# EDI 시스템의 정보보호 관리 모델링

○윤명근,* 권태경,* 송주석,* 강창구**
*연세대학교 컴퓨터과학과 정보통신연구실, **한국전자통신연구소

## Security Management Model for Electronic Data Interchange System

○Myungkeun Yoon,* Taekyoung Kwon,* Jooseok Song,* Chang-Goo Kang**
* Yonsei University, ** Electronics and Telecommunications Research Institute

**요 약**

본 논문에서는 EDI 시스템의 정보보호 관리를 위한 요구사항 및 기능을 정립하고, 관리 기능의 구현을 위한 정보보호 관리 모델을 설계한다. 정보보호 관리를 위해서는 ITU 권고안 X.700[4]의 OSI 정보보호 관리 영역을 확장하여, 권고안 X.800[2]의 관리 요구사항을 만족하도록 한다. 정보보호 관리 모델의 설계는 X.402 및 X.435[1]를 근간으로 설계된 한국통신의 KT-EDI를 기본 골격으로 하며[7], 본 모델에서는 관리의 안전성과 효율성을 제공한다.

## 1. 서론

정보 사회의 도래와 함께 기업체 혹은 국가 기관에서는 전자 문서를 서로 교환할 수 있는 정보통신 시스템을 구축하게 되었고, 이는 EDI라는 전자문서 교환 시스템의 등장을 이루게 되었다. EDI 시스템에서 주로 다루어지는 문서는 주문서, 계약서, 협정서 등 계약 당사자들 간에 이해 관계가 있는 중요한 정보뿐만 아니라 기업체간의 신용 및 거래에 관련된 내용이기 때문에 EDI 시스템에서 처리하는 메시지 내용을 안전하게 관리하는 것은 매우 중요한 문제라고 할 수 있다[13].

국내의 EDI 시스템 개발을 살펴보면 한국통신의 KT-EDI는 기본적인 시스템 구현을 국제 표준안에 따라 하였고 표준안에서 권고하는 정보보호 서비스를 위해서는 정보보호 기능 모듈을 별도로 개발 중에 있다. 이와 같이 안전성이 요구되는 정보보호 기능 모듈은 별도로 개발되거나 관리될 필요가 있다. 정보보호 기능 모듈을 별도로 관리했을 때에는 모듈의 갱신이나 사고 처리가 효과적이고 안전하게 이루어지므로 정보보호 관련 정보나 기능 모듈의 안전성을 향상시킬 수 있다는 장점이 있다.

본 논문에서는 정보보호 관리 영역을 관리 정보뿐만 아니라 정보보호 기능 모듈의 관리까지 확장하도록 한다. 이와 같은 관점에서 본 논문에서는 EDI 시스템의 정보보호 관리를 위한 모델을 설계한다. 먼저 2장에서는 EDI 관리에 관한 전반적인 사항을 검토하며 본 논문에서 제안하는 모델의 설계 목표를 설정한다. 3장에서는 ITU-T 권고안인 X.800을 근간으로

EDI 시스템을 위한 정보보호 관리 요구 사항을 정립하며 이 요구 사항을 만족하기 위한 관리 기능을 정의한다. 4장에서는 정보보호 관리 기능을 구현하기 위한 모델을 설계하며 정보보호 관리의 안전성과 효율성을 제공한다.

## 2. EDI 시스템 관리

본 장에서는 EDI 시스템 표준 및 개발에 대한 사항과 시스템 관리에 대해서 설명한다.

### 2.1 EDI 시스템

EDI는 전자문서 교환 시스템으로서 다양한 종류의 문서를 전자적으로 교환할 수 있도록 하기 위하여 메시지 시스템을 근간으로 개발되었다. ITU-T(구 CCITT)는 1984년에 저장후 전송(store-and-forward) 방식을 사용한 메시지 시스템의 권고안인 X.400을 발표하였으며, 이후 1988년부터는 ISO와 공동으로 권고안을 갱신하여 왔는데 현재는 X.400/1993이 발표되어있다. X.400의 부수적 권고안인 X.402에서는 MHS(Message Handling System)의 전반적인 구조를 다루고 있으며, X.435에서는 MHS를 기반으로한 EDI 시스템에 대해서 다루고 있다. 한편, 이 두 문서에서는 전자문서의 정보보호 서비스에 대해서도 권고하고 있다. EDI 시스템의 개발은 국내 및 국외에서 활발하게 진행되고 있으며, 기존의 X.25 기반 구현에서 탈피하여 TCP/IP를 기반으로 하는 인터네트까지 확산되고 있다.

