通信情報保護學會論文誌
第7卷 第2號, 1997. 6

EDI를 위한 정보보호 관리

권 태 경*, 강 지 원*, 윤 명 근*, 송 주 석*, 강 창 구**

Security Management for Electronic Data Interchange

Taekyoung Kwon, Jiwon Kang, Myungkeun Yoon,
Jooseok Song and Chang-Goo Kang

요 약

본 논문에서는 ITU-T X.400 권고안 시리즈를 근간으로 국내외에서 구축되고 있는 EDI(Electronic Data Interchange) 시스템의 정보보호 관리를 위한 모델을 설계하였다. 따라서 먼저 상업정보를 다루는 EDI 시스템의 정보보호 관리를 위한 요구사항 및 기능을 정의하였으며, 이를 제공하기 위한 모델을 설계하였다. 이 모델은 X.400을 근간으로 한 기존 EDI 시스템에 정보보호 기능을 추가한 SEDI(Secure EDI) 모델을 기반으로 설계되었는데 그 특징은 X.800을 기초로 본 논문에서 정의한 정보보호 관리 기능을 제공하기 위한 구조이며 또한 기존의 EDI 시스템에 정보보호 기능을 더할 경우 함께 추가되어야 할 정보보호 관리 기능을 위한 구조를 갖는 것이다.

Abstract

In this paper, we design a model of security management in the EDI(Electronic Data Interchange) system implemented on the basis of ITU-T X.400 series. First of all, we defined requirements and functions for providing the security management facility in the EDI system which manipulates a lot of commercial documents. The model to satisfy the requirements is also designed for SEDI(Secure EDI) system which provides security services.

1. 서 론

정보화 사회의 발전으로 인하여 컴퓨터 통신이 모든 분야에서 필수적으로 활용되고 있으며 국내외적으로 급속한 확대 추세를 보이고 있다. 컴퓨터 통신을 통해서 다양한 분야의 정보들이 저장 및 유통되고 있는데, 결국 이것은 각 분야에 걸친 다량의 정보들이 전자화되

* 연세대학교 컴퓨터과학과 정보통신연구실
* * 한국전자통신연구원

어 가고 있음을 의미한다. 이와 같이 첨단 기술의 보유 능력과 정보력의 격차가 국력의 우열로 이어지는 새로운 국면을 맞게 되면서 각국은 고도 정보화사회를 조기에 실현시키기 위한 노력을 한층 더하고 있다. 특히 개방 환경하에서 거래, 구매, 주문 등에 해당되는 상업 정보 문서의 구조화 및 자동화된 전송 기능을 제공하기 위한 방법으로서 EDI(Electronic Data Interchange) 개념이 개발되었으며, 이것은 ITU-T X.400 시리즈 MHS(Message Handling System) 권고안의 기본적인 전자 메시지 기능을 기반으로 구축되어 사용되고 있다.[1,3] 그러나 한편으로 최근 이러한 추세와 함께 EDI 문서의 정보보호 문제가 주요 이슈로서 대두되고 있는데, 이것은 민감한 상업 정보에 대한 안전 대책을 세우지 않았을 경우 사회적, 경제적으로 심각한 문제가 발생할 수 있다는 인식과 함께, 이미 정보화에 따른 부작용으로서 드러나고 있는 각종 정보침해 사례에 의한 영향이라고 할 수 있겠다. 따라서 1988년에 정의된 MHS 정보보호 기능 및 1991년에 정의된 X.435 EDI 권고안에 따른 정보보호 기능을 제공하는 EDI 시스템개발 사례가 늘어나고 있는 추세이며, 국내에서도 이미 한국통신에서 개발한 KT-EDI 시스템에 정보보호 기능을 추가한 SEDI(Secure EDI) 시스템을 한국전자통신연구소에서 개발하고 있다.[6,10]

개방 시스템 구조를 기반으로 제공되는 서비스인 EDI 서비스는 X.700 권고안에 따라서 개방 시스템을 위한 5개 영역별 관리 기능을 제공하도록 해야 하며,[4] 여기에 정보보호 관리 기능도 포함된다. 그러나 일반적으로 정보보호 기능 모듈은 KT-EDI에서의 예와 같이 기존 EDI 시스템에 새롭게 추가되도록 개발되고 있으며, X.435에 따라 정보보호 기능을 포함한 새로운 EDI 시스템을 개발할 경우에도 민감한 정보보호 기능 모듈 및 서비스에 대한 관리는 개별적인 영역에서 이루어질 필요가 있다.

따라서 본 논문에서는 이와 같은 관점에서 X.700의 정보보호 관리 영역을 구체화하기 위하여, X.800 개방형 시스템[2]의 정보보호 구조 권고안을 근간으로 EDI 시스템의 정보보호 관리를 위한 요구사항 및 기능을 정립한 후 이를 위한 모델을 설계하도록 한다. 이 모델은 한국통신의 KT-EDI를 기반으로 설계되었는데 그 특징은 X.800을 기초로 본 논문에서 정의한 정보보호 관리 기능을 제공하기 위한 구조이며 또한 기존의 EDI 시스템에 정보보호 기능을 추가할 경우에 함께 추가되어야 할 정보보호 관리 기능을 위한 구조를 갖는 것이다. 따라서 본 논문에서는 이것을 EDI를 위한 추가적 정보보호 관리라고 한다.

본 논문의 구성을 살펴보면 먼저 2장에서 X.800 권고안을 근간으로 EDI 정보보호 관리를 위한 요구사항 및 기능을 정립하고, 3장에서는 정보보호 기능을 추가한 SEDI 시스템을 소개한다. 4장에서는 이 시스템 모델을 기반으로 정보보호 관리 기능을 추가하기 위한 시스템 개념을 설명하고, 5장에서 구체적인 관리 구조를 설계한 후, 6장에 결론을 맺는다.

2. EDI 정보보호 관리 요구사항 및 기능

본 장에서는 EDI 시스템의 정보보호 관리 요구사항을 정립하는 한편 정립된 요구사항들을 만족시키기 위한 관리 기능을 정립한다. 앞에서 설명한 바와 같이 본 논문에서는 X.700 권고안의 정보보호 관리 영역의 기능을 확장하기 위하여 X.800 권고안의 정보보호 관리 요구사항을 준수하도록 한다. 권고안 X.800은 개방형 시스템에서의 정보보호 구조에 대해서 기술하고 있다. 그러나 이 권고안에서는 무엇을 해야하는가에 대해서만 다루고 있으며 어

떻게 해야하는가에 대해서는 구체적으로 언급하지 않고 있다.[4,2] 즉, 정보보호 관리에 대한 내용들이 추상적으로만 기술되어있기 때문에 응용 분야에 적용시키기 위해서는 요구사항들을 구체적으로 정립하고 이와 같은 요구사항들을 만족시키기 위한 기능을 정립하는 과정이 필요하다. 따라서 본 장에서는 먼저 EDI 시스템을 위한 요구사항과 기능을 정립한다.

