通信情報保護學會誌
第2卷, 第1號, 1992. 3

보안기능이 부가된 메세지 처리 시스템 고찰

A Study of Secure Message Handling System

김 화 수*

1. 서 론

오늘날 컴퓨터 사용의 급격한 증가와 더불어 컴퓨터를 이용한 정보교환이 절실히 요구되고 있으며, 이를 충족시킬 수 있는 컴퓨터 통신 기술은 사회 각 분야에서 필수적인 도구가 되고 있다.

정보통신 분야에 널리 보급되고 있으며 가장 관심이 많은 분야중의 하나가 메세지 처리 시스템(MHS : Message Handling System)이다. 이 MHS는 store-and-forward 방식의 전자 메일 서비스를 제공해 주는 시스템으로서 CCITT에서는 X.400 계열의 표준안을 권고하고 있다. 이는 기존 전자메일과는 달리 전화망, 데이타망을 비롯한 여러 네트워크를 통한 문자, 도형, 화성, 음성 등의 다중매체(Multi-Media) 처리능력을 가진다.

컴퓨터시스템 혹은 컴퓨터망에서의 데이타 처리 과정에는 정보에 대한 불법적인 엑세스(access), 도청(eavesdropping), 수정(modifying), 삭제(deleting), 재전송(replying), 삽입(inserting), 순서 변경, 미확인 발신자 및 수신자 등의 위협을 내포하게 된다. 특히 비밀 내용을 포함하고 있는 정보가 유출된다면 개인이나 단체, 또는 국가에 커다란 불이익을 미칠 수 있다. 따라서 컴퓨터 시스템이나 통신 시스템을 통한 정보의 조작에는 적절한 보호 대책이 필수적이므로 본 고의 제 2 장에서는 메세지 처리 시스템에 관한 일반적인 고찰을 하였으며, 제 3 장에서는 메세지 처리 시스템의 주요 구성품인 사용자 처리기(UA : User Agent), 메세지 전송 처리기(MTA : Message Transfer Agent), 메세지 저장체(MS : Message Store), 접근 유니트(AU : Access Unit) 중에서 사용자 처리기 및 메세지 전송 처리기에 대한 구조 및 안전 메세지 처리 방식을 살펴 보았다. 또한 기존의 메세지 처리 시스템에서 사용중인 인증방식을 살펴보고 추후 개선 연구되어야 할 방향을 제시하고자 한다.

2. 메세지 처리 시스템의 개념 및 구조

2. 1 메세지 처리 시스템의 개념 및 모형화

80년대 초에 이기종 컴퓨터 사이에서의 메세지 교환을 위한 표준화 작업의 결과로서 '84년 10월에 CCITT에서 X.400이라는 메세지 표준 프로토콜을 발표하게 되었고, '88년에 다시 개정되어 여러가지 기능이 추가되었다. 메세지 처리 시스템은 OSI 모델에 적합한 최초의 표준화 응용의 하나로서 채

* 국방대학원 전자계산학과

택되어 응용 계층에서 조작되도록 만들어졌는데, 사용자간에 투명하게 자료 전송을 할 수 있도록 함으로서 폭넓은 정보 전송의 매개체가 되었다. 그러나 아직 개발 단계를 벗어나지 못해 정의되지 않은 영역도 많이 있다. 메세지 처리 시스템이 CCITT의 X.400 형태로 개발되고 있는 동안에 OSI에서도 이와 유사한 프로토콜인 MOTIS(Message Oriented Text Interchange System)를 개발해왔다. 개발 과정에서 OSI와 CCITT가 서로 협력해서 발전해 왔기 때문에 전반적인 기능이 거의 비슷하므로, 본 고에서는 CCITT에서 권고한 X.400을 중심으로 살펴보기로 한다.

