SEDI의 정보보호 서비스 모듈 관리 시스템 설계

○강지원,* 권태경,* 송주석,* 강창구**
*연세대학교 컴퓨터과학과, **한국전자통신연구소

Design of Management System for Secure EDI Subsystem

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

요 약

본 논문에서는 ITU-T X.800 권고안의 요구 기능을 중심으로 SEDI(Secure EDI) 시스템의 정보보호 서비스 모듈들을 관리하기 위한 시스템 구조를 설계하였다. 관리자인 ESM(EDI Security Management) 모듈과 관리 대행자인 SMA(Security Management Agent) 모듈을 새롭게 설계하였다. 특히, ESM과 SMA 간의 관리 정보의 교환때문에 전체적인 성능 저하가 발생하지 않도록 SMA에 필터링 기능을 제안하였다.

1. 서론

컴퓨터와 통신 기술의 급속한 발전에 따라 최근 기업 또는 공공기관 사이에는 정보 교환을 기존의 문서에 의한 전달 방법에서 탈피하여 컴퓨터를 통한 전자적인 문서 교환 체계로 바꾸고자 하는 요구가 점차 증가하고 있다. 이러한 역할을 수행하는 시스템이 바로 전자 문서 교환 시스템(Electronic Data Interchange: EDI)이다. 현재, EDI 시스템은 주로 무역 및 금융 분야에서 이용되고 있는데 이 분야에서 사용되는 문서는 계약 당사자들간에 이해 관계가 있고 기업체간의 신용 및 거래에 관련된 주문서, 계약서, 협정서 등이다. 따라서, EDI 시스템에서 처리하는 메시지 내용을 의도적이거나 비의도적인 위협으로부터 안전하게 관리하는 것은 매우 중요한 문제라고 할 수 있다.

최근 한국통신에서 개발한 표준 EDI 시스템(KT-EDI)에 X.402 및 X.435에서 권고하는 정보보호 서비스 기능을 제공하도록 하기위해 국내의 한 연구기관에서는 정보보호 기능 모듈들을 별도로 개발중에 있다. 이와 같이 정보보호 기능 모듈들을 추가한 KT-EDI 시스템을 SEDI(Secure EDI) 시스템이라고 부른다.

본 논문에서는 SEDI 시스템의 정보보호 서비스 모듈을 관리하기 위한 시스템을 ITU-T X.800 권고안에서 정의하는 정보보호 요구사항에 따라 설계하였다. 이어지는 2장에서는 SEDI 시스템에 대한 개요와 함께 정보보호 관리 구조에 대해서 표준안을 근간으로 설명하

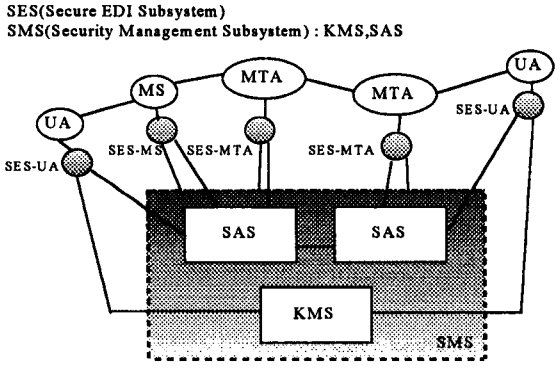
며, 3장에서는 정보보호 서비스 모듈 관리 시스템의 전체적인 구조를 설계한다. 4장에서는 관리 시스템의 세부 모듈 구조에 대해서 설명하도록 한다.

2. SEDI 시스템 및 관리 구조

이 장에서는 KT-EDI에 정보보호 모듈이 첨가된 SEDI 시스템에 대해 살펴보고 X.800과 M.3000 시리즈의 정보보호 요구 기능을 만족하는 안전하고 효율적인 정보보호 관리 구조를 제시한다.

