
고가용성을 고려한 전자메일통제시스템의 우회 모델 및 응용

김 영 수*, 서 정 석**

Indirection Model and Application of Electronic Mail Control System Considering High Availability

Young Soo Kim*, Jung Seok Suh**

요 약

전자상거래를 위한 마케팅 수단으로서 전자메일이 보편적으로 사용되면서 스팸메일이 급격히 증가하고 있다. 이의 억제를 위한 전자메일통제시스템은 기술적이고 경제적 대안으로 필터시스템과 과금시스템을 사용하고 있으나 차단오류와 과금저항으로 인한 전자메일의 수신과 가용성을 제한한다. 이의 해결을 위해서 불법적인 전자메일은 억제하지만 송·수신자에게 유익하고 합법적인 전자메일이 폐기되고 상실되는 것을 방지할 수 있는 전자메일통제시스템의 우회 모델을 제안하고 이를 사용하여 전자메일의 유용성과 가용성을 높여줄 수 있는 웹기반의 전자메일통제시스템을 구현하여 모델의 실용성을 검증하였다.

ABSTRACT

These days, Electronic mail is being used in everyday's life. And on the other hand, we are facing spam mails' problems. Spam mails are widely used by means of marketing in e-Commerce. To block these spam mails, we are using filtering or pricing systems. But these solutions are raising other problems such as impediment in reception or availability caused by false positive or payment resistance. To solve these problems, we propose an Indirect Model on Electronic Mail Control System(IMEMCS) which controls an unsolicited electronic mail and prevents a useful electronic mail from discarding. We design and implement the IMEMCS to enhance the usefulness and the availability. Being tested the IMEMCS to verify the usability and the efficiency, it gave us a very successful result.

키워드

스팸메일, 전자메일통제시스템, 차단시스템, 과금시스템, 우회모델

1. 서론

오늘날 대부분의 기업에서는 적어도 하나 이상

의 전자메일시스템을 사용하고 있다. 이들 전자메일시스템은 신속하고 경제적이며 효과적인 방식으로 문서의 전달과 정보의 교환 그리고 의사소통을

*국민대학교 정보관리학과

접수일자 2005. 3. 10

**나사렛대학교 인터넷정보학과

위한 서비스를 제공하는 반면 이의 남용에 따른 스팸메일로 인해서 수신자의 사생활 침해와 사회적 비용의 증가 그리고 업무생산성의 저하와 같은 문제를 야기하고 있다[1]. 따라서 스팸메일로 인한 피해의 확산과 악용을 방지하기 위해서 전자메일통제시스템은 핵심요소로 필터시스템을 사용해서 불법적인 스팸메일을 차단하고 있다. 그러나 금칙어나 전자메일주소를 활용해 스팸메일을 막아주는 필터시스템은 합법적인 전자메일을 스팸메일로 분류하는 판정의 오류가 빈번하다[2]. 이는 전자메일의 배달과 수신을 제한하고 전자메일의 유용성을 감소시킨다. 따라서 스팸메일을 억제하면서 유용성을 증가시킬 수 있는 전자메일통제시스템으로 필터시스템을 우회하는 기능을 갖는 과금시스템이 필요하다. 과금시스템은 전자메일의 남용을 억제하고 필터로 인한 수신 제한을 극복함으로써 스팸메일을 차단하고 마케팅 기회를 확대한다. 그러나 과금시스템은 전자메일의 전송을 위해서 전자우표나 부하과중과 같은 형태의 서비스 사용료를 지불해야 하기 때문에 사용자가 전자메일의 사용을 외면함으로써 전자메일의 가용성을 저해한다[3]. 따라서 전자메일의 송·수신자가 필터로 인한 수신 장애를 극복하고 과금으로 인한 가용성의 저해를 방지할 수 있는 전자메일통제시스템으로 필터시스템과 과금시스템을 우회하는 기능을 제공할 필요가 있다. 이를 위해서 불법적인 스팸메일은 억제하지만 송·수신자에게 유익한 합법적인 전자메일이 폐기되고 상실되는 것을 방지하면서 전자메일의 유용성과 가용성을 증가시킬 수 있는 분리하고 통합되는 구조를 갖는 전자메일통제시스템의 우회모델을 제안한다. 전자메일통제시스템의 우회모델은 그림 1과 같이 전자메일시스템의 차단필터모델과 접근통제시스템의 우회모델을 분석해서 도출하고 이의 실용성을 검증하기 위해서 응용시스템을 개발한다.