2.1 EDI 시스템 정보보호 관리 요구사항

X.800 권고안은 OSI에 적용되는 정보보호 구조에 대해서 기술하고 있으며 정보보호 서비스와 메카니즘, 그리고 정보보호 관리에 대한 권고안을 포함한다. EDI 정보보호 관리의 목적은 EDI의 정보보호 기능을 유지 및 제어하기 위한 것이라고 할 수 있으며, 이를 위해서는 다음과 같은 기능들이 필요하다.[2]

- 정보보호 관련 정보의 수집 및 분배 : 정보보호 관련 사건에 관한 원격보고 및 기록, 그리고 정보보호 관련 정보를 유통한다.
- 정보보호 서비스 및 메카니즘의 수행 상태 검사 : 정보보호 기능의 수행 여부를 효율적으로 검사한다.
- 정보보호 관리 정책 실현 : 특정한 관리 정책에 따른 정보보호 서비스와 메카니즘의 개시 및 삭제를 한다.

본 논문에서는 X.800 권고안에 따라 EDI 정보보호 관리 요구사항을 네 가지 영역으로 구체적으로 나누었다. 네 가지 영역에는 시스템 정보보호 관리 영역, 정보보호 서비스 관리 영역, 정보보호 메카니즘 관리 영역 그리고 정보보호의 관리 영역이 있다.[2]

(1) 시스템 정보보호 관리

시스템 정보보호 관리는 EDI 환경의 전체적인 정보보호 측면의 관리와 관련된다. 여기에는 정보보호 정책 관리와 정보보호 기능 모듈의 결함/구성 관리가 포함된다.

- 정보보호 일관성 유지 관리 : 정보보호 관리자는 비밀성, 무결성, 접근 제어, 인증, 감사 등에 대한 필요한 정책을 수립하고, 이를 실현하기 위한 EDI 정보보호 모듈을 일관성 있게 구현 및 배포할 수 있어야 한다.
- 다른 EDI 관리 기능들과의 MIB 공유 : OSI 관리 영역 중 정보보호 관리를 제외한 네 가지 영역에 대한 EDI 관리 기능과의 일관성 유지 및 상호 작용이 고려되어야 하며, MIB의 공유를 통해서 안전한 관리 정보의 참조가 이루어져야 한다.
- 다른 정보보호 관리 영역과의 상호 작용 : 정보보호 서비스 관리 및 정보보호 메카니즘 관리 등과 같은 다른 영역과의 일관성 유지 및 상호 작용이 고려되어야 한다.
- 관리 명령 전달 및 사건 보고 관리 : 관리자의 관리 명령이 안전하게 전달되어야 하며, 시스템의 보안 침해가 발생하거나 정보보호 모듈의 결함 또는 구성에 관한 변화가 발생할 경우 이에 대한 보고가 이루어져야 한다.
- 정보보호 기능 모듈의 결함 및 복구 관리 : 정보보호 기능 모듈에 대한 결함 및 복구 규칙을 규정하고, 결함 발생시 수집된 결함 결과를 바탕으로 복구할 수 있어야 한다.
- 정보보호 기능 모듈의 구성 및 등록 관리 : 새로운 정보보호 기능 모듈이 추가되거나 모듈 구성의 변경이 발생하면 전체

시스템의 조화로운 동작을 위해서 일관된 등록 관리가 이루어져야 한다.

- 정보보호 감사 관리 : EDI 시스템의 보안 침해 사건의 규정 및 침해에 대한 기록의 원격 수집, 보고가 이루어져야 한다.

(2) 정보보호 서비스 관리

정보보호 서비스 관리는 특정 정보보호 서비스에 대한 관리에 해당되며, X.402 및 X.435에 정의되어 있는 EDI 시스템을 위한 정보보호 서비스를 고려한다.

- 정보보호 서비스 개시 및 폐지 : X.402 및 X.435를 근간으로 하여 서비스에 대한 목표를 정의하고, 새로운 서비스를 등록하거나 등록 정보를 갱신할 수 있어야 한다.
- 정보보호 서비스 등급별 제공을 위한 프로화일 관리 : 관리자의 의도에 따라 유사한 목표를 갖는 서비스 및 서비스의 등급을 구분하여 서비스를 관리할 수 있어야 한다.
- 정보보호 서비스 대 메카니즘 등록 관리 : 가용 메카니즘의 활성화/비활성화 및 서비스 대 메카니즘의 연결 관리가 가능해야 한다.

(3) 정보보호 메카니즘 관리

정보보호 메카니즘 관리는 특정 정보보호 메카니즘에 대한 관리에 해당되며, X.402 및 X.435에 정의되어 있는 EDI 시스템을 위한 정보보호 서비스를 위해서 필요한 메카니즘들을 고려한다.

- 키 관리 : 키의 생성, 등록, 분배, 저장 그리고 폐기에 관련된 관리가 이루어져야 한다.
- 정보보호 메카니즘 등록 및 설정 관리 : 암호화, 디지탈 서명, 접근제어, 무결성, 인증 등의 메카니즘 모듈을 등록하고 유지할 수 있어야 한다.

(4) 관리 정보의 보호

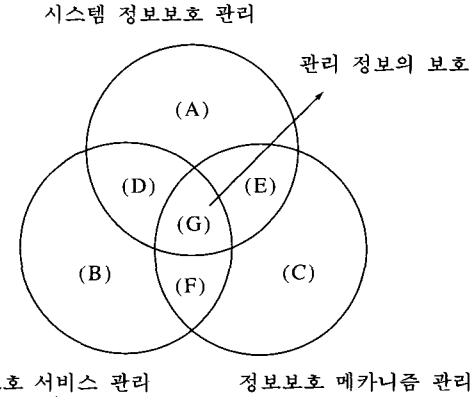
관리 정보의 보호는 관리 프로토콜, 특히 정보보호 관리에 관한 정보의 보호 측면과 관련되며 타 관리 정보와의 일관성 및 타 관리 정보의 보호 측면도 포함한다.