한국통신에서는 이미 X.402 및 X.435를 근간으로한 KT-EDI 시스템을 개발하였으며[12], 한국전자통신연구소에서는 이 시스템에 정보보호 기능 모듈을 추가한 SEDI(Secure EDI) 시스템을 개발 중에 있다[11].

### 2.2 OSI 관리 영역

ITU-T 권고안인 X.700에서는 OSI(Open Systems Interconnection) 시스템들의 관리에 관한 프레임워크를 제시하고 있다. 이 권고안에서는 관리 기능을 설계할 때 기능별로 효율적인 설계를 할 수 있도록 관리 활동을 5개 영역으로 분류하고 있다[4]. 관리 영역에는 결함 관리, 구성 관리, 성능 관리, 계정 관리, 정보보호 관리 등이 있으며, 본 논문에서는 정보보호 관리 영역을 중심으로 EDI 정보보호 관리에 대해서 다루도록 한다.

### 2.3 EDI 시스템 정보보호 관리

앞에서 설명한 바와 같이 KT-EDI의 정보보호 서비스는 SEDI의 추가적인 기능 모듈을 통해서 이루어지는데, 이와 같이 방대한 전자정보 메시지와 시스템 정보 메시지를 취급하는 EDI 구조에서는 정보보호 모듈을 별도로 개발 및 관리할 필요가 있다. 이와 같은 시도는 상대적으로 민감한 정보보호 모듈의 갱신이나 사고 처리가 유연하게 이루어질 수 있을 뿐만 아니라, 보안 레벨과 같은 정보보호 관련 정보나 정보보호 기능 모듈의 안전성을 보다 높일

수 있다.

본 논문에서는 EDI의 나머지 4개 관리 영역과 정보보호 관리 영역을 분리하도록 하며, 특히 정보보호 관리를 위해서는 X.700의 정보보호 관리 영역을 확장하여 정보보호 기능 모듈들에 대한 나머지 4개 영역 기능을 포함하도록 한다.

## 3. 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 X.700의 정보보호 관리 영역의 기능을 확장하기 위하여 ITU-T 권고안인 X.800의 정보보호 관리 요구사항을 준수하도록 한다. 권고안 X.800은 개방형 시스템에서의 정보보호 구조에 대해서 기술하고 있다[2]. 그러나 이 권고안에서는 무엇을 해야하는가에 대해서만 다루고 있으며 어떻게 해야하는가에 대해서는 언급하지 않고 있다. 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 논문에서는 먼저 EDI의 정보보호 관리를 위해서 무엇을 어떻게 해야하는가를 정의한다.

### 3.1 EDI 시스템 정보보호 관리 요구사항

X.800은 OSI에 적용되는 정보보호 구조에 대해서 기술하고 있으며 정보보호 서비스와 메커니즘, 그리고 정보보호 관리에 대한 권고안을 포함한다. 본 논문에서는 X.800에 나와있는 권고안을 근간으로 EDI 정보보호 관리를 위한 구체적인 요구사항을 정립한다.

EDI 정보보호 관리의 목적은 EDI의 정보보호 기능을 유지 및 제어하기 위한 것이다. 이를 위해서는 정보보호 관련 정보의 수집 및 분배, 정보보호 서비스 및 메커니즘의 수행 상태 검사, 그리고 정보보호 관리 정책 실현이 필요하다.

● **정보보호 관련 정보의 수집 및 분배** : 정보보호 관련 사건에 관한 원격보고 및 기록, 그리고 정보보호 관련 정보를 유통한다.

● **정보보호 서비스 및 메커니즘의 수행 상태 검사** : 정보보호 기능의 수행 여부를 효율적으로 검사한다.