본 논문은 다음과 같이 구성된다. 2절에서는 전자메일통제시스템의 차단필터모델과 접근통제시스템의 우회모델을 분석하고 3절에서는 전자메일통제시스템의 우회 및 응용모델을 제안한다. 4절에서는 모델의 실용성을 검증하기 위하여 전자메일통제시스템의 우회모델을 구현한다. 5절에서는 결론과 시사점을 기술한다.

II. 전자메일통제시스템의 연구 모델

12.1 전자메일시스템의 차단필터 모델

인터넷 기술의 발달과 더불어 사용자들은 전자메일을 정보교환과 그룹 메일링서비스 그리고 마케팅의 수단으로 활용하고 있다. 전자메일은 저렴하고 효과가 크다는 점에서 매우 유용한 마케팅 수단이 될 수 있지만 수신자가 원하지 않는데도 계속 뿌려지는 전자메일은 더 이상 마케팅 수단으로서의 가치가 없는 사회적 공해에 불과하다[4].

인터넷을 통하여 다수의 수신자에게 전송되는 원하지 않는 상업성 전자메일인 스팸메일은 수신자의 사생활 침해와 사회적 비용의 증가 그리고 업무의 생산성 저하와 같은 많은 사회적 문제를 야기하고 있다. 이의 해결을 위해서 전자메일시스템은 스팸메일을 차단하는 기능을 제공한다. 전자메일시스템의 송·수신과 차단필터 과정은 그림 2와 같다. 전자메일시스템은 전송을 위한 통신 표준안으로 ITU (International Telecommunications-Union)의 X.400을 수용하고 사용자 에이전트(MUA: Mail User Agent)와 메일배달 에이전트(MTA: Mail Transfer Agent) 그리고 메일저장함(MS: Mail Store)을 구성요소로 한다[5].

전자메일의 송·수신을 위해서 송신자는 전자메일서버시스템에 접속하여 전자메일클라이언트인 MUA로 메시지를 작성한 후에 SMTP(Simple Mail Transfer Protocol)를 이용해서 전자메일 메시지를 제출한다. 송신측 MTA는 SMTP를 이용하여 수신측 전자메일서버시스템의 MTA로 전달한다. 수신측 MTA는 전자메일의 도착자가 자신이라면 필터링 과정을 수행한 후에 수신인의 메일함인 MS에 저장한다. 수신측 전자메일서버시스템은 수신자가 로그인 했을 때 전자메일이 도착했다는 메시지를 통보하고 수신자가 MUA를 실행하여 전자메일의 개봉을 요청하면 메일함에 있는 전자메일을 POP(Post Office Protocol)을 사용해서 배달한다.

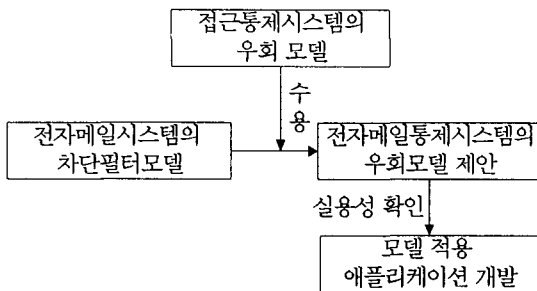


그림 1. 연구모델

Fig. 1 The model of research approach

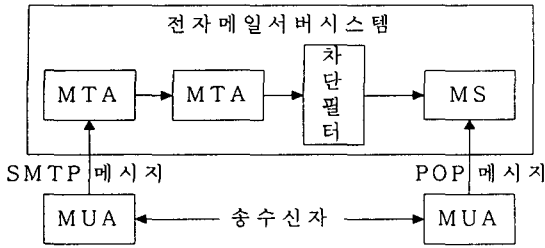


그림 2. 전자메일시스템의 차단필터 모델
 Fig. 2 The blockage filter model of electronic mail system

전자메일시스템의 차단필터 모델은 송·수신자에게 유익하고 합법적인 정상메일을 스팸메일로 분류하여 폐기하는 False Positive 문제를 야기한다 [6].