- 관리 정보의 안전한 유통, 저장, 백업 : 전체 시스템의 안전성과 성능면을 면밀히 비교하여 시스템의 특성에 맞도록 관리 정보를 안전하게 유지해야 한다.

이와 같은 요구사항을 만족하기 위해서는 다양한 관리 기능이 필요하다. 다음 2.2절에서는 이를 만족하기 위한 관리 기능을 정의하도록 한다.

2.2 EDI 시스템을 위한 정보보호 관리 기능

앞에서 정의한 EDI 정보보호 관리 요구사항을 만족하기 위해서 필요한 기능을 정립한다. 여기서 정의하는 기능을 위해서는 EDI 정보보호 관리 시스템이 일반적인 관리 구조로서 관리자(manager) 모듈과 관리대행자(agent) 모듈로 구성되어야 한다.



[그림 1] 정보보호 관리 기능 영역도

위의 [그림 1]은 앞에서 정의한 EDI 정보보호 관리 요구사항을 만족하기 위한 정보보호 관리 기능을 영역별로 도시한 것이다. 여기서 요구사항의 영역에 해당하는 시스템 정보보호 관리, 정보보호 서비스 관리, 정보보호 메카니즘 관리 그리고 관리 정보의 보호 등의 4개 영역을 대영역이라고 부르고, (A)에서 (G)의 영역을 소영역이라고 부르기로 한다. 이와 같이 관리 영역을 세분화시킨 이유는 소영역에서 관리 기능 대 요구사항을 보다 세밀하게 표현하기 위한 것이며, 따라서 (A),(B),(C)는 각 영역에만 해당하는 기능을, 그리고 (D),(E),(F)는 2개 영역의 중복 기능을 나타낸다. (G)는 3개 영역에 모두 해당되는 관리 기능이다. 각 영역의 기능은 [표 1]과 같이 정의된다.

표 1 EDI 정보보호 관리 기능

영 역	기 능
(A)	1. 결함 상태와 감사 추적 검사를 위한 폴링(Polling) 및 폴링 간격 수정 2. 폴링 대상 모듈 선택 3. 원격지에서 수집 및 보고될 결함의 종류 선택 4. 정보보호 침해의 기록 및 보고의 관련된 임계값 수정
(B)	1. 정보보호 서비스의 등록 및 갱신 2. 정보보호 서비스의 개시 및 폐지 3. 분류된 서비스 프로파일의 설정 및 수정 4. 결함 및 정보보호 침해를 발견하기 위한 정보보호 서비스 폴링
(C)	1. 정보보호 메카니즘의 등록 및 갱신 2. 정보보호 메카니즘의 활성화 및 비활성화 3. 결함 및 정보보호 침해를 발견하기 위한 정보보호 메카니즘 폴링
(D)	1. 정보보호 서비스 모듈에서 사건 발생시 원격지에서의 능동적인 사건 보고 2. 정보보호 서비스 모듈에 대하여 강제 폴링이 시도되었을 경우 수동적인 사건 보고 3. 정보보호 침해 사건 발생시 발견 및 기록
(E)	1. 정보보호 메카니즘 모듈에서 사건 발생시 원격지에서의 능동적인 사건 보고 2. 정보보호 메카니즘 모듈에 대하여 강제 폴링이 시도되었을 경우 수동적인 사건 보고
(F)	1. 서비스 대 메카니즘 테이블의 설정 및 수정 2. 정보보호 서비스를 위한 가용 메카니즘의 등록 및 수정
(G)	1. 서로 다른 관리 기능간의 일관성 유지 및 상호 작용 해결을 위한 MIB 공유 2. 키 길이 및 종류 선택, 그리고 안전한 키 생성, 분배 및 폐기를 위한 파라메터 설정 3. 암호화 방법을 이용한 관리 정보의 안전한 저장 및 분배

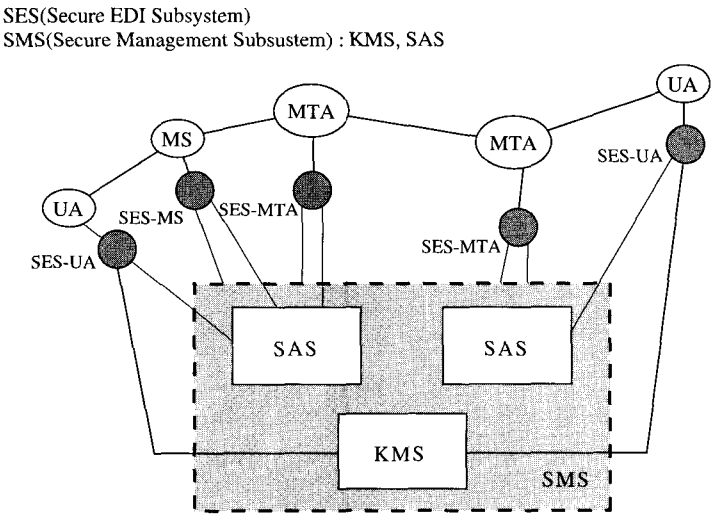
이와 같은 기능을 통하여 EDI 정보보호 관리를 수행할 수 있다. 본 기능을 실현시키기 위해서는 무엇보다도 EDI를 위한 정보보호 기능이 구현되어야 하며, 이에 대한 관리 구조를 체계적으로 설계해야 한다. 따라서 본 논문의 근간 모델인 SEDI 시스템 모델을 살펴본 후 정보보호 관리 기능을 제공하기 위한 EDI 정보보호 관리 시스템 모델을 설계하도록 한다.

3. SEDI 시스템 및 관리 구조

이 장에서는 KT-EDI 시스템에 정보보호 모듈이 첨가된 SEDI 시스템에 대해 살펴보고 정보보호 관리 구제에 대해서 검토하도록 한다.

