수집과 빈도분석을 통한 스팸메일 차단 방법

백 기 영[†] · 김 승 해[††] · 최 장 원[††] · 류 재 철[†††]

요 약

인터넷을 이용한 이메일은 이제 소수의 통신 수단이 아닌 일반인이 널리 사용하는 기본적인 통신 수단으로 자리잡고 있으며, 이에 따른 스팸메일의 피해 규모도 날로 커지고 있다. 현재 다양한 방법의 스팸메일 차단 방법이 제안되고 수행되고 있으나 다양해지는 스팸메일에 대응하기에는 역부족이다. 이 논문에서 제시한 스팸메일 차단 방법은 수집, 빈도분석과 차단의 3단계로 구성되며, 수집되는 스팸메일을 이용하여 다양한 스팸메일에 대응할 수 있으며, 변화하는 스팸메일의 형태에 대해서도 대응할 수 있는 구조를 가지고 있다.

A spam mail blocking method using collection and frequency analysis

Ki-Young Baek[†] · Seung-Hae Kim[††] · Jang-Won Choi[†††] · Jae-Cheol Ryou[††††]

ABSTRACT

The email using internet is situated by means of basic communication method that ordinardy people use. Thereby damage scale of the spam mail becomes wider. The many blocking methods of the spam mail are proposed and archived. But they are insufficient to block various types of spam mail. The blocking method of spam mail proposed by this paper is consisted of 3 steps (collection, frequency analysis and blocking). It can effectively block various types of spam mail using collected spam mail and various forms of spam mail that changes.

키워드 : 스팸메일(Spam mail), 광고(unsolicated commercial), 메일(mail), 차단(block), 수집(collection)

1. 서 론

인터넷을 통한 네트웍의 발달은 사회 전체의 패러다임을 변화시켰으며, 현대사회를 정보화 시대로 이끌고 있다. 특히 이메일은 기존의 방식에 비해 정보의 교환이나 의사소통에 있어서 보다 빠르고 효과적인 방식으로 사람들에게 편리를 제공해왔다. 그러나 이러한 정보화시대의 병폐들 중 하나로서 스팸메일의 문제가 제기되었고, 오늘날 인터넷상의 네트웍 운영자, 기업 및 여타 조직과 개인사용자들에게까지 광범위하게 문제를 야기하고 있다.

스팸메일이 사회문제로 등장한 것은 불과 2-3년 사이의 일이지만, 사회 전체에 미치는 영향력은 그 어떤 정보화 역기능보다 크고도 넓다. 2002년 12월 네티즌 2000명을 대상으로 조사한 바에 따르면, 가장 피해를 입은 정보화 역기능으로 개인정보침해(32.7%)나 바이러스 피해(7.7%)보다 "스팸메일(50.6%)"을 꼽았다. 물론 단일 피해규모로는 개인정보침해나 바이러스 피해가 스팸메일로 인한 것보다 크겠지만, 스팸메일은 일상적이고 보다 대중적으로 발생하는 피해이기 때문이다.

이에 따라 스팸메일을 차단하기 위한 여러 가지 방법들이 연구되고 있으나 스팸메일을 차단하기 위해서는 기술적으로도 어려움이 많지만 기술적인 문제 외에 스팸메일에 대한 인식이 주관적인 데에 따른 어려움도 많다. 예를 들어 어떤 사람에게는 받기를 원하지 않은 성인광고 메일이 다른 사람들에게는 성인 사이트에 대한 정보를 얻는 메일일 수 있으므로, 이를 스팸메일로 구분해야 되는 가에 대한 판단의 어려움이 있다.

일반적으로 스팸메일에 대한 정의는 "인터넷을 통하여 다수의 수신자에게 전송되는 원하지 않는 상업성 메일"로 규정짓고 있다[1].

대표적인 스팸메일 차단 방법으로는 스팸메일의 제목이나 내용, 보낸 사람을 필터링하여 스팸메일을 차단하는 일반적인 방법과 스팸메일 발송 서버의 IP를 신고하여 이를 차단하는 RBL(Real-time Black-hole List)[2]와 같은 방법이 있으며, 향상된 스팸메일 차단 방법으로 스팸메일 헤더나 보낸 사람, 내용에 존재하는 단어의 빈도를 조사하여 파악하는 SpamAssassin[3]과 같은 방법이 있다.

SapmAssassin에서의 가장 큰 문제점은 룰을 만드는 데에 있다. 일정기간 들어오는 메일에 대해 스팸메일인지 일반메일인지 판별을 해 줌으로써 새로운 룰을 생성할 수 있

※ 이 논문은 정보통신부 대학 IT 연구센터 육성지원사업에 의한 것임.
† 정 회 원 : ㈜시큐컴 인터넷보안부 부장
†† 정 회 원 : 한국과학기술정보연구원 연구원
††† 종신회원 : 충남대학교 컴퓨터과학과 부교수
논문접수 : 2004년 6월 8일, 심사완료 : 2004년 9월 13일

으나, 사용자가 스팸메일에서 나타나는 특징과 일반메일에서 나타나는 특징을 분석하여 룰을 생성해야 한다. 이와 같은 방식 때문에 SpamAssassin은 새로운 형태의 스팸메일에 대한 대응이 느리며, 룰 추가가 힘든 문제점이 있다. 또한 메일의 내용에 대해 빈도조사를 시행함으로써 스팸메일 검사 시간이 오래 걸린다는 단점이 있다.

이에 기존의 스팸메일 차단 방법의 단점을 보완한 수집, 분석, 차단의 3단계로 구성된 스팸메일 차단 방법을 제안한다.

2. 스팸메일 차단 기술

대표적인 스팸메일 차단 기술로는 다음과 같은 것들이 있다.

2.1 RBL(Realtime Blackhole List)

RBL[2]은 MAPS(Mail Abuse Prevention System) RBL이라고 하여, 사용자들의 신고에 의한 스팸메일 발송 서버의 IP 리스트를 유지한다. 접수된 스팸메일 발송 서버의 리스트는 일정 기간 서버에 존재하며, 메일 서버의 관리자가 요청하기 전까지는 스팸메일 발송 서버로서 남게 된다.

이와 같은 리스트는 사용에 있어서 일정한 금액을 요구하며, RBL을 지원하는 메일 서버 프로그램에서 주기적으로 스팸메일 발송 서버의 리스트를 가져와 스팸메일을 차단하며, 대부분의 메일 서버 프로그램에서 RBL을 지원한다.