따라서 스팸메일의 억제력을 강화하고 전자메일의 유용성을 확보할 수 있는 해결책으로 필터시스템을 우회하는 구조를 갖는 전자메일통제시스템이 필요하다.

2.2 접근통제시스템의 우회 모델

접근통제시스템의 목적은 컴퓨팅자원과 통신자원 그리고 정보자원에 대하여 허가되지 않는 접근을 방어하는 것이다[7]. 이를 위하여 접근통제시스템은 사용자의 요청을 수신하고 사용자를 인증하고 권한부여를 수행한다[8].

접근통제시스템의 우회모델은 그림 3과 같다. 접근통제시스템은 수신한 인증데이터를 사용해서 사용자를 인증하고 권한정보를 획득한다[9]. 접근통제시스템은 인증에 기반을 두고 접근통제를 수행하는 반면 우회시스템은 기밀데이터를 사용하여 정상적인 접근통제절차를 우회한다. 접근통제시스템은 사용자가 허가 받지 않는 자원을 사용하려는 시도를 차단하는 반면 우회시스템은 정상적인 보호 수단을 우회할 수 있는 숨겨진 메커니즘으로서 접근 인증의 정상적인 방법을 사용하지 않는 접근을 허용한다[10].

우회시스템은 불법적인 접근을 위한 통로로 사용하는 대신 보안시스템을 우회해서 신속하고 간편한 접근을 위한 관문으로 활용된다. 제품공급사의 유지보수 개발자나 필드서비스 기술자는 시스템에 신속하고 제한없이 접근하기 위한 통로로 우회시스템을 이용한다.

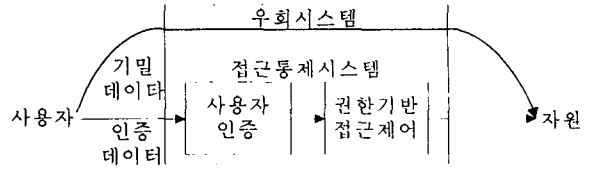


그림 3. 접근통제시스템의 우회 모델
 Fig. 3 The indirection model of access control system

필터시스템은 합법적인 정상메일을 불법적인 스팸메일로 판단하는 False Positive를 야기함으로써 유용하고 합법적인 전자메일의 수신을 제한한다. 이는 인터넷 사용자가 유용한 전자메일을 수신하는 것을 제한하고 송신주체인 개인사업자나 기업이 마케팅을 위한 전자메일의 사용을 제한한다. 따라서 전자메일에 대한 유용성의 저하와 가용성의 제한을 해결하기 위해서 그림 6과 같이 필터시스템을 우회하고 전자메일통제시스템에 통합되는 과금시스템을 설계하였다. 송신자는 과금시스템에서 획득한 전자우표나 퍼즐의 해와 같은 과금토큰을 부착한 전자메일을 전송한다. 과금시스템은 과금토큰이 부착되지 않은 전자메일은 필터시스템으로 포워딩하고 과금토큰을 부착한 전자메일의 경우에는 과금토큰의 유효성을 확인한 후에 메일박스에 전자메일을 전달하는 반면 그렇지 않은 경우에는 송신자에게 이러한 사실을 통보하도록 과금시스템에게 피드백한다.

