EDI 보안 감사 추적 서비스 시스템 구현

정 경 자[†] · 김 기 중[†] · 서 경 란[††] · 류 근 호[†††] · 강 창 구[††††]

요 약

본 논문은 기업간의 표준화된 서식에 의해 거래 정보를 전달하는 전자 문서 교환 시스템(EDI)에서 발생할 수 있는 법적 분쟁을 해결하기 위한 보안 감사 추적 서비스 시스템을 구현하였다. 구현된 EDI 보안 감사 추적 시스템은 X.400 및 X.435에 정의한 보안 감사 요구사항과 보안 서비스 프로토콜을 충족한다. 본 연구의 EDI 보안 감사 시스템의 구성 모듈은 사건 분류기, 감사 기록기, 감사 이력 저장기 그리고 감사 제공기로 구성된다. 사건 분류기는 EDI 망을 통해 전달된 정보를 감사 서비스별로 분류한다. 감사 기록기는 사건 분류기에 의해 분류된 감사 정보를 사건이 발생된 시간 정보와 결합하여 색인을 구성하며 감사 이력 저장기는 시간이 흐름에 따라 증가된 감사 정보를 버퓨밍하는 기능을 한다. 마지막으로 감사 제공기는 저장된 감사 정보를 이용하여 감사 서비스를 제공해 주는 역할을 하는 모듈이다. 감사 제공기는 부인 봉쇄 서비스, 증명 및 검증 서비스, 보안 관리 서비스, 그리고 자료 접근 서비스 등을 제공하도록 하였다. 본 EDI 보안 감사 추적 서비스 시스템은 감사 정보에 발생 시간을 색인으로 감사 정보를 구축하므로 시간 색인을 통해 보다 빠르게 감사 정보를 제공할 수 있다.

Implementation of Audit Trail Service System for EDI Security

Kyeong Ja Jeong[†] · Ki Jung Kim[†] · Kyong Ran Seo[††] · Keun Ho Ryu[†††] · Chang Gu Kang[††††]

ABSTRACT

In this paper, we implement the Audit Trail Service System for the EDI Security. It has solved a law dispute between enterprises by informations that have generated by the EDI service system. The audit trail service system implemented for EDI security satisfies the requirements of audit and the protocol of the security service of X.435 and X.400. The EDI Security Audit System consists of the event discriminator, the audit recorder, the audit archiver, and the provider of audit services. The event discriminator classifies the transmitted data from the EDI network to audit services. The audit recorder constructs an index that has combined time information with audit informations which are classified by the event discriminator. The audit archiver performs the vacuumming of added audit informations by passing time. The audit provider is a module that carries out the audit trail services by using stored audit informations. The audit provider supports audit servies, which are non-repudiation, proof and probe, controller of security, and accessing information. The audit trail service system for EDI security constructs audit information by using index that is combining time information, so it supports especially fast accessing audit information.

※본 연구는 1996년 한국전자통신연구소의 연구비 지원으로 수행되었음.

† 준 회 원:충북대학교 컴퓨터과학과
†† 정 회 원:한국통신기술 첨단통신사업실
††† 종신회원:충북대학교 컴퓨터과학과
†††† 정 회 원:한국전자통신연구원

논문접수:1996년 7월 4일, 심사완료:1997년 1월 7일

1. 서 론

컴퓨터 통신의 급속한 보급과 확대로 많은 정보들이 통신망을 통해 처리되고 있다. 컴퓨터 통신의 파급은 통신을 통해 신속하고 간편하게 많은 서비스를 제공받을 수 있지만 정보 노출, 정보의 손실 및 변경 등의 문제가 발생할 수 있다. 그러므로 컴퓨터 통신의 확대와 비례하여 정보의 보안 문제도 그 비중이 증가되어야 한다. 전산망을 통한 전자 정보 처리시 보안 서비스는 기본적인 요소가 되어야 하며 보안 서비스시 발생되는 정보는 이용자간의 분쟁에 대비하여 보안 서비스 정책의 한 영역인 보안 감사 서비스 시스템에서 감사 정보로 구축되어야 한다[12, 15, 16].

컴퓨터 통신을 이용하여 기업간의 표준화된 서식에 맞추어 정보를 교환하는 전자 문서 교환 시스템인 EDI (Electronic Data Interchange)와 같은 상거래 정보를 취급하는 시스템에서는 정보 보안 서비스의 한 영역으로 보안 감사 서비스 시스템이 기본적으로 포함되어야 한다[3, 7]. EDI의 보안 감사 추적의 종류는 실시간 감사와 일괄처리 감사가 있다. 실시간 감사는 EDI 시스템 운용시 시스템을 저해하는 요인을 감지하여 즉시 경고 조치를 취하는 감사이다. 일괄처리 감사는 보안 서비스가 이루어지는 동안 감사 대상이 되는 자료를 발췌하여 향후 EDI 이용자간에 분쟁이 발생하였을 경우 이를 해결하기 위한 감사가 된다.

본 논문은 일괄처리 EDI 보안 감사 추적 서비스 시스템을 구축하는 것이다. 이 시스템은 EDI 이용자간에 분쟁이 발생할 경우 저장된 감사 정보를 이용한 감사 시스템이다. 보안 감사 추적 서비스는 부인 봉쇄서비스, 증명 및 검증 서비스, 보안 관리 서비스 그리고 자료 접근 서비스로 정의한다. 이 서비스는 ISO 개방형 통신 모델에서 EDI 시스템을 위한 보안 서비스인 인증(Authentication), 접근제어(Access Control), 무결성(Integrity), 보안 감사 추적(Security Audit Trail), 데이터 비밀성(Confidentiality), 키관리(Key Management)의 한 요소로 사용자에게 EDI 메시지의 전송 현황에 대한 보안 정보를 제공해 준다[4, 5]. 즉, 정보 교환에 따르는 중요한 상황과 전송한 메시지가 수신자에게 정확하게 도착하였는지의 여부, 실제로 수신자가 메시지를 접수하였는지 등에 관한 정보를 사용자에게 제공해 준다.

EDI 보안 감사 추적 서비스을 위한 시스템 구성 모듈은 사건 분류기, 감사 기록기, 이력 저장기, 그리고 감사 제공기로 구성된다. 감사 분류기는 EDI 망을 통해 전달되는 정보 중에서 감사에 필요한 정보만을 발췌하고 이들 정보를 감사 서비스별로 분류하여 감사 저장기에 전달한다. 감사 저장기는 감사 분류기에 의해 전달된 감사 정보를 감사 제공기에 의해 제공되는 서비스를 기준으로 시간과 기본키에 대한 색인을 구성한다. 감사 이력 저장기는 EDI에서 발생된 많은 자료를 보다 빠르고 효율적인 자료 접근을 위해 시간이 경과된 자료를 대용량의 기억장치로 이동시키는 버퍼링을 처리하는 모듈이다. 그리고 감사 제공기는 저장된 감사 정보를 통해 보안 감사 추적 서비스를 수행한다.