2.1 SEDI 시스템 개요

한국통신에서는 ITU-T X.400 시리즈의 통신 표준과 UN/EDIFACT의 문서 표준을 근간으로 KT-EDI 시스템을 개발하였다. KT-EDI는 EDI의 기본 구성요소인 UA(User Agent), MS(Message Store), MTA(Message Transfer Agent)로 이루어진다. UA는 사용자를 위해 메시지(전자 우편)를 처리하거나 생성하며, MS는 메시지를 저장하는 기능을 수행한다. 또한 MTA는 네트워크상에서 다른 MTA나 자신의 영역내의 UA에게 메시지를 전달하는 역할을 한다. SEDI 시스템은 각 구성 요소들에 위치하여 정보보호 서비스를 제공하는 SES(Secure EDI Subsystem) 모듈과 이 SES 모듈들을 관리하는 SMS(Security Management Subsystem) 모듈로 구성되어 있다. [그림 1]은 정보보호 서비스를 제공하는 SEDI 시스템의 전체적인 구조를 나타낸다.



[그림 1] SEDI 시스템 구조

SEDI 시스템은 정보 보호 서비스를 제공하기 위해 KT-EDI 시스템의 UA, MS, MTA 각각에 SES 모듈들을 추가하고 이들을 관리하는 SMS를 추가한 시스템이다. SES는 EDI

시스템에서 제공해야 하는 정보 보호 서비스를 처리하는 주 기능을 담당한다. SES는 UA, MS, MTA 각각의 구성요소들에 위치하며, 각 구성 요소는 SES 인터페이스를 이용하여 해당 서비스의 요청을 수행한다. SMS는 SES에서 정보 보호 서비스를 처리하는 과정에서 필요한 정보의 제공 및 저장 기능을 수행한다. SMS는 정보 보호 서비스를 처리하기 위해 필요한 키의 생성, 분배, 관리 및 보증서 관리를 담당하는 키 관리 시스템(Key Management System:KMS)과 각 구성 요소들에서 발생한 정보 보호 관련 사건들을 저장하고 필요시 검색할 수 있도록 하는 정보보호 감사 시스템(Security Audit Subsystem:SAS)으로 구성된다..

2.2 정보보호 관리 구조

정보보호 관련 모듈은 대개 높은 안전성을 요구하는 정보를 다루기 때문에 다른 모듈들과는 별도로 개발되고 관리될 필요가 있다. SEDI 시스템은 KT-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 다섯가지 영역으로 구분한다. 그러나 여기서 정의하는 정보보호 관리 기능은 정보보호 경보 보고, 보안 감사 추적, 접근 제어 등의 기능만을 포함하고 있다.

따라서 SEDI의 정보보호 서비스 모듈에 대한 전체적인 관리를 위해서는 개방형 시스템에서의 정보보호 구조에 대한 권고안인 ITU X.800을 근간으로 하여 새로운 정보보호 관리 구조를 설계할 필요가 있다.

X.800 권고안에서는 정보보호 관리의 범주를 시스템 정보보호 관리, 정보보호 서비스 관리, 정보보호 메카니즘 관리, 관리정보의 보호 등과 같이 네 가지로 구분하고 있다. 이와 같은 정보보호 관리 구조에서는 정보보호 서비스 제공 모듈에 대한 정보보호 관리에만 국한시키지 않고 X.700에 나와 있는 계정관리와 구성관리 기능도 수행할 수 있다.

3. 정보보호 서비스 모듈 관리 시스템

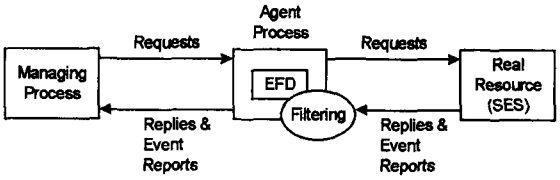
본 장에서는 SEDI 시스템 정보보호 서비스 모듈 관리를 위한 시스템의 구조에 대해서 다루도록 한다.

3.1 관리 모델 기본 구조

개방형 시스템에서 일반적인 관리 모델은 관리자(Manager)와 관리대행자(Agent) 구조로 구성된다. 본 논문에서는 이와같은 관리 시스템의 기본 구조를 바탕으로 [그림 2]에서와 같이 관리 모델을 설정한다.

