안전한 EDI 서비스를 위한 접근제어 모델 설계

박 진 호* 정 진 욱**

송호대학 정보산업계열 전임강사*

성균관대학교 전기전자 및 컴퓨터공학부 교수**

요 약

EDI는 은행업무, 무역, 의학, 출판 등의 다양한 활동이나 사업에 관련된 메시지를 컴퓨터들간에 상호 교환한다는 개념이다. 그러므로, 보안성, 신뢰성 및 특수 기능성이 EDI 시스템의 절대적 요구사항이다. 이러한 요구사항 중 보안성에 대한 요구사항을 만족시키기 위한 접근제어 모델을 설계하고자 한다. 정보 시스템에 있어서의 접근제어는 실체에 대한 모든 접근은 보안정책에 의해서 정해진 접근모드나 규칙에 따라 발생한다는 것을 보장하기 위한 것이다. 본 논문에서는, 접근제어 모델을 위한 보안정책을 신분기반 정책, 규칙기반 정책, 직무기반 정책 측면에서 제시한다. 정의한 보안정책을 수행하기 위해서 유도된 접근제어 규칙과 오퍼레이션에 기초한 안전한 EDI 서비스를 제공하기 위한 접근제어 모델을 설계한다. 제안한 접근제어 모델은 EDI 메시지에 대한 무결성, 비밀성 및 흐름제어를 제공한다.

Design of Access Control Model for Secure EDI Service

Jin-Ho Park* Jin-Wook Chung**

ABSTRACT

EDI is basically the concept of computer-to-computer exchange of messages relating to various types of activities or business areas, such as banking, trade, medicine, publishing, etc. Therefore, security, reliability and special functionality will be implicit requirements of EDI systems. We will design access control model to content security of these requirements. Access controls in information systems are responsible for ensuring that all direct access to the entities occur exclusively according to the access modes and rules fixed by security policies. On this paper, security policies for access control model are presented from the viewpoints of identity-based, rule-based, role-based policy. We give a design of access control model for secure EDI service based on the derived access control rules and operations to enforce the defined security policies. The proposed access control model provides integrity, confidentiality and a flow control of EDI messages.

1. 서 론

현대 사회에 있어서 정보 통신 분야가 보편적인 분야로 되어감에 따라, 정보 통신 분야에 대한 다양한 요구가 발생되었다. 정보 통신망을 통한 방대한 양의 문서 조회, 파일 전송 등이 그러한 요구의 대표적인 예가 될 수 있고, 이러한 요구 중 전 세계적으로 연결된 다양한 시스템에 대한 각종 문서의 생성, 전송, 처리를 하는 전자 우편은 사무실에서 문서 처리와 통신의 문제를 해결하는 유효한 수단으로 중요시되고 있다. 이와 같은 전자 우편 기능을 공중 서비스하기 위한 메시지 교환 시스템, 즉 메시지 핸들링 시스템이 ITU-T에 의해서 X.400으로 표준화되었다[1].

X.400에 정의된 메시지 핸들링 시스템을 이용하는 것 중 기업체나 국가기관 등의 상호 문서교환의 요구가 증가됨에 따라 교환되는 문서 양식의 표준화 및 통신 방법에 대한 표준화가 필요하게 되었다. 이러한 표준화 요구는 X.435 EDI (Electronic Data Interchange) Messaging System을 통해 표준화 되어가고 있다[1]. 기존의 통신망을 통해 EDI을 구성하고 사용함에 있어서 가장 중요시되어야 할 문제점이 전송되는 정보에 대한 보안 문제이다.

EDI 시스템에 있어서의 보안은 주로 EDI 메시지의 전송과 수신에 관계된다. EDI 메시지를 보내는 사람은 메시지를 보내도 된다는 권한을 부여받아야만 하고, EDI 메시지는 정확한 목적지에 메시지 내용의 노출 및 수정 없이 도착해야만 한다. 추가로, 메시지를 받은 사람은 받지 않았다고 부인할 수 없어야 하며, 보낸 사람도 역시 보내지 않았다고 부인할 수 없어야만 한다. 이와 같이 기본적인 EDI 보안 서비스는 인증, 비밀성, 무결성, 부인봉쇄가 있다.

이러한 기본적인 보안 서비스 중 문서의 내용이 권한 없는 자에 의해 노출되고 수정되는 것을 방지하기 위한 비밀성과 무결성의 보장은 접근제어를 통해서 이루어진다.

본 논문에서는 이러한 EDI 문서에 대한 비밀성과 무결성을 보장하고 문서의 흐름제어가 가능한 접근제어 모델을 OSI 표준에 따라 설계하고자 한다.

II. 안전한 EDI서비스를 위한 접근제어

2.1 접근제어 개념

접근제어의 목적은 컴퓨팅 자원, 통신 자원 및 정보자원 등에 대하여 허가되지 않은 접근을 방어하는 것이다[2,3,4]. 허가되지 않은 접근이란 불법적인 자원의 사용, 노출, 수정, 파괴와 불법적인 명령어 수행을 포함하고 있다. 즉, 접근제어는 각 자원에 대한 비밀성, 무결성, 가용성 및 합법적인 이용과 같은 정보보호 서비스에 직접적으로 기여하게 되며 이러한 서비스들의 권한 부여를 위한 수단이 된다[5].

접근제어의 결정은 어떤 개시자가 어떤 타겟에 대하여 어떤 목적을 갖고, 어떤 조건하에서 접근할 수 있는지를 다루는 문제이다. 즉, 이러한 결정은 접근제어 정책에 반영이 되고, 접근 요청은 접근 정책을 시행하는 접근제어 메커니즘을 통하여 시행된다.

