6] 정크메일 패킷 헤더 분석

도 메일 사용자가 수신하기를 원하지 않는 메일일 경우 정크메일의 범주로 판별하여 불필요한 메일이나 정크메일은 개인별로 삭제할 수 있도록 메일을 격리 분류해 수신자가 받고 싶은 메일만 수신할 수 있는 2차 정크메일 차단 시스템을 구현 하였다. 이러한 격리 처리 절차는 새로운 메일이 도착하면, 일정기간 사용자의 메시지 처리과정을 관찰하여, 개인적인 룰을 형성하고, 만들어진 룰을 바탕으로 메일을 처리한다. 격리 처리 대기 중인 메일 중 사용자가 원하지 않는 메일은 삭제한다. 여기서 격리처리에 이용되는 알고리즘은 베이시안 알고리즘을 적용하였다[16,17].

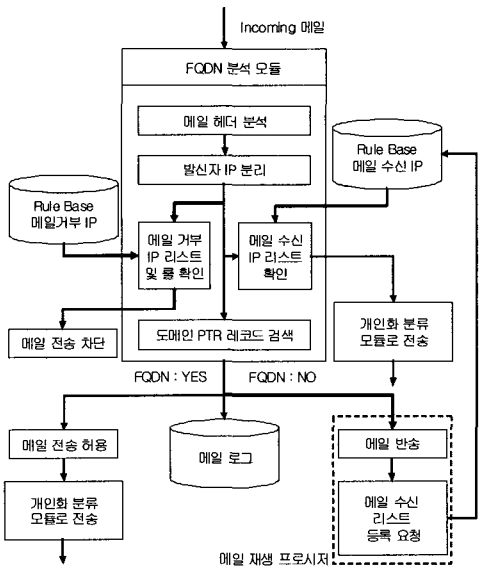
3.2 FQDN 확인과 개인화 분류를 이용한 정크메일 차단 시스템 구현

본 연구에서 구현한 1차 정크메일 차단 시스템인 FQDN 확인을 이용한 정크메일의 차단 모듈과 알고리즘은 [그림 7], [그림 8]과 같다. 먼저 인터넷 영역에서 메일이 도달하게 되면, FQDN 분석모듈은 수신된 메일의 헤더에서 메일 발신자 IP 주소를 분리해 낸다. 추출해 낸 IP 주소가 룰 베이스(Rule Base)의 메일 수신 거부 IP 리스트에 포함되어 있으면 차단하고, 메일 수신 IP 리스트에 포함되어 있으면, 다음 단계를 거치지 않고 바로 개인화 격리 처리 모듈로 포워드 한다.

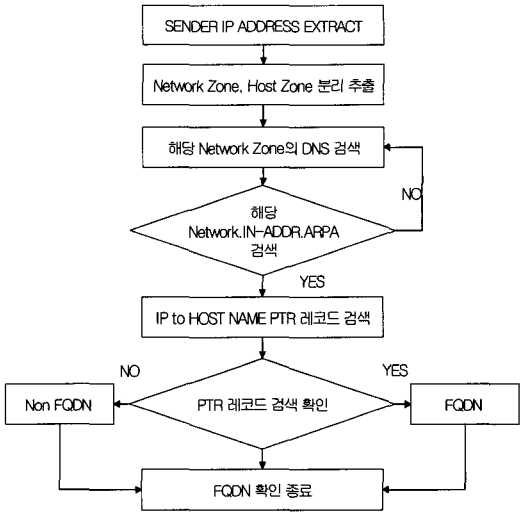
[표 2] 정크메일 필터 룰

	정크메일 필터 룰
1	From, To, 구문이 표준에 맞지 않는 메일 차단
2	From, To, Subject, Date에 값이 없는 메일 차단
3	To 이하의 수신자 도메인이 수신 서버 도메인과 일치하지 않을 경우 차단
4	메일 릴레이 시도 차단