본 논문의 구성은 다음과 같다. 2장에서는 EDI 보안 분류로 감사 서비스를 정의하기 위한 보안 위협 요소와 EDI 보안 서비스를 살펴 본다. 3장에서는 시간 개념과 EDI 감사 추적 시스템에서 시간 정보의 적용을 설명하고 4장에서는 EDI 감사 추적 서비스 시스템을 위한 감사 서비스를 정의하고 이를 바탕으로 5장에서는 시스템 구현에 대한 내용을 다루며 마지막으로 결론을 맺는다.

2. EDI 보안 분류

2.1 감사 서비스와 EDI 위협 요소

감사 서비스란 거래로부터 관련된 레코드나 보고서의 추적 또는 레코드나 보고서로부터 원시 거래 자료를 추적하기 위해 선택적으로 제공하는 문서적인 근거 레코드의 집합을 정의한다.

감사 서비스는 거래(transaction)가 이루어졌을 때 어떤 사용자(which user)가 무슨 자원(what resource)을 어느 정도의 양(how much)을 사용하였는 지에 대한 로깅(logging)개념에서 출발하였다. 최근의 감사 개념은 사용자나 프로세서가 어떤 일반적이거나 또는 중요한 객체에 대해 접근하는 상황의 기록 및 검사나 보안 기법을 우회하려는 불법적 시도를 기록하여 불의의 상황에 대처할 수 있는 근거를 제공해 줄 수 있는 정보시스템의 보안개념 및 접근추적의 개념으로 확대되었다[16].

보안 시스템에서는 보안 감사 추적을 위해 감사 대

상이 되는 감사 주체, 객체 그리고 감사 서비스를 위한 방법 등을 선택하여야 하며 이를 기반으로 감사 서비스 시스템은 다음과 같은 요구사항을 반영시켜야 한다. 첫째, 자원의 보호를 위하여 패스워드의 불법적 사용이나 변경 사항, 지정된 사용자의 행위, 시스템 명령어의 부당한 사용을 감시해야 한다. 둘째, 지정된 자원에 대한 접근, 침해 및 변경의 실패나 성공 등을 기록하여야 한다. 셋째, 보안 침해에 대한 대응 조치를 구비해야 하며 비인가된 정보 흐름에 대한 감사기록이 이루어져야 한다[10, 11, 12].

EDI 시스템은 메시지 전송이 분산 환경에서 이루어지므로 다양한 보안성 위협에 대한 정보 보호의 강력한 보호 수단이 요구된다. [2]에서 정의한 보안 위협 요소는 다음과 같이 네가지로 분류된다.

① 접근 위협 요소: 부당한 사용자가 메시지 전송 시스템에 접근하는 경우

② 메시지간 위협 요소: 메시지간 위협은 메시지 통신시 외부의 허용받지 않은 처리기로 부터 야기되며 다음과 같은 종류가 된다.
- 사칭: 통화의 상대방을 모르고 사용자가 쉽게 정보를 노출시키는 경우
- 메시지 수정: 허용받지 않은 처리기에 의해 수정된 메시지가 수신자에 전달되는 경우
- 재송: 허용받지 않은 처리기가 메시지를 수신하여 의도한 수신자에게 다시 메시지를 전송하도록 하여 의도된 수신자로 부터 더 많은 정보를 추출하는 경우
- 전송량 분석: 도청자가 자료의 흐름을 분석하는 경우

③ 메시지 내부 위협요소: 메시지 통신자 간의 메시지의 부인 및 보안 수준 위반 등

④ 데이터 저장기 위협 요소: 메시지 전송 시스템이 소유한 저장기에 데이터가 메시지 전송시 이상 현상으로 경로설정 정보의 수정 및 선행 수신 등이 된다.

위와 같은 위협 요소에 대비하여 EDI 보안 서비스 처리시 발생되는 정보을 감사 추적 시스템에 저장하여 문제 발생시 분쟁을 해결하기 위한 근거 자료로 제시되어야 한다. 정의된 보안 위협 요소는 EDI 보안 감사 추적 시스템에서 제공할 서비스를 분류하는 기준이 된다.

2.2 EDI 보안 서비스

EDI 보안 서비스는 주로 MHS(Message Handling System) 내에서 이루어지며 보안 감사 추적은 보안 서비스에 대한 자료 추적을 통하여 감사 자료의 효율적 관리 및 사용자에 대한 서비스로 이루어진다.

2.2.1 MHS의 구성 요소

MHS는 사용자, UA(User Agent), AU(Access Unit), MS(Message Store), MTA(Message Transfer Agent)로 구성된다.

① 사용자: 인간 또는 응용 프로세서가 될 수 있으며 메시지를 보내는 입장은 송신자(originator)라 하고 받는 입장은 수신자(recipient)라 한다. 사용자는 MHS를 바로 사용할 수 있는 직접 사용자와 Teletex, Telex 또는 기존의 우편시스템과 같은 통신 시스템에서 MHS를 사용하는 간접사용자로 분류한다.

② MTA: Store-and-Forward 방식으로 메시지를 수신측 UA/MS와 상호작용하여 MTA로 전송한다. MTA는 봉투(envelop)-제출(submission), 전송(transmission), 배달(delivery)의 세 종류 제어 정보를 처리하며 이를 이용하여 메시지 전송을 수행한다.

③ UA: 직접 사용자, MTA와 MS 간의 메시지 교환을 제어하는 응용프로그램이며 메시지 편집, 보관 및 MTA, MS와의 메시지 제출, 배달 및 검색 기능을 제공한다.

④ AU: 다른 통신 시스템과 MHS 서비스를 받지 못하는 통신 시스템에게 제한적이긴 하지만 MHS를 사용할 수 있게 해 준다. 현재 정의되어 있는 외부 통신 시스템 AU는 PDAU(Physical Delivery Access Unit), TLMAU(Telematic Access Unit), TLXAU(Telex Access Unit) 등이 있다.

⑤ MS: 사서함과 같은 기능을 가지고 있으면서 메시지 저장, 검색 및 관리 기능을 제공한다. 사용자는 UA를 통해 MS로 전달된 배달된 메시지를 검색하면 된다.