미 국방성에서 기밀 분류된 방법으로부터 유래하는 MAC(Mandatory Access Control)과 DAC(Discretionary Access Control) 정책의 개념은 위에서 제시된 3가지 요소를 확장 혼합하고 있다. MAC정책은 자동적으로 시행되는 어떤

규칙에 기반하고 있다. 그러한 규칙을 실제로 시행하기 위하여 사용자와 타겟에 대해서 광범위한 그룹 형성이 요구된다. DAC 정책은 특별한 사용자별로 정보에 대한 접근을 제공하고 추가적 접근제어를 그 사용자에게 일임한다[2,3].

OSI 보안 구조에서는 MAC/DAC 용어를 사용하지 않고 신분-기반(identity-based)과 규칙-기반(rule-based) 정책으로 구분하고 있다[6,7]. 실제적인 목적에 있어서 신분-기반과 규칙-기반 정책은 각각 DAC 및 MAC 정책과 동일하다[3].

접근제어 모델은 크게 2가지의 범주로 나누어진다. 즉, 임의적 접근제어 모델(DAC)과 강제적 접근제어 모델(MAC)로 나누어진다. 임의적 접근제어 모델은 각 사용자와 시스템의 타겟들을 위하여 타겟에 대한 사용자의 허락된 액세스 권한을 명시한 규칙과 사용자의 신분에 기초하여 정보에 대한 사용자의 접근을 통제한다.

임의적 접근제어 모델의 가장 기본적 모델로는 액세스 행렬을 이용한 HRU 액세스 행렬 모델이다[8]. 이 모델은 보안을 형성할 목적으로는 처음 제안된 모델로써, 타겟과 개시자 및 권한 부여 집합에 의하여 특징 지워지는 상태(state)의 식으로 보안 시스템을 보여준 모델이다. 대부분의 임의적 접근제어 모델은 액세스 행렬 모델의 확장형으로 간주될 수 있다. 시스템 상태를 그래프 구조를 이용하여 표현한 Take-Grant 모델은 권한 확대의 문제에 중점을 둔 모델이다[9].

강제적 접근제어 모델은 시스템에 개시자와 타겟의 등급에 기초해서 정보에 대한 접근을 통제하는 모델로써, 타겟은 정보를 저장하고 있는 피동적 존재이고, 개시자는 타겟을 액세스하는 능동적 존재이다.

개시자와 타겟의 등급에 기초하는 BLP 모델이 강제적 보안 모델의 기본적 모델이고[10,11], 이와 비슷한 모델로써 정보의 무결성을 보호하기 위한 목적의 Biba 모델이 있다[12]. 강제적 액세스 정책의 일반화는 보안 등급의 격자(lattice)를 기초로한 Denning에 의해 제안된 정보 흐름 제어 시스템으로 대표되어 진다[13,14].

2.2 접근제어의 필요성

안전한 EDI 서비스를 제공하기 위해서 접근제어가 제공해야 하는 보안 서비스를 컴퓨터 시스템, 통신망과 EDI 사업자 측면으로 나누어 고려함으로써 접근제어에 대한 필요성을 기술한다.

2.2.1 컴퓨터 시스템상의 접근제어

- 거래 승인된 정보의 전송전 불법 변조금지
- 수신 보관된 각종 거래자료의 불법 변조금지
- 거래 처리 프로그램의 갱신, 사용권한 추가등록 등을 사용자 개인 또는 부서별로 허가
- 거래 정보의 비밀등급별로 개인 또는 부서별 제한된 접근 허용
- 터미널의 부당한 사용 방어(사용자 인증, 사용보드, 제한시간 등의 배경 정보 지정)
- 거래 처리 주기에서 서로 다른 시점의 각 단계별 불법 변조, 부정, 사기, 오류방지(시안→구매허가→주문→상품인수→지불 등)

2.2.2 통신상의 접근제어

- 비밀로 분류된 자료가 통신망상에서 허가되지 않은 개시자에 노출되지 않도록 비밀 취급 등급을 개시자 및 타겟에 연결하여 관리
- 통신 매체 및 기타 장비에 대하여 허가되지 않은 접근을 방어
- 통신제어 및 중계 장비에 부당히 접근하여 메시지의 변조를 할 수 없는 접근제어 및 암호

화 기법 적용 (중계자 개입 포함)
- 통신망을 특별히 이용하는 EDI사용자로 구성된 폐쇄 집단 구성 고려

2.2.3 EDI 사업자 접근제어

- 승인 받지 않은 자료의 시스템 유입 및 불법 사용자 접근 방어
- 우편함의 제한된 접근 허용 및 우편함으로부터 고의적 메시지 인출 지연 방지
- 통신망용 소프트웨어 및 관련 자료에 대한 불법적 접근 방지
- 통신망상에서 전문 EDI 사업자의 불법적인 사용자 정보 접근 방지
- 서비스의 제한된 제공과 분쟁시 해결할 수 있는 각종 접근자료의 수집, 관리(서비스의 개시, 중단, 제한 서비스 등 포함)

Ⅲ. 안전한 EDI서비스를 위한 접근제어 정책

비밀성과 무결성을 제공하고 흐름제어가 가능한 보안 모델을 설계하기 위한 정책들을 기술한다.

3.1 용어 정의

접근 정책 기술 및 설계에 필요한 용어를 정의한다.

- 실체(entity)

EDI 망에 있어서 모든 보안에 적절한 요소들을 실체라 한다. 실체에는 사용자, 개시자, 타겟, 프로그램, 프로세스 등이 있다.

- 개시자(initiator)

상대 실체(entity)들에 대해서 접근을 시도하는 실체이다. 본 논문에서의 개시자는 인간 사용자 및 프로세서이다.

- 타겟(target)

접근이 시도될 수 있는 실체이다.

- 접근제어 정보 : ACI(Access Control Information)

접근제어 결정을 위해 접근제어 결정 정보와 함께 접근제어 정책 규칙에 적용되는 정보.