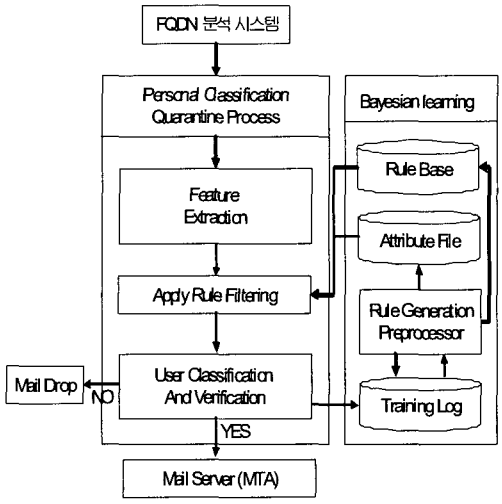
메일 수신 IP 리스트나 메일 거부 IP 리스트 어느 쪽에도 속하지 않은 IP 주소는 [표 2]에 열거된 룰 베이스(Rule Base)내의 기본적인 정크메일 차단 필터 룰에 적용되는지 아닌지를 검사 받고, 도메인의 PTR 레코드 검색을 거쳐 FQDN(Fully Qualified Domain Name)인지 아닌지를 판별 받는다[18]. FQDN의 판별 여부는 [그림 9]의 FQDN 확인 알고리즘의 절차에 의해 확인 된다. 추출해낸 메일 발신자의 IP 주소에서 네트워크 존과 호스트 주소를 분리해 낸 다음 해당 네트워크 존의 DNS 서버를 찾게 된다. 해당 DNS 서버를 찾았으면, IP 에서 호스트 이름을 찾는 정보를 제공하는 IN- ADDR.ARPA 정보를 검사하게 된다. IN-ADDR. ARPA의 존 정보에서 호스트의 IP 주소에 해당하는 PTR 레코드와 도메인 이름이 검색되면 FQDN(Fully Qualified Domain Name)이 되며, 그렇지 않고 상위 DNS 시스템에서도 PTR 레코드 정보가 검색되지 않으면 FQDN이 아니다[14][15]. FQDN으로 판정 받으면 메일 전송에 대한 허가를 하고 다음 단계인 개인화 분류 시스템으로 포워드 된다. 만약 FQDN으로 판정 받지 못한 메일 발신자에게는 메일을 반송 시키되, 메일 관리 홈페이지에 메일 수신 리스트로 등록 요청을 하도록 내용을 추가하여 메일을 반송 시킨다. 메일 수신 리스트에 등록된 메일은 FQDN 확인 절차를 거치지 않고 메일 전송 허가를 받도록 한다. 이와 같이 별도의 메일 수신 리스트를 만들도록 한 이유는 정상적인 메일이지만 IP 주소를 검색하여 PTR 레코드 검색 결과가 성공적이지 못할 경우를 대비하여 준비한 리사이클 서브 프로시저(Recycle Sub Procedure)이며, 발신 전용의 대량의 정크메일의 경우 반송되는 메일에 대한 처리를 못하기 때문에 정크메일에 대해서는 자동으로 차단하여 삭제하게 된다.



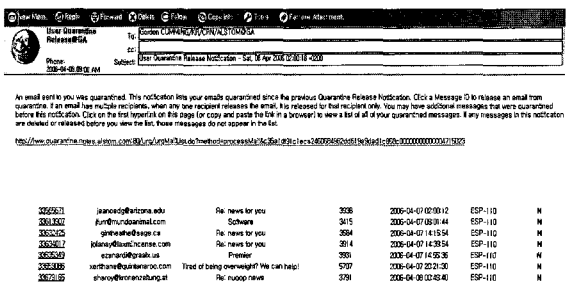
[그림 7] FQDN 확인 모듈



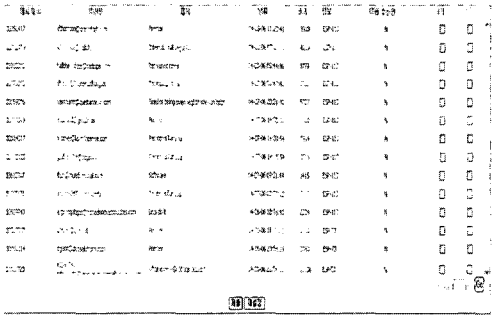
〔그림 8〕 FQDN 확인 알고리즘



〔그림 9〕 개인화 격리 처리(Quarantine Process) 모듈 Process[17]