RBL은 SMTP(Simple Mail Transport Protocol) 프로토콜[4] 상에서 스팸메일을 차단하기 때문에 특별한 스팸메일 방지 기술이 필요한 것도 아니며, 스팸메일 검사 시간이 짧고, 메일 서버에 부담을 적게 준다.

그러나 메일 서버 사용자의 스팸메일 발송에 의해 메일 서버 전체 이용자가 피해를 볼 수 있으며, Spoof된 IP를 이용하여 스팸메일을 발송할 경우 선의의 사용자가 피해를 볼 수 있는 단점이 있다.

2.2 필터링

대부분의 메일 서버 프로그램에서 제목, 보낸 사람, 받는 사람, 내용에 대한 필터링을 제공하며, 필터링을 좀 더 효과적으로 하기 위해 메일 서버와 같이 붙어서 동작하는 procmail[5]이라는 프로그램도 있으며, 필터링을 좀 더 편하게 하며, 변조된 스팸메일을 차단하기 위해 정규 표현식(Regular Expression)을 이용한 필터링을 지원하는 프로그램도 많이 있다.

또한 Microsoft Outlook Express나 Netscape Messenger와 같은 MUA(Mail User Agent)에서도 필터링을 지원하여[6] 간단하게 제목에 "(광고)"가 들어간 메일을 스팸메일로 분류함으로써 많은 효과를 볼 수 있다.

그러나 스팸메일이 점점 지능화됨에 따라 제목에 "(광고)"의 변종인 "강고" 또는 "정보"와 같은 단어를 넣기도 하며, 일반 메일이나 쇼핑몰에서 전송하는 청구서와 같은 형태의 스팸메일을 작성함에 따라 이와 같은 방법은 큰 효과를 볼 수 없다는 단점이 있다.

2.3 Spam Net

SpamNet[7]은 대부분의 스팸메일은 같은 내용을 많은 사용자에게 전달한다는 점을 이용한 것으로 사용자들이 스팸메일을 신고하며, 사용자들이 신고한 스팸메일에서 같은 것이 일정 개수 이상이 되면 이를 스팸메일로 구분 짓는 방식이다.

스팸메일로 구분된 메일은 내용에서 해쉬값을 추출하여 데이터베이스에 저장하며, 이를 요청하는 사용자에게 전달하여 스팸메일 판별의 자료로 활용할 수 있도록 한다. 자료의 요청은 년단위로 일정 금액을 납부한 사람만이 요청할 수 있다.

또한 스팸메일에 대해 신고한 사람의 신뢰성을 확보하기 위해 "Trust Level"을 두어, 처음에 시작하는 사용자는 0이란 값을 가지고 시작하며, 자신이 신고한 스팸메일이 스팸메일로 판별되어 데이터베이스에 들어가는 확률이 높아질 때마다 "Trust Level" 값이 올라가게 된다.

"Trust Level" 값이 높은 사용자들이 신고한 스팸메일은 좀 더 빨리 스팸메일로 등록되게 되며, "Trust Level"이 높은 사용자에게는 일정기간 동안 스팸메일 데이텁베이스를 이용할 수 있는 특권을 제공한다.

2.4 SpamAssassin

SpamAssassin[3]은 메일에서 스팸이 가질 수 있는 요소를 분석하여, 각각의 요소에 대해 점수를 주어 모두 합산한 점수가 일정 이상이면 스팸으로 판별하는 방식이다. 점수를 주는 방식에서 스팸에서 제외될 수 있는 요소는 −점수를 스팸으로 판별할 수 있는 점수는 +점수를 주어, 일반 메일을 스팸메일로 판별할 가능성을 줄인다.

메일의 전체 부분에 대해 수행한 결과값이 5 이상이면 스팸으로 판별하며, <표 1>과 같이 스팸메일 판별 과정을 메일 헤더에 넣어서 스팸메일로 판별된 메일에 대한 자세한 정보를 볼 수 있어 잘못된 룰셋 사용을 방지할 수 있다.

<표 1> SpamAssassin 예제

```
SPAM :                                  Start SpamAssassin results
SPAM : This mail is probably spam.  The original message has
       been altered
SPAM : so you can recognise or block similar unwanted mail in
       future.
SPAM : See http://spamassassin.org/tag/ for more details.
SPAM :
SPAM : Content analysis details :   (13.3 hits, 5 required)
SPAM : Hit! (4.3 points)  Reply-To : is empty
SPAM : Hit! (0.8 points)  Found an X-Em-Version : header
SPAM : Hit! (0.0 points)  BODY : Includes a URL link to send an
       email
SPAM : Hit! (3.2 points)  HTML-only mail, with no text version
SPAM : Hit! (1.9 points)  Subject is all capitals
SPAM : Hit! (3.1 points)  Subject is full of 8-bit characters
SPAM :
SPAM :                                  End of SpamAssassin results
```

또한 SpamAssassin의 룰셋은 로컬 네트웍에서 전송된 메일과 외부 네트웍에서 전송된 메일에 대해 각각 다른 값을 부여하여, 로컬 네트웍에서 전송된 메일에 대해 스팸메일로 판별될 가능성을 줄이고 있다.

SpamAssassin은 메일을 3가지 부분으로 나누어 검사하며 각각의 부분은 다음과 같다.

■ 헤더 분석

메일의 헤더[8]에는 기본적인 보낸 사람, 받는 사람, 제목과 같은 메일의 기본정보에서부터 MUA 고유의 정보를 나타내는 X 어플리케이션 헤더까지 많은 정보를 담고 있다. SpamAssassin에서는 이런 메일이 고유정보에 점수를 부여하고 있다.

예를 들면, 메일이 X x 헤더를 포함하고 있으면 +4.300, From 형식이 something-offers 형식이면 +4.300, 보낸 사람의 메일 주소가 whitelist에 있으면 -100과 같은 값을 준다.

■ 본문 분석

스팸메일은 독특한 본문 스타일을 가지고 있다. 예를 들면, 텍스트로 구성된 메일을 포함하지 않은 HTML로만 구성된 메일, HTML의 Heading 태그의 잦은 사용, 색이 들어간 글자의 사용과 같은 것들이다.

SpamAssassin에는 이러한 스팸메일의 특징을 룰로 만들어 검사한다.

■ 블랙리스트

mail-abuse.com[2]나 ordb.org[9]의 스팸메일 발송리스트를 이용하여 스팸메일을 차단한다.