메세지처리 시스템에 의해 수행되는 기본적인 동작은 통신 시스템을 통한 메세지 전달이다. 메세지의 전형적인 형태는 인벨로프(envelope)와 메세지의 내용으로 구성된다. 인벨로프 부분은 메세지의 전송에 영향을 주는 필수적인 지시 사항뿐만 아니라 발신자와 수신자의 주소를 포함하게 된다. 특히 이러한 지시 사항은 메세지 전송시스템의 보조 서비스를 얻기 위해서는 필수적이다. 메세지의 내용 부분은 내용 변환의 보조 서비스가 요청되는 경우를 제외하고는 메세지 전송시스템에 의해 침해되지 않는다. 메세지 처리 시스템의 가장 간략한 모델은 다음 그림 2.1과 같이 나타낼 수 있다.

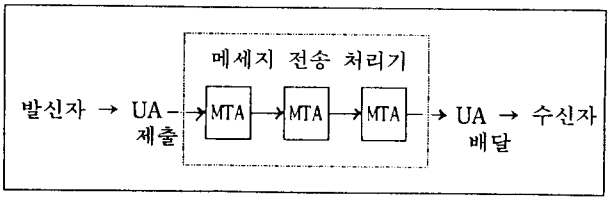

그림 2.1 단순한 메세지 전달 모델

이 모델의 기본적인 요소로서 임의의 사용자로부터 다른 사용자에게 메세지를 보내는 발신자(Originator)가 있고, 메세지를 받으려는 수신자(Recipient)가 있다. 발신자는 메세지를 작성하기 위해 사용자 처리기를 제출한다. 사용자 처리기는 메세지 전송 처리기로부터 수신자에게 보낼 메세지를 배달 받게 된다. 이와 같이 일련의 과정을 거치면서 메세지가 전송된다.

2. 2 메세지 전송 시스템

메세지 전송 시스템은 사용자 처리기, 메세지 전송 처리기, 메세지 저장체, 접근 유니트들의 모임으로 구성되어 있으며, 국제적인 메세지 전송 서비스를 제공하는 분산된 형태의 시스템이다.

2. 2. 1 사용자 처리기

사용자 처리기는 사용자에게 메세지 전송 처리기에 대한 접근을 제어하는 것으로서, 기능은 메세지 전송 처리기에 대해 메세지를 작성하여 제출하고, 메세지 전송 처리기로부터 전송된 메세지를 배달받아 메세지를 수신자에게 전달한다. 메세지 제출을 준비하는 동안 사용자는 메세지를 편집기, 철자 검사기, 문서 작성기로서 다양하게 사용할 수 있다. 또한 사용자는 사용자 처리기를 통해 이전에 받았던 메세지를 검색하고, 메세지를 다른 사용자에게 전송한다. 사용자 처리기와 메세지 전송 처리기간의 접속 방법은 메세지들의 물리적 환경에 따라 다양해질 수 있다. 한편, 사용자 처리기가 제공하는 서비스들에는 전송 메세지의 주소를 설정하고, 경로 배정, 분류에 따른 정보의 분배, 날

짜와 시간의 표시 등을 제공하게 된다.

2. 2. 2 메세지 전송 처리기

메세지 전송 처리기의 일차적인 기능은 사용자 처리기나 메세지 저장체로부터 제출 받은 메세지를 보관하였다가 목적하는 수신자에게 배달하는 것으로서, 세가지 형태의 서비스(제출 서비스, 관리 서비스, 전달 서비스)를 사용자 처리기나 또는 유니트에게 제공하게 된다.

2. 2. 3 메세지 저장체

메세지 저장체에는 사용자 처리기와 메세지 전송 시스템간의 중간 역할을 수행하는 것으로서 메세지 저장체 서비스는 사용자 처리기에게 대리 메세지 전송 시스템 서비스 제공자인 메세지 전송 처리기의 역할을 대신하여 제출, 검색, 관리 포트로서 메세지 전송 시스템의 배달, 제출, 관리 포트 서비스를 제공받게 된다.