2.2.2 EDI 보안 서비스

EDI 보안 서비스는 주로 X.400 프로토콜인 MHS (Message Handling System)[2]내에서 서비스가 이루어지며, MHS에서 제공되어야 하는 보안 서비스는 권고안[3, 4]에 정의되어 있다. 그러나 EDI에서는 기본적인 보안 서비스 이외에 발생할 가능성이 있는 법적 분쟁을 처리할 수 있도록 추가적인 서비스가 요구되는데 이것을 위해 X.435 프로토콜[5]에서는 EDI 메시지 인증과 부인봉쇄 서비스가 추가로 정의되어 있다.

〈표 1〉 메시지 전송 보안 서비스
〈Table 1〉 Security sevices for the message transfer

구간 / 서비스	UA/UA	UA/MS	MS/MTA	UA/MTA	MTA/MS	MTA/MTA	MTA/UA	MS/UA
송신 인증								
메시지 송신 인증	*	*	-	*	-	-	-	-
검증 송신 인증	-	-	*	*	-	-	-	-
제출 보고	-	-	-	-	*	*	*	-
제출 증명	-	-	-	-	-	-	*	-
배달 증명	*	-	-	-	-	-	-	a)
보안 접근 관리								
봉쇄 실체 인증	-	*	*	*	*	*	*	*
보안 문맥	-	*	*	*	*	*	*	*
데이터 기밀성								
접속 기밀성	-	*	*	*	*	*	*	*
내용 기밀성	*	-	-	-	-	-	-	-
메시지 흐름 기밀성	*	-	-	-	-	-	-	-
데이터 무결성								
접속 무결성	-	*	*	*	*	*	*	*
내용 기밀성	*	-	-	-	-	-	-	-
메시지 순서 무결성	*	-	-	-	-	-	-	-
부인봉쇄								
송신 부인봉쇄	*	-	-	*	-	-	-	-
제출 부인봉쇄	-	-	-	-	-	-	*	-
배달 부인봉쇄	*	-	-	-	-	-	-	a)
메시지 보안 레이블링								
메시지 보안 레이블링	*	*	*	*	*	*	*	*
보안 관리								
자격증명 변경	-	*	-	*	*	*	*	-
등록	-	*	-	*	-	-	-	-
MS 등록	-	*	-	-	-	-	-	-
EDIM 책임인증								
EDI 통지 증명	*	-	-	-	-	-	-	-
검색 증명	-	*	-	-	-	-	-	-
전달 증명	-	-	-	-	-	*	-	-
EDIM 책임 부인봉쇄								
EDI 통지 부인봉쇄	*	-	-	-	-	-	-	-
EDI 검색 부인봉쇄	-	*	-	-	-	-	-	-
EDI 전달 부인봉쇄	-	-	-	-	-	*	-	-
EDI 내용 부인봉쇄	*	-	-	-	-	-	-	-

a) 수신 MS에 의해 송신 UA로 서비스 제공

〈표 1〉은 ISO 7498-2에 근거한 메시지 전송 보안 서비스이며 * 기호는 각각의 보안 서비스가 MHS의 처리기인 UA, MS, MTA 중 어느 구간에 위치해야 할 지를 나타내고 있다. 메시지 전송 보안 서비스는 크게 송신 인증(Origin Authentication), 보안 접근 관리(Secure Access Management), 데이터 기밀성(Data Confidentiality), 데이터 무결성(Data Integrity), 부인봉쇄(Non-repudiation), 메시지 보안 레이블링(Message Security Labeling), 보안 관리(Security Management), EDIM(Electronic Data Interchange Message) 책임 인증(Responsibility Authentication), EDIM 책임 부인봉쇄(Non-repudiation of EDIM Responsibility) 등으로 분류된다[10, 11, 13].

이와 같은 보안 서비스들은 메시지 처리시 송신자에 의해 제출되는 메시지가 메시지 전송 시스템을 통해 전송되고 수신자에게 배달될 때 서비스 되어야 하는 요소이다. 이러한 서비스는 메시지 전달 시스템에서 제출 포트, 배달 포트, 관리 포트 및 MTA 간에 전달에서 이루어진다.

EDI 감사 추적 시스템은 메시지 전송 보안 서비스를 기반으로 대상이 되는 감사 정보를 정의하며, 감사 정보를 파악하여 이들 감사 정보를 기반으로 EDI에서 제공해야 하는 감사 추적 서비스를 정의한다.

3. 시간 개념의 적용

EDI 보안 서비스시 발생하는 감사 정보는 시간 의존적인 정보이므로 사건이 발생된 시간을 감사 정보에 대한 색인으로 사용할 경우 보다 효율적으로 감사 정보를 검색할 수 있다.

본 장에서는 자료에 적용할 수 있는 시간의 종류와 EDI 감사 정보에서 시간 개념을 적용하는 방법에 대해 기술한다.

3.1 자료에 따른 시간의 종류

현실 세계에서 발생하는 자료에 대해 적용할 수 있는 시간의 종류는 거래시간(Transaction Time)과 유효시간(Valid Time)이 있다. 거래시간은 자료가 시스템에 저장된 시간을 의미하며 유효시간은 실세계에서 사건이 발생된 시간을 나타낸다.

거래시간은 시간 의존적인 자료가 시스템에 저장

된 시간을 의미하며 물리적 시간(Physical Time)이라고도 한다. 거래시간은 시스템 클럭에 의해 처리되므로 사용자가 임의로 변경할 수 없으며 거래시간과 관련된 정보는 한 번 기록이 되면 수정이 불가능하다. 그리고 유효시간은 현실 세계에서 실제적으로 사건이 발생된 시간을 수록하는 논리적인 시간(Logical Time)이며 사용자가 사건이 발생된 시간을 기록하며 유효시간과 관련된 정보는 후에 자료의 오류가 있을 경우 수정이 가능하다. 이 밖에도 사용자가 정의하는 사용자 정의시간(User-defined Time)과 사용자가 정보를 사용하기 위하여 자료를 참조하는 참조시간(Reference Time) 등도 있다[1, 8, 9].

3.2 EDI 감사 정보에 시간 개념 적용

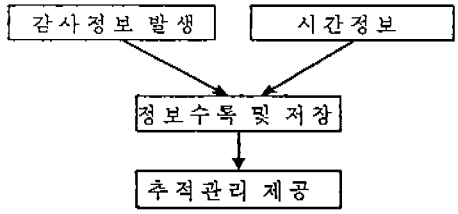
EDI 감사 추적 서비스를 위한 정보는 EDI 보안 서비스 처리시 생성된 데이터 중 감사를 위해 필요한 데이터를 보안 감사 추적 시스템에 전달되면 보안 감사 추적 시스템은 전달된 데이터를 감사 서비스가 용이한 형식으로 분류하여 저장 및 관리하게 된다. 감사 추적 시스템에서 유지·관리하는 보안 감사 정보는 EDI 시스템 특성상 시간의 흐름에 따라 대량의 정보를 취급해야 한다. 그러므로 효율적인 자료의 저장과 감사시 저장된 자료를 빠른 검색을 통해 서비스를 제공해야 한다.