관리자는 관리자 모듈에서 제공하는 GUI(Graphical User Interface) 환경에서 실제 자원인 SES 모듈을 관리한다. 그러나 관리자 모듈은 직접 SES 모듈을 관리하도록 하는 것이

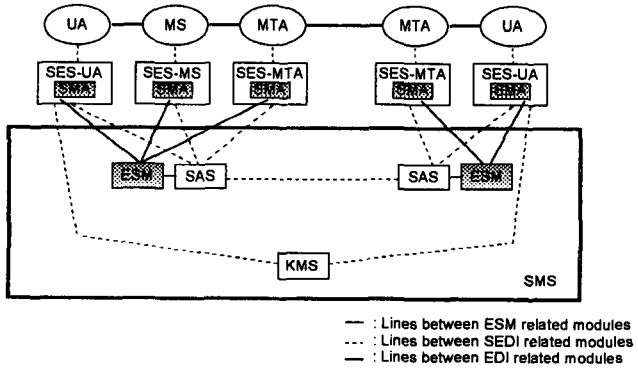
아니라 관리 대행자 모듈을 통해서 관리하게 된다. 이 때 관리자 모듈에서 관리 대행자 모듈로 전달되는 명령은 관리 기능 처리 요구에 해당하며, 관리 대행자에서 관리자 모듈로 전달되는 정보는 요구에 대한 응답이나 사건 보고에 해당한다.



[그림 2] 관리 모델 개념도

하나의 관리자 모듈이 많은 관리 대행자 모듈들과 메시지 교환을 할 경우, 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 사건 전송 분류기(Event Forwarding Discriminator:EFD)가 관리자가 정한 필터링 기준에 따라 발생하는 사건들에 대한 분류를 하고, 이 중 특정한 사건들에 대해 관리자에게 보고되지 않도록 하는 것이다. 이 때 필터링의 기준은 메시지의 종류와 네트워크 상황에 따라서 관리자가 임계치를 임의로 조정해 줄 수 있다.

3.2 관리 시스템 구조



[그림 3] 관리 시스템 전체 구조도

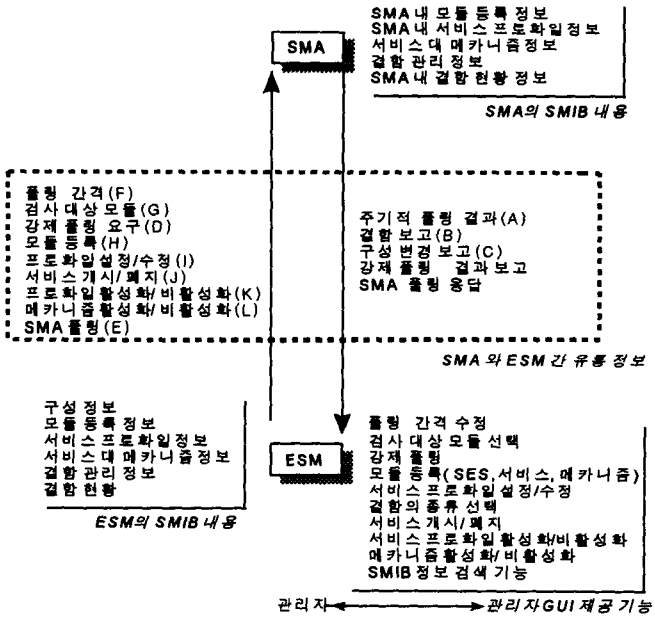
앞에서 언급한 관리 모델 기본 구조를 바탕으로 SEDI의 SES 모듈 관리 시스템을 설계한다. SES 관리 시스템은 X.800 권고안을 근간으로 하므로 SES의 각 모듈에 대한 관리와 함께 전체 EDI 시스템의 정보보호 관리 기능을 제공한다.