3.1 SEDI 시스템 개요

1984년에 처음으로 정의된 X.400 MHS 권고안은 ITU-T 및 ISO(International Standards Organization)의 합의로 1988년에 두 조직의 인준하에 표준을 이루었으며, 1991년에는 EDI 서비스를 위한 권고안 X.435를 발표하였다. X.400 시리즈는 F.400으로도 일컬어진다. 국내에서도 이와 같이 MHS 시스템을 기반으로한 EDI 시스템 개발 사례가 점점 늘어나고 있는데, 한 예로서 한국통신에서는 이미 KT-EDI라는 이름으로 EDI 시스템을 개발하였다.[6] KT-EDI는 EDI 서비스를 위한 메시지 처리 기본 구성요소인 UA(User Agent), MS(Message Store), MTA(Message Transfer Agent)로 이루어진다. UA는 사용자를 위해 메시지(전자우편)를 처리하거나 생성하고 MS는 메시지를 저장하는 기능을 수행한다. 또한 MTS(Message Transfer System)을 구성하는 MTA는 네트워크 상에서 다른 MTA나 UA에게 메시지를 전달하는 역할을 한다.[3] 한편 한국전자통신연구소에서는 KT-EDI 시스템의 각 구성 모듈에 추가하기 위한 정보보호 서비스 제공 모듈인 SES(Secure EDI Subsystem)를 개발하고 있으며 이를 관리하기 위한 구조 개념인 SMS(Security Management Subsystem)를 추가해서 SEDI 시스템을 구축하고 있다. [그림 2]는 정보보호 서비스를 제공하는 SEDI 시스템의 구조를 나타낸다.[10]



[그림 2] SEDI 시스템 구조

SEDI 시스템은 정보 보호 서비스를 제공하기 위하여 KT-EDI 시스템의 UA, MS, MTA 각각에 SES 모듈들을 추가하고 이들을 관리하기 위한 SMS를 추가한 시스템이다. SES는 EDI 시스템에서 제공해야 하는 정보 보호 서비스를 처리하는 주 기능을 담당한다. SES는 UA, MS, MTA 각각의 구성 요소들에 위치하며, 각 구성 요소는 SES 인터페이스를 이용하여 해당 서비스의 요청을 수행한다. SMS는 SES에서 정보 보호 서비스를 처리하는 과정에

서 필요한 정보의 제공 및 저장 기능을 수행한다. SMS는 정보 보호 서비스를 처리하기 위해 필요한 키의 생성, 분배, 관리, 제공 및 보증서 관리를 담당하는 KMS(Key Management System)과 각 구성 요소들에서 발생한 정보보호 관련 사건들의 저장 및 검색 기능을 수행함으로써 관리자에게 감사 기능을 제공하는 SAS(Security Audit Subsystem)로 구성되어 있다.[10]

3.2 정보보호 관리 구조

정보보호 관련 모듈은 대개 높은 안전성을 요하는 정보를 다루기 때문에 다른 모듈들과는 별도로 개발되고 관리될 필요가 있다. 한국통신에서도 KE-EDI의 일반 서비스 모듈과 정보보호 서비스 및 관리 모듈을 구분하여 개발하고 있다. 한편 ITU X.700 권고안에서는 관리 기능 영역을 결함 관리, 계정 관리, 구성 관리, 성능 관리, 정보보호 관리 등의 5개 영역으로 구분한다.[4] 그러나 여기서 정의하는 정보보호 관리 기능, 즉 보안 경보 보고, 보안 감사 추적, 접근 제어 등의 기능만으로는 SEDI의 정보보호 서비스 모듈 관리 문제를 해결할 수 없다.

따라서 본 논문에서는 개방형 시스템에서의 정보보호 구조에 대한 권고안인 ITU X.800을 근간으로하여, EDI 시스템을 위하여 추가적인 정보보호 관리 기능을 제공할 수 있는 구조를 설계한다.

X.800에서는 정보보호 관리의 범위를 시스템 정보보호 관리, 정보보호 서비스 관리, 정보보호 메카니즘 관리, 관리정보의 관리와 같이 4가지로 나누고 있다. 본 논문에서 제시하는 정보보호 관리 구조에서는 SES에 대한 관리를 정보보호 서비스 제공 모듈에 대한 정보보호 관리에만 국한시키지 않고 X.700에 나와 있는 나머지 4개 영역에 관한 관리도 수행하게 된다.

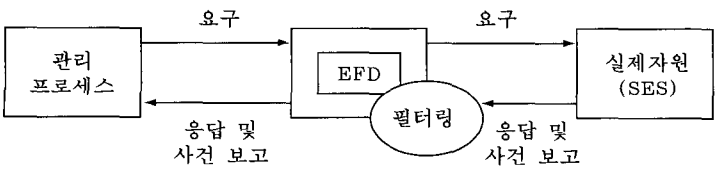
4. EDI 정보보호 관리 모델

본 장에서는 SEDI 시스템 정보보호 서비스 모듈 관리를 위한 시스템의 구조를 설계한다.

4.1 관리 모델 기본 구조

정보보호 서비스 모듈 관리를 위해서 본 시스템은 OSI 관리의 일반적인 형태인 관리자-관리대행자(Manager-Agent) 구조로 관리 환경을 이루도록 한다.[9] 먼저, 관리 시스템의 기본 구조에 대해서 설명한다. 본 시스템의 근간이 되는 관리 모델 개념도는 [그림 3]와 같다.

관리자는 관리 프로세스 모듈에서 제공하는 GUI(Graphical User Interface) 환경에서 실제 자원에 해당하는 SES 모듈을 관리하도록 한다. 그러나 관리자 모듈은 직접 SES 모듈을 관리하도록 하는 것이 아니라 관리 대행자 모듈을 통해서 관리하게 된다. 이 때 관리자 모듈에서 관리 대행자 모듈로 전달되는 명령은 관리 기능 처리 요구에 해당하며, 관리 대행자에서 관리자 모듈로 전달되는 정보는 요구에 대한 응답이나 사건 보고에 해당한다.