- 접근제어 결정 정보 : ADI(Access control Decision Information)

특정한 접근제어 결정을 하는데 있어서 접근제어 결정 함수(ADF)에서 이용하는 부분적인 ACI.

- 보유한 ADI

미래의 접근제어를 결정할 때 사용하기 위해서 이전의 접근제어 결정으로부터 ADF에 보유하고 있는 접근제어 결정 정보(ADI)

- 접근제어 시행 함수 : AEF(Access control Enforcement Function)

개별 접근제어 요구에 대한 하나의 개시자와 하나의 타겟간에 설정된 접근 경로의 일부이면서, ADF에 의해서 만들어지는 접근제어 결정을 시행하는 함수이다.

- 접근제어 결정 함수 : ADF(Access control Decision Function)

모든 접근제어 요구에 대해서, ACI와 ADI를 가지고 접근제어 정책 규칙을 적용하여 접근제어 결정을 하는 함수이다.

- 보안 등급(security level)

실체의 비밀성 수준을 나타내는 계층적 분류 체계로서 Top Secret 〉 Secret 〉 Confidential 〉 Unclassified와 같이 분류한다.

- 무결성 등급

실체가 소유하는 정보의 수정에 관한 권한의 수

준을 나타내는 계층적 분류 체계로서 Crucial 〉 Very Important 〉 Important와 같이 분류한다.

o 보안 범주(category)

실체의 집합을 분류하는 비계층적 분류 체계로서, 각각의 범주에 속하는 실체들은 자신이 속한 범주에 맞는 보안 등급과 비밀성 등급을 소유하며, 수행할 수 있는 일의 종류도 다르다.

o 보안 레이블(security label)

데이터 항목, 물리적 자원 및 사용자와 같은 실체에 부여된 보안 속성 정보의 집합이다. 보안 레이블은 보안 등급과 보안 범주로 구성되며, 규칙 기반 정책 수행에 사용되는 정보이다.

o 지배(domination) 관계

두 실체에 대해서 각각의 보안 레이블을 상호 비교하여 계층적 분류 체계인 보안 등급이 우세하고, 비계층적 분류 체계인 보안 범주가 다른 보안 범주를 포함할 때 지배관계가 성립한다.

o 접근 모드(access mode)

개시자가 타겟에 대하여 수행할 수 있는 접근 권한을 접근 모드라고 한다.

o 오퍼레이션(operation)

개시자가 타겟에 대하여 수행할 수 있는 동작을 오퍼레이션이라고 한다.

3.2 접근 모드 정의

설계하고자 하는 시스템에서는 다음과 같은 접근제어 모드를 제공한다. 개시자는 타겟에 대하여 접근제어 정책의 규칙에 의해 다음 모드 중 하나를 허가받고, 허가받은 모드를 정해진 타겟에 대하여 수행한다.

o observe

한 개시자가 타겟에 대하여 observer 접근 모드를 가지고 있을 때 개시자는 타겟의 내용을 관찰할 수 있다.

o modify

한 개시자가 타겟에 대하여 modify 접근 모드를 가지고 있을 때 개시자는 타겟의 내용을 수정할 수 있다.

o delete

한 개시자가 타겟에 대하여 delete 접근 모드를 가지고 있을 때 개시자는 타겟의 내용을 삭제할 수 있다.

3.3 접근제어 오퍼레이션 정의

한 개시자가 한 타겟에 대하여 수행할 수 있는 동작을 오퍼레이션이라고 한다. 오퍼레이션은 접근제어 메커니즘을 수행하기 위한 모든 기능을 제공하며, 이러한 오퍼레이션을 이용하여 접근제어 메커니즘을 표현하고자 한다.

o login

통신망 상의 실체가 통신망에 접속된 시스템을 사용하기 위해서 시스템에 로그인할 수 있게 해주는 함수

o observe

자신이 로그인한 시스템이나 통신망 상의 다른 시스템 상의 정보의 내용을 관찰할 수 있게 해주는 함수

o modify

타겟의 정보 내용을 수정할 수 있게 해주는 함수

o delete

타겟의 정보를 삭제할 수 있는 함수

o execute

타겟 프로그램을 실행시켜 주는 함수

o create

새로운 정보를 생성시켜 주는 함수

o move

타겟의 정보를 통신망 상의 다른 시스템으로 복사하는 함수

3.4 접근제어 정책

3.4.1 ACI 관리 정책

접근제어에 필요한 모든 정보를 가지고 있는 ACI의 유지 및 관리를 위한 정책으로서 ACI 관리에 필요한 규칙들을 표현한다.

ACI를 구성하는 항목 : identifier, owner, security label, integrity level, role, 통신망 상의 위치(IP address).

- o 모든 실체는 ACI에 존재한다.
- o 모든 실체는 ACI에 보안 레이블을 명시한다.
- o 모든 실체는 ACI에 무결성 등급을 명시한다.
- o 모든 실체는 ACI에 직무를 명시한다.
- o 모든 실체는 ACI에 소유권자를 명시한다.
- o 새로운 실체 생성시 ACI에 등록한다.
- o 실체의 보안 정보 수정시 ACI에도 수정한다.
- o 실체의 삭제시 ACI에서도 삭제한다.
- o 실체 생성시 생성된 실체는 생성자의 ACI를 상속한다.

3.4.2 소유권자 관리 정책

- o 모든 실체는 자신의 소유권자가 있다.
- o 생성된 실체는 생성자의 소유권자를 상속한 다.
- o 소유권자의 변경은 소유권자 및 허가받은 자만이 변경한다.
- o 메시지 전달 후 전달된 메시지에 대한 소유권자는 타겟이 된다.