감사 정보는 시간축에 따라 계속적으로 발생하는 사건으로 EDI에서는 자료의 거래와 관련된 모든 정보를 보관 유지하여 법적인 분쟁이 생기거나 권한이 있는 사용자가 감사자료에 대한 서비스를 요구할 경우 로그 화일 또는 데이터베이스로 구축된 감사 화일을 이용하여 적절한 처리를 수행해야 한다.

감사 서비스 화일을 구성하는 자료는 시간 종속적인 자료이므로 사건에 따라 사건이 발생한 실제시간인 유효시간과 정보가 수록된 거래시간을 결합하여 자료를 구성할 경우 사용자를 위한 서비스나 불법 침입 등에 대한 처리를 보다 정확하고 신속하게 처리할 수 있다.

실세계의 사건은 시간 종속적인 사건과 시간 독립적인 사건으로 나눌 수 있다[17]. 시간 종속적인 사건의 경우 항목에 명시적으로 시간 정보를 추가하여 관리할 수 있다. 예를 들면, EDI 시스템에서 "A 회사에서 B 회사로 보내진 발주서를 모두 검색하라?"와 같은 질의를 입력하면 시간과 관계없이 A 회사에서 B 회사로 보낸 발주서를 모두 출력해 주어야 한다. 또 다른 질의로 "1996년 5월 13일에 A 회사에서 B 회사로 발주한 문서를 검색하라?"는 질의가 입력되면 "1996년 5월 13일"을 키(key)로 하여 시간 색인을 통해 요구하는 문서를 빠른 시간내에 검색가능해야 한다.

EDI의 이력 데이터의 유지 관리는 문서의 유효기간을 정하여 유효기간이 초과된 자료에 대해서는 사용자의 요청 없이 자동적으로 시스템에 의해 제 2의 저장 장소로 전이될 수 있도록 이력 관리를 수행할 경우 감사 서비스시 발생하는 오버헤드를 줄일 수 있으며 축적된 많은 감사자료를 쉽게 관리하고 사용자에게 제공할 수 있다. (그림 1)과 같이 감사 정보가 발생될 경우 감사 정보에 대한 시간값을 추출하여 감사 정보와 함께 시간 정보를 기록하며 감사 정보 기록시 시간 색인을 생성하여 감사 정보 추적에 이용한다.



(그림 1) 감사 추적 자료 저장 접근
(Fig. 1) Access and record of audit trail informations

4. EDI 감사 추적 시스템을 위한 감사 서비스

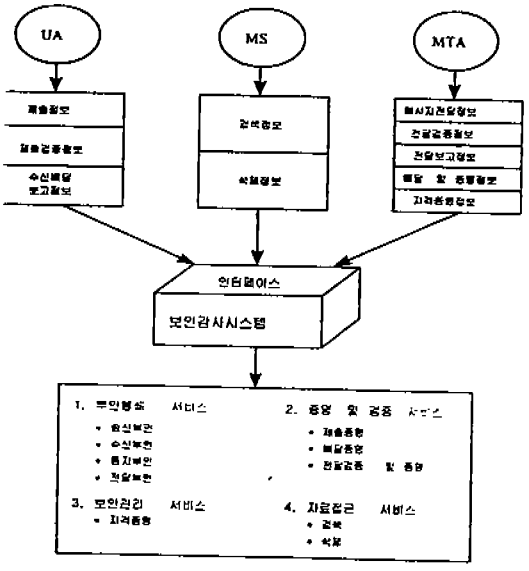
본 EDI 보안 감사 추적 서비스 시스템에서 제공하는 감사 서비스는 EDI 보안 서비스 처리시 생성된 정보들을 분류하여 부인봉쇄 서비스, 증명 및 검증 서비스, 보안관리 서비스와 자료접근 서비스 등으로 정의한다.

(그림 2)는 EDI 보안 감사 추적 시스템에 의해 제공되는 감사 서비스가 된다. MHS의 처리기인 UA, MS, MTA로부터 보안 감사에 필요한 정보들이 보안 감사 추적 시스템으로 전송되고 감사 추적 시스템은 사용자에게 부인봉쇄, 증명 및 검증, 보안관리, 자료접근 서비스를 제공한다.

4.1 부인봉쇄 서비스

부인봉쇄 서비스는 메시지가 제출 또는 배달된 후 제 3자에게 변경할 수 없는 증명을 제공하는 것으로 증명 서비스보다 강력한 서비스로 부인봉쇄 서비스에 속하는 서비스들은 송신 부인 봉쇄, 수신 부인 봉쇄, 통지 부인 봉쇄와 전달 부인 봉쇄 서비스가 있다.

송신 부인 봉쇄 서비스는 메시지 제출자가 메시지 제출 사실을 부인하는 경우 메시지 수신자는 자신이 수신한 메시지에 대하여 제출자가 메시지를 제출하였다는 증빙 자료를 제공하여 주는 서비스이다. 수신 부인 봉쇄 서비스는 메시지 제출자가 메시지를 제출하여 MTA를 통하여 수신자에게 배달되었는데 시간 경과 후 상호 기업간의 분쟁이 발생되어 수신자가 메시지 수신 사실을 부인하는 경우에 증빙 자료를 제공하여 주는 서비스이다. 통지 부인 봉쇄 서비스는 EDIM 전송시 함께 보낸 EDIM에 대한 통지 사실에 대하여 긍정 통지, 부정 통지, 회송 통지 여부에 대한 감사 정보를 제공하여 주는 서비스이다. 전달 부인 봉쇄 서비스는 송신 MTA와 수신 MTA 사이에 메시지 전달에 대한 감사 정보를 제공해 주는 서비스로 전달 정보, 수신 MTA로부터의 전달보고, MTA의 전달 검증 등에 관한 감사 정보를 제공해 준다.



(그림 2) 감사 서비스
(Fig. 2) Audit services

4.2 증명 및 검증 서비스

증명 및 검증 서비스는 발신 MTA와 수신 MTA가 메시지를 받은 사실을 부인하는 경우 제공하는 서비스이다. 세부 서비스로는 제출증명 서비스, 배달증명 서비스, 검증 및 전달 증명 서비스가 있다.