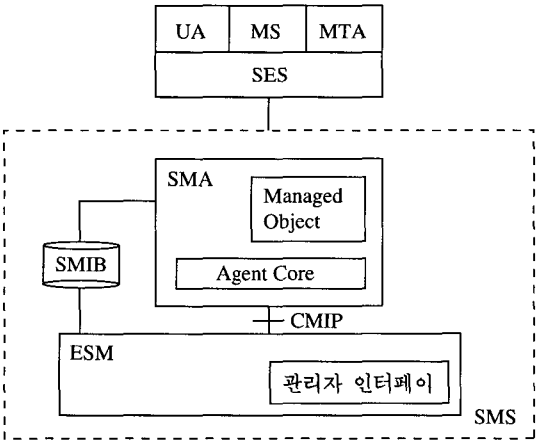


[그림 3] 관리 모델 개념도

하나의 관리자 모듈이 각 SES 모듈에 연결되어 있는 많은 관리 대행자와 메시지 교환을 이루게 되며, 따라서 응답과 사건 보고는 매우 빈번하게 이루어지게 된다. 이와 같은 정보보호 관리 활동 자체가 전체적인 시스템의 오버헤드로 작용한다면 이는 시스템의 성능에 큰 영향을 미치는 결과를 초래한다. 따라서 관리자와 관리대행자 간에 주고 받는 관리 정보는 필터링을 통하여 제한할 필요가 있다. 즉, 관리대행자에 내장된 사건전송분류기(Event Forwarding Discriminator : EFD)가 관리자가 정한 필터링 기준에 따라 발생하는 사건들에 대한 분류를 하고, 이 중 특정한 사건에 대해 관리자에게 바로 보고하지 않고 오직 자신의 데이터베이스에 저장한다. 필터링의 기준은 메시지의 종류와 네트워크 상황에 따라서 관리자가 임계치를 조정해 줄 수 있도록 한다.

4.2 정보보호 관리 모델 설계

본 논문에서 설계하는 정보보호 관리 시스템은 SMS(Security Management System)라고 호칭하며 앞에서 설명한 바와 같이 관리자-에이전트 구조를 갖는다. SEDI의 SMS 구조에 적합한 모델로서 같은 약어를 갖도록 명명하였다. SMS는 각 MHS 요소의 정보보호 모듈, 즉 예를 들면 SEDI의 SES 모듈들에 대하여 정보보호 관리를 수행한다. ESM(EDI Security Manager)은 관리자 모듈로서 관리자의 명령을 해당 SMA(Security Management Agent)에 전달하거나 SMA로부터 수집한 정보를 바탕으로 2.2장에서 정의한 기능들을 수행한다.



[그림 4] 정보보호 관리 시스템의 구조

[그림 4]에서와 같이 ESM과 SMA는 관리 시스템의 기본 구조인 관리자-에이전트 관계를 이루고 있다. SMA는 SES의 각 기능모듈의 상태와 SMA 자체의 상태에 대해서 관리객체(managed-object:MO) 형태로 정보를 보관한다. SES 상태에 대한 질의나 SES 변경 정보는 ESM에서 SMA로 전달된다. SMA와의 인터페이스 프로토콜로는 CMIP(Common Management Information Protocol)을 사용하도록 한다.[5] 그러나 CMIP을 이용한 구현을 위해서는 X.25상에서 구현된 EDI 시스템이 완전한 OSI 계층 구조로 구성되어야 하며, CMIP을 위해 충분한 자원이 제공 되야 하므로 구현에 어려움이 따른다. 따라서, TCP/IP 환경이 가능한 경우에는 CMOT(CMIP Over TCP/IP)나 SNMP(Simple Network Manage

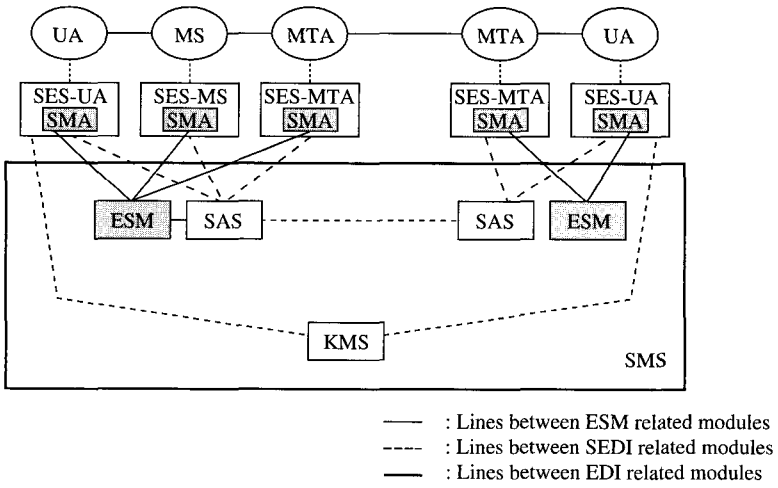
ment Protocol)를 사용할 수 있다. 이와 같이 ESM은 관리 프로토콜을 통하여 메시지를 주고 받으며 관리 기능을 수행한다. SMA는 ESM으로부터의 요구에 맞는 응답을 하며 문제가 발생하면 자발적으로 ESM에게 보고하기도 한다.

SMIB(Security Management Information Base)는 EDI에서 필요로 하는 모든 정보보호 관련 정보의 개념적인 저장소이다. ESM과 SMA는 필요한 지역 정보를 각자의 SMIB에 저장해두고 참조한다. SMIB는 분산된 형태의 정보 저장소이고 일관성 유지를 위해 안전하게 관리되어야 하며, 따라서 SMIB 정보 갱신 이전에는 항상 정보보호 관리자의 신분이 먼저 확인되어야한다. SMA에서 관리되는 메카니즘과 서비스는 다음과 같다.

- 메카니즘 : 암호화 알고리즘, 디지털 서명 알고리즘, 해쉬함수, 실체 인증 메카니즘, 감사 추적 메카니즘, 키관리 메카니즘
- 서비스 : 데이터 비밀성, 데이터 무결성, 부인 봉쇄, 발신 인증, 책임 인증
  cf) 책임 인증 : EDI 통지 증명, 검색 증명, 전달 증명 등이 있다.

4.3 SEDI를 위한 정보보호 관리 모델

SEDI에서 현재 SMS를 구성하고 있는 감사 모듈과 키관리 모듈만으로는 X.800에 나오는 정보보호 관리 요구 사항을 만족시키지 못하는 부분들이 존재하게 되고, SES에 대한 관리 영역이 그 예이다. 이 문제를 해결하기 위해서 앞에서 설명한 관리 모델 기본 구조를 바탕으로 SEDI의 SES 관리 시스템을 설계한다. SES 관리 시스템은 X.800 권고안을 근간으로 하므로 SES의 각 모듈에 대한 관리와 함께, 전체 EDI 시스템의 정보보호 관리 기능을 제공하게 된다.