3.4.3 보안 레이블 관리 정책

- o 모든 실체는 자신의 보안 레이블을 소유한다.
- o 보안 레이블에는 보안 범주(category), 보안 등급을 명시한다.
- o 새로운 실체 생성시 생성자의 보안 레이블을 상속받는다.
- o 개시자는 자신의 보안 레이블을 변경할 수 없다.
- o 개시자는 타겟의 보안 레이블을 변경할 수 없다.
- o 타겟은 타겟의 보안 레이블을 변경할 수 없다.
- o 실체의 보안 레이블 변경은 보안 레이블 변경 권한자만이 할 수 있다.

3.4.4 신분 기반 정책

BLP 모델의 ds-property를 기초로한 개시자나 또는 그들이 속해 있는 그룹들의 신분에 근거하여 타겟에 대한 접근을 제한하는 방법으로서, 모든 개시자와 타겟은 ACI에 선언되어 있어야 하고, 개시자의 보안 범주(category)와 타겟의 보안 범주가 같아야만 어떤 접근 모드를 요구할 수 있다.

- o 모든 개시자와 타겟은 ACI에 존재한다.
- o 개시자는 타겟의 보안 범주를 지배한다.

3.4.5 규칙 기반 정책

정보의 비밀성과 무결성 보장을 위해서 BLP 모델과 Biba 모델을 병행 이용한다. BLP 모델에서는 No Read-Up과 No Write-Down을 기본 원리로 이용하는 ss-property와 *-property를 이용하여 비밀성 보장을 제공하고, Biba 모델에서는 No Read-Down, No Write-Up을 기본 원리로 이용하는 엄격한 무결성 정책(strict integrity policy)을 이용하여 무결성을 제공한다.

개시자가 자신과 동일한 보안 레이블을 가진 타겟의 정보를 관찰하여 하위의 보안 레이블을 가진

타겟으로 전달하는 것을 방지하기 위한 정보 흐름 제어를 위해서 복사하는 정보의 보안 레이블과 복사되는 타겟의 보안 레이블이 동일하야 하고, 개시자의 보안 레이블이 타겟의 보안 레이블을 지배해야 한다.

- o 다음을 만족시킬 때 observe 동작을 수행할 수 있다.
  - 개시자의 보안 레이블은 타겟의 보안 레이블을 지배한다.
  - 타겟의 무결성 등급이 개시자의 무결성 등급을 지배한다.
- o 다음을 만족시킬 때 modify 동작을 수행할 수 있다.
  - 개시자는 타겟의 소유권자이다.
  - 개시자와 타겟의 보안 레이블이 일치한다.
  - 개시자와 타겟의 무결성 등급이 일치한다.
- o 다음을 만족시킬 때 delete 동작을 수행할 수 있다.
  - 개시자는 타겟의 소유권자이다.
  - 개시자의 보안 레이블이 타겟의 보안 레이블을 지배한다.
  - 개시자의 무결성 등급이 타겟의 무결성 등급과 일치한다.
- o 다음을 만족시킬 때 move 동작을 수행할 수 있다.
  - 개시자는 타겟 메시지의 소유권자이다.
  - move를 수행하는 개시자는 타겟 메시지와 타겟의 보안 레이블을 지배한다.
  - 타겟 메시지와 타겟의 보안 레이블이 일치한다.
  - 타겟 메시지와 타겟의 무결성 등급이 일치한다.

3.4.6 직무 기반 정책

직무 기반 정책에서는 Clark-Wilson 모델을 응용하여 개시자의 직무를 판단하고, 타겟과의 규칙 기반 정책을 수행한 결과를 이용해서 개시자가 타겟에 대해서 수행할 수 있는 직무의 프로그램을 허가한다.

- o 개시자는 타겟의 소유권자이다.
- o 개시자의 직무로서 수행 가능한 프로그램이어야 한다.
- o 개시자의 보안 레이블이 요구한 프로그램의 보안 레이블을 지배한다.
- o 개시자의 무결성 등급이 요구한 프로그램의 무결성 등급과 일치한다.

Ⅳ. 접근제어 메커니즘 설계

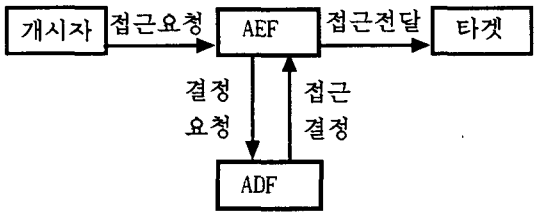
4.1 접근제어 모델 정의

설계할 접근제어 모델은 ISO/IEC DIS 10181-3 Security frameworks in open systems - Access control에서 정의한 접근제어 모델을 따른다.

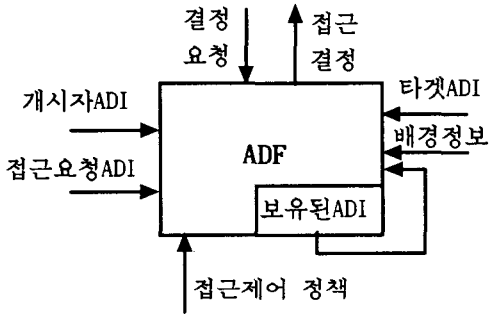
이 접근제어 모델에서는 접근제어 요청이 있을 때 접근제어 결정 요구를 하고, 결정된 접근제어를 시행하는 접근제어 시행 함수인 AEF와 AEF로부터의 접근제어 결정 요구가 있을 때 접근제어 규칙에 따라 접근제어 결정을 수행하는 함수인 ADF의 두 가지 요소로 이루어진 모델이다.