2.5 베이시안 필터링(Bayesian Filtering)

폴 그래험(Paul Graham)이 2002년 9월에 발표한 "A Plan for Spam"[10]이란 글은 베이시안 필터링에 근거해서 개개인마다 다른 스팸판별 규칙을 생성하고 이를 이용하여 스팸을 차단하는 방법에 대해 소개한다.

베이시안 필터링 기술은 미래 상황을 추측할 수 있게 해주는 18세기 토마스 베이시스(Thomas Bayes)의 "확률론"에 근거한 것으로, 요점은 다음과 같다.

어떤 사람에게는 스팸이 될 수 있는 메시지가 다른 사람에게는 유용한 정보가 될 수 있다는 사실에 대해 베이시안 스팸 필터'는 각 개인별 스팸 분류 기준에 대한 학습을 한다.

이러한 학습 과정을 통해 '베이시안 스팸 필터'는 시간이 지남에 따라 그 효율성이 배가되고, 일반적으로 99.8퍼센트의 차단률 및 0.05퍼센트의 오탐지율을 보인다. 그러나 이와 같은 방법은 개인의 학습에 따라 스팸메일을 차단하는 데에는 효과가 좋으나 다수의 사용자에 대해 학습을 시키고 스팸메일을 차단하는 데에는 큰 효과를 발휘하지 못하는 단점이 있다.

3. 수집과 빈도 분석을 이용한 스팸메일 차단 방법

제안하는 스팸메일 차단 방법은 수집, 분석, 차단의 3부분으로 구성된다.

기본적인 아이디어는 스팸메일을 수집하고, 수집한 스팸메일을 분석하여, 스팸메일을 정의할 수 있는 정규화된 룰을 생성하며, 이 룰을 이용하여 받는 메일에 대해 스팸메일 검사를 하여 차단하는 것이다.

이에 대해 스팸메일 수집에서는 "스팸메일을 어떻게 수집할 것인가?"에 관한 스팸메일 수집 방법에 관해 제안하며, 스팸메일 분석에서는 "모아진 스팸메일에서 어떤 부분을 분석하여, 어떤 식의 정규화된 룰을 생성할 것인가?"에 관한 스팸메일 분석 방법을 제안하고, 스팸메일 차단에서는 "분석한 정보를 이용하여 어떻게 차단할 것인가?"에 관한 스팸메일 분석 방법에 관해 제안한다.

3.1 스팸메일 수집

스팸메일 수집에 있어서 스팸메일의 수집은 위에서 언급한 것처럼 실시간으로 이루어져야 스팸메일 차단에 효과적이며, 자동화된 도구를 이용하여 이루어 질 수 있어야 된다.

(1) 스팸메일 수집 방법

메일이 인터넷에서 중요한 통신 수단으로 자리 잡음에 따라 대부분의 통신은 메일을 이용하여 이루어지고 있으며, 이에 따라 여러 개의 메일 주소를 사용하게 된다. 또한 무료로 서비스하는 대형 메일 업체들이 증가하고, 가입만 하면 메일 주소를 무료로 쓸 수 있게 해 주는 인터넷 쇼핑몰 들이 늘어감에 따라 사용하지 않는 메일 주소가 늘어나게 된다.

사용하지 않은 메일 주소에 전달된 메일을 살펴보면 대부분이 자신이 받고자 하지 않은 스팸메일이 주를 이룬다. 이는 가입할 때 사용한 메일 주소 또는 인터넷상의 게시판이나 Usenet과 같은 뉴스 그룹에 포스팅 할 때 사용한 메일 주소를 이용하여 스팸메일을 발송을 하기 때문에 사용하지 않아도 원치 않는 스팸메일을 전달 받게 된다.

스팸메일 수집은 이런 스팸메일 발송 도구의 동작 방식을 이용한 것인데, 수집은 다음과 같은 과정을 거친다.

첫째, 사용하지 않은 가상의 메일 주소를 여러 개 생성한다.

둘째, 가상의 메일 주소를 이용하여 사람들이 많이 사용하는 게시판에 포스팅하거나 메일 주소가 노출되는 뉴스 그룹에 포스팅한다.

셋째, 메일 주소 수집기[11]는 게시판 또는 뉴스 그룹에서 사용자의 메일 주소를 수집하고, 메일 주소에 스팸메일을 발송한다.

넷째, 가상의 메일 주소로 도착하는 모든 메일은 스팸메일로 판단하고 저장한다.

스팸메일 수집에 대한 기본적인 아이디어는 메일 받기를 동의하지 않은 메일 주소로 도착한 모든 메일은 스팸메일로 판단하며, 이를 위해 가상의 사용하지 않은 메일 주소를 여러 개 생성하여 메일 주소가 노출되도록 한 후에, 스팸메일 발송을 유도하는 것이다.

위와 같은 스팸메일 수집에 있어서 다른 메일에 대한 판단 자료로 사용하기 위해서는 다음과 같은 조건을 만족해야 된다.

수집된 스팸메일과의 단순 비교를 통해 스팸메일을 판단할 경우, 일반적으로 전송되는 스팸메일보다 수집된 스팸메일이 먼저 도착해야만 판단의 자료로 사용할 수 있다.

많은 스팸메일을 지속적으로 받을 수 있어야 된다.

위의 조건을 만족하기 위해서 본 논문에서는 다음과 같은 방법을 제안한다.

■ 스팸메일의 빠른 수집

스팸메일 발송기는 스팸메일의 발송 시간을 줄이기 위해서 스팸메일 발송 리스트를 사용자의 메일 주소를 사용자 아이디와 사용자 도메인으로 분리하여 정렬한 후에, 같은 호스트 내의 사용자에게는 동시에 스팸메일을 발송하여 스팸메일 발송시간을 줄이고 있다.

따라서 스팸메일 수집을 위한 가상의 메일 주소는 아이디와 도메인 모두를 일반적인 문자열 정렬에서 상위에 위치할 수 있도록 숫자 또는 영문 알파벳의 처음 부분인 a, b와 c등을 이용하여 생성하며, 길이가 짧은 문자열이 길이가 긴 문자열에 비해 정렬에서 상위에 위치함으로 짧은 도메인 및 아이디를 사용하여 생성한다.

■ 많은 스팸메일을 지속적으로 수집

스팸메일 발송자가 사용하는 스팸메일 발송기는 스팸메일 발송 리스트를 가지고 있으며, 이를 주기적으로 업데이트 하고 다른 사람들을 통해 전달된다. 이에 따라 한번 스팸메일 발송 리스트에 메일 주소가 등록되면 그 뒤로부터 전달 받는 스팸메일의 양은 기하급수적으로 증가하게 된다.