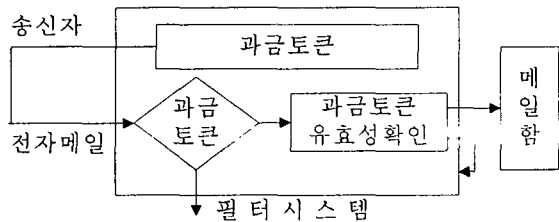


그림 6. 과금시스템의 응용 모델
 Fig. 6 The application model of pricing system

스팸메일의 피해를 방지하기 위해서 전자메일 주소를 은폐시키려는 인터넷 사용자와는 달리 기업과 교육기관 그리고 정부기관은 고객과 학생 그리고 국민의 의견을 청취하기 위해서 전자메일의 주소를 적극적으로 공개한다[13]. 이러한 목적의 전자메일은 무료로 이용할 수 있도록 과금시스

템을 우회할 수 있는 통로를 제공해야한다. 이를 위한 퍼미션시스템의 응용 모델은 그림 7과 같다. 송신자는 전자메일을 전송하기 이전에 퍼미션시스템에게 전자메일주소를 퍼미션데이터로서 등록한 후 전자메일을 전송한다. 퍼미션시스템은 전자메일을 전송한 송신자의 전자메일주소가 퍼미션데이터로서 존재하는 경우에는 과금시스템을 우회해서 메일함에 전달하는 반면 그렇지 않은 전자메일주소의 경우에는 과금시스템을 경유하도록 포워딩한다.

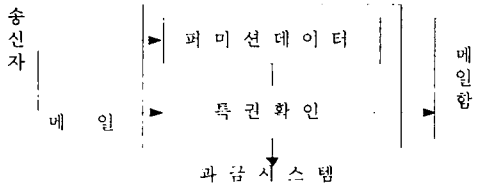


그림 7. 퍼미션시스템의 응용모델
Fig. 7 The application model of permission model

전자메일통제시스템을 위한 데이터 구조는 그림 8과 같이 전자메일주소를 사용한다. 전자메일의 송신자는 과금시스템과 퍼미션시스템을 위한 전자메일주소를 등록해서 구성하는 반면 필터시스템을 위한 데이터 구조는 수신자가 전자우편주소를 등록하여 구성한다

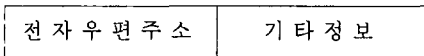


그림 8. 전자메일통제시스템의 데이터 구조
Fig. 8 The data structure of electronic mail control system

IV. 응용 시스템의 설계 및 모델의 검증

4.1 전자메일통제시스템의 응용구조

전자메일통제시스템의 우회모델은 웹기반 전자메일시스템을 사용하여 구현한다. 웹기반 전자메일시스템의 기본구조는 그림 9와 같다[14]. 대부분의 송신자는 전자메일의 전송방법으로 웹기반 인터페이스를 사용한다. 웹기반 전자메일의 사용자는 HTTP프로토콜을 사용해서 연결된 WebMail 서버시스템을 통해서 SMTP서버시스템과 간접적으로 연결해서 전자메일을 송·수신하는 반면 송신자시스템에서 실행되는 아웃룩 익스프레스와 같은 전자메일 클라이언트는 SMTP프로토콜을 사용해

서 SMTP서버시스템과 직접적으로 접속해서 전자메일을 송·수신한다.

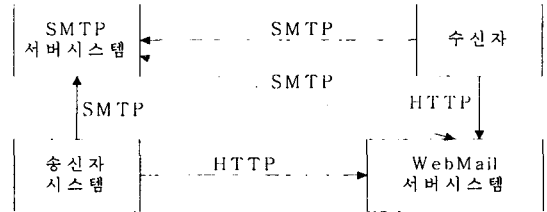


그림 9. 웹기반 전자메일시스템의 송·수신구조
Fig. 9 The transmission architecture of web based electronic mail system