이러한 모델을 이용하여 구성하고자 하는 접근제어 구조는 개시자와 타겟에 AEF를 포함하고 외부의 제 3 기관에 ADF를 위치시키는 입력 접근제어와 출력 접근제어의 혼합형으로 구성한다. ADF를 수행할 제3기관에 접근제어에 필요한 모든 정보를 가지고 있는 ACI를 위치시킨다. 개시자가 요청한 접근을 개시자의 AEF에 제출하고, ADF로부터 승인을 받으면 개시자의 AEF가 요청된 접근을 타겟 AEF에게 제출하고, 다시 ADF

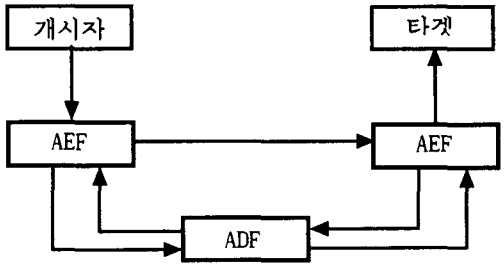
에게 승인을 요구한다. ADF로부터 승인을 받으면 타겟에 대하여 승인 받은 접근을 수행한다.



(그림 1) OSI 접근제어 모델



(그림 2) ADF 모델



(그림 3) 접근제어 구성 방법

(그림3)의 접근제어 구성방법은 개시자의 AEF가 수행한 출력(outgoing) 접근제어가 개시자 지역의 접근제어 요소들의 타겟에 대한 불법적 접근제어를 방어할 수 있고, 타겟 지역의 접근제어 시스템에 대한 신뢰도와 관계없이 안전한 접근제어를 제공할 수 있다. 출력 접근제어가 수행된 후 다시 타겟에서의 입력(incoming) 접근제어를 수행함으로써 권한 없는 제3자의 위장 접근제어가 ADF의 보유된 ADI로부터 방어될 수 있다.

4.2 접근제어 메커니즘 표기법 정의

- I : 접근제어의 개시자 집합, i∈I
- T : 접근제어의 타겟 집합, t∈T
- M : 접근 모드 집합, M={o, m, d}, m∈M
- R : 개시자 및 타겟의 직무 집합, r∈ R
- S_Level(a) : 보안 등급 함수
- I_Level(a) : 무결성 등급 함수
- Category(a) : 보안 영역 함수
- S_Label(a) : 보안 레이블 함수
- Role(a) : 직무 함수
- owner(a) : 소유권자 함수
- get_ACI(a) : ACI 요구 함수
- inherit(a,b,c) : 상속 함수 ; a의 b를 c에게 상속한다.
- dominate(a,b) : a ≥ b or a ⊇ b
- equal(a,b) : dominate(a,b) & dominate (b,a)
- exist_ACI(a) : ACI에 대해서 a의 존재여부 확인 함수
- C_SLabel : 현재 보안 레이블
- C_ILevel : 현재 무결성 등급
- S_Label_V : 보안 레이블 변수
- I_Level_V : 무결성 등급 변수
- Login_ACI : login을 수행하는 실체의 ACI
- create_ACI(a) : a의 ACI 신규 등록 함수
- delete_ACI(a) : a의 ACI 삭제

4.3 접근제어 규칙

안전한 EDI 서비스를 제공하기 위해 제시한 접

근제어 정책을 수행하기 위한 접근제어 규칙을 제안한다. 이 규칙들은 정보의 비밀성 보장을 위해서 BLP 모델의 ds-property, ss-property와 *-property를 기본으로 하여 정보의 무결성 보장을 위한 Biba 모델의 강력한 무결성 정책을 이용한 개선된 접근제어 규칙을 제안한다. 제안된 규칙 중에는 정보의 흐름을 제어하기 위한 것과 개시자의 직무에 기초하여 수행가능 한 직무 관련 프로그램만을 수행할 수 있도록 하는 Clark- Wilson 모델에 기초한 접근제어 규칙도 제안한다.

4.3.1 임의 접근제어 규칙(discretionary access control rule)

BLP 모델의 임의 보안 특성(discretionary security property)을 이용한 규칙으로서 개시자가 타겟에 대하여 수행하고자 하는 접근제어 모드가 있을 때 개시자와 타겟은 실체로서 ACI에 존재해야 하고, 개시자와 타겟의 보안 레이블 중 보안 범주(category)가 같아야 한다.

```
d_acr(i, t) =
  TRUE : if i∈exist_ACI(i) &
             t∈exist_ACI(t) &
             dominate(Category(i),
                      Category(t))
  FALSE : otherwise
```

4.3.2 단순 접근제어 규칙(simple access control rule)

단순 접근제어 규칙은 BLP 모델의 단순 보안 특성(simple security property)을 이용한 것으로서 비밀성 보장을 위한 기본 원리인 No Read-Up을 만족시키기 위한 것이다. 개시자가 타겟에 대하여 어떤 접근제어 모드를 수행하기 위해서는 개시자의 보안 레이블이 타겟의 보안 레이블에 대하여 지배관계를 만족해야 하고, 타겟의 무결성 등급이 개시자의 무결성 등급을 지배해야 한다.

```
s_acr(i, t, m) =
  TRUE : if dominate(S_Label(i), S_Label(t))
             & dominate(I_Level(t), I_Level(i))
  FALSE : otherwise
```

4.3.3 강력 접근제어 규칙(strict access control rule)

강력 접근제어 규칙은 BLP 모델의 스타 보안 특성(star security property)과 Biba 모델의 엄격한 무결성 정책(strict integrity policy)의 특성을 이용하고 정보에 대한 무결성을 보장하기 위한 접근제어 규칙이다. 이 규칙은 무결성 기본 원리 중의 하나인 No Read-Down 을 만족시키기 위해서 개시자의 보안 레이블과 타겟의 보안 레이블이 일치하고 각각의 무결성 등급이 일치할 때만 modify 접근 모드를 허가한다.

```
st_acr(i, t, m) =
  TRUE : if m = 'o' &
           dominate(S_Label(i), S_Label(t))
           & dominate(I_Level(t), I_Level(i))
  TRUE : if m = 'm' &
           equal(S_Label(i), S_Label(t)) &
            equal(I_Level(i), I_Level(t))
  TRUE : if m = 'd' &
           dominate(S_Label(i), S_Label(t))
           & equal(I_Level(i), I_Level(t))
  FALSE : otherwise
```