● **정보보호 관리 정책 실현** : 특정한 관리 정책에 따른 정보보호 서비스와 메커니즘의 개시 및 삭제를 한다.

X.800 권고안에 따라 EDI 정보보호 관리 요구사항을 네 가지 영역으로 나누었다. 네 가지 영역에는 시스템 정보보호 관리 영역, 정보보호 서비스 관리 영역, 정보보호 메커니즘 관리

영역 그리고 정보보호의 관리 영역이 있다.

**(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 메커니즘 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 메커니즘 등록 관리** : 가용 메커니즘의 활성화/비활성화 및 서비스 대 메커니즘의 연결 관리가 가능해야 한다.

**(3) 정보보호 메커니즘 관리**

정보보호 메커니즘 관리는 특정 정보보호 메커니즘에 대한 관리에 해당되며, X.402 및 X.435에 정의되어 있는 EDI 시스템을 위한 정보보호 서비스를 위해서 필요한 메커니즘들을 고려한다.

● **키 관리** : 키의 생성, 등록, 분배, 저장 그리고 폐기에 관련된 관리가 이루어져야 한다.

● **정보보호 메커니즘 등록 및 설정 관리** : 암호화, 디지탈 서명, 접근제어, 무결성, 인증 등의 메커니즘 모듈을 등록하고 유지할 수 있어야 한다.

**(4) 관리 정보의 보호**

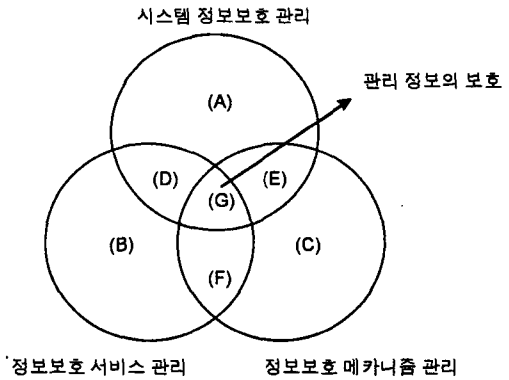
관리 정보의 보호는 관리 프로토콜, 특히 정보보호 관리에 관한 정보의 보호 측면과 관련되며 타 관리 정보와의 일관성 및 타 관리 정보의 보호 측면도 포함한다.

● **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 3.2절에서는 이를 만족하기 위한 관리 기능을 정의하도록 한다.

## 3.2 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 관리자(manager) 모듈과 에이전트(agent) 모듈로 구성되어야 한다.




[그림 1] 정보보호 관리 기능 영역도

위의 [그림 1]은 X.800을 근간으로 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 메커니즘 관리 그리고 관리 정보의 보호 등의 4개 영역을 대영역이라고 부르고, (A)에서 (G)의 영역을 소영역이라고 부른다. 소영역은 관리 기능 대 요구사항을 세밀하게 표현하기 위해서 정의하였으며, 따라서 (A)에서 (C)는 각 영역에만 해당하는 기능을, 그리고 (D)에서 (F)는 2개 영역에 중복되는 기능을 나타낸다. 또한 (G)는 3개 영역에 모두 해당되는 사항으로서 관리 정보의 보호 영역의 요구사항을 만족하기 위한 관리 기능이 여기에 해당된다. 각 영역에 해당되는 기능은 [표 1]에서와와 같이 정의된다.

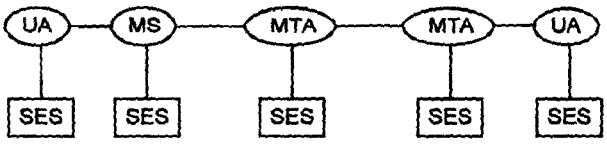
| 영역 | 기능 |
|---|---|
| (A) | 1. 결함 상태와 감사 추적 검사를 위한 폴링(Polling) 및 폴링 간격 수정<br>2. 폴링 대상 모듈 선택<br>3. 원격지에서 수집 및 보고될 결함의 종류 선택<br>4. 정보보호 침해의 기록 및 보고의 관련된 임계값 수정 |
| (B) | 1. 정보보호 서비스의 등록 및 갱신<br>2. 정보보호 서비스의 개시 및 폐지<br>3. 분류된 서비스 프로파일의 설정 및 수정<br>4. 결함 및 정보보호 침해를 발견하기 위한 정보보호 서비스 폴링 |
| (C) | 1. 정보보호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

[표 1] EDI 정보보호 관리 기능

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. 다음 장에서는 EDI 시스템에서 정보보호 관리 시스템 모델을 설계하도록 한다.