메세지 저장체의 기본적인 기능은 단 하나의 메세지 처리 시스템 사용자를 대신해서 배달된 메세지를 받아 사용자 처리기가 계속 검색할 수 있도록 보관하는데 있으며, 실제는 메세지 전송 처리기에 통과시키는 식으로 사용자 처리기에 간접 메세지 제출과 메세지 관리 서비스를 제공하게 된다. 이를 위해서는 메세지 저장체 내에 메세지 전달 기능이 있어야 한다.

2. 2. 4 접근 유니트

접근 유니트는 메세지 처리 시스템과 외부 통신 서비스간의 게이트 웨이를 제공한다. 정의된 접근 유니트의 세가지 형태는 물리적 배달 시스템에 대한 메세지 처리 시스템 접근과 텔렉스 시스템, 텔리텍스 시스템에 대한 메세지 처리 시스템의 접근을 허용한다. 즉, 다른 망(非컴퓨터 통신)에 연결되어 메세지 처리 시스템을 이용하려는 사용자를 도와주는 역할을 한다.

3. 보안기능이 부가된 메세지 처리 시스템 고찰

3. 1 안전한 사용자 처리기 고찰

메세지처리 시스템의 보안을 위하여 제안된 사용자 처리기에 대한 구성은 다음 그림 3.1과 같이 크게 세 부분으로 나누어 볼 수 있는데, (i) 메세지 부분의 관리를 담당하는 부분으로서 전체적인 메세지처리 시스템을 관리하기 위한 관리 모듈과 시스템에 접근하려는 모든 사람들의 권한을 검사하는 권한검사 모듈로 생각할 수 있다. (ii) 실제 사용자와 인터페이스 하는 부분으로서 패스워드를 사용함으로써 접근 가능한지를 조사하는 접근 검사 모듈과 실제적인 작업을 수행하기 전에 그일에 대한 권한을 검사하여 그 일을 선택하는 선택 모듈이 있다. (iii) 실제적인 인증을 담당하는 부분으로서 적법한 권한이 주어진 사용자가 비밀 메세지를 전송, 검색, 수정, 출력 혹은 암호화하여 저장하는 기능을 담당한다. 이것은 또한 일시적인 비밀메세지를 저장하는 저장장치와 키 관리 기능으로 생각할 수 있다. 그리고, 메세지 처리기외의 인터페이스를 유지함으로써 전송모듈과 편집 모듈이 필요하게 될 것이다.

인증 방식은 크게 두가지 나누어 볼 수 있는데 (i) 평문의 메세지에 대한 경우 송신자와 수신자가 공통적으로 알고 있는 비밀 패스워드를 이용하는 방법이 있고, (ii) 송신자와 수신자의 비밀키를 관리하는 키 관리 시스템에서 제공하는 키를 이용해서 암호화된 문장을 평문으로 바꿀 수 있다면 적법하다는 것이 증명되므로 문제가 해결될 수 있다.

3. 2 안전한 메세지 전송 처리기 고찰

2장에서 이미 설명한 바와 같이 메세지 전송 처리기의 기능은 사용자 처리기 또는 다른 메세지 처리기로 부터 전송된 메세지를 수신하여 자신에 속한 사용자 처리기 또는 우선순위에 따라 다른