〔그림 10〕 개인화 분류 확인 요청



〔그림 11〕 개인화 분류 확인

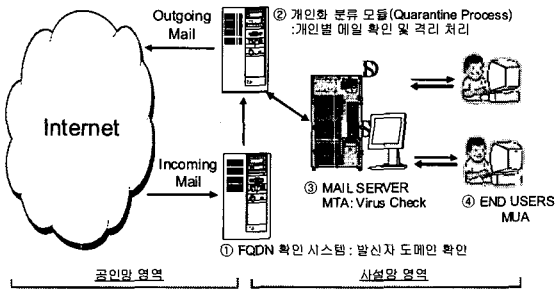
FQDN 확인 모듈에서 정상 도메인에서 발송한 메일로 판별되면 개인화 격리 처리 시스템으로 전송되어 〔그림 9〕의 격리 프로세스(Quarantine Process)를 진행하게 된다. 이 단계에서는 1차적으로 FQDN 확인을 거친 전자우편에서 특정 단어로 구별되는 특징들을 추출해 낸 다음, 룰 베이스와 속성파일로부터 정크메일로 특징지을 수 있는 요소들과 비교해 스코어링을 하게 된다[7,18].

누적된 수치를 비교한 결과 정량적으로 정크메일로 판별된 메일들은 Quarantine Notification을 해당 메일 수신자들에게 보내서 메일 수신자로 하여금 직접 확인 작업을 하게 한다. 〔그림 10〕의 화면은 메일 수신자들에게 정크메일 판별 확인을 요청하는 격리 처리 확인 요청 (Quarantine Notification) 메시지이다. 사용자들이 메일 송수신에 사용하는 메일 클라이언트에 격리 처리 대기 중인 메일들의 리스트를 격리 처리 시스템과의 연결성을 쉽게 하기 위해 웹 인터페이스의 링크를 삽입하여 사용자별로 보내며, 메일 송신자와 메일의 사이즈, 수신된 날짜를 표기하여 보낸다.

Quarantine Notification을 받은 메일 수신자는 메시지 ID와 링크된 웹 인터페이스에서 정크메일인지 아닌지를 직접 판별하여 삭제하거나 격리 프로세스를 해제(Release)하여 메일서버로 포워딩시킨다. 〔그림 11〕은 웹 인터페이스에서 수신자가 받기를 원하는 메일을 확인하여 격리 프로세스에 제출하는 화면을 나타낸 것이다.

본 연구에서 구현한 시스템 구성도는 〔그림 12〕

와 같이 설명 할 수 있다. FQDN 확인 시스템을 메일을 수신하는 최전방에 위치시켜 수신되는 전자우편의 발신지를 먼저 확인해, 발신전용 시스템에서 전송되는 메시지인지 아닌지를 먼저 점검하도록 했다. 정크메일의 특성상 발신 전용 주소에서 대량으로 뿌려지는 메시지의 비중이 가장 많기 때문에, 1차적으로 발신전용 메시지들을 제거한 후 정크메일의 판별 여부를 확인하는 것이 정크메일 판별 프로세서에 필요한 시스템의 비용을 최소화 할 수 있다.

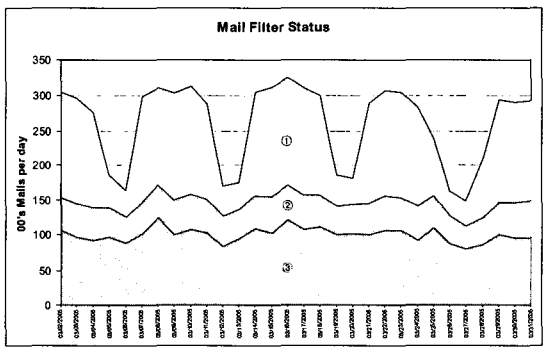


〔그림 12〕 FQDN 확인과 개인화 분류를 이용한 개선된 정크메일 차단 시스템 구성

FQDN 확인 시스템을 통과한 메일들은 그 수가 현저하게 줄어든 상태에서 개인화 분류 모듈에 의해 다시 정크메일 확인 작업을 거치고 여기에서 다시 소수로 추려진 메일만이 메일서버로 포워드 되어 바이러스 검사를 받게 된다. 따라서 정상적인 메일로 판별 된 메일에 대한 부분만 바이러스 탐색기에서 바이러스 검사를 받도록 하여, 모든 수신 메시지들의 바이러스 검색에 필요한 시간을 최소화 하였다. 따라서 정크메일 차단에서 바이러스 검사까지 〔그림 2〕와 같은 기존의 메일 시스템보다 메일 전송 지연에 따른 문제를 보완 하여 사설망 내부에서의 메일 송수신 효율을 강화 시켰다.