[그림 3]과 같이 정보보호 관리 기능을 위해서 설계되어 있는 SEDI의 SMS 영역에서 관리자 모듈인 ESM(EDI Security Management) 모듈을 두고, SES 모듈에 관리대행자 모듈인 SMA(Security Management Agent) 모듈을 두는 구조를 한다. 또한 ESM 모듈은 감사 관리와 키 관리를 위해서 설계된 SAS와 KMS 모듈과 연동하도록 한다.

따라서 ESM 모듈은 각 MTA마다 하나씩 존재하며, 해당 영역내의 SES 모듈들과 연결된 SMA를 통해서 실제 SES 모듈을 관리한다. SMA 모듈은 SES 모듈의 하부 단위 모듈에 위치하여 SES 모듈들을 관리하며, EFD를 통해 관리 정보를 필터링하여 자신의 데이터 베이스에 저장하고 필요시 ESM 모듈로 보고한다. ESM과 SMA의 상세 구조에 대해서는 4장에서 설명하도록 한다.

3.3 관리 정보 정의

ESM과 SMA는 다양한 관리 정보를 서로 교환하게 된다. 이것을 관리자 GUI 환경에서 제공하는 기능과 함께 도시하면 다음의 [그림 4]와 같다.

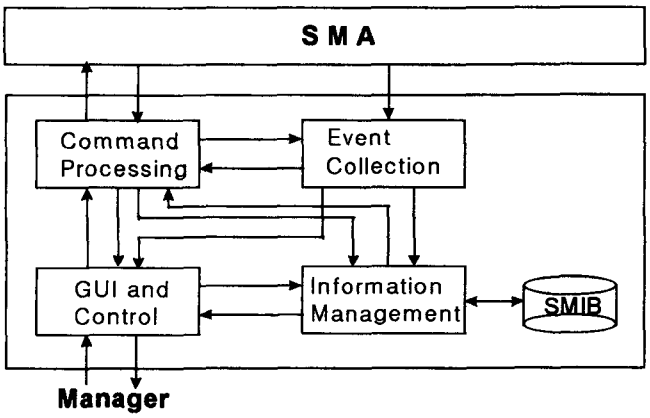


[그림 4] ESM-SMA의 관리 정보 및 관리자 GUI 기능

4. ESM 및 SMA 설계

4.1 ESM 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 5]와 같이 GUI 제어 기능부, 사건 수집 기능부, 데이타 관리부, 명령 기능부로 구성되어 있다.



[그림 5] ESM 기능 구조도

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.

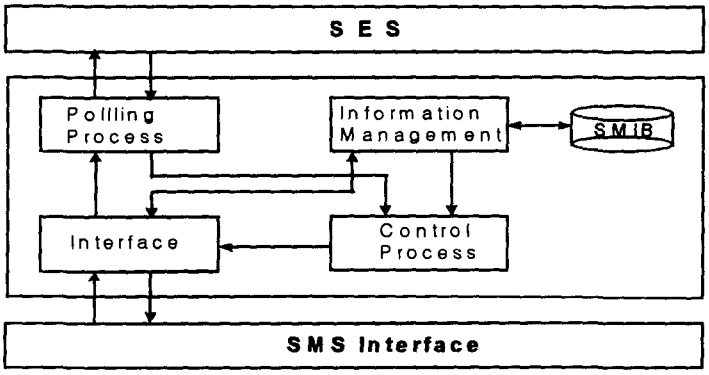
데이터 관리부는 논리적 관리 정보 저장소인 SMIB를 관리한다. GUI 제어 기능부와 명령 기능부로부터 해당 관리 정보의 등록, 갱신, 삭제를 의뢰받아 관리를 수행한다. SMIB에 저장되는 관리 정보의 유형은 구성 정보, 모듈 등록 정보, 서비스 프로화일 정보, 서비스 대메커니즘 정보, 결함 관리 정보, 결함 현황 정보 등이 있다.