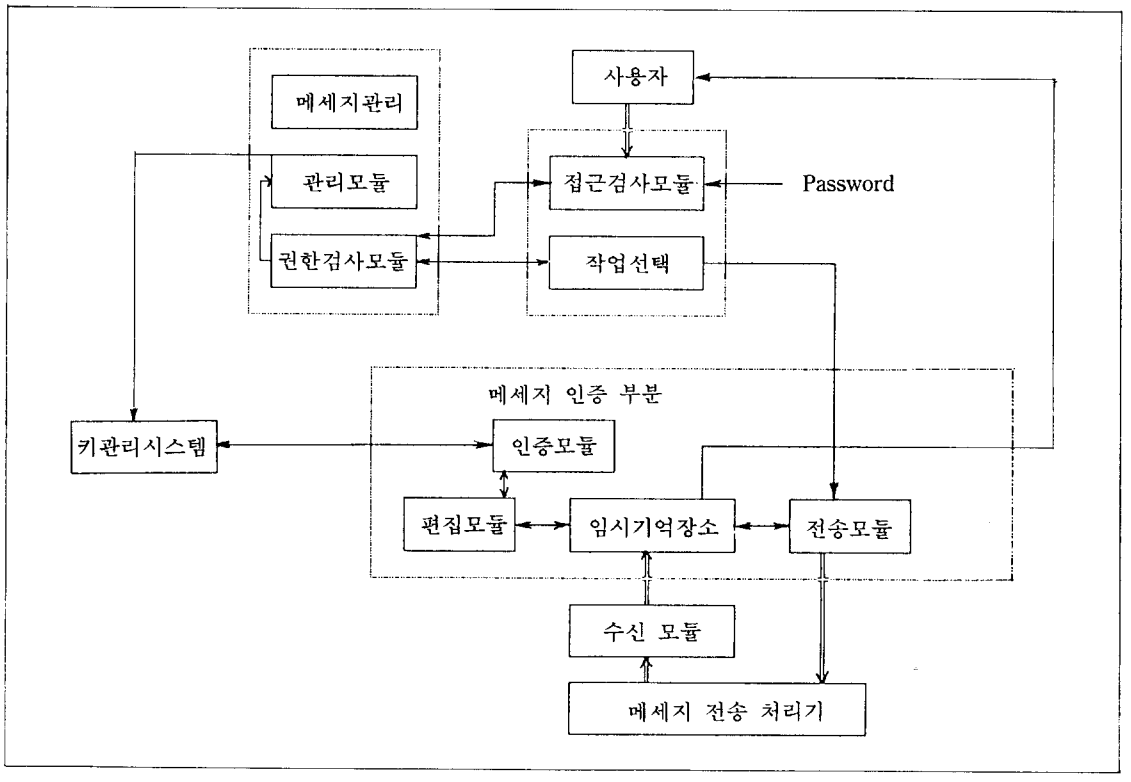

그림 3.1 사용자 처리기의 구조

메세지 전송 처리기로의 중계역할을 수행하게 된다.

메세지 전송 처리기는 크게 몇 가지의 서브 모듈로 분류 할 수 있는데 (i) 자신이 속한 사용자 처리기에 대한 메세지 배달을 하거나 사용자 처리기로 부터 제출을 받는 메세지 처리 모듈이 있다. (ii) 메세지 수신 모듈로서 기능은 다른 메세지 전송 처리기로 부터 메세지를 수신하고 필요시에는 복호화를 수행하게 된다. 또한 메세지가 자신에 속한 사용자 처리기의 주소를 갖고 있다면, 사용자 처리기로 부터 복호화된 메세지를 배달하게 된다. (iii) 메세지 전송모듈로서 기능은 다른 메세지 전송 처리기로 메세지를 전송하는 것이다. 즉, 자신의 메세지 수신 모듈에 도착한 메세지가 또 다른 메세지 전송 처리기로 가기를 원한다면 필요에 따라 복호화된 메세지를 다시 암호화를 하게 된다. (iv) 메세지전달 모듈로서 메세지 큐라는 우선순위를 목적으로 하는 일시저장 장치가 있어, 메세지 전달모듈에 도착한 메세지의 순서대로 우선순위를 부여하여 메세지 전송모듈로 보내는 기능을 한다. (v) 키 분배센터로서, 암호화와 복호화를 하기 위한 키의 생성 및 분배를 하게 된다. 이와같은 메세지 전송 처리기의 구조에서 암호화와 복호화를 하게 되면 자연적으로 메세지의 최종 목적지에 도달 했을 경우, 키의 비교에 의해 인증의 문제가 해결될 수 있다.