오늘날 구축되어 운영하는 대부분의 전자메일시스템은 인터넷 사용자가 사용료를 지불하지 않고 언제든지 전자메일을 보낼 수 있는 특징을 가지고 있다. 이는 사용자가 전자메일을 보낼때 인증과 같은 절차가 필요 없고 전자우표나 부하가중과 같은 형태의 서비스 사용료를 지불하지 않기 때문에 전자메일의 남용을 가져온다. 이러한 무분별하고 무차별적으로 보내지는 스팸메일을 차단하기 위해서 전자메일시스템은 MTA와 MS사이에서 스팸메일을 차단하는 필터를 내장하고 있다[15]. 그러나 차단 필터는 정상메일을 스팸메일로서 분류해 폐기하거나 정상적인 메일 업무를 불가능하게 만든다[16]. 따라서 불법적인 전자메일을 차단하지만 금지하지 않은 방법이 필요하다. 이를 위해서 그림 10과 같이 WebMail서버시스템에 필터시스템을 우회하는 과금시스템과 전자메일을 전송하기 위한 비용을 지불하지 않으면서 차단필터에 의해서 수신 제한을 받지 않는 퍼미션시스템을 구현하고 SMTP서버시스템의 필터시스템과 통합하는 구조로 설계하였다. 이는 전자메일통제시스템의 우회모델을 구현하기 위해서 기존의 전자메일시스템을 변경할 필요가 없고 전자메일의 가용성과 유용성을 증가시킨다.

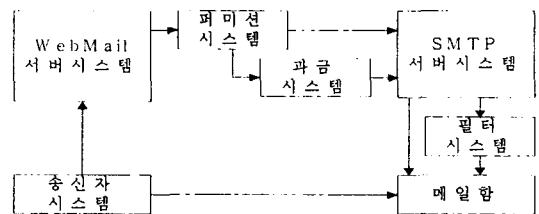


그림 10. 전자메일통제시스템과 응용시스템의 통합구조
Fig. 10 The integration architecture of electronic mail control system and application system

4.2 모델의 검증

전자메일통제시스템의 우회모델에 대한 실용성을 확인하기 위하여 그림 11과 같이 SMTP 프로토콜을 사용하는 X.400 기반 전자메일시스템의 필터시스템을 사용하고 HTTP 프로토콜을 사용하는 웹기반의 전자메일시스템에서 과금시스템과 퍼미션시스템을 구현하고 이의 실험데이터를 비교분석하였다.

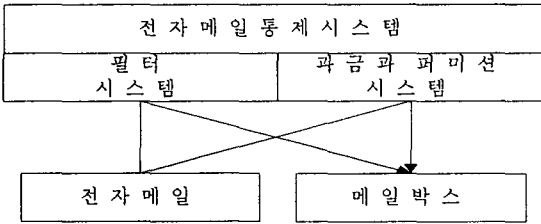


그림 11. 실용성 평가 모델
Fig. 11 The evaluation model of practicality

전자메일에 대한 가용성의 크기를 비교하기 위해서 실용성 평가모델에 따른 접근통제시스템의 기술 유형을 표 1과 같이 분류하고 평가번호를 부여해서 반복실험을 수행하였다.

표 1. 전자메일통제시스템의 평가기술
Table. 1 A evaluation technology of electronic mail control system

평가번호	전자메일통제시스템의 기술유형
1	퍼미션시스템
2	과금시스템
3	차단필터시스템

전자메일통제시스템의 평가기술에 대한 비교평가를 위해서 전자메일통제시스템을 구성하는 서브시스템의 부분집합을 <표 2>와 같이 전자메일통제시스템의 기술유형에 부여된 평가번호의 조합을 통해서 구성하고 반복실험을 통해서 비교 평가하였다. 전자메일통제시스템의 하위시스템인 부분집합의 번호가 5와 6 그리고 7은 각각 퍼미션시스템과 과금시스템 그리고 필터시스템과 같은 단일의 서브시스템을 사용해서 구현한 후 실험하는 경우에 해당된다. 이러한 부분집합의 실험이 가지는 의미는 전자메일통제시스템의 단일 서브시스템들에 대한 수신제한의 정도를 비교하는 대신 전체적인 면에 대한 배달의 신뢰성을 비교하고 실험에 대한 결과의 오류를 감소하기 위해서이다.