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

4.2 SMA 구조

SEDI의 정보보호 서비스 모듈(SES)을 관리하기 위한 관리 대행자인 SMA 모듈은 [그림 3]에서와 같이 SES의 하부 단위모듈로 위치한다. SMA는 관리자의 요청에 의한 관리 동작과 관리자원의 상태 변화를 감시하여 얻은 관리 정보를 ESM에게 보고하는 기능을 수행한다. SMA와 ESM 모듈은 CMIP과 SNMP 등의 표준 통신 프로토콜을 통하여 관리 정보를 교환하며, SES의 내부 단위 모듈과는 IPC 메커니즘(pipe) 혹은 파라메타 전달을 통하여 통신한다.

SMA의 기능 구조는 [그림 6]과 같이 제어 기능부, 인터페이스 기능부, 데이타 관리부, 폴링 기능부 등의 네 가지 기능으로 구성된다.



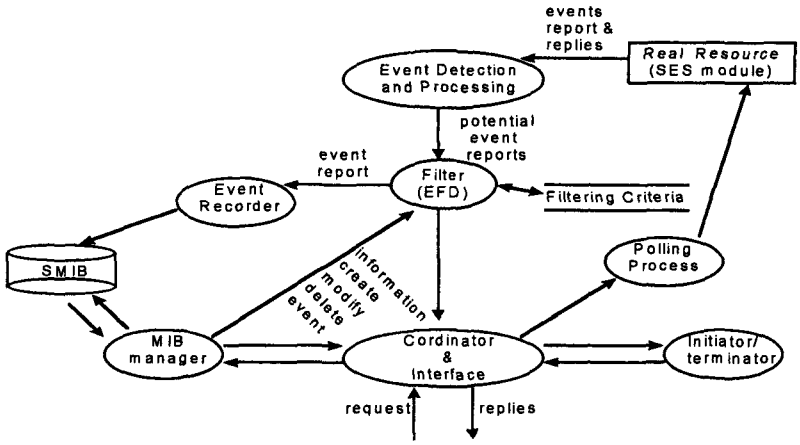
[그림 6] SMA의 기능 구조도

(1) 제어 기능부

제어 기능부는 [그림 7]과 같이 SMA의 전체적인 기능 제어 및 조정 기능과 사건 분류 및 전송 기능을 담당한다. 사건 분류 및 전송 기능은 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 종료(initiator/terminator)와 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.



[그림 7] SMA 세부 기능 구조도

(3) 데이터 관리부

데이터 관리부는 SMA에 저장되는 지역 SMIB의 관리를 담당한다. ESM의 등록, 검색, 갱신, 삭제 요청을 받아 자신의 SMIB로 관리 동작(MIB managing)을 수행한다. 또한, 제어 기능부에서 필터링된 사건 보고들를 저장(event recorder)하며 관리자의 필터링 기준을 등록 및 갱신하는 기능 등이 포함된다. 지역 SMIB에 관리되는 정보는 모듈 등록 정보, 서비스 프로화일 정보, 서비스 대 메커니즘 정보, 결함 관리 정보, 결함 현황 정보 등이 있다.

(4) 폴링 기능부

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

4.3 SMA 필터링 시나리오

(1) 시나리오 환경 설정

본 논문에서 설계한 SMA의 모델은 주기적 폴링에 대한 응답과 SMIB 정보 관리에 따른 부가적인 관리 정보들을 필터링하도록 설계하였다. 이 설계 모델에 대한 필터링을 전형적인 SNMP 환경에서 매 15분마다 한 번씩 관리자원들의 상태를 폴링하는 시스템으로 가정한다. 그리고 관리자와 관리 대행자 간에는 LAN으로 구성되어 있으며, 내부 메시지 처리 시간이 50 ㎳이고 네트워크 지연이 1 ㎳라고 가정한다.

또한, 앞의 [그림 4]에서 정의한 관리 정보 메시지가 1일 동안 평균적으로 [표 2]와 같이 형태별로 발생하고 이에 대한 필터링 기준도 아래의 [표 1]과 같다고 가정한다. 여기서 필터링 기준은 카운터에 의한 임계값을 지정하는 방법을 사용한다.