메세지 처리 시스템의 보안을 위한 메세지 전송 처리기에 대한 구성은 다음 그림 3.2와 같이 나타낼 수 있다.

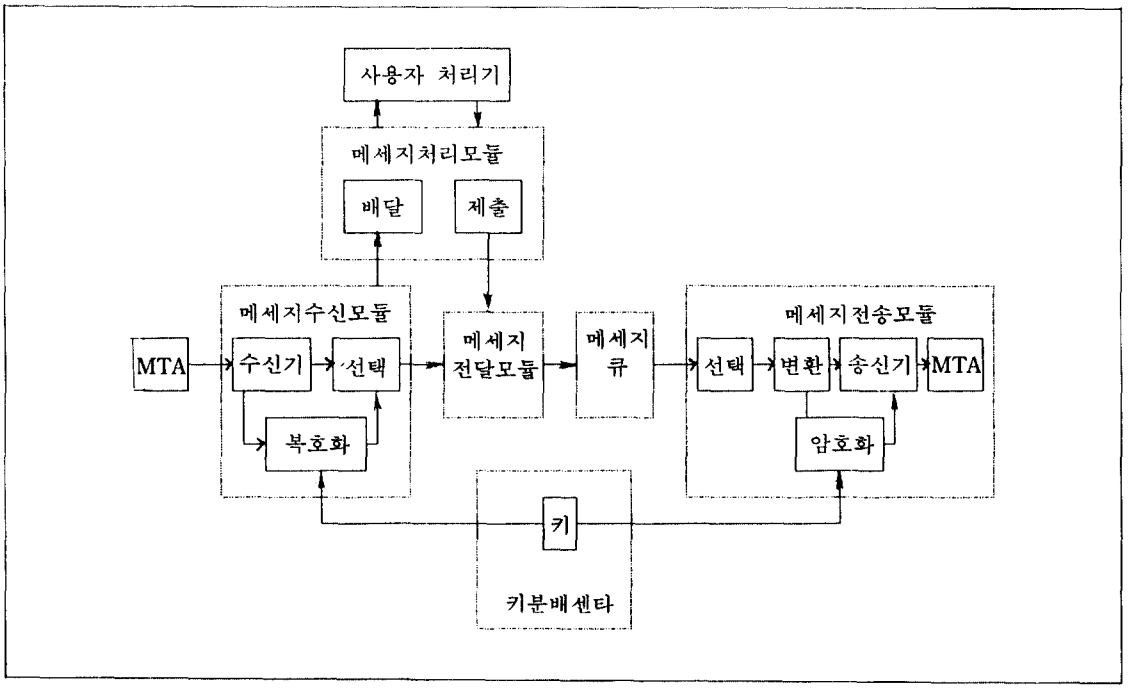

그림 3.2 메세지 전송처리기의 구조

3. 2 메세지 인증 방식 고찰

대표적인 인증 방법에는 (i) 메세지의 내용에 어떤 일정량의 시간 변화량을 할당하여 송신자와 수신자가 이미 알고 있는 시간 변화량을 비교하여 전송된 각 메세지의 순서를 유지하는 방법이 있고, (ii) 전송할 메세지에 대하여 어떤 함수를 적용하여 비교적 적은 고정길이의 중복코드를 생성하여, 전송할 메세지에 부가하여 보내는 것으로서, 생성코드와 수신 메세지를 함수 적용한 코드와 비교하여 변화가 없는가를 조사하는 방법이다. 그 밖에도 몇 가지 방법이 있으나 본 고에서는 전송 선로상에서의 효율 관점에서 두 번째 방법에 대한 기존의 메세지 인증방식을 고찰해 보고자 한다. 기존의 메세지 인증방식은 메세지 M을 K비트씩 N개의 블록 M_i (길이 K 비트, i=1..N)로 분할시켜, 각각의 블록에 대한 해쉬함수 h에 의해 r비트의 인증 메세지 h(M)을 구한다. 이렇게 구한 인증 메세지와 원래의 메세지를 붙여서 그림 3.3−1과 같이 확장된 메세지 M을 만들어 K 비트씩 암호화하여 송신하는 방식이다.