Ⅳ. 사용결과 및 평가

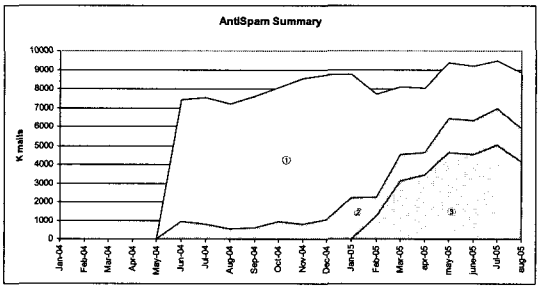
본 연구에서 구현한 FQDN 확인과 개인화 격리 처리를 이용한 정크메일 차단 시스템의 특징은 기존의 정크메일 차단 시스템이 제공하는 내용별 메일 분류 기능에 초점을 맞추지 않았다. 이는 메일 시스템을 이용하는 사용자들의 요청에 의한 것으로 업무에 필요한 것 이외의 메일을 읽어 보고 분류하는데 소요되는 시간을 줄이고, 정크메일에 편승해서 침입하는 악성코드를 메일 시스템에 도달되기 이전에 차단하도록 하여 시스템을 보호하고 메일 시스템의 처리 효율을 높이기 위한 것이다. 하지만 정크메일을 차단하는데 있어 오탐지율을 최소로 하기 위해서 격리 처리(Ouarantine Process) 과정을 통해 메일 수신자가 불분명한 메일들은 수신자가 확인 후 수신하도록 시스템을 구성하였다. FQDN 확인과 개인화 격리 처리를 이용한 정크메일 차단 시스템에 대한 평가는, 이 시스템에서 처리하는 메일들 중 얼마만큼의 메일 트래픽이 각 단계의 차단 시스템에서 차단되고, 기존의 메일 시스템과 비교해서 효율적으로 시스템이 운용되는지를 비교 하였다. 이는 차단 시스템의 각 단계별 버려지는 메일 트래픽과 시스템 연산에 필요한 자원이 얼마만큼 절약되는지를 분석하였다. 본 연구에서 구현한 시스템의 평가를 위하여 1개월간 시스템에서 처리한 메일의 분류 내역과 1, 2차 정크메일 차단 시스템이 구현되기 전후 6개월간의 정크메일과 정상메일 처리내역을 분석하여 영역별 도표로 도식화 하였다.



〔그림 13〕 FQDN과 개인화 분류를 이용한 정크메일 차단
① Incoming Mails
② Quarantine Mails
③ Delivered Mails to Users

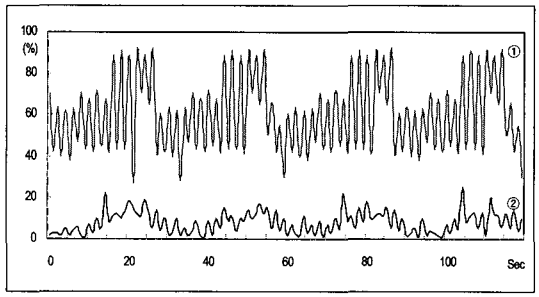
〔그림 13〕에서 ①, ②, ③번 영역의 합산된 수치는 시스템에 전달되는 모든 메일의 양을 나타낸다. ② 번 영역은 FQDN 확인과정을 거쳐 정상적인 도메인에서 발송한 메일이라고 판별된 메일들 중 격리처리 절차(Quarantine Process)에 의해서 버려지는 메일의 양을 나타내는 영역이다. ③번 영역은 1차 정크메일 차단 시스템과 2차 정크메일 차단 시스템을 모두 통과해서 사용자에게 전달된 메일의 양을 나타내는 영역이다. 전자 우편의 전송되는 추이를 보면, 월요일에서 금요일 사이에 꾸준히 수신되는 메일의 양이 많았다가 토요일과 일요일의 휴일에 메일의 수신 량이 줄어드는 굴곡의 추이를 볼 수 있다. 외부