제출증명은 메시지가 전송되기 위하여 전송 타당성을 검증한 검증 정보 자료와 UA를 통하여 MTA로부터 메시지가 제출되었다는 감사 정보 자료를 제공해 준다. 배달증명 서비스는 수신 MTA가 수신 UA에 메시지를 전송한 정보를 제공하여 주는 서비스로 수신 UA측의 수신 사실에 대한 증빙 자료로서 활용된다. 검증 서비스는 메시지가 전송될 MTA에 메시지 전송에 타당성을 검증해 주는 서비스이다. 마지막으로 전달 증명 서비스는 UA가 제출한 서류가 송신 MTA에서 수신 MTA로 전달된 정보에 대하여 감사 정보 자료를 제공하여 준다.

4.3 보안관리 서비스

보안관리 서비스는 두가지로 자격 증명 변경과 사용자 등록 서비스가 있다.

자격 증명 서비스는 EDI 사용자가 MTA 등록시 사용 등급과 변경 사항을 제공해 주는 서비스이다. 사용자 등록 서비스는 EDI 사용자가 MS나 MTA에 등록된 사실인지를 검사해 주는 서비스가 된다.

4.4 자료접근 서비스

이 서비스는 MHS의 처리기인 MS와 관련된 서비스로 EDI 사용자가 MS에 저장된 정보를 언제, 누가, 어떠한 정보를 접근하였는 지를 알려주는 서비스로 검색 서비스와 삭제 서비스가 있다.

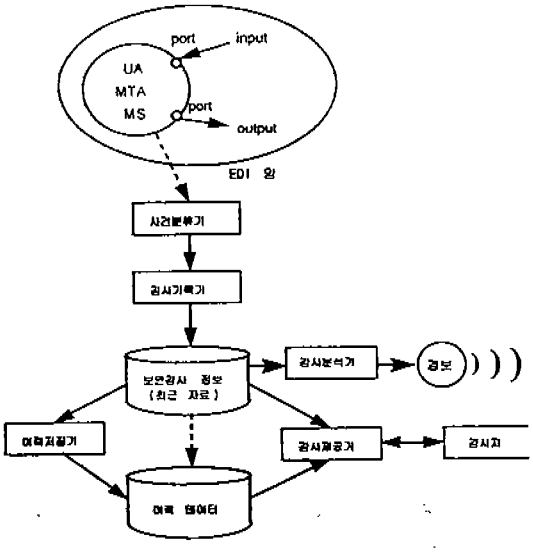
5. EDI 보안 감사 추적 시스템 구현

본 장에서는 EDI 보안 감사 추적 시스템 모델과 구현을 설명한다. EDI 보안 감사 추적 시스템은 감사 정보 저장시 시간 개념을 적용하여 시간의 흐름에 따라 증가되는 감사 정보를 효율적으로 관리할 수 있다.

5.1 시스템 모델

EDI에서 보안 감사 추적 서비스를 위해 처리되어야 할 기능에는 사건 구별 기능, 감사 기록 기능, 감사 제

공 기능, 감사 분석 기능, 감사 저장 기능 등이 있는데 각각의 기능을 담당하는 모듈들(사건분류기, 감사기록기, 이력저장기, 감사제공기)이 모여서 (그림 3)과 같은 EDI 보안 감사 추적 시스템을 구성하게 된다. 일반적으로 EDI 망에서는 각 처리기가 포트를 통해 입·출력을 하게 되고, 그러한 EDI 망으로 부터 필요한 메시지가 감사 추적 시스템의 입력으로 이용된다.



(그림 3) 보안 감사 추적 서비스 시스템 구조
(Fig. 3) System structure of security audit trail service

본 감사 서비스 시스템의 장점은 시간지원 개념을 적용하여 감사자료를 구성하므로 시간 정보를 이용하여 효율적인 자료 검색이 가능하다. 시간에 따라 발생된 감사 레코드들은 감사 기록기에 의해 보안감사 서비스 저장기에 모두 저장·관리되며 일정한 시간 단위에 따라 오래된 감사자료는 보안감사 서비스 저장기에서 감사 이력저장소로 자료의 전이가 발생한다. 전이된 감사 레코드들은 시간 색인으로 구성되는 저장 구조를 갖는다. 이러한 기법을 이용하여 시간에 따라 발생되어 기록된 감사자료들은 감사 제공자에 의해 어느 시점(event)에 발생된 감사 자료뿐만 아니라 일정한 시간 간격(interval) 동안에 발생된 이력 감사 자료들을 제공해 줄 수 있어 보안 감사 추적 시스템의 기능을 다양하게 지원할 수 있다.

5.2 시스템 구성 모듈

이 절에서는 (그림 3)의 각 모듈들의 기능과 구현 사항을 기술한다. 구현 환경은 Spark 20 워크스테이션의 UNIX 운영체제 하에서 C 언어와 X Motif 윈도우 관리자를 사용하여 구현하였다. 위에서 설계된 사건분류기, 감사기록기, 감사 이력 저장기는 EDI 망으로부터 발생되는 자료를 언제든지 처리할 수 있도록 항상 동작하며, 감사제공기는 사용자의 요청이 있거나 문제 발생시 감사자가 작동시킬 수 있다.

5.2.1 사건분류기

사건분류기(event discriminator)는 바인드된 각 UA, MTA, MS로 부터 전달되어 온 정보를 받아 메시지별 분류를 수행하여 감사 레코드를 구성하는 처리기이다. 사건 분류기의 입력 정보는 〈표 1〉에 정의된 보안 서비스시 UA, MTA와 MS에서 다음과 같은 정보를 입력으로 받는다.

- UA: "제출", "제출증명", "제출 검증" 서비스에서 감사와 관련된 정보
- MTA: "배달보고", "자격증명", "전달보고", "메시지 전달", "전달검증" 서비스에서 감사와 관련된 정보
- MS: 자료의 "검색" 및 "삭제" 서비스시 감사에 필요한 정보

사건분류기는 EDI 망을 통해 감사 추적 시스템에 전달된 각 메시지가 어느 처리기로 부터 전달되고 어떠한 서비스에 대한 정보인지를 메시지 전송시 메시지 헤더에 기록된 구분자를 통해 감사 레코드를 구성한다. (그림 4)는 사건 분류기가 메시지 구분자를 이용하여 정보를 분리하는 알고리즘이다.