이때 수신측에서는 수신한 인증자 h'(n)과 수신문 M'로 부터 생성한 인증 메세지 h(M')가 일치하는가를 판정하여, 일치하게 되면 통신로에서의 수정 등이 없다고 인정하여 그것을 받아들이게 되고, 그렇지 않으면 재전송을 요구하게 된다. 이 방식은 전체통신 선로상에서 메세지의 에러율은 낮출 수 있으나 통신로의 효율은 매우 나쁘게 되는 경향이 있다.

그것의 성능은, 에러 없이 받아들여질 확률, 에러 발생을 검출하여 재전송 요구 확률, 에러가 발생해도 바르다고 인식하여 받을 확률을 이용하여 나타낼 수 있는데 각각을 $P_c(q)$, $P_d(q)$, $P_u(q)$라 하면,

$P_c(q)=q^N$

$P_d(q)=(1-q^N)\ (1-2^{-k})$

$P_u(q)=(1-q^N)\ 2^{-k}$

이때, 메세지가 에러 포함할 확률 P를 구하면,

$$P_e=\frac{P_u}{P_c+P_u}=\frac{(1-q^N)2^{-k}}{q^N+(1-q^N)2^{-k}}$$

다음은 전송률 r_A를 구하면 매회 받아들이는 확률

$P_a=P_c+P_u$로서 나타나므로, $r_A\frac{N+\alpha}{P_a}$ 로 나타낼수 있다.

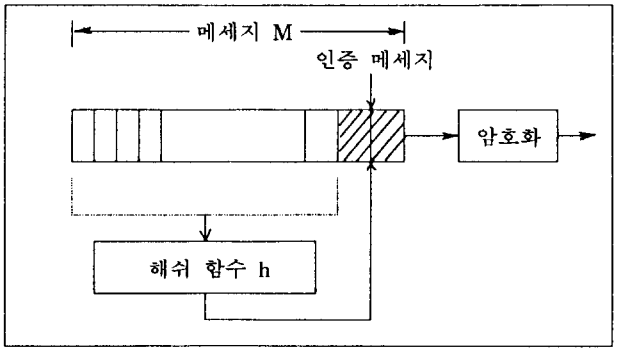

그림 3.3-1. 기존의 메세지 인증 방식

그러나, 기존의 방식에서는 메세지 단위로 인증을 함으로서 페이지의 에러율은 낮출 수 있으나 전송 효율이 나빠지게 되기 때문에 이러한 결점을 개선하기 위해 그림 3.3-2와 같이 블록별로 인증 메세지를 해쉬 함수를 통해 구한 결과와 원래의 메세지를 붙여서 암호화 하여 송수신하는 방법에 대한 연구가 필요하다고 생각된다. 이와 같은 방식은 기존의 방식보다는 메세지 에러율이 다소 나쁘게 되나 효율을 높일 수 있게 된다. 에러율이 나쁜 것은 연속하는 두개의 블록을 연쇄시켜서 인증 메세지를 부가함으로서 에러율을 개선시킬 수 있다. 이 방식의 성능은 앞에서의 방법과 같이 구할 수 있다.

$$P_e(q)=1-(1-k)^N=1-\{\frac{q}{q+(1-q)2^{-k}}\}^N$$

$r_B=N/P_a$ 으로서 구체적인 수치를 대입하면 기존의 방식보다 효율적이라고 볼 수 있다.