스팸메일을 지속적으로 받기 위해서는 스팸메일 발송 리스트에서 누락되지 않고 지속적으로 리스트에 등록되어 있어야 된다. 스팸메일 발송기에서는 스팸메일을 전달 받는 사용자가 메일을 확인 하는 지 여부를 주기적으로 검사하여 메일을 수신하지 못하거나 확인하지 않는 사용자의 리스트는 발송 리스트에서 제외한다.

사용자의 메일 사용 여부를 검사하기 위해 스팸메일에 수신 확인 가능한 컨텐츠를 첨가하거나 수신 거부 방법을 첨가하여 수신 거부한 사용자에 대해서는 메일의 내용을 확인한다고 판단하고 주기적으로 스팸메일을 발송한다.

따라서 스팸메일 수집 시에 위와 같은 방법에 대응하기 위해 자동적으로 메일의 내용을 확인하며, 수신 거부를 할 수 있도록 한다.

3.2 스팸메일 분석

스팸메일 수집에서 스팸메일을 수집할 수 있는 방법을 제안했으며, 이에 따라 대량의 스팸메일을 수집할 수 있다. 스팸메일 분석에서는 이를 분석하여 스팸메일 차단의 판단 자료로 이용할 수 있는 분석자료를 생성한다.

스팸메일 분석에서 중점을 둔 부분은 다음과 같다.

1. 스팸메일 차단에서 스팸 차단율을 높이기 위한 분석 자료를 생성한다.
2. 새로운 종류의 스팸메일에 대해서도 판단할 수 있는 자료를 생성한다.
3. 스팸메일 차단에서 판단 시간을 빠르게 할 수 있는 자료를 생성한다.

위와 같은 중점 사항에 따라 제안하는 분석방법은 다음과 같이 크게 3부분으로 구성된다.

■ 비교정보 저장
- 스팸메일 판단 시에 저장된 정보와 비교하여 판별

■ 빈도 조사
- 스팸메일 판단 시 메일 헤더 빈도를 조사하여 판별

■ 내용 비교
- 스팸메일 판단 시에 내용의 Hash 값을 저장하여 판별

(1) 비교정보 저장

비교정보는 스팸메일 판단 시에 가장 빠른 시간내에 판단할 수 있는 자료가 되며, 다음과 같은 유형의 스팸메일을 판단하기 위해 사용된다.

■ 일반 메일 형식의 제목을 가진 스팸메일

사용자의 확인을 유도하기 위해 일반적인 메일의 형태를 가지고 발송되며, 예를 들어 다음과 같은 제목을 가진다.

Re : That movie
한번 연락드리려니 쑥스럽네요. ^^;;
수진아 네가 찾던거 같아…

■ 제목은 다르나 보낸 사람과 발송 서버가 같은 스팸메일

같은 제목에 의한 스팸메일 차단을 방지하기 위해 스팸메일 발송기는 제목이나 내용에 랜덤한 숫자나 알파벳을 추가하여 스팸메일을 작성한다. 이와 같은 경우에 제목이나 내용만 바뀌고 보낸 사람이과 스팸메일 발송 서버는 같은 경우가 대부분이며, 예를 들면 다음과 같다.

추석선물 고민하지마세요 풍요로움과 따뜻함을 느낄 수 있는 선물 06007469

위와 같은 형태의 스팸메일을 차단하기 위해 비교정보 저장에서는 다음과 같은 정보를 저장한다.

- 메일의 제목
  메일의 보낸 사람과 보낸 서버
- 메일의 제목을 저장할 때에는 제목이 같은 일반 메일이 스팸메일로 분류될 가능성이 있기 때문에 제목의 길이를 제한하여, 일정 길이(한글 6자, 영문 10자) 이상 되는 제목만을 저장한다.

  또한 메일의 보낸 사람과 보낸 서버의 내용을 저장하여 이를 같이 비교하는 이유는 메일의 보낸 사람은 위조가 가능하기 때문에 일반 사용자의 메일 주소가 스패머의 메일 주소로 분류되어 스팸메일로 분류될 수 있으며, 보낸 서버와 같은 경우에도 스팸메일 중계서버로 이용되어 잠시 동안만 스팸메일의 발송 서버로 활용되는 경우가 있기 때문에, 이 둘을 같이 비교한다.

(2) 빈도 조사

빈도 조사 방법은 수집된 스팸메일을 분석하여 비슷한 유형의 다른 스팸메일을 차단하기 위한 정보를 생성한다. 빈도 조사 방법은 앞에서 설명한 SpamAssassin에서 사용한 방법과 비슷한 형식으로 조사하며, SpamAssassin의 단점을 보완하여 정확하고 빠른 스팸차단이 가능하게 한다.

SpamAssassin의 기본 아이디어는 각각의 메일에 대해 SpamAssassin에서는 Score라 불리는 일종의 점수를 부여한다. 이 점수는 스팸메일일 가능성이 있는 단어에 대해서는 +값을 일반 메일일 가능성이 있는 단어에 대해서는 - 값을 부여하며, 5점 이상이 될 때에는 스팸메일로 판별하고 처리한다.

SpamAssassin에서는 스팸메일일 가능성이 높은 단어에 대해서는 높은 + 값의 가중치를 주며, 일반메일일 가능성이 높은 단어에 대해서는 낮은 -값의 가중치를 준다. 예를 들면, From 주소가 something-offers 형식을 가지면 +4.300을 부여하고, From 주소가 사용자의 whitelist에 존재하면 100을 주어 스팸검사에서 제외하도록 한다. SpamAssassin의 점수 부여 방식은 기존에 미리 등록된 단어에 대한 가중치를 이용하여 점수를 부여하며, 관리자가 들어오는 메일에 대해 스팸메일과 일반메일을 구분해 줌으로써 새로운 룰셋을 만들어 낼 수 있다.

이와 같은 SpamAssassin의 방식은 스팸메일 차단에 좋은 효과를 보이며, 일반메일이 스팸메일로 분류될 가능성을 줄이지만, 실질적으로 다음과 같은 문제점이 있다.

- 기존에 만들어진 룰셋 외에 새로운 방식의 스팸메일에 대해서는 차단하기 힘들다.
- 메일의 모든 내용을 룰셋과 비교 검사하여 점수를 생성함으로 스팸메일 검사 시간이 오래 걸린다.

제안하는 스팸메일 차단 방법에서는 스팸메일이라고 확신할 수 있는 메일을 실시간으로 다양한 메일 주소를 통해 수집할 수 있다. 이와 같이 수집되는 스팸메일을 이용하여 기존의 SpamAssassin의 단점을 해결하고자 하며, 제안하는 빈도 조사 방법은 다음과 같다.