[그림 5] SES 관리 시스템 개념도

먼저 앞의 [그림 5]에서와 같이 정보보호 관리 기능을 위해서 설계되어 있는 SEDI의 SMS 영역에 본 관리 모델을 적용하도록 하며, 감사 관리와 키 관리를 위해서 설계된 SAS(Security Audit System)와 KMS(Key Management System) 모듈과 연동하도록 한다. 이 관리 모델은 [그림 4]에서 도시한 바와 같이 관리자 모듈인 ESM과 관리 대행자 모듈

인 SMA을 포함한다. ESM은 각 MTA마다 하나씩 존재하며, 해당 영역의 각 SES 모듈과 연결된 SMA를 통해서 실제 SES 모듈을 관리한다. SMA는 해당 EDI 구성 요소의 SES의 자원을 관리하는 한편, EFD 기능을 통하여 관리 정보를 필터링하여 자신의 데이터 베이스에 저장하고 필요시 ESM 모듈로 보고한다. ESM과 SMA의 상세 구조에 대해서는 다음 5장에서 설명하도록 한다.

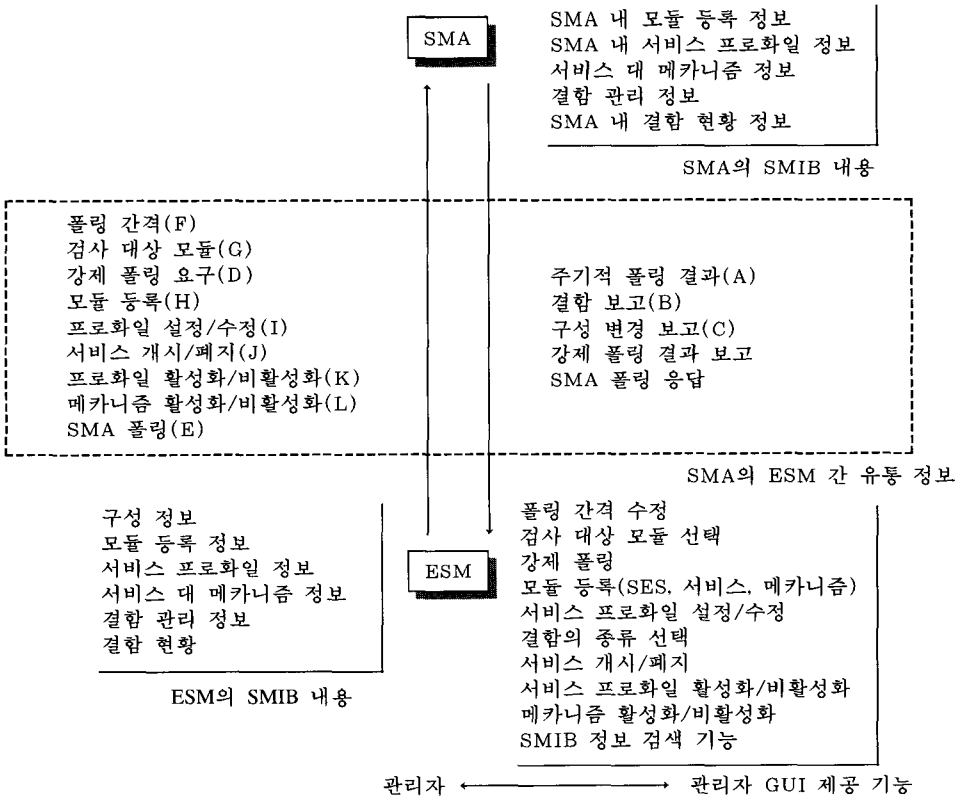
5. ESM 및 SMA 설계

기존의 SMS는 KMS와 SAS만으로 구성되어 있으며, X.800에 나오는 정보보호 관리 요구 사항을 만족시키기 위해서는 감사모듈과 키 관리 모듈이외에도 EDI에서 제공하는 정보보호 서비스를 관리해주는 모듈이 필요하게 된다. 본 장에서는 X.800에 제시된 정보보호 관리 요구사항을 만족시키기 위한 모듈로서 ESM(EDI Security Management)과 SMA(Security Management System)를 세부 설계하도록 한다.

5.1 관리 정보 정의

ESM과 SMA를 정보보호 관리 시스템에 추가함으로서 폴링 간격 수정, 검사 대상 모듈 선택, 강제 폴링, 모듈 등록, 서비스 프로화일 설정/수정, 결함의 종류 선택, 서비스개시/폐지, 서비스 프로화일 활성화/비활성화, 메카니즘 활성화/비활성화, SMIB정보 검색 기능 등을 수행함으로써 X.800에 나와있는 정보보호 관리 요구 사항을 만족시킨다. 이와같은 기능을 수행하기위해서는 SMA와 ESM이 내부적으로 가지고 있어야하는 MIB와 서로 주고받는 메시지가 정의되어야 한다.

이것을 관리자 GUI 환경에서 제공하는 기능과 함께 도시하면 다음 [그림 6]과 같다.



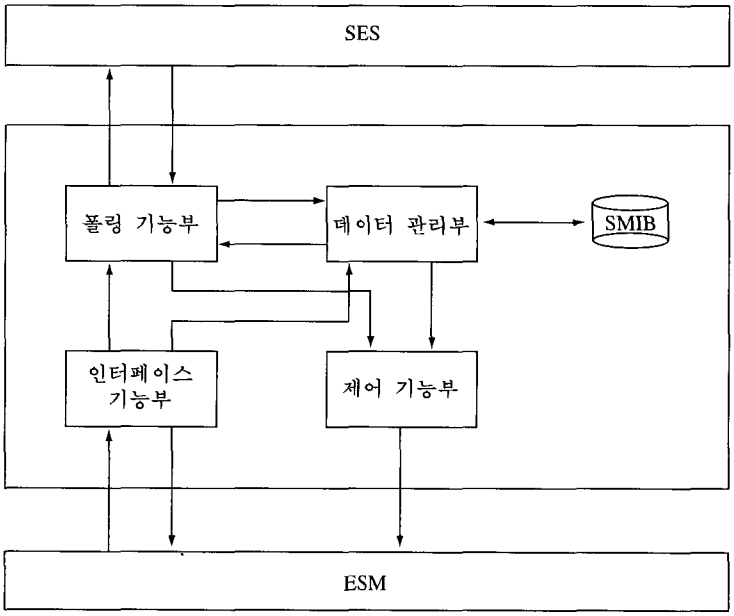
[그림 6] ESM-SMA의 관리 정보 및 관리자 GUI 기능

예를 들어 관리자로부터 SES모듈내의 암호화 메카니즘에 대한 폴링 간격 수정 명령을 GUI를 통해 받아들이면 ESM이 가지고 있는 내부 MIB에 폴링 간격 레코드 값을 변경하고 SMA에게 폴링 간격 변경 메시지를 보낸다. SMA는 자신이 가지고 있는 MIB의 해당 레코드의 값을 수신된 메시지의 값으로 변경한 뒤 변경된 간격으로 폴링을 수행한다.