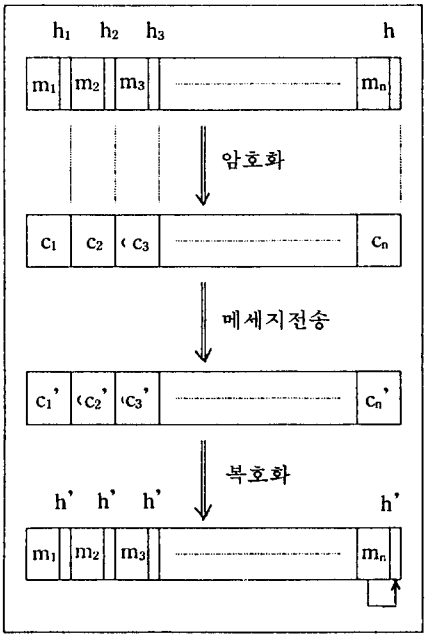

그림 3.3-2. 메세지 블록별 인증하는 방식

4. 결 론

본 고에서는 전반적인 메세지 처리 시스템의 구성과 각 처리기들간의 관계 및 기능을 살펴 보았고, 현대 사회가 정보화 사회로 가는 이 시점에서 컴퓨터 통신의 보안에 관한 문제가 제기 된다는 것을 인식하여 보다 안전한 메세지 전송 시스템을 구축하기 위하여 보안기능이 부가된 사용자 처리기 및 메세지 전송 처리기에 중점을 두어 고찰하였다. 또한 CCITT 권고안에서 제시한 보안 개념을 바탕으로 이미 이전에 제시했던 메세지 처리 시스템에 적합한 인증 방법을 고찰하였고, 보다 효율적이고 안전한 인증 알고리즘을 통해서 상호간의 신뢰성 있는 통신을 가능하게 할 수 있도록, 접근 기법이 상이한 인증방법에 대한 연구 방향을 제시하였다. 본 고를 바탕으로 앞으로의 연구방향은, 본 고에서 개념적으로 살펴보았듯이 보안 기능이 부가된 사용자 처리기 및 메세지 전송 처리기를 사용시 발생하는 오버해드를 감소시키고 보다 효율적이고 체계적인 보안 메세지 처리 시스템의 구현을 위해 계속적인 연구와 개발이 이루어질 수 있도록 해야 할 것이며, 또한 제시한 인증 방법에 관한 연구도 병행되어야 할 것이다.

참 고 문 헌

1. 차경돈, 홍기융, 김동규, "Secure MHS를 위한 부인봉쇄 서비스," 통신정보 보호 학술 발표 논문 Vol. 1, No. 1, 1991.

2. P. Schicker, "Message Handling System and Distributed Application," North-Holland, 1989.

3. D.E. Denning, Cryptography and Data Security, Addision-Wesley, 1982.

4. 한국정보고학회 정보통신연구회, 情報通信技術, 第4卷 第1號(通卷 제8卷), 1990년 6월.

5. 정민화, 크립토 시스템을 이용한 메세지 처리 시스템에 관한 연구, 석사학위 논문, 국방대학원, 1990.

6. CCITT Eight Plenary Assembly, Recommendations X.400-X.430 : Data Communication Networks Message Handling Systems, CCITT Red Book Vol. VII. 7, Malaga-Torremolinos, Oct. 1984.

7. 한국데이타통신주식회사, 메세지 핸들링 시스템(CCITT 권고안)-Recommendation Message Handling Systems.

□ 著者紹介

金 和 洙(正會員)

1976년 3월 海軍士官學校 卒業(理學士)
1984년 7월 美國 海軍大學院(U.S. Naval Postgraduate School) 電算學科 碩士
1990년 8월 美國 Case Western Reserve University 電算學科 博士
1990년 8~1991년 5 海軍本部 通信監室 運營課長
1991년 6월~現在 : 國防大學院 教授(海運中領)
관심분야 : 병렬처리, 인공지능 및 전문가 시스템, 데이타 통신, 암호학