## 4. EDI 정보보호 관리 모델 설계

본 장에서는 앞에서 정의한 EDI 정보보호 관리 요구사항과 기능을 근간으로 하여 EDI의 정보보호 관리 시스템을 설계한다. 설계를 위한 기본 EDI의 구조는 KT-EDI에 정보보호 기능을 추가한 SEDI를 기본 골격으로 한다. 따라서 시스템 구조상의 기본적인 용어는 SEDI에서 정의한 것을 사용하기로 한다. 이미 설명한 바와 같이 SEDI는 X.400에 따라 구현된 기본적인 EDI 시스템인 KT-EDI 구조에 X.402 및 X.435에서 권고하는 정보보호 서비스 기능을 추가한 EDI 모델이다. 따라서, SEDI에는 정보보호 서비스 기능을 수행하기 위한 모듈이 각 MHS 요소에 추가되어 있으며 이것을 SES(Secure EDI Subsystem)라고 한다. 즉, SES는 정보보호 모듈로서 각 MHS 요소에서 정보보호 서비스를 제공한다. SES가 제공하는 서비스는 비밀성, 무결성, 인증, 접근 제어, 부인 봉쇄, 디지털 서명 등의 일반적인 서비스 영역으로 구분할 수 있다. SEDI의 구조를 도시하면 다음 그림과 같다.

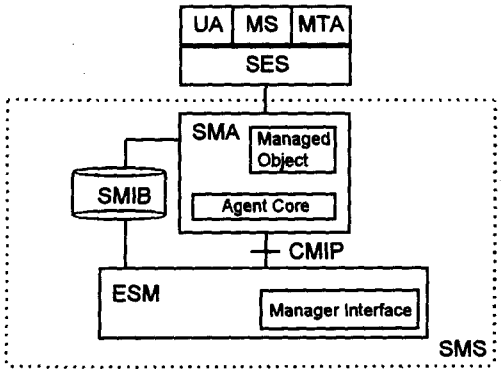



[그림 2] SEDI의 구조

기본적인 MHS 요소에는 UA(User Agent), MTA(Message Transfer Agent), 그리고 MS(Message Store)가 있으며, 각 요소에 SES가 추가된 것이 SEDI이다. UA는 사용자를 위해 메시지(전자 우편)를 처리하거나 생성하는 기능을 수행한다. MTA는 네트워크 상에서 메세지를 전달하는 역할을 한다. MS는 메시지를 저장하는 기능을 수행한다. SES는 각각의 MHS 요소들에게 X.402와 X.435에 나와있는 정보보호 기능을 제공한다.

### 4.1 정보보호 관리 시스템의 구조

정보보호 관리 시스템은 SMS(Security Management System)라고 호칭하며 다음 그림에서와 같이 관리자-에이전트 구조를 갖는다. SMS는 각 MHS 요소의 SES에 대하여 정보보호 관리를 수행한다. ESM(EDI Security Manager)은 관리자 모듈로서 관리자의 명령을 해당 SMA(Security Management Agent)에 전달하거나 SMA로부터 수집한 정보를 바탕으로 3장에서 정의한 기능들을 수행한다.