- 스팸메일 분석과 검사 시간을 줄이기 위해 빈도 조사 및 검사는 메일의 헤더로 제한한다.
- 실시간으로 스팸메일의 수집이 가능하기 때문에 빈도 조사의 가중치에 시간의 개념을 넣는다.
- 빈도조사는 보낸 서버에 대해 수행한다.

메일의 헤더 부분에서 중요하게 생각할 수 있는 부분은 다음과 같다.

- Received
- From
- To
- Subject
- X Application 헤더

위와 같은 메일 헤더 중에서 빈도 조사에서는 보낸 메일 서버를 나타내는 Received 를 사용한다.

메일은 여러 개의 메일 서버를 거칠 때마다 메일 서버를 거쳐서 전송되었다는 것을 의미하는 Received 헤더를 포함시킨다. 따라서 Received 헤더를 추적하면 스팸메일을 발송한 원래 서버의 IP를 알아낼 수 있으며, 스팸메일을 전송하는 스패머들은 대량의 스팸메일을 전송하기 위해 Relay 제한이 풀려 있는 메일 서버를 스팸메일 전송의 중계서버로 이용한다. 따라서 같은 메일 서버로부터 단시간 내에 많은 스팸메일이 도착한다면 스팸메일을 보낸 메일 서버는 스팸메일의 중계서버로 이용된다고 볼 수 있다.

스팸메일 발송 서버를 이용한 빈도 조사에서 가중치를 결정하기 위해 2만개의 스팸메일을 분석하였으며, 스팸메일은 SpamArchive[12]의 스팸메일을 이용하였다.

SpamArchive는 스팸메일의 연구를 위해 스팸메일을 모아 저장/배포하며, 이는 스팸메일 방지 도구를 이용한 자동화된 방법과 사용자들이 수동으로 검색한 스팸메일을 전송함으로써 이루어지고 있다. 현재 하루에 5천 개의 스팸메일이 저장되며, 지금까지 22만 개 정도의 스팸메일이 저장되어 있다.

〈표 2〉 보낸 서버 빈도

보낸 서버	빈 도
10.2.202.xxx	615
216.65.3.xxx	110
204.200.197.xxx	90
205.158.62.xxx	74
216.65.3.xxx	65
216.65.64.xxx	59
205.158.62.xxx	56
205.158.62.xxx	41
66.14.165.xxx	23
68.171.98.xxx	20
68.19.91.xxx	16
67.15.24.xxx	15
68.218.161.xxx	13
69.44.166.xxx	12
219.153.1.xxx	12

위와 같은 빈도가 높은 보낸 서버에 대해 각각의 스팸메일을 받은 시간 사이의 간격을 조사하였으며, 간격은 1시간 이내는 10분 단위로 하며, 하루 이내에는 1시간 간격으로 조사하였다.

<표 3>의 자료를 이용하여 보낸 서버의 가중치를 설정하며, 점수(Score)가 50이 넘으면 스팸메일 판별 규칙의 자료로 활용한다. 스팸메일 판별 규칙의 기준이 되는 점수인 50은 임의로 설정하였으며, 각각의 시간 간격 내에 몇 개의 스팸메일을 받을 경우에 판별 규칙으로 활용할 것인가를 이용하여 가중치 값을 설정하였다.

보낸 서버 가중치 값의 설정은 스팸메일에 대한 피해를 줄이는 방향으로 정하였으며, 단기간 내에 많이 발송되는 것들에 대해서는 가중치 값을 높게 두어 빠른 대처를 할 수 있도록 하고, 상대적으로 빈도가 적은 것들에 대해서는

〈표 3〉 보낸 서버의 시간 간격에 따른 분포

시간 간격	빈 도														
	615	110	90	74	65	59	56	41	23	20	16	15	13	12	12
10	495	36	1	8	20	18	6	3	20	8	14	13	10	1	9
20	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1
30	4	1	1	1	1	2	1	1	1	1	0	0	1	1	1
40	2	1	1	2	1	4	1	1	0	1	0	0	0	1	0
50	2	1	1	1	1	1	1	1	0	1	0	0	0	1	0
1시간	3	1	1	1	1	1	1	1	0	1	0	0	0	1	0
2시간	12	5	5	1	1	1	1	1	0	1	0	0	0	1	0
3시간	13	2	7	1	1	1	2	1	0	1	0	0	0	1	0
4시간	10	2	15	2	1	1	1	1	0	2	0	0	0	1	0
5시간	11	4	10	4	1	1	1	2	0	1	0	0	0	1	0
6시간	9	2	8	4	1	1	3	1	0	1	0	0	0	1	0
7시간	5	4	1	1	1	1	1	1	0	0	0	0	0	0	0
8시간	11	1	2	3	1	1	1	1	0	0	0	0	0	0	0
9시간	1	1	1	4	1	1	1	1	0	0	0	0	0	0	0
10시간	2	1	1	2	1	1	1	1	0	0	0	0	0	0	0
11시간	2	1	1	1	1	1	1	1	0	0	0	0	0	0	0
12시간	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
13시간	1	1	1	1	1	1	3	1	0	0	0	0	0	0	0
14시간	2	1	1	1	1	1	1	1	0	0	0	0	0	0	0
15시간	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
16시간	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
17시간	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
18시간	1	1	9	1	1	1	1	1	0	0	0	0	0	0	0
19시간	1	1	1	1	4	1	1	1	0	0	0	0	0	0	0
20시간	1	1	2	1	2	1	1	1	0	0	0	0	0	0	0
21시간	1	1	5	1	2	2	2	1	0	0	0	0	0	0	0
22시간	1	1	1	1	2	2	1	1	0	0	0	0	0	0	0
23시간	4	1	1	2	1	1	1	1	0	0	0	0	0	0	0
24시간	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
그 외	13	33	7	23	11	7	16	9	0	0	0	0	0	0	0

가중치 값을 낮게 두어 정확성을 높게 하였다.

<표 4>는 <표 3>를 이용하여 만든 보낸 서버 가중치 값이며, <표 3>을 보면 대부분의 스팸메일은 같은 서버에서 10분 내에 발송된 다는 것을 알 수 있으며, 10분 내에서도 2~3분 사이에 발송되는 것들이 대부분이다. 따라서 10분 이내에 발송된 스팸메일일 경우에 2개를 받으면 바로 스팸메일 판별 규칙의 자료로 활용될 수 있도록 하여, 빠른 차단이 될 수 있도록 하였다.