5.2 SMA의 구조

SEDI의 정보보호 서비스 모듈(SES)을 관리하기 위한 관리 대행자인 SMA는 SES내에 위치하게된다. SMA는 관리자의 요청에 의한 관리 동작과 관리자원의 상태 변화를 감시하여 얻은 관리 정보를 ESM에게 보고하는 기능을 수행한다. SMA와 ESM 모듈은 CMIP, SNMP 등의 표준 통신 프로토콜을 통하여 관리 정보를 교환하며, SES의 내부 단위 모듈과는 IPC 메카니즘 혹은 파라메타 전달을 통하여 통신한다.

SMA의 구조는 [그림 7]과 같이 제어 기능부, 인터페이스 기능부, 데이터 관리부, 폴링 기능부 등의 네 가지 기능영역으로 구성된다.



[그림 7] SMA의 기증 구조도

(1) 제어 기능부

제어 기능부는 SMA의 전체적인 기능 제어 및 조정 기능과 사건 분류 및 전송 기능을 담당한다. 사건 분류 및 전송 기능(Event Forwarding Discriminator)은 SES 또는 SMIB로부터 받은 사건 보고를 ESM에게 보고할지를 필터링 기준에 따라 검사한다. 필터링후 자신의 SMIB에 데이터 관리부를 통해 이를 기록하고 관리자에게 보고할 내용은 인터페이스부를 거쳐 보고한다. 또한 기능 제어는 SMA 기능 개시 및 종료와 각 기능부에 대한 제어 기능을 수행한다.

(2) 인터페이스 기능부

인터페이스 기능부는 SMA와 ESM간의 관리 정보 유통과 관련하여 각 기능부와 ESM 모듈간의 인터페이스, ESM의 요청을 수신하여 해당 기능부에 메시지 내용을 전달, 다른 기능부로부터의 사건 보고 및 응답을 ESM에게 보고하는 기능을 수행한다.

(3) 데이터 관리부

데이터 관리부는 SMA에 저장되는 지역 SMIB의 관리를 담당한다. ESM의 등록, 검색, 갱신, 삭제 요청을 받아 자신의 SMIB로 관리 동작을 수행한다. 또한, 제어 기능부에서 필터링된 사건 보고를 저장하며 관리자의 필터링 기준을 등록 및 갱신하는 기능 등이 포함된다. 지역 SMIB에 관리되는 정보는 모듈 등록 정보, 서비스 프로화일 정보, 서비스 대 메카니즘 정보, 결함 관리 정보, 결함 현황 정보 등이 있다.

(4) 폴링 기능부

폴링 기능부는 SES의 각 모듈에 대해 관리자가 지정한 시간 간격으로 폴링을 수행하고 SES 모듈의 폴링 결과 및 우발적인 사건 발생을 감시하고 사건에 부가적인 정보(발견 시간 등)를 더하여 제어 기능부로 전달하며 그리고 관리자의 강제적 폴링 요청을 받아 폴링을 수행하는 기능을 포함한다.

5.3 ESM의 구조

ESM은 정보보호 감사 시스템(SAS)과 같은 컴퓨터 내에서 작동하거나 또는 동일한 레벨의 컴퓨터에서 동작한다. SMA에게 관리자원에 대한 상태를 요청하고 이에 대한 응답을 받아 SMIB에 관리 정보를 저장하고 필요시 관리자에게 GUI를 통해 제공한다. 이 모듈은 [그림 8]와 같이 GUI 제어 기능부, 사건 수집 기능부, 데이터 관리부, 명령 기능부로 구성된다.

GUI 제어 기능부는 ESM의 관리자 환경 제어 및 사건 처리 기능을 수행한다. 사건 처리 기능에는 관리자 GUI를 통한 사건 보고가 포함되며, 기능 제어는 ESM 기능 개시, 각 기능부 개시, 관리자 GUI 환경 개시, 관리자 GUI 입력 처리, 관리자 GUI 출력 처리 등을 포함한다.

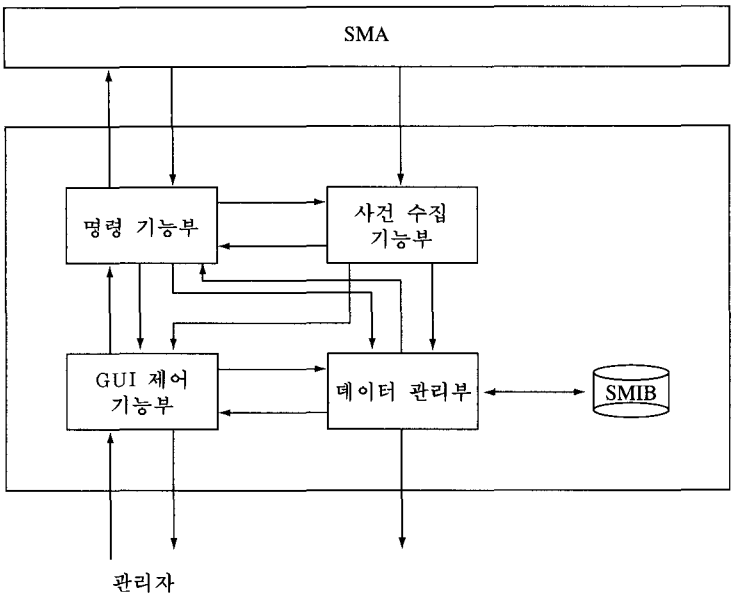
사건 수집 기능부는 SMA로부터 보고되는 사건을 수집하여 데이터 관리부와 관리자에게 전달하는 기능을 담당한다.

데이터 관리부는 논리적 관리 정보 저장소인 SMIB를 관리한다. GUI 제어 기능부와 명령 기능부로부터 해당 관리 정보의 등록, 갱신, 삭제를 의뢰받아 관리를 수행한다. SMIB에 저장되는 관리 정보의 유형은 구성 정보, 모듈 등록 정보, 서비스 프로화일 정보, 서비스 대 메카니즘 정보, 결함 관리 정보, 결함 현황 정보 등이 있다.