[그림 3] 정보보호 관리 시스템의 구조

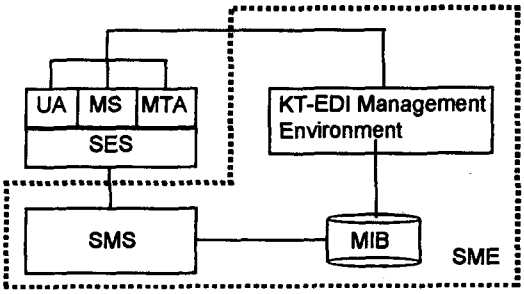
[그림 3]에서와 같이 ESM과 SMA는 관리 시스템의 기본 구조인 관리자-에이전트 관계를 이루고 있다. SMA는 SES의 각 기능모듈의 상태와 SMA 자체의 상태에 대해서 관리객체(managed-object: MO) 형태로 정보를 보관한다. SES 상태에 대한 질의나 SES 변경 정보는 ESM에서 SMA로 전달된다. SMA와의 인터페이스 프로토콜로는 CMIP(Common Management Information Protocol)[6]을 사용하도록 한다. 그러나 CMIP을 이용한 구현을 위해서는 X.25상에서 구현된 EDI 시스템이 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 Management 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 메커니즘과 서비스는 다음과 같다.

● **메커니즘** : 암호화 알고리즘, 디지털 서명 알고리즘, 해쉬함수, 실체 인증 메커니즘, 감사 추적 메커니즘, 키관리 메커니즘

● **서비스** : 데이터 비밀성, 데이터 무결성, 부인 봉쇄, 발신 인증, 책임 인증

### 4.2 정보보호 관리 시스템을 포함하는 EDI 관리 환경

정보보호 관리 영역을 제외한 KT-EDI의 나머지 관리 영역, 즉 결함 관리, 구성 관리, 계정 관리 그리고 성능 관리에 관한 기능 또한 OSI 관리 표준안을 지향하며, 관리자-에이전트 구조로 관리가 행해져야 한다. 따라서 본 연구에서 설계하고 구현하는 정보보호 관리 시스템과 구성면에서 같으며 다음 그림과 같이 나머지 관리 환경과 정보보호 관리 시스템 환경을 묶을 수 있다. 이것을 SME(SEDI Management Environment)라고 부른다.




[그림 4] SME의 구조

SME는 기존의 KT-EDI 관리 환경과 정보보호 관리 시스템 환경이 병합되어 OSI 관리의 표준 기능을 지향하고 있다. 본 구조에서는 2장에서 설명한 바와 같이 정보보호 관리의 효율성과 안전성을 위해서 정보보호 관리는 기타 나머지 관리 영역과 분리되어 이루어진다.

## 5. 결론

본 논문에서는 EDI 시스템의 정보보호 관리를 위한 모델을 설계하였다.

먼저 EDI 관리에 관한 전반적인 사항을 검토한 후 제안하는 관리 모델의 설계 목표를 설정하였다. 이어서 권고안 X.700의 정보보호 관리 기능 영역을 확장하여 권고안 X.800에서 정의하는 개방 시스템 정보보호 관리 요구 사항을 근간으로 EDI 정보보호 관리 요구 사항을 정립하였다. 또한 이 요구 사항을 만족하기 위한 관리 기능을 정의하였으며, 정의된 정보보호 관리 기능을 구현하기 위한 모델을 설계하였다. 설계한 모델에서는 EDI 정보보호 관리의 안전성과 효율성을 제공한다.

향후 연구에서는 기타 관리 영역과의 상호작용 문제에 대해서 다루어야 하며, 완전한 관리 시스템의 구현이 이루어져야 할 것이다.

## Acknowledgement :

현재 한국전자통신연구소는 연세대학교 및 충북대학교, 덕성여자대학교, 대전대학교와 공동으로 SEDI 정보보호 관리 시스템인 SMS를 개발 중에 있다. SMS의 핵심 모듈인 감사 관리 모듈과 키 관리 모듈의 프로토타입은 이미 구현 완료 단계에 있으며, 전체 관리 모듈을 총괄하는 SMS의 프로토타입은 검토 단계에 있다.

## References :

[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 applications, 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 10040, Information Technology - Open Systems Interconnection - System Management Overview, 1991

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

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

[8] 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

[9] 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

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

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

[12] 강창구, "EDI 정보보호기술," NETSEC-KR'96, 1996, pp. 421-436

[13] 정보보호 서비스 제공을 위한 안전성 서버 개발, 1995년 12월, 한국전자통신연구소