관리 정보	A	B	C	D	E	F	G	H	I	J	K	L
발 생 수	96	5	5	24	24	5	4	4	4	4	4	4
필터링 기준	(1,2,E)	(1,1,E)	(1,2,E)	(1,1,E)	(1,1,E)	(1,0,D)	(1,0,D)	(1,1,E)	(1,1,E)	(1,1,E)	(1,1,E)	(1,1,E)

[표 1] 1일 관리 정보 발생 수 및 필터링 기준표

(2) 시나리오 결과

관리 정보 형태			A	B	C	D	E	F	G	H	I	J	K	L	계
필 터 통 과 율			1/2	1	1/2	1	1	0	0	1	1	1	1	1	
필터링 후의 사건 보고의 수			48	5	2.5	24	24	0	0	4	4	4	4	4	123.5
실행시간 ~ms~	필 터 미사용	Manager 폴 링	19392	1010	1010	4848	4848	1010	808	808	808	808	808	808	36966
		Agent 폴 링	9696												27270
	필 터 사 용	Manager 폴 링	9696	1010	505	4848	4848	505	404	808	808	808	808	808	25858
		Agent 폴 링	4848												21008

[표 2] 사건 보고의 수 및 실행시간

사건 보고의 수는 주어진 필터링 기준에 따라 필터링을 한 후의 경우가 필터링을 전혀 하지 않았을 경우의 사건 보고의 수보다 1일 평균 약 59.5개를 감소시킨다. 또한, 이에 따른 관리자와 관리 대행자 간의 사건 보고 요청 및 응답을 위해 걸리는 실행시간은 필터링을 하는 경우가 필터링을 하지 않을 경우보다 더 우수하다. 그리고 주기적인 폴링을 관리자 주도로 하는 방법보다 관리 대행자가 지정한 시간에 스스로 하는 방법이 다소 실행시간을 줄여준다. 필터링을 사용하고 관리 대행자에 의한 주기적 폴링을 실시하는 경우가 가장 빠른 실행시간을 갖는다. 그러나, 이와 같이 관리자와 관리 대행자 간의 주고받는 정보의 수를 감소시켜 관리 성능을 높이는 대신에 사건 보고의 차단으로 인해 관리자의 MIB를 갱신할 수 없기 때문에 관리자가 관리를 원하는 어느 시점에서 어떤 사건의 결과에 대해 자신의 MIB에 저장된 이전의 내용을 참고할 수도 있다.

5. 결론

본 논문에서는 SEDI 시스템에 대한 전반적인 개요와 함께 정보보호 관리 구조에 대해서 X.800 권고안을 근간으로 설명하였다. 또한, 이를 바탕으로 정보보호 서비스 모듈 관리 시스템의 전체적인 구조와 관리자(ESM) 모듈과 관리 대행자(SMA) 모듈의 세부 구조와 기능들을 설계하였다. 특히, 관리 대행자는 정상적인 폴링 결과나 중요하지 않은 사건 보고들을 관리자가 제한하도록 설계하였다.

본 논문에서 제안하는 설계 구조는 이미 감사관리모듈(SAS)과 키관리모듈(KMS)을 포함하고 있는 SMS를 바탕으로 설계하였으며, 향후 이 모듈들과의 상호작용 문제도 고려하여야 할 것이다.

[참고 문헌]

[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] Lee Labare, "Management By Exception: OSI Event Generating, Reporting, and Logging," Proceedings 2nd International Symposium on Intergrated Network Management, 1991, pp. 227-242.

[6] Amatzia Ben-Artzi, "Network Management of TCP/IP Networks: Present and Future," IEEE Network Magazine, July. 1990. pp. 35-43.

[7] Young-Chul Shim, "Developing Managed System in a Telecommunication Management Network," International Conference on Communications vol. 1, June. 1996. pp. 17-21.

[8] Bruno Studer, "Secure Network Management - Integration of Security Mechanism into Network Management Protocols," INFOCOM, 1994.

[9] 정보보호 서비스 제공을 위한 안전성 서버 개발, 1995년 12월, 한국통신연구소