5.2.2 감사 기록기

감사기록기(audit recorder)는 사건분류기가 분류한 감사 정보 레코드를 DBMS(UniSQL)[18]를 이용하여 처리시간 및 자료 구분자를 통하여 데이터베이스로 구축한다. 이 때 적용되는 기법은 Object-Oriented 기법을 이용하여 각 정보 레코드들을 클래스별로 상위 및 하위 클래스를 구성하여 데이터베이스로 구축된다. 구축된 데이터베이스는 감사제공자가 질의어를 통하여 쉽게 감사 자료를 제공 받을 수 있도록 융통

```
#include "audit.h"

/**************사건 분류기****************/
/* 메시지 형태 즉, "audit.h"에 저장된 정보를*/
/* 이용하여 레코드에 저장                  */
/*****************************************/
EventDiscrimiator(msg)
{
        char Ttems[MAX_ITEMS][MAX_CHAR];
        int    i, herder;

        GETItemsFromMessage(Items, msg);

        switch(header) {
                case Submission  :  /* 메시지 헤더 1000 */
                        if(IsContentIDDuplicate(Items[i] == DUPLICATE) {
                                printf("Error    : ContentIdentifier");
                                printf("\"%s\" is duplicated!\n", Items[1]); }
                        else {
                                WriteCOMMONinSubmission(Items);
                                WriteUAinSubmission(Items);
                        }
                        break;
                case ProbeOfSubmission:  /* 메시지 헤더 1100 */
                                :
                                :
                case MsRegister :   /* 메시지 헤더 3200 */
                        WriteRegister(Items);
                        break;
        }
}
```

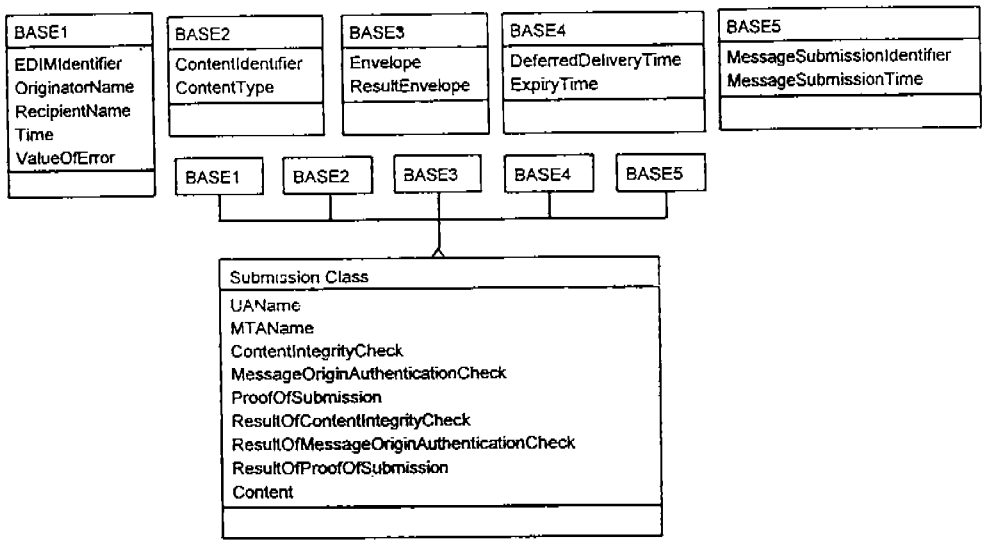
(그림 4) 사건 분류 알고리즘
(Fig. 4) Algorithm of the event discriminator

성을 제공한다.

UniSQL을 이용하여 구성된 감사 정보에 대한 스키마는 총 31개의 클래스로 구성가 된다. 이 중에서 12개의 클래스는 여러 클래스에 공통적으로 이용되는 항목들로 이들 상위 12개 클래스 정보는 감사 서비스를 기반으로 구성된 19개의 하위 클래스에서 그대로 상속받게 된다. 아래의 (그림 5)는 "Submission" 클래스로 이 클래스는 상위 클래스로 5개의 클래스에서 정보를 받게 된다. 이와 같이 UniSQL로 구성된 감사 정보는 여러 서비스에서 이용하는 공통적인 클래스를 상위 클래스로 구성하고 하위 클래스는 감사 서비스가 용이하게 감사 서비스에 따라 클래스를 구성한다.

5.2.3 감사 이력 저장기

감사 이력 저장기(audit archiver)는 감사 서비스 저장기에 저장된 자료를 시간 처리 단위(time ganularity)로 이동시켜 이력 버전(history version)을 생성하는 즉, 버큐밍(vacuumming)을 수행하는 처리기이다. 시간 경과에 따라 발생되는 정보를 모두 현재버전(current version)으로 유지할 경우 정보의 양이 매우 방대해져 데이터 검색 시간이 길어진다. 이는 시스템 성능을 저해시키는 요인이 되므로 버큐밍 기법을 통해 현재 버전을 정해진 범위의 양을 초과하는 경우 이력 버전으



(그림 5) 감사 클래스 예
(Fig. 5) A example of an audit class

```
/*******      데이터 전이 알고리즘    ********/
/* disk_check_processor : 디스크의 공간 영역을 검사하여 버퓨밍을 결정 */
/* data_transfer_processor :  disk_check_processor()로 부터 버퓨밍      */
/* 요청이 있을 경우 데이터와 인덱스 전이 수행                          */


disk_check_processor()
{
      do {
            if(current_disk_free_space <= F_block) then
                  data_transfer_processor();
            else break;
      } while(FOREVER);
}

data_transfer_processor()
{
      V_C = 0;
      while(V_C < Capacity) {
            if(Op_Leaf is not exist) then
                  select a leftmost Leaf_Node;
            else
                  select a OP_Leaf;
            V_C = V_C +1;
      }
      write_data_process();
      transfer_index_process();
}
```

(그림 6) 감사 이력 저장 알고리즘
(Fig. 6) Algorithm for recording historical audit data

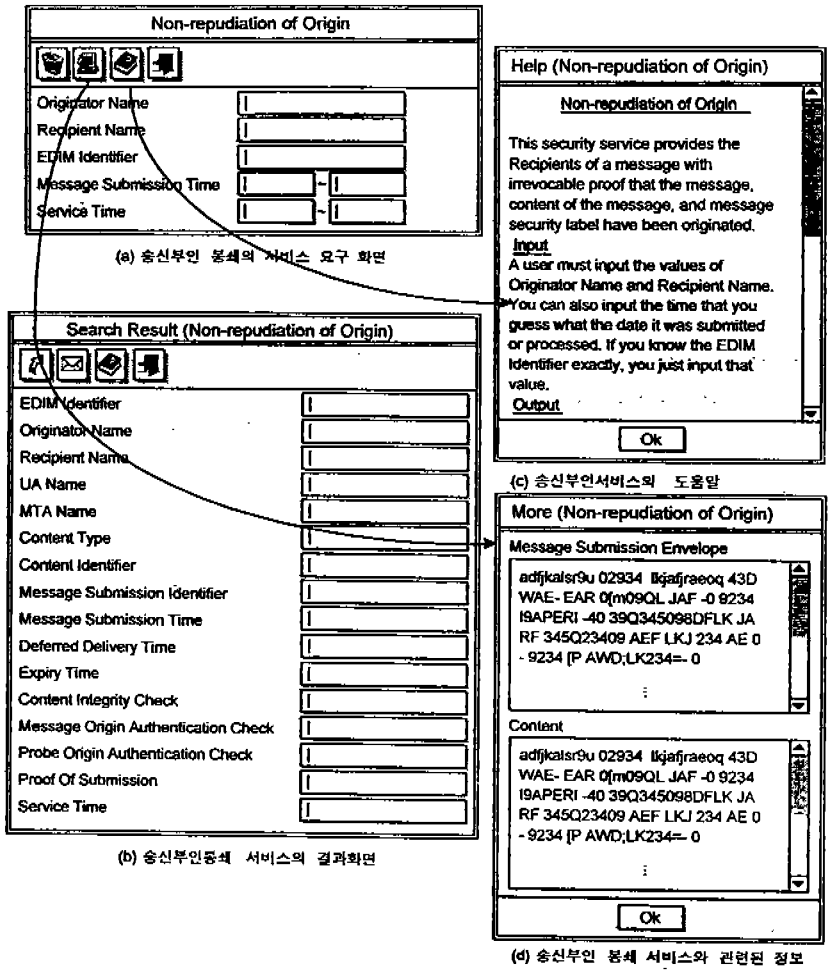
로 전이시키는 것이 필요하다.