그 외에는 6시간까지는 대부분 비슷한 분포를 보이나 10분 이내에 비해 반 정도의 빈도를 가지므로, 6시간 이내에 대해서는 5개의 스팸메일일 경우에 스팸메일 판별 규칙의 자료 활용될 수 있도록 하였다.

24시간 이내에는 6시간 이내보다 빈도가 낮으므로 가중치를 낮게 두었으며, 그 외의 자료를 분석해 보면, 대부분이 2~3일 이후에 발송된 것이므로, 2일 동안 업데이트가 없을 경우 판별규칙에서 제외함으로써 일시적으로 스팸메일 발송 서버로 이용된 경우에 피해가 없도록 하였다.

〈표 4〉 보낸 서버 가중치

마지막 수신 시간	가중치
10분 이내	+25
6시간 이내	+10
24시간 이내	+2
2일간 업데이트 없을 경우	판별규칙에서 제외

위와 같은 가중치를 적용하여 스팸메일 판별 규칙의 자료를 구성하며, 보낸 서버에 따른 판별 규칙은 <표 5>와 같다.

〈표 5〉 발송서버 스팸메일 판별 규칙

서버 IP	Score	마지막 수신 날짜
138.25.2.24	147	2003-08-22 14:45:33
128.37.24.52	30	2003-08-22 04:32:23

3.3 스팸메일 차단

위의 분석에서 만들어진 스팸메일 판별 규칙을 이용하여 스팸메일을 차단한다. 스팸메일 차단에서는 스팸메일 검사 시간을 단축하기 위해 수행시간이 빠른 검사 방법을 먼저 수행하며, 검사 수행 순서 및 방법은 다음과 같다.

1. 비교정보 검사

비교정보 판별 규칙을 이용하여 스팸메일을 검사하는 것으로 판별 규칙에서 제목이 같은 것이 있나 검사하며, 보낸 사람과 보낸 서버가 같은 판별 규칙이 존재하나 검사한다.

2. 빈도 검사

스팸메일 빈도 판별 규칙에서 Score가 50이 넘은 항목에 대해 검사한다.

3. 내용정보 검사

내용에서 링크와 이미지의 URL들의 해쉬값을 비교한다.

4. 제목을 이용한 필터링

국내에서의 이메일을 이용한 광고는 "(광고)"를 메일의 제목에 붙이도록 법으로 규제되어 있다. 따라서 이를 이용하여 제목에 "(광고)"가 들어간 메일에 대해 검사한다.

3.4 기존 방법과의 비교

〈표 6〉 스팸메일 차단 방법 비교

	제안하는 방법	RBL	SpamAssassin
스팸메일 수집 방법	자동 수집	사용자 등록	사용자 판별에 의한 Learning
가중치 적용	빈도 + 시간	X	빈도
스팸정보 공유 가능	가능	가능	서버별
스팸정보 분석 시간	중간	빠름	느림(본문분석)
서버 부하	중간	낮음	높음(본문분석)
차단 방법의 다양성	다양한 방법	보낸 메일서버 IP	빈도 조사

4. 시험 결과

제안한 아이디어를 검증하기 위한 시험환경을 구축하였으며, 기존의 스팸방지 시스템에 대한 시험 항목 및 결과에 대해 설명하면 다음과 같다.

4.1 스팸메일 방지 시스템 시험 항목

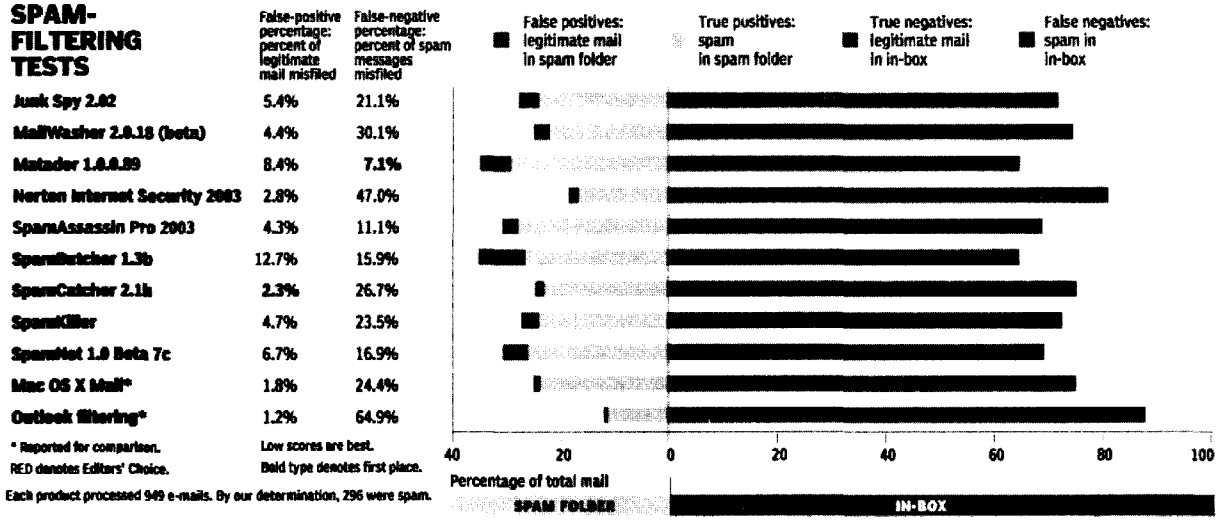
스팸메일 방지 시스템에 대한 시험은 크게 2가지로 분류되는데, 자세한 내용은 다음과 같다.

- 얼마나 정확하게 스팸메일을 판별하느냐에 관한 정확성 시험
- 사용의 편의성에 관한 시험

(1) 정확성 시험

PC Magazine에서는 2003년 2월에 몇 개의 제품을 이용하여 스팸메일 판별의 정확성을 측정하는 시험을 하였으며, 시험 환경은 다음과 같다.

리뷰어가 사용하는 실질적인 이메일 주소에서 도착하는 메일을 이용하여 시험하였으며, 일부 미리 메일을 등록하여 스스로 판별규칙을 생성하는 프로그램들이 있어서, 36시간 동안 도착한 172개의 메일을 기본적인 학습(Learning)에 사용했다.



(그림 1) 스팸메일 판별 정확성 시험

실질적인 테스트를 위해서 949개의 메일을 사용했으며, 기본적으로 다음과 같은 4가지 항목을 검사했다.