인터넷 망으로부터 메일 시스템에 전달되는 전자우편의 양은 엄청나게 많지만, 사용자들이 수신하기를 원하는 메일의 양은 ③번 영역, 즉 전체 수신되는 메일의 양 대비 32% 수준임을 알 수 있다. 그리고 FQDN 발송 주소지의 도메인 검색만으로 차단할 수 있는 정크메일의 양은 ①번 영역에 해당하는 전체 수신 메일의 53%에 이르고, 개인별 격리 프로세스에 의해서 버려지는 메일의 수는 15% 정도임을 1달 동안의 로그 분석결과 알 수 있었다. 하지만 FQDN 확인과정에 있어 일부 메일 서버들이 공인 IP 부족이나 메일시스템의 보호를 위해 시스템을 사설 망 안쪽에 두었을 경우, 메일을 교환해 주는 메일 서버와 DNS Name Resolution 설정을 할 때 PTR 레코드에 대한 설정을 제대로 하지 않았거나, 인터넷 망의 공인 IP 대역에서 C Class 가 아닌 서브넷(Subnet)을 이용하여 메일 서버와 DNS Server를 구현 하였을 경우 Classless Name Resolution 설정을 해주지 않아서 PTR 레코드를 이용한 Reverse Name Resolution이 불가능 한 경우가 발생 하였는데, 이럴 경우 메일 재생 서브 프로시저(Recycle Sub Procedure)에 의해 메일 발신자로부터 메일을 다시 수신 받도록 하였고, FQDN 확인 절차를 통과해 User Quarantine Process에서 사용자별로 격리처리를 하도록 하였다.



〔그림 14〕 Anti Spam Summary
① Incoming Mails
② 기존 시스템에 의한 차단
③ 개선된 시스템에 의한 차단

〔그림 14〕는 개선된 정크메일 차단 시스템을 이용하기 이전 6개월과 이후 6개월의 메일 처리내역을 분석하여 기존의 메일 처리 시스템과 개선된 정크메일 차단 시스템의 성능을 분석한 결과이다. ①, ②, ③번 영역의 합산된 수치는 시스템에 유입되는 전체 메일들의 양을 나타낸다. ②번 영역의 수치는 기존의 정크메일 차단에 사용되었던 컨텍스트 필터(Context Filter)방법에 의해 사용자에게 전달된 메일의 양을 나타내고, ③번 영역의 수치는 개선된 정크메일 차단 시스템에 의해 수신자에게 전달된 메일의 양을 나타낸다. 그림에서 보는 것처럼 FQDN과 개인화 분류를 이용해 구현한 정크메일 차단 시스템은 기존 시스템 보다 정크메일을 더 효율적으로 차단하였으며, 기존의 메일시스템과는 달리 개인이 확인하는 격리 처리(Quarantine Process)에 의해 정크메일 오류 탐지에 의한 손실되는 전자우편이 없도록 하였다. 또한 내부로 유입되는 대량의 메일 트래픽을 단계적으로 차단하여, 메일서버에서 바이러스 검색이나 룰 베이스(Rule Base) 갱신에 소요되는 시스템 비용을 기존 시스템 보다 많이 절감 하였고, 메일 시스템이 보다 안정적으로 운영되도록 하였다. 〔그림 15〕 시스템 부하 비교는 〔그림 12〕의 ③ Mail Server의 CPU 부하를 120초 동안 기존의 메일처리 시스템 환경에서의 CPU 부하와, 개선된 메일 처리 시스템에서의 CPU 부하로서 비교한 그림이다. 〔그림 14〕 Anti-Spam Summary에서 볼 수 있듯이 기존의 시스템에서는 ②, ③번 영역을 합친 양 의 메일 트래픽을 처리 해 왔지만, 개선된 시스템에서는 단계적인 정크메일 차단으로 실제 메일 서버에서는 ③번 영역 양만큼의 메일 트래픽을 처리하기 때문에 메일 서버에서의 메일 송, 수신 처리에 필요한 자원이 기존 시스템에 비해서 절약 되고 효율적으로 운용 되고 있음을 보이고 있다.