표 2. 전자메일통제시스템의 구성요소
Table. 2 A component of electronic mail control system

부분집합번호	평가번호
1	1 2 3
2	1 2
3	1 3
4	2 3
5	1
6	2
7	3

전자메일의 도착유무를 비교하기 위해서 실험의 대상이 되는 전자메일에 퍼미션토큰과 과금토큰을 부착하고 블랙리스트에 포함되지 않는 전자메일주소를 사용해서 전자메일통제시스템의 우회시스템에 적용시킨 후에 도착여부를 반복적으로 측정하여 실험하였다. 전자메일의 도착함수는 퍼미션토큰과 과금토큰 그리고 블랙리스트에 포함되지 않는 전자메일주소를 독립변수로 두고 실험하였다. <표 3>에서 보는 것과 같이 좌측상단의 영역에서는 전자메일이 대부분 도착하는 것을 확인할 수 있다. 이는 도착함수의 파라미터로서 토큰을 부착하고 전자메일통제시스템의 우회기술을 다수 조합해서 구성하는 경우로서 대부분의 전자메일이 도착하는 것을 보증한다는 것을 확인할 수 있다. 이는 전자메일의 가용성과 유용성을 확보하기 위해서는 전자메일통제시스템의 우회모델을 통합해서 사용할 필요가 있음을 확인할 수 있다.

표 3. 전자메일의 배달(도착:O, 차단:X, 부착:T, 미부착:F)

Table. 3 A delivery of electronic mail

부분집합번호		1	2	3	4	5	6	7
도착함수								
F (퍼미션토큰, 과금토큰, 화 이트리스트)	TTF	O	O	O	O	O	O	O
	TFF	O	O	O	O	O	O	X
	TFT	O	O	O	O	O	X	O
	FTT	O	O	O	O	X	O	O
	FFT	O	O	O	O	X	X	O
	FTF	O	O	X	O	X	O	X
	TFF	O	X	O	X	O	X	X
FFF	X	X	X	X	X	X	X	

V. 결론

스팸메일은 어제 오늘의 문제는 아니지만 갈수록 그 피해가 이만저만 심각한 게 아니다. 그러나 스팸을 차단하기 위해서 전자메일을 못하게 해서 는 안된다. 불법적인 전자메일은 규제하되 합법적인 마케팅을 위한 전자메일의 송·수신은 보장해야 한다. 이를 위해서 송신자에게 전자메일의 사용에 대한 비용을 지불하게 하면서 필터시스템을 우회할 수 있는 과금시스템을 구축해서 운영할 필요가 있고 공개적인 전자메일의 송·수신 통로로서 과금시스템을 우회하는 퍼미션시스템을 전자메일통제시스템의 통합된 부분으로 사용할 필요가 있다. 과금시스템은 전자메일을 전송하기 위해서 송신자에게 시스템의 부하를 감내하거나 신뢰성을 입증하기 위하여 과금토권을 부착하게 하므로 경제이론에 따르면 스팸메일은 감소한다. 그러나 과금시스템이 스팸메일의 억제 기능을 발휘하면서 전자메일의 유용성을 보장하는 역할을 수행하지만 송신자는 업무의 협조처리와 의견개진을 위한 전자메일에 과금에 따른 서비스 사용료를 지불하는 것을 원치 않는다. 따라서 필터시스템과 과금시스템으로 인한 전자메일의 수신을 제한받는 전자메일의 송신자로부터 거센 불만이 제기될 수 있다. 따라서 전자메일통제시스템은 필터시스템과 과금시스템을 우회할 수 있는 퍼미션시스템을 서비스시스템으로 사용할 필요가 있다. 이를 위한 전자메일통제시스템의 우회모델로 차단필터시스템과 과금시스템 그리고 퍼미션시스템을 분리하고 통합해서 사용될 수 있도록 제안하고 구현하였다. 전자메일통제시스템의 우회 모델은 송신자와 수신자 그리고 전자메일서비스 제공업자에게 잇점을 제공한다. 송신자는 허가되고 보증된 배달을 통해서 수신자의 제한을 극복하고 전자메일의 가용성을 확보함으로써 수신자의 신뢰를 경험하고 높은 개봉 비율과 ROI(Return Of Investment)를 달성한다. 수신자는 주문거래와 뉴스정보 그리고 옵트인(opt-in) 마케팅 메시지가 필터시스템과 과금시스템에 의해서 더 이상 상실되지 않는다. 또한 전자메일서비스 제공업자는 현행 전자메일시스템을 확장해서 전자메일통제시스템을 구축할 수 있게 되어 구축비용을 감소시킬 수 있고 수신과 배달의 제한을 극복함으로써 송·수신자를 만족시킬 수 있다. 향후 전자메일통제시스템과 통합해서 사용할 수 있는 전자메일의 보호를 위한 암호화 프로토콜에 대한 연구가 필요하다.