명령 기능부는 SMA 폴링, 관리자에 의한 강제적 폴링과 폴링 결과를 데이터 관리부에 전달하는 기능과 관리자의 명령 전달 기능을 담당한다.

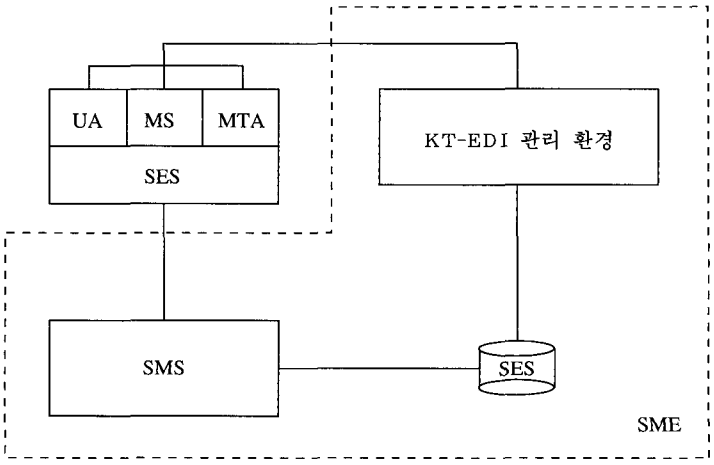
6. 결론

본 논문에서는 ITU-T X.800 개방형 시스템의 정보보호 구조 권고안을 근간으로 EDI 시스템의 정보보호 관리를 위한 요구사항 및 기능을 정립한 후 이를 위한 모델을 설계하였다. 이 모델은 한국통신의 KT-EDI를 기반으로 설계하였으며, 그 특징은 X.800을 기초로 본 논문에서 정의한 정보보호 관리 기능을 제공하기 위한 전반적인 구조에 해당하며 또한



[그림 8] ESM 기능 구조도

기존의 EDI 시스템에 정보보호 기능을 추가할 경우에 함께 추가되어야 할 정보보호 관리 기능을 위한 구조를 갖는다는 것이다. 따라서 X.700에서 권고하는 개방형 시스템을 위한 5개 관리 영역중 정보보호 관리 영역을 분리하도록 하였다. 그러나 EDI 시스템의 일관된 관리 환경의 구축을 위해서 추가적으로 구축된 정보보호 관리 영역은 기존 관리 영역과의 상호작용이 고려되어야 한다. 이것에 대한 개념도는 [그림 9]와 같으며, 그림의 예와 같이 MIB의 공유를 통하여 기존의 관리 영역과 통합된 관리 환경을 제공하도록 해야한다.



[그림 9] SME의 구조

이것을 SME(SEDI Management Environm -ent)라고 부르며, 기존의 KT-EDI 관리 환경과 정보보호 관리 시스템 환경이 병합되어 OSI 관리의 표준 기능을 지향하고 있다. 본 구조에서는 정보보호 관리의 효율성과 안전성을 위해서 정보보호 관리는 기타 나머지 관리 영역과 분리되어 이루어진다. 향후 연구에서는 이와 같이 상호작용을 해결하기 위한 MIB를 설계해야하며, 또한 구체적인 구현이 이루어져야 하겠다.

참 고 문 헌

[1] ITU-T X.435, Message handling systems : Electronic data interchange messaging system, 1992.

[2] ITU-T X.800, Data communication networks : open systems interconnection (OSI) : Security, structure and applicat -ions, 1991

[3] ITU-T X.402, Message handling systems : Overall architecture, 1992

[4] ITU-T X.700, Management framework for Open Systems Interconnection(OSI) for CCITT applications, 1992

[5] ISO/IEC 9596 - 1, Information Technology - Open Systems Interconnection - Common Management Information Protocol Specification - Part 1: Specification, 1990

[6] W. Seo, "X.435 KT-EDI System Implem -entation," Proceedings of 1993 EDICOM, 1993, pp. 159-170

[7] P. Johnson, "Security and Security Management-Overview of Concepts, Standards Status and Some Current Issues," Proceedings of 1993 IEEE Network Operations and Management Symposium, 1992, pp. 670-679

[8] B. Studer, "Secure Network Management : Integration of Security Mechanisms into Network Management Protocols," Proceedings of 1994 IEEE Network Operations and Management Symposium, 1994, pp. 497-507

[9] Open Networking with OSI, A. Tang and S. Scoggins, Prentice Hall, 1992

[10] 윤이중, 이정현, 김대호, 이대기, "안전한 EDI 시스템 설계," 통신정보보호학회지, 제5권, 제4호, 95년 12월호, pp. 27-37

□ 著者紹介

권 태 경

1992년 2월 연세대학교 전산과학과 학사(이학사)
1995년 2월 연세대학교 전산과학과 석사(이학석사)
1995년 ~ 현재 연세대학교 컴퓨터과학과 박사과정 재학중

※주관심 분야 : 컴퓨터 통신망 보안, 암호학, PCS, 지능망 시스템, EDI 시스템

강 지 원

공군 학군 15기 임관
금오공대 전자공학과(공학학사)
1997년 2월 연세대학교 컴퓨터과학과 석사(공학석사)
1997년 ~ 현재 공군 작전사령부 전산실 근무

※ 주관심 분야 : EDI 시스템, ATM

윤 명 근

1973년생
1996년 2월 연세대학교 컴퓨터과학과 학사
1996년 ~ 현재 연세대학교 컴퓨터과학과 석사과정 재학중

※ 주관심 분야 : PCS 이동 관리, PCS 신호처리, EDI 시스템

송 주 석

1976년 2월 서울대학교 전기공학과 학사
1979년 2월 한국과학원 전기 및 전자공학과 졸업 석사
1988년 8월 Univ. of California at Berkeley 전산과학과 박사
1979년 2월 ~ 1982년 2월 한국전자통신연구원 전임연구원
1988년 9월 ~ 1989년 2월 Naval Postgraduate School Information System Department 조교수
1989년 3월 ~ 현재 연세대학교 컴퓨터과학과 교수

※ 주관심 분야 : 프로토콜 공학, ATM 통신망, 통신망 보안 등

강 창 구

1979년 2월 : 한국항공대학 항공전자공학과 졸업(공학사)
1986년 2월 : 충남대학교 대학원 전자공학과(공학석사)
1993년 충남대학교 대학원 전자공학과(공학박사)
1979년 ~ 1982년 : 한국공군 기술장교
1987년 ~ 현재 : ETRI 책임 연구원