〔그림 15〕 시스템 부하 비교
① 기존의 메일 처리 시스템
② 개선된 메일 처리 시스템

V. 결 론

인터넷을 이용한 전자우편은 이제 소수의 통신 수

단이 아닌 일반인이 널리 사용하는 기본적인 통신 수단으로 자리 잡고 있으며, 이에 따른 정크메일의 피해 규모도 날로 커지고 있다. 현재 다양한 방법의 정크메일 차단 방법이 제안되고 수행되고 있으나 다양해지는 정크메일에 대응하기에는 역부족이고, 대응 비용 또한 급격히 증가 하고 있다. 본 연구에서 구현한 FQDN(Fully Qualified Domain Name)과 개인화 격리처리를 이용한 정크메일 차단 시스템은 대부분의 정크메일이 인터넷 망의 공인 IP에서, 수집된 대량의 메일링 리스트를 이용하여 발신 전용으로 발송 된다는 특성에 착안하여, 별도의 메일 분류에 필요한 알고리즘 없이 단순히 메일 헤더를 분석하여 정해진 형식에 맞게 메일이 발송 되었는지, 메일이 정상적인 도메인(Fully Qualified Domain)으로부터 발송 되었는지 확인하는 기능으로 메일 시스템에 유입되는 엄청난 양의 정크메일트래픽을 차단하였고, FQDN의 조건을 충족 하지 못하는 도메인에서 발송된 메일들을 2차적으로 베이시안 알고리즘을 이용한 개인화(Personalized) 격리 처리(Ouarantine Process) 작업을 거쳐서 최종적으로 수신자가 원하는 메일들만 받아 볼 수 있도록 하였다. 메일 수신자 자신들이 메일의 수신여부를 최종적으로 판단하기 때문에 정크메일의 오류 탐지율을 획기적으로 줄이고, 룰 베이스 갱신과 바이러스 검색 등의 메일 서버에서 필요한 프로세스에 소요되는 시간과 비용을 줄여 전체적으로 사용자에게 전달되는 전자우편이 효율적으로 관리되도록 하였다. 기존의 정크메일 차단 시스템은 단순히 컨텍스트 필터링의 룰 베이스에 기반을 둔 패턴 매치 차단 방법을 사용하기 때문에 메일 차단 시스템에서 수신자에게 정상적인 메일이 도달하기까지 많은 절차와 연산 작용을 거쳐야 되고 메일에 유입되는 엄청난 양의 정크메일에 대해서 모두 룰 베이스를 적용하기 때문에 사용자에게 전달되는 메일을 추출해 내는 시간과 비용이 매우 비효율적이었고 시스템에 부담을 많이 주었다. 본 연구에서 구현한 시스템은 현재 발생하고 있는 정크 메일들의 특징을 분석해서 발신 전용 IP 메일 서버에서 발생하는 메일 트래픽이 가장 많다는 것에 착안하여 이에 효율적으로 대응할 수 있도록 두 단계에 거쳐 유입되는 메일들을 걸러내도록 하였다. 하지만 정크메일의 패턴이 다양해지고 정크메일 발송 기술 또한 발전하기 때문에 향후 연구에서도 정크메일 차단 시스템은 지속적로 변하는 정크메일 발송 기술의 추이를 메일 로그 분석 등의 기술 분석을 통하여 이에 대응하도록 지속적으로 발전 시켜야 한다.

참 고 문 헌

[1] S. Atkins, "Size and cost of the problem," in Proceedings of the Fifty sixth Internet Engineering Task Force (IETF) Meeting, (San-Francisco, CA), Spam Con Foundation, March 2000.

[2] 백기영, 이철수, 류재철, "URL 빈도분석을 이용한 스팸메일 차단 방법," 정보보호학회논문지 제 14권 제 6호 2004.12.

[3] 김성찬, 이상훈, 전문석, "정크메일 차단을 위한 FQDN 확인 시스템의 구현 및 평가," 정보처리학회논문지 C 12-C권 제 3호 2005.6.