(그림 6)은 버퍼링 과정에 관한 알고리즘으로 일정한 주기마다 자기디스크에 있는 정보를 광학 디스크와 같은 대용량의 메모리로 이동시킨다. disk_check_process()는 자기 디스크에 정보가 입력될 디스크에서 허용하는 정보의 양을 검사하여 임의의 범위를 초과하는 경우 데이터 전이 알고리즘인 data_tramsfer_processor()를 호출한다. 데이터 전이 알고리즘은 데이터 용량 만큼의 정보를 인덱스의 좌측노드에서 선택하여 데이터 전이를 수행한다.

5.2.4 감사제공기

감사제공기(audit provider)는 감사 점검자로 부터 감사자료 제공을 요청 받으면 최근의 자료는 감사 저장기 즉 데이터베이스로 부터 이력 감사 자료는 감사 이력 저장기로 부터 감사자료를 제공받아 감사점검자에게 감사 서비스 레코드를 제공하는 역할을 수행한다.

감사제공기에 의해 제공되는 감사 서비스의 종류는 부인봉쇄 서비스, 증명 및 검증 서비스, 보안관리 서비스, 그리고 자료접근 서비스 등이 된다. 사용자는 제공받고자 하는 서비스에 따라 주메뉴를 선택한 후 주메뉴에 딸린 부메뉴를 통하여 실제적인 서비스를



(그림 7) 송신 부인 봉쇄 서비스

(Fig. 7) Service of nonrepudiation of origin

받게 된다. 감사 제공기의 사용자 서비스 화면은 X Motif 윈도우 관리자를 사용하여 구축하였으며 사용자가 GUI화면으로 감사 정보에 대한 요구를 감사자에게 요청한다.

감사 제공기에 의해 검색되는 감사 정보의 처리 절차는 다음과 같다.

① 사용자는 GUI 화면으로 감사 서비스를 선택하고 각 감사 서비스에서 요구하는 자료 값을 입력한다.

② 감사 제공기는 GUI를 통해 입력된 정보를 SQL 정형 질의로 변형한다.

③ SQL 형식의 감사 질의는 감사 저장기 즉, 데이터베이스를 접근하여 요구한 정보를 찾으며 만약 요구한 자료가 데이터 전이가 이루어진 자료일 경우 이력 감사 저장기에 감사 정보를 요구한다.

④ 감사 제공기는 사용자가 요구한 정보를 찾았을 경우 GUI 화면에 감사 정보를 출력한다.

본 시스템의 감사제공기에서 제공하는 서비스는 첫째 송신, 수신, 통지와 전달 부인에 대한 부인봉쇄 서비스가 있고 둘째, 송신 MTA, 수신 MTA에서 메시지 전송 사실을 확인시켜 줄 수 있는 제출 증명과 배달증명 서비스가 있다. 그리고 보안 관리를 위한 자격증명 서비스가 있으며 마지막으로 자료접근과 관련된 검색과 삭제 증명에 대한 서비스를 제공한다.

(그림 7)의 GUI 화면은 부인 봉쇄 서비스에서 송신 부인 봉쇄에 관한 화면이다.

(그림 7)의 (a)는 EDI 사용자가 감사자에게 송신 부인 봉쇄를 요청할 경우 감사자가 감사 추적 서비스의 주메뉴에서 송신 부인 봉쇄를 선택할 경우 나타나는 화면이다. 감사자는 서비스를 요청한 사용자에게 입력 정보로 송신자 이름, 수신자 이름, EDIM 번호, 메시지를 송신한 시간과 메시지가 서비스된 시간을 받아 감사 정보를 검색하여 (b)와 같은 결과 화면을 출력한다.

(그림 7)의 (c)는 "도움말" 버튼을 누를 경우 현재 서비스하고자 하는 송신 부인 봉쇄에서 요구하는 입력 정보와 그에 따라 검색되는 출력 정보에 대한 정보를 서비스해 준다. 그리고 (d)는 사용자가 (b)와 같은 결과 화면으로 만족하지 못하여 감사자에게 더 자세한 감사 정보를 요구할 경우 추가로 제공되는 화면이 된다.

6. 결 론

본 논문은 EDI 보안 서비스의 한 요소인 감사 추적 서비스 시스템을 구축하기 위해 X.400과 X.435에서 정의한 보안 서비스를 기반으로 감사 서비스 시스템의 요구사항 분석을 통한 EDI 보안 감사 서비스를 정의하였으며 정의된 감사 서비스를 제공하기 위한 감사 추적 서비스 시스템 모델을 설계 및 구현하였다.

본 EDI 감사 추적 서비스 시스템의 구성 모듈들은 사건 분류기, 감사 기록기, 이력 저장기와 감사 제공기로 구성된다. 사건 분류기는 EDI 보안 서비스시 발생되는 정보를 EDI 망을 통해 전달받아 감사 레코드를 만든다. 감사 기록기는 각 레코드를 구별할 수 있는 키 값과 시간 정보로 색인으로 하여 UniSQL을 통해 자기 디스크에 감사 정보를 기록한다. 이력 저장기는 일반 문서의 유효 보존 기간이 있는 것처럼 일정 시간이 경과된 감사 정보를 제2의 저장소로 전이시키는 모듈이다. 감사 제공기는 저장된 감사 정보를 이용하여 감사 서비스를 제공한다.