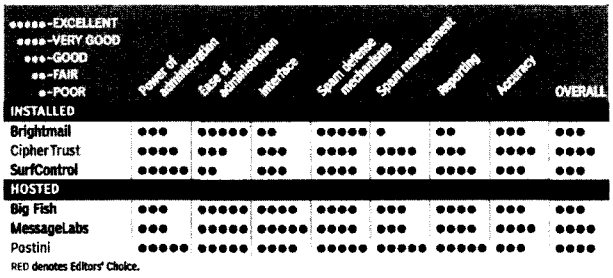
- 일반메일인데 스팸메일로 처리한 비율 (FPP : False-positive Percentage)-일반적으로 오탐지율이라고 칭한다.
- 스팸메일인데 일반메일로 처리한 비율 (FNP : False-negative Percentage)
- 전체 스팸메일 중에 스팸메일로 처리한 비율 (TPP : True-positive Percentage)
- 전체 일반메일 중에 일반메일로 처리한 비율 (TNP : True-negative Percentage)

시험결과는 (그림 1)과 같으며, 이 시험의 목적은 일반메일인데 스팸메일로 처리한 비율(FPP) 및 스팸메일인데 일반메일로 처리한 비율(FNP)의 낮추는 것이다.

(2) 사용의 편의성에 관한 시험

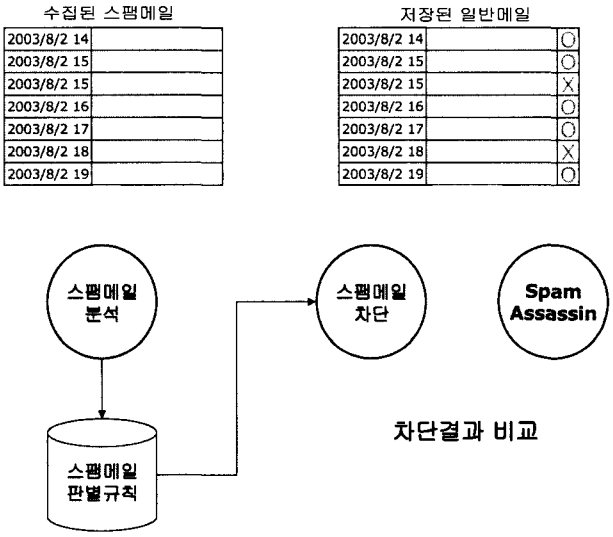
사용의 편의성에 관한 시험은 실질적으로 사용자가 스팸메일 방지 시스템을 사용하려고 할 때 얼마나 많이 기능이 있으며, 얼마나 편하게 사용할 수 있느냐에 관한 시험으로 다음과 같은 항목을 시험하며, (그림 2)는 PC Magazine에서 수행한 수행 결과이다.

- 관리의 편의성 (Ease of Administration)
- 관리 기능의 다양성 (Power of Administration)
- 인터페이스 (Interface)
- 스팸방지 방법 (Spam defense mechanism)
- 스팸메일 관리 (Spam management)
- 보고서 작성 (Reporting)
- 정확성 (Accuracy)



(그림 2) 스팸메일 방지 시스템의 편의성 시험

4.2 시험환경 구축



(그림 3) 시험환경 구축

제안한 스팸메일 차단방법의 효율성을 검증하기 위해 (그림 3)과 같은 시험환경을 구축하였으며, 시간을 기준으로 수집된 스팸메일과 저장된 일반메일을 이용하여 제안한

스팸메일 차단 방법과 SpamAssassin의 스팸메일 차단방법의 효율성을 비교하였다.

각각의 구성요소에 대한 설명은 다음과 같다.

■ 수집된 스팸메일

가상의 이메일 주소로 전송된 모든 메일은 스팸메일이며, 이를 전송받은 시간에 따라 데이터베이스에 저장하였다. 저장된 스팸메일은 어떠한 분석이나 가공도 하지 않았으며, 전송된 상태로 저장된다.

■ 저장된 일반메일

10명의 사용자에게 전송되는 메일을 전송된 시간별로 저장하며, 전송 받은 원본 그대로를 저장한다. 저장된 메일은 사용자가 판별하여 각각의 메일이 스팸메일인지 스팸메일이 아닌지에 관한 정보를 가지고 있으며, 스팸메일 차단시에 이 자료를 이용하여 에러율을 계산한다.

■ 스팸메일 분석

시뮬레이션 시간에 따라 주어진 스팸메일을 분석하여 스팸메일 판별규칙을 생성하고 이를 스팸메일 판별규칙 데이터베이스에 저장한다.

■ 스팸메일 판별규칙

스팸메일 분석 결과로 나온 스팸메일 판별 규칙이며, 시뮬레이션 시간에 따라 계속 변한다.

■ 스팸메일 차단

스팸메일 판별규칙을 이용하여 시뮬레이션 시간에 주어진 일반메일을 검사하여 스팸메일을 차단한다. 스팸메일 차단 결과 및 검사를 수행하는데 소요된 시간을 기록한다.

■ SpamAssassin

SpamAssassin의 기본적인 설정을 이용하여 스팸메일 차단율을 검사한다.

(1) 시험 결과 비교 항목

스팸메일 검사 후에 각각의 검사 결과와 SpamAssassin의 수행 결과와 비교할 항목은 다음과 같다.

■ 스팸메일 차단율

스팸메일 차단 검사에 사용된 일반메일은 미리 스팸메일인지 일반메일인지가 표시되어 있으며, 이를 이용하여 스팸메일 차단 후에 스팸메일로 제대로 판단했는지에 관한 정보를 기록한다.

■ 스팸메일 오탐지율(FPP)

일반메일을 스팸메일로 판단하는 확률을 비교한다. 스팸메일 차단에서 스팸메일로 많이 판단하면 좋은 방법으로 생각할 수 있으나, 일반 메일을 스팸메일로 오판하는 결과도 중요한다. 따라서 일반메일을 스팸메일로 판단하는 확률을 비교한다.

■ 일반메일 오탐지율(FNP)

스팸메일을 일반메일로 판단하는 확률을 비교한다.

■ 스팸메일 검사 시간

스팸메일 검사에 걸리는 시간을 비교한다. 스팸메일 검사 수행시간이 길어지게 되면 사용자에게 그만큼 늦게 메일이 전달될 수 있으므로, 스팸메일 검사 수행시간을 비교한다.