4.3.4 흐름 제어 규칙(flow control rule)

흐름 제어 규칙은 상위의 보안 레이블을 가진

실체가 하위 보안 레이블을 소유한 실체로의 상위 보안 레이블 정보를 전달해 주는 것을 방지하기 위한 규칙이다. 즉, 하위의 보안 레이블을 소유한 실체가 제3자인 상의 보안 레이블의 실체로 가장하거나 결탁하여 정보를 observe할 수 없게 하기 위한 것이다. 개시자가 한 타겟이 소유한 정보(t1)를 다른 타겟(t2)으로 전달하기 위한 copy 접근 모드는 개시자는 두 타겟에 대하여 보안 레이블이 지배 관계에 있어야 하고, 두 타겟간에는 보안 레이블과 무결성 등급이 일치해야만 한다.

```
fcr(i, t1, t2) =
  TRUE : if dominate(S_Label(i), S_Label(t1))
         & dominate(S_Label(i), S_Label(t2))
         & equal(S_Label(t1), S_Label(t2))
         & equal(I_Level(t1), I_Level(t2))
  FALSE : otherwise
```

4.3.5 실행 제어 규칙(execute control rule)

실행 제어 규칙은 Clark-Wilson 모델을 기초로 하여 자신의 직무로 수행할 수 있는 프로그램만을 실행할 수 있는 규칙이다. 개시자의 직무가 타겟(프로그램)을 수행할 수 있는 직무이고, 개시자의 보안 레이블이 타겟의 보안 레이블과 지배 관계에 있고, 두 실체간의 무결성 등급이 일치해야만 execute 접근 모드를 수행할 수 있다.

```
ecr(i, t) =
  TRUE : if equal(Role(i), Role(t)) &
         dominate(S_Label(i), S_Label(t))
         & equal(I_Level(i), I_Level(t))
  FALSE : otherwise
```

4.4 접근제어 오퍼레이션 설계

4.4.1 login

사용자가 시스템을 사용할 수 있도록 하기 위해서 자신이 사용하는 시스템에 로그인 시켜주는 오퍼레이션으로서, 입력한 사용자의 보안 레이블과 무결성 등급을 ACI의 것과 비교하여 로그인 성공 여부를 결정한다.

```
login(identifier, S_Label_V, I_Level_V)
{
  C_SLabel ← S_Label_V
  C_ILevel ← I_Level_V
  if exist_ACI(identifier)
  then login start
    Login_ACI = get_ACI(identifier)
    if C_SLabel = S_Label(Login_ACI) &
      C_ILevel = I_Level(Login_ACI) &
    then C_Role ← Role(Login_ACI)
      login OK
  endif
}
```

4.4.2 create

개시자가 자신의 시스템이나 타겟 시스템에 새로운 메시지를 생성할 수 있도록 해주는 오퍼레이션으로서, 개시자는 타겟에 대하여 modify 접근 모드를 가지고 있어야 하고, 생성된 메시지에는 자신의 보안 레이블과 무결성 등급 및 소유권자를 상속한다.

```
create(i, t1, t2)
{
  if d_acr(i, t1) &
    s_acr(i, t1, m) &
    st_acr(i, t1, m)
  then i create t2 at t1
    inherit(i, t2, S_Label(i))
```

```
    inherit(i, t2, I_Level(i))
    inherit(i, t2, owner(i))
    create_ACI(t2)
  endif
}
```

4.4.3 observe

개시자가 타겟의 메시지 내용을 볼 수 있게 해주는 오퍼레이션으로서, 타겟에 대하여 임의 접근 제어 규칙, 단순 접근제어 규칙, 엄격한 접근제어 규칙을 만족시키면 메시지를 볼 수 있다.

```
observe(i, t)
{
  if d_acr(i, t) & s_acr(i, t, o) &
    st_acr(i, t, o)
  then i observe t
  endif
}
```

4.4.4 modify

타겟의 내용을 수정할 수 있는 오퍼레이션으로서, 개시자는 타겟 메시지의 소유권자이고, 타겟에 대하여 modify 접근 모드를 가지고 있어야 한다.

```
modify(i, t)
{
  if i = owner(t) & d_acr(i, t) &
    s_acr(i, t, m) & st_acr(i, t, m)
  then i modify t
  endif
}
```

4.4.5 delete

개시자가 타겟 메시지를 지울 수 있게 해주는 오퍼레이션으로서, 개시자는 타겟 메시지의 소유권자이고, 타겟에 대하여 delete 접근 모드를 가지고 있어야 한다.

```
delete(i, t)
{
  if i = owner(i) & d_acr(i, t) &
    s_acr(i, t, d) & st_acr(i, t, d) &
  then i delete t & delete_ACI(t)
  endif
}
```

4.4.6 execute

개시자가 타겟 프로그램을 실행시킬 수 있게 해주는 오퍼레이션으로서, 개시자는 타겟에 대하여 modify 접근 권한을 가지고 있고, 실행 제어 규칙을 만족시켜야 한다.

```
execute(i, t)
{
  if d_acr(i, t) & s_acr(i, t, m) &
    st_acr(i, t, m) & ecr(i, t)
  then i execute t
  endif
}
```

4.4.7 move

개시자가 한 타겟의 메시지를 다른 타겟으로 이동시킬 수 있게 하는 오퍼레이션으로서, 개시자는 타겟 메시지에 대해서 observe 접근 권한을 가지고, 타겟에 대해서는 modify 접근 권한을 가져야 한다. 그리고 흐름제어 규칙을 만족시켜야 한다.

```
move(i, t1, t2)
{
  if i = owner(t1) & d_acr(i, t1) &
    s_acr(i, t1, o) & st_acr(i, t1, o) &
```

```
    d_acr(i, t2) & s_acr(i, t2, m) &
    st_acr(i, t2, m) & fcr(i, t1, t2)
  then i move (t1→t2)
  endif
}
```