본 감사 서비스에서 제공되는 서비스는 부인 봉쇄 서비스, 증명 및 검증 서비스, 보안 관리 서비스 그리고 자료 접근 서비스가 있다. 부인 봉쇄 서비스는 세부 항목으로 송신 부인 봉쇄, 수신 부인 봉쇄, 통지 부인 봉쇄와 전달 부인 봉쇄 서비스로 나누어지며 증명 및 검증 서비스의 세부 항목은 제출 증명 서비스, 배달증명서비스 그리고 검증 및 전달 증명 서비스가 제공된다. 또한 보안 관리 서비스는 자격 증명 서비스와 사용자 등록 서비스가 있으며 자료 접근 서비스는 검색 서비스와 삭제 서비스가 세부 서비스로 제공된다. 이와 같은 감사 서비스는 EDI 이용자간에 분쟁이 발생할 경우 이를 해결하기 위한 근거 자료로 사용된다. EDI 시스템에서 취급되는 문서의 양은 시간이 흐름에 따라 계속적으로 증가되므로 효율적인 관리를 통해 빠르게 감사 정보를 제공해야 한다. 그러므로 본 감사 추적 서비스 시스템에서는 시간 값을 색인으로 구성하였으며 감사 이력 저장기를 사용하여 유효 기간이 지난 감사 정보 등을 광디스크와 같은 기억장치로 이동시키도록 하였다.

앞으로 연구해야 할 사항은 본 논문에서 설계된 모

델을 EDI 보안 서비스 시스템과 접목하여 EDI 망에 연동시키는 작업이 필요하다. 그리고 본 시스템에서는 일괄처리 감사만을 지원하므로 실시간 감사 처리 및 감사 분석기 설계 및 구현도 차후의 연구 과제가 된다.

참 고 문 헌

[1] Michel E. Adiba and Brue G. Linsay, "Database Snapshots," Proc. 6th International Conference on VLDB, pp. 86-91, 1980.

[2] ITU-T Recommendation X.400, "Message Handling Systems And Service Overview", 1990.

[3] ITU-T Recommendation X.402, "Message Handling Systems: Overall Architecture", 1992.

[4] ITU-T Recommendation X.411, "Message Handling Systems: Message Transfer System: Abstract Service Definition And Procedure", 1992.

[5] ITU-T Recommendation X.435, "Message Handling Systems: EDI Messaging System", 1992.

[6] ITU-T Recommendation X.736, "Information Technology-Open System Interconnection-System Management: Security Alarm Reporting Function", 1992.

[7] ISO/IEC 10181-7.2, "Information Technology-Open System Interconnection Security Frame works in Open Systems-Part7: Security Audit Framework", Aug., 20, 1993.

[8] Keun Ho Ryu, "A Temporal Database Management Main Memory Prototype," Univ. of Arizona, TempIS TR No. 26, July 1991.

[9] Richard Snodgrass and Ilsoo Ahn, "Temporal Databases," IEEE Computer, Vol. 19, No. 9, Sep. pp. 35-42, 1986.

[10] 김기중, 류근호, "시간지원 정보와 EDI 보안 감사 서비스", 안전한 EDI 관련 심포지움, 한국정보통신연구소, 1995.

[11] 김기중, 서경란, 정경자, 류근호, "EDI용 보안 감사 시스템 설계", 제2차 안전한 EDI 관련기술 심포지움, 한국전자통신연구소, 1996.

[12] 김동규, "MHS(Message Handling System) Security 서비스 기능 체계 연구", '92 통신학술연구과제, 1993.

[13] 류근호, "EDI 시스템의 감사추적 기법에 관한 연구", 한국전자통신연구소 연구보고서, 1995.

[14] 서경란, 김기중, 정경자, 류근호, 신종태, "시간지원 개념을 이용한 EDI 보안 감사 추적 시스템", 데이터베이스 연구회 논문집, 1996.

[15] 윤이중, "안전한 EDI_UA의 설계", 안전한 EDI 관련 기술 심포지움 발표집, 한국전자통신연구소, 1995.

[16] 이강수, "EDI 보안 감사 요구사항 분석", 안전한 EDI 관련기술 심포지움 발표집, 한국정보통신연구소, 1995.

[17] 정경자, 전근환, 류근호, "시간지원 데이터 베이스 거래시간 지원을 위한 거래시간 로그와 연산자의 설계 및 구현", 한국정보과학회 논문지, 제22권 제 6호, 1995.

[18] UniSQL/X Database Management System User's Manual, UniSQL, Inc. May 1995.

정 경 자

1988년 충북대학교 전산통계학과 졸업(이학사)

1993년 충북대학교 대학원 전자계산학과 졸업(이학석사)

1993년~현재 충북대학교 대학원 전자계산학과 박사과정

1995년~현재 충청전문대학 멀티미디어과 전임강사

관심분야: 시간지원 데이터베이스, 데이터베이스 보안, 시공간 데이터베이스, 질의 최적화, 멀티미디어 데이터베이스

김 기 중

1983년 공군사관학교 졸업
1987년 서울대학교 계산통계학과 졸업
1995년 충북대학교 대학원 전자계산학과 졸업(이학석사)
1995년~현재 충북대학교 대학원 전자계산학과 박사과정
관심분야:시간지원 데이터베이스, 데이터베이스 보안, 전산망 보안

서 경 란

1995년 충북대학교 컴퓨터과학과 졸업(이학사)
1997년 충북대학교 대학원 전자계산학과 졸업(이학석사)
1996년 12월~현재 한국통신기술 첨단통신 사업실 근무
관심분야:시간지원 데이터베이스, 데이터베이스 보안, 멀티미디어 시스템

류 근 호

1976년 숭실대학교 전산학과 졸업(학사)
1980년 연세대학교 산업대학원 전산전공(공학석사)
1988년 연세대학교 대학원 전산전공(공학박사)
1976년~1986년 육군군수 지원사 전산실(ROTC장교), 한국전자통신연구소(연구원), 한국방송통신대 전산학과(조교수) 근무
1989년~1991년 Univ. of Arizona TempIS연구원
1986년~현재 충북대학교 컴퓨터과학과 교수겸 컴퓨터 정보통신 연구소장
관심분야:시간지원 데이터베이스, 시공간 데이터베이스, DBMS 및 OS, 객체 및 지식베이스 시스템

강 창 구

1979년 2월 한국항공대학 항공전자공학과 공학사
1986년 2월 충남대학교 대학원 전자공학과 공학석사
1993년 8월 충남대학교 대학원 전자공학과 공학박사
1979년~1982년 한국공군 기술장교
1987년~현재 한국전자통신연구원 책임연구원, 부호4 실장
관심분야:부호이론, 통신 프로토콜, 통신 및 컴퓨터 보안, 정보보호 서비스 및 메카니즘