4.3 시험 결과

10명의 사용자에 대해 2주간의 데이터를 이용하여 시험했으며, 1달치의 수집된 스팸메일을 자료로 이용하였다. <표 7>에서 괄호 안의 숫자는 SpamAssasin에 대해 시험한 결과이며, 사람이 판독한 실제일반메일과 실제 스팸메일의 개수를 시험 결과에 표시했다.

〈표 7〉 시험 결과

날짜	전체 메일	실제 일반 메일	일반 메일	실제 스팸 메일	스팸 메일	스팸 오탐지 (FPP)	일반메일 오탐지 (FNP)
4/11	313	138	141(126)	175	172(187)	5(6)	8(10)
4/12	484	223	227(204)	261	257(280)	6(7)	10(13)
4/13	377	171	172(154)	206	205(223)	5(6)	6(7)
4/14	365	199	198(178)	166	167(187)	5(6)	4(5)
4/15	496	232	237(213)	264	259(283)	7(9)	12(15)
4/16	436	206	212(190)	230	223(246)	5(6)	11(14)
4/17	357	154	157(141)	203	200(216)	4(5)	7(9)
4/18	105	54	56(50)	51	49(55)	0(0)	2(2)
4/19	366	185	190(171)	181	176(195)	4(5)	9(11)
4/20	518	235	244(219)	283	274(299)	6(7)	15(19)
4/21	466	221	228(205)	245	238(261)	6(7)	13(16)
4/22	273	145	144(129)	128	129(144)	4(5)	3(3)
4/23	169	90	93(93)	79	76(86)	2(2)	5(6)
합계	4725	2253	2299(2069)	2472	2426(2662)	59(71)	105(130)
비율		49%	49%(44%)	52%	51%(56%)	3%(3%)	4%(5%)

<표 7>의 시험 결과에서 살펴보면 전체 메일의 약 50% 이상이 스팸메일로 판명되었으며, 일반 메일을 스팸메일로 판별하는 오탐지율은 4%대로 비교적 낮은 편이며, SpamAssasin과 같은 경우에는 스팸메일 판별률은 높

게 나왔지만 일반 메일 오탐지율이 높게 나와 정형화된 필터에서 일반 메일을 스팸메일로 판별하는 비율이 높은 것으로 나타났다.

5. 결 론

인터넷을 이용한 이메일은 이제 소수의 통신 수단이 아닌 일반인이 널리 사용하는 기본적인 통신 수단으로 자리 잡고 있으며, 이에 따른 스팸메일의 피해 규모도 날로 커지고 있다. 현재 다양한 방법의 스팸메일 차단 방법이 제안되고 수행되고 있으나 다양해지는 스팸메일에 대응하기에는 역부족이다.

따라서 이 논문에서는 수집, 빈도분석과 차단의 3단계로 구성된 스팸메일 차단 방법을 제시했다. 가상 메일 주소를 만들어서 이를 통해 받는 모든 메일을 스팸메일로 규정하고 이를 빈도 분석을 통해 스팸메일 차단의 자료를 만들어 스팸메일을 차단한다.

이와 같은 방법은 다양한 스팸메일에 대응할 수 있으며, 위의 시험 결과와 마찬가지로 기존의 스팸메일 방지 솔루션보다 스팸메일 탐지율은 떨어지지만 일반메일 오탐지율이 낮아 일반메일을 스팸메일로 차단할 가능성이 적으며, 좀 더 많은 스팸메일 데이터를 수집한다면 스팸메일 탐지율도 기존의 스팸메일 방지 솔루션 보다 높을 것으로 생각한다.

이 논문에서 제시한 스팸메일 판별 방법은 시험의 결과와 같이 다양한 스팸메일에 대응할 수 있으며, 변화하는 스팸메일의 형태에 대해서도 대응할 수 있는 구조를 가지고 있으나 진화하는 스팸메일은 내용 스크램블 및 URL 변조와 같은 방법을 사용하여 스팸메일 차단을 점점 더 어렵게 만들고 있다. 이에 따라 이 논문에서 제안한 분석 방법에 위와 같은 부분에 대한 추가적인 연구가 필요하다고 생각한다.

참 고 문 헌

[1] Paul Hoffman, Dave Crocker, Unsolicited Bulk Email : Mechanisms for Control(IMC, Internet Mail Consortium), 1998. 5. http://www.imc.org/ubesol.html

[2] MAPS(Mail Abuse Prevention System), http://www.mailabuse.com

[3] RFC821, "Simple Mail Transfer Protocol"

[4] procmail, Mail Processing and SmartList mailing list suites, http://www.procmail.org

[5] 마이크로소프트 아웃룩 익스프레스 필터 설정 방법, http://www.spamcop.or.kr/mbSpam/emai_outexpress.jsp

[6] SpamNet, http://www.spamnet.org

[7] SpamAssassin, http://www.spamassassin.org

[8] RFC2045, "Multipurpose Internet Mail Extensions(MIME) Part One : Format of Internet Message Bodies"

[9] ORDB(Open Relay DataBase), http://www.ordb.org

[10] Paul Graham, "A Plan for Spam", http://www.paulgraham.com/spam.html

[11] Email Spider Easy, http://www.emailtool.com/features html

[12] SpamArchive - provides a database of known spam http://www.spamarchive.org

백 기 영

e-mail : cloud@cqcom.com

1996년 충남대학교 컴퓨터과학과(학사)

1998년 충남대학교 대학원 컴퓨터과학과 (석사)

1998년~현재 충남대학교 대학원 컴퓨터과학과 박사과정

2000년~현재 ㈜시큐컴 인터넷보안부 부장

관심분야 : 보안 프로토콜, PKI, 디렉토리 서버

김 승 해

e-mail : shkim@kisti.re.kr

1997년 한남대학교 학사

2003년 전북대학교 석사

2004년~현재 전북대학교 정보보호공학 박사과정

1996년~현재 한국과학기술정보연구원 연구원

관심분야 : 라우팅, 정보보호, 차세대인터넷

최 장 원

e-mail : jwchoi@kisti.re.kr

1996년 홍익대학교 학사

1998년 홍익대학교 석사

2003년~현재 고려대학교 컴퓨터학과 박사과정

1998년~현재 한국과학기술정보연구원 연구원

관심분야 : 분산컴퓨팅, 그리드컴퓨팅, ATM

류 재 철

e-mail : jcryou@home.cnu.ac.kr

1985년 한양대학교 산업공학과(학사)

1988년 Iowa State University 전산학과 (석사)

1990년 Northwestern University 전산학과(박사)

1991년~현재 충남대학교 컴퓨터과학과 부교수

관심분야 : 컴퓨터 및 통신망 보안, 전자상거래, 분산