[4] 박광진, 공진동, 황성원, "2003년 정보화 역기능 실태조사," 한국정보보호 진흥원, 2003년 개인 인터넷 이용자의 정보화 역기능 실태조사 보고서 pp. 43-63, 2003.12.

[5] M. Salib, "Heuristics in the blender," in Proceedings of the 2003 Spam Conference, (Cambridge, US), 2002.

[6] J. Weaver, "AOL escalates Spam warfare," MSNBC, March 2003.

[7] 박정선, 김창민, 김용기, "퍼지 관계 곱을 이용한 내용기반 정크메일 분류 모델," 정보과학회 논문지 소프트웨어 및 응용 제 29권 제10호 pp. 726-734, 2002.10.

[8] 정옥란, 조동석, "개인화된 분류를 위한 웹 메일 필터링 에이전트," 정보처리학회논문지 B 제10-B권 제 7호 pp. 853-861, 2003.12.

[9] P. Pantel and D. Lin, "Spam corp. : A Spam classification & organization program," in Learning for Text Categorization : Papers from the 2000 Workshop, (Madison, Wisconsin), AAAI Technical Report WS-98-05, 2000.

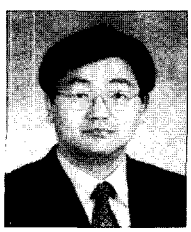
[10] 서정우, 손태식, 서정택, 문종섭, "n-Gram 색인화 Support Vector Machine을 사용한 스팸메일 필터링에 대한 연구," 정보보호

학회논문지 제14권 제2호 pp. 23-31, 2004. 4.
[11] T. Oda and T. White, "Developing an immunity to Spam," in Proceedings of the Genetic and Evolutionary Computation Conference (GECCO 2003), (Chicago), July 2003.
[12] M. Sahami, S. Dumais, D. Heckerman, and E. Horvitz, "A Bayesian approach to filtering junk E-mail," in Learning for Text Categorization : Papers from the 2000 Workshop ,(Madison, Wisconsin), AAAI Technical Report WS-98-05, 2000.
[13] G. Lindberg, "Anti-Spam Recommendations for SMTP MTAs," Chalmers University of Technology, RFC2505, February 2000.
[14] D.Eastlake, C. Kaufman, "Domain Name System Security Extensions," RFC 2065, January 2000.
[15] H. Eidnes, G. de Grouts, "Class less IN-ADDR.ARPA delegation" RFC 2317, March 1998
[16] Ion. A, Georgios. P, Vangelis. K, Georgios. S, Constantine. D, "Learning to Filter Spam E-Mail: A Comparison of a Naive Bayesian and a Memory-Based Approach", PKDD 2000, pp. 1-13, Sep 2000.
[17] Mehran. S, Susan. D, David. H, Eric. H, "A Bayesian Approach to Filtering Junk E-Mail", In AAAI-98 Workshop on Learning for Text Categorization. 1998
[18] Yanlei. D, Hongjun. L, and Dekai. W,"A Comparative Study of Classification Based Personal E-Mail Filtering", 4th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD'00). Pp. 408-419, 2000.

〈著者紹介〉

김 성 찬 (Sung-Chan Kim) 정회원
2000년 10월 ~ 현재: (주) 유코레일 정보시스템부 차장
2002년 2월: 숭실대학교 정보통신학과 석사
2005년 2월: 숭실대학교 정보통신학과 박사 수료
<관심분야> 유, 무선 네트워크, 정보보안

천 준 호 (Junho Choun) 정회원
2003년 2월: 숭실대학교 컴퓨터학과 학사
2005년 2월: 숭실대학교 컴퓨터학과 석사
2005년 3월~현재: 숭실대학교 컴퓨터학과 박사과정
<관심분야> 네트워크 보안, 무선 라우팅 보안, 암호학



전 문 석 (Moon-Seog Jun) 정회원
1980년 2월: 숭실대학교 전자계산학과 학사
1986년 2월: University of Maryland 전산과 석사
1989년 2월: University of Maryland 전산과 박사
1989년: Morgen State University 전산수학과 조교수
1989~1991년: New Mexico University 부설 Physical Science Lab. 책임연구원
1991년~현재: 숭실대학교 컴퓨터학과 정교수
〈관심분야〉 네트워크 보안, 컴퓨터 알고리즘, 암호학