〈표 1〉 오퍼레이션과 접근제어 규칙과의 관계

구 분	임의접근 제어규칙	강력접근 제어규칙	실행제어 규칙	흐름제어 규칙
login	Y			
create	Y	Y		
observe	Y	Y		
modify	Y	Y		
delete	Y	Y		
execute	Y	Y	Y	
move	Y	Y		Y

4.5 설계한 접근제어 메커니즘의 구조

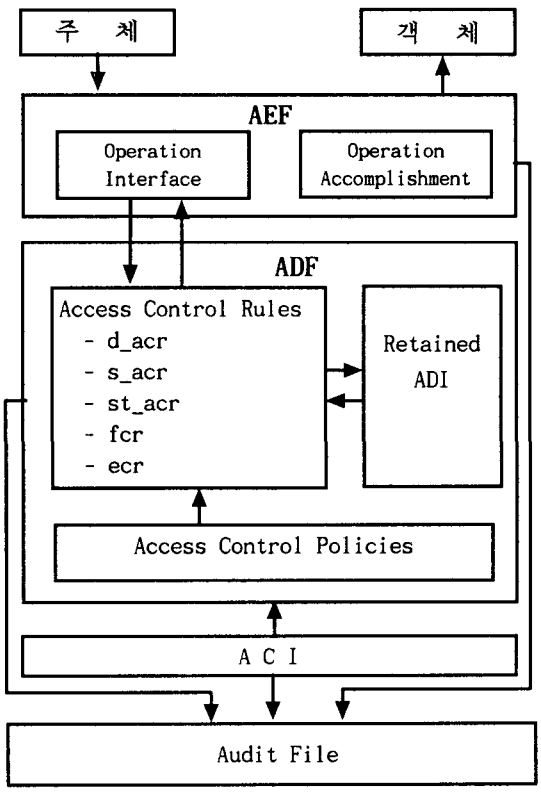
본 연구에서 설계한 접근제어 메커니즘의 구조는 OSI 표준의 개념적 모델을 기초로 하여 설계하였다. 이 모델에는 접근제어 결정 요구 및 시행을 담당하는 AEF와 접근제어 정책 및 규칙에 따라 접근제어 결정을 수행하는 ADF가 있다(그림4).

AEF에는 개시자가 타겟에 요구한 접근 모드나 오퍼레이션에 대한 ADF와의 오퍼레이션 인터페이스(operation interface)와 결정된 오퍼레이션에 대한 수행을 담당하는 오퍼레이션 수행(operation accomplishment)이 있다. ADF에는 접근제어 요구에 대한 결정을 위한 접근제어 규칙 및 보유한 ADI가 접근제어 결정을 수행한다. ACI는 ADF가 접근제어 결정을 수행하는데 필요한 모든 정보를 가지고 있다.

4.6 접근제어 구조가 결합된 EDIMS 구조

본 연구에서 설계한 접근제어 모델을 EDI 메시지 통신 환경(EDIME)의 EDI 메시지 통신 시스템(EDIMS)에 적용한 구조는 (그림5)와 같다.

각 UA와 PDAU에 AEF를 배치하고, ADF와 ACI는 EDIMS내에 하나씩 배치한다. 각각 하나씩의 ADF와 ACI를 EDIMS에 배치하는 것은 접근제어 결정의 일관성과 ACI의 접근제어 정보에 대한 관리의 용이성을 제공한다.



(그림 4) 접근제어 메커니즘 구조

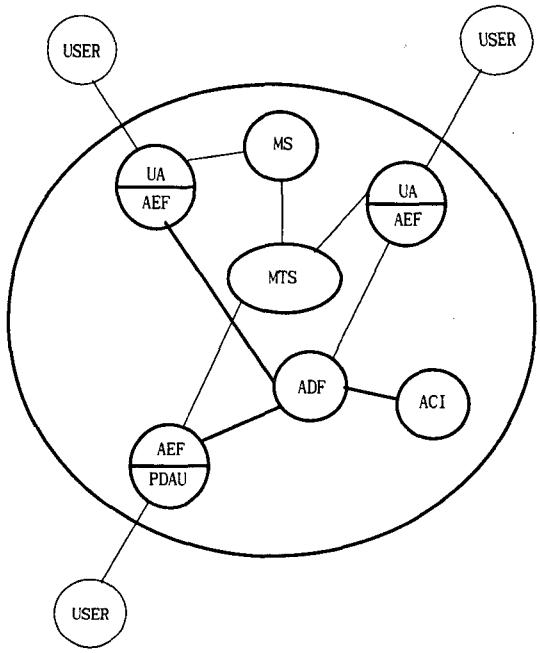
메시지의 header 부분에서 개시자와 타겟을 알아볼 수 있고, 각 개시자와 타겟에 관련된 모든 정보는 ACI에서 관리된다. EDIMS에서 교환되는

모든 문서 양식은 문서 고유의 기능에 따라 보안 등급이 할당되고, 직무를 표현할 수 있다. 즉 header 부분에 표현된 문서의 양식 정보 등을 이용하여 접근제어를 수행할 수도 있다. 그러므로, MTS 내의 모든 MTA는 UA의 AEF와 같은 형태의 AEF을 이용하여 메시지 전송 경로에 대한 접근제어를 수행할 수도 있다.

