

# 다단계 보안 스키마 설계를 위한 IDEA 방법론의 확장

김 정 종<sup>†</sup> · 박 운 재<sup>††</sup> · 심 갑 식<sup>†††</sup>

## 요 약

다단계 데이터베이스 응용의 설계는 복잡한 과정이며, 적절한 모델을 이용하여 개체나 그의 연관 보안 등급을 모호하지 않게 표현해야 한다. 또한, 다단계 데이터베이스 응용에 대한 의미를 가능한 한 정확하게 파악하는 것도 중요하다.

비보호 데이터베이스 응용 설계를 위한 IDEA 방법론은 데이터 집약 시스템에 초점을 두고 있기 때문에, 그 객체 모델에서는 응용에 대한 객체의 정적 구조와 그의 관련성을 서술한다. 다시 말해서, IDEA 방법론의 객체 모델은 객체의 정적 서술을 하기 위한 확장된 객체-관련성 모델이다. IDEA 방법론이 다단계 보안 데이터베이스 응용을 위해 개발되지 않았지만, 기존의 방법론을 활용함으로써 그 방법론에서 개발된 여러 기법들을 이용할 수 있다. 즉, 이 방식은 다단계 보안 스키마를 처음부터 개발하는 것보다 더 용이하다.

본 논문에서는 IDEA 방법론의 객체 모델에 보안 특징을 첨가하고, 이 모델을 다단계 보안 객체 지향 스키마로의 변환을 제시한다. 이 다단계 보안 스키마는 Informix-Online/Secure, Trusted ORACLE, Sybase Secure SQL Server와 같은 여러 상용 다단계 보안 데이터베이스 관리 시스템으로 자동 변환하기 위한 일반적인 스키마를 설계하는 예비 연구가 될 것이다.

## The extension of the IDEA Methodology for a multilevel secure schema design

Jung-Jong Kim<sup>†</sup> · Woon-Jae Park<sup>††</sup> · Gab-Sig Sim<sup>†††</sup>

## ABSTRACT

Designing a multilevel database application is a complex process, and the entities and their associated security levels must be represented using an appropriate model unambiguously. It is also important to capture the semantics of a multilevel database application as accurate and complete as possible.

Owing to the focus of the IDEA Methodology for designing the non-secure database applications on the data-intensive systems, the Object Model describes the static structure of the objects in an application and their relationships. That is, the Object Model in the IDEA Methodology is an extended Entity-Relationship model giving a static description of objects. The IDEA Methodology has not been developed the multilevel secure database applications, but by using an existing methodology we could take advantage of the various techniques that have already been developed for that methodology. That is, this way is easier to design the multilevel secure schema than to develop a new model from scratch.

This paper adds the security features to the Object Model in the IDEA Methodology, and presents the transformation from this model to a multilevel secure object oriented schema. This schema will be the preliminary work which can be the general scheme for the automatic mapping to the various commercial multilevel secure database management systems such as Informix-Online/Secure, Trusted ORACLE, and Sybase Secure SQL Server.

† 종신회원 : 경남대학교 컴퓨터공학과 교수  
†† 정 회 원 : 한국섬유패션대학 전자계산과 교수  
††† 종신회원 : 진주산업대학교 교양과정부 교수  
논문접수 : 1999년 7월 12일, 심사완료 : 2000년 3월 6일

## 1. 서 론

현재 대부분의 데이터베이스 응용들은 전통적인 데이터베이스 관리 시스템에 기초한다. 객체 지향 시스템이 시장에 출현하고 객체-관련성 모델[4]의 대중성과 활용도가 증가함에 따라, 설명되어야 할 문제는 확장 객체-관련성 스키마를 이에 대응하는 객체 지향 스키마로 사상(mapping)하는 방법이다.

보안 응용 설계란 객체 그리고 그들간의 관련성을 정의하는 것이며 복잡하다. 우선, 객체 그리고 그것과 연관된 보안등급은 적절한 모델을 이용하여 모호성이 없게 표현되어야 한다. 또한, 가급적 정확하고 완전하게 의미(semantics)를 파악하는 것이 중요하다. 그런 후, 분류된 정보(classified information)를 참조할 때 나올 수 있는 오류(error)와 잠재적인 비권한 추론(potential unauthorized inference)을 찾아내기 위해서 요구사항을 분석해야 한다.

다단계 데이터베이스 응용에서는 모든 객체들은 서로 다른 보안등급을 가질 수 있다. 보안등급 집합은 부분순서 격자(partially-ordered lattice:  $U < C < S < TS$ )를 형성한다. 여기서 기호( $<$ ,  $>$ ,  $\leq$ ,  $\geq$ )는 격자 모델에서 지배 관계(dominance relationship)를 나타내는데 사용된다.

객체 지향 스키마 설계는 객체 모델에서의 관련성을 객체들간의 참조가 되는 객체-값 속성으로 변환하는 것이다. 왜냐하면 객체 지향 모델에서 관련성은 객체-값 속성이 되기 때문이다. 관계형 모델에서 관련성은 관련된 테이블을 연결하여 조인(join) 연산을 할 수 있도록 동일 도메인에 대한 속성 집합으로 모델된다.