참고문헌

- [1] Abadi, M. et al., "Certified E-mail with a light on Line Trusted Third Party: Design and Implementation," n Proceedings of the Eleventh International World Wide Web Conference pp.387-395, May, 2002.
- [2] Pollock, S. "A Rule-Based Message Filtering System," ACM Transactions on Office Information Systems, pp.232-254, 1998.
- [3] Cynthia, D. and N, Moni "Pricing via processing or combatting junk mail," In Processings of Crypto, pp 139-147, 1992.
- [4] Mackay, E. "Diversity inthe Use of Electronic Mail," ACM Transactions on Office Information Systems, pp.380-397, 1998.
- [5] Hughes, L. "Internet E-mail; Protocols, Standards, and Implementation," Artech house, Norwood, MA, 1998.
- [6] David, A. M. Daniel "Controlling spam through lightweight currency," In Proceedings of the Haeaii International Conference on Computer Science, Jan. 2004.
- [7] 김영수, 메시지보안시스템의 인증 프로토콜 설계 및 검증, 박사학위논문, 국민대학교 대학원, 2003.
- [8] Jajodia, S., et al., "Flexible Support for Multiple Access Policies," ACM Trans. on Database Systems pp. 214-260, Jun.. 2001.
- [9] Sandhu, R., et al., "Role Based Access Control Models," IEEE Computer, 29(2), 1996.
- [10] Yao. C., "Theory and applications of trapdoor functions," In Proceedings of the Twenty-Third Annual IEEE Symposium on Foundations of Computer Science, pp. 80-91, 1982.
- [11] Abadi, M. et al., "Certified E-mail with a light on Line Trusted Third Party: Design and Implementation," Proceedings of the Eleventh International World Wide Web Conference pp.387-395, May, 2002

- [12] Telang, R. "Information Overload and Pricing of Communication Services," Carnegie Mellon University Working Paper, 2002.
- [13] Fahlman, S., "A way to control unwanted E-mail and telephone calls," IBM Systems Journal 41, pp.759-766, June, 2002.
- [14] Hoffman, P. "SMTP service extension for secure SMTP over Transport Layer Security," RFC3207 Feb., 2002.
- [15] Jonscher, D., R, Dittrich, "A Configurable Access Control System Interoperable Environment," Database Security IX, Chapman and Hall. 1996.
- [16] Joshi, J.B.D. et al., "Security Models for Web-based Applications," Communications of the ACM, 2. pp. 44-52, 2001.

저자소개

김 영 수(Young Soo Kim)



1989년 2월:전북대학교졸업(경영학사)
1992년 2월:경희대학교대학원 졸업
(경영학 석사)
2003년 8월:국민대학교 대학원 졸업
(정보관리학박사)

※관심분야: 전자상거래, 인터넷응용, 분산정보 시스템, 정보보안

서 정 석(Jung Seok Suh)



1987년 9월:Drexel University,
MBA(MIS):경영정보관 대학원졸업
1990년1월:Boston University Com-
puter Science:전산학 대학원졸업

2000년 8월:국민대학교 박사학위 취득
현재 나사렛대학교인터넷정보학과교수