V. 결 론

안전한 EDI 서비스 제공을 위한 접근제어 모델은 EDI 메시지에 대하여 비밀성과 무결성의 보장 및 정보의 흐름 제어가 가능해야 한다. 본 논문에서는 안전한 EDI 서비스를 위한 요구사항을 ACI 관리 정책, 소유권자 관리 정책, 보안 레이블 관리 정책, 신분 기반 정책, 규칙 기반 정책, 직무 기반 정책 등의 보안 정책들로 표현하고, 각 정책들의 목적을 만족시키기 위한 접근제어 규칙을 작성하고, 접근제어 서비스를 제공하기 위한 오퍼레이션의 설계에 중점을 두었다. 접근제어 모델을 설계하기 위해서 OSI 표준안의 개념적 모델(그림 1)을 기초로 하여 입력 및 출력 접근제어(그림3) 구성 방법으로 접근제어 모델을 설계하였다.

이러한 구성 방법을 사용함으로써 통신망 상에서 이루어지는 모든 접근제어에 대한 감시 및 감사가 용이하고, 전체 통신망에 대한 ACI의 관리가 용이해진다. AEF를 포함하고 있는 모든 개시자와 타겟은 자신의 시스템에 접근하여 접근제어를 수행한 모든 개시자에 대한 감사 파일 작성이 용이하며, 제3기관에서 보유하고 있는 감사 파일과 ADI를 이용하여 접근제어에 대한 부인봉쇄를 제공한다.



(그림 5) 접근제어 서비스 제공된 EDIMS 구조

컴퓨터 시스템, 통신망과 EDI 사업자 관점에서의 접근제어의 필요성들은 크게 불법적인 권한 행사, 불법적인 정보 유통과 통신망 상의 정보 노출의 3가지 보안 영역으로 구분할 수 있다. 본 연구에서 설계한 접근제어 모델은 보안 레이블, 무결성 등급, 직무, 소유권 등을 이용하는 다단계 보안 체계를 이용하여 권한의 불법적 사용을 방지하였다. 이러한 다단계 보안 체계를 이용하여 각 보안 등급간의 정보의 흐름을 제한함으로써 정보의 불법적 유통을 차단하였다. 그리고, 메시지의 전송 경로에서의 정보의 불법적 노출에 대한 보안 문제는 개시자와 타겟이 일정한 접근제어 규칙을 만족시키면 메시지의 전송이 허가되는 형태이며, 전송되는 메시지는 인증이나 암호화 기법에 의해서 암호화된 상태의 메시지이므로 권한 없는 사용자에 대한 메시지 내용의 노출 위협은 없다.

본 논문에서 설계한 접근제어 모델은 접근 권한의

불법적 사용을 방지함으로써, EDI 정보에 대한 무결성 및 비밀성을 보장하였고, 다단계 보안 등급을 엄격히 시행함으로써, 정보의 불법적 유통을 차단할 수 있었다.

참 고 문 헌

[1] ITU-T Recommendation X.400 to X.435 Data Communication Networks Message Handling Systems.

[2] Ingrid M. Olson, Marshall D. Abrams, Computer Access Control Policy Choices , Computers & Security, Vol. 9, 1990, pp699-714.

[3] Warwick Ford, Computer Communicat-ion Security , Prentice Hall, 1993.

[4] Silvana Castano, Mariagrazia Fugini, Pierangela Samarati, DATABASE SECURITY, Addison-Wesley, 1994.

[5] Shari Lawrence Pfleeger, A Framework for Security Requirements , Computer & Security, Vol.10, 1991, pp515-523.

[6] ISO/IEC DIS 10181-1 Information Technology - Open Systems Interco nnection - Security Frameworks in Open Systems-Part 1: Security Frameworks Overview , 1993.

[7] ISO/IEC DIS 10181-3 Information Technology - Open Systems Intercon nection - Security Frameworks in Open Systems-Part 3: Access Control , 1993.

[8] Harrison M.A., Ruzzo W.L., Ullman J.D., "Protection in Operating System", Comm. ACM, 1976.

[9] Johnes A.K., Lipton R.L., Synder L., "A Linear Time Algorithm for Deciding Security", In Proc., 17th Annual Symp. On Foundations of Computers Science, 1976.

[10] Bell D.E., La Padula L.J., Secure computer systems : mathematical foundations and model , Technical Report M74-244, The MITRE Corp., Bedford, MA, 1974

[11] E.E.O. Roos Lindgreen, I.S. Hersch berg, On the validity of the Bell-LaPadula model , Computer & Security, Vol. 13, 1994, pp317-333.

[12] Biba K. J., "Integrity Considerations for Secure Computer Systems", ESD-TR-76-372, The MITRE Corp., 1977.

[13] D.E. Denning, A Lattice Model of Secure Information Flow , Comm. ACM, Vol. 19, No. 5, May 1976, pp236-243.

[14] Ravi S. Sandhu, Lattice-Based Access Control Models , IEEE, 1993.

[15] Eike Born , Helmut Stiegler, Discreti-onary access control by means of usage conditions , Computer & Security, Vol.13, 1994, pp437-450.

[16] Belden Menkus, Concerns in Computer Security , Computer & Security, Vol.11, 1992, pp211-215.

[17] Sead Muftic, Ahmed Patel, Peter

Sanders, Rafael Colon, Jan Heijnsdijk, Unto Pulkkinen, Security Architecture for Open Distributed Systems , John Wiley & Sons, 1993.

[18] Charles P. Pfleeger, Security in Computing , Prentice Hall, 1989.

박 진 호

1995년 대전대학교 전자계산학과(공학사)

1997년 대전대학교 컴퓨터공학과(공학석사)

1997년 ~ 현재 성균관대학교 전기전자 및 컴퓨터공학부(박사과정)

2000년 ~ 현재 송호대학 정보산업계열 전임강사

정 진 욱

1979년 성균관 대학교 대학원 (공학석사)

1991년 서울 대학교 대학원 계산통계학과(이학박사)

1973-1985 한국과학기술연구소 실장

현재 성균관 대학교 전기전자 및 컴퓨터 공학부 교수