비보호 데이터베이스 응용 설계를 위한 IDEA 방법론[3]은 데이터 집약 시스템에 초점을 두고 있기 때문에, 그 객체 모델에서는 응용에 대한 객체의 정적 구조와 그의 관련성을 서술한다. 다시 말해서, IDEA 방법론의 객체 모델은 객체의 정적 서술을 하기 위한 확장된 객체-관련성 모델이다. IDEA 방법론이 다단계 보안 데이터베이스 응용을 위해 개발되지 않았지만, 기존의 방법론을 활용함으로써 그 방법론에서 개발된 여러 기법들을 이용할 수 있다. 즉, 이 방식은 다단계 보안 스키마를 처음부터 개발하는 것보다 더 용이하다.

SQL 표준이 다단계 SQL을 위한 시발점이지만, 각각의 MLS DBMS들은 서로 다른 다단계 확장을 구현하므로, 다단계 데이터베이스 응용 설계자가 그들을

각각 이해해야 하고 다르게 적용해야 한다. 이런 복잡성을 해결하려면 이들 MLS DBMS에 대한 스키마를 자동으로 생성해 주는 다단계 데이터베이스 설계 도구가 필요하다. 이를 위해서는 중간 단계인 표준 모델이 있어야 한다. 이런 표준 모델이 잘 설정되면, 다단계 데이터베이스 자동화 설계 도구가 이 모델을 각각의 목표 시스템인 MLS DBMS로 변환할 것이다.

본 논문은 다단계 데이터베이스 자동화 설계 도구를 구현하기 위한 이전 단계인 다단계 보안 스키마의 설계에 대한 기초 연구이다. 방법은 IDEA 방법론의 객체 모델에 보안 특징을 첨가하고, 이 모델을 다단계 보안 객체 지향 스키마로의 변환을 제시한다. 이 다단계 보안 스키마는 Informix-Online/Secure, Trusted ORACLE, Sybase Secure SQL Server와 같은 여러 상용 다단계 보안 데이터베이스 관리 시스템으로 자동 변환하기 위한 일반적인 스킴을 설계하는 예비 연구가 될 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 설명하고, 3장에서는 다단계 객체 모델의 구성요소를 서술한다. 그리고 4장에서는 다단계 객체 모델을 다단계 보안 객체 지향 스키마로 변환하는 규칙들을 제시하며, 마지막 5장에서는 결론 및 추후 연구방향을 논한다.

## 2. 관련 연구

Fugini[11]는 보안 데이터베이스 설계를 위한 최초의 연구를 했으며, ER 모델에 보안 특징을 첨가하여 다단계 보안 데이터베이스를 설계하는 문헌은 [12, 16, 17]이다. 보안 의미(security semantics)에 대한 포괄적인 연구는 [21, 22]에 설명되어 있으며, 보안 관련 추상화를 포함하여 일반의 의미 데이터 모델을 확장함으로써 보안을 위한 의미 데이터 모델을 개발한다.

다단계 데이터베이스 응용의 설계에 대한 [2, 19, 21, 28]의 연구는 다단계 데이터베이스 응용을 표현하기 위해 객체-관련성 모델(entity-relationship model)이나 의미 데이터 모델(semantic data model)의 변형을 활용한다. 이 모델들에서는 응용에 대한 정적(static) 요구사항뿐만 아니라 동적(dynamic) 및 기능적(functional) 요구사항 표현에 초점을 두고 있다.

Pernul[18]의 연구에서는 객체-관련성 모델과 데이터 흐름도(data flow diagram)를 이용하여 다단계 데이터베이스 응용의 정적 및 기능적 요구사항을 파악한

다. Sell[20]은 다단계 데이터베이스 설계를 위한 MOMT (Multilevel Object Modelling Technique)라는 방법론을 제안한다. 그러나 MOMT라는 객체 모델로부터 다단계 관계형 모델로의 변환을 설명하고 있다.

객체-관련성 모델을 객체 지향 스키마로 변환하는 두 가지 방법이 있다. 첫 번째 방법은 각각의 객체와 관련성을 객체로 변환하는 것이며[15], 두 번째 방법은 참조(reference)를 사용하여 관련성을 객체 클래스로 통합하고, 각각의 삼항 관련성(ternary relationship)에 대해서는 하나의 객체 클래스를 만드는 것이다[13]. 그러나 이들 방법에서는 보안 개념이 없다.

SORION[29]에서는 ORION 객체 지향 모델을 확장하여 강제적 정책(mandatory policy)이라는 접근제어를 시행한다. SORION에서도 객체의 분류등급(classification), 분류등급 요구조건 등과 같은 성질들을 제시하고 있지만, SORION는 객체 지향 데이터베이스 시스템에서 강제적 보안성에 초점을 두고 있다.

본 논문에서는 다단계 응용 영역에 대한 사용자 요구사항을 분석하여 다단계 객체 모델을 표현하는 개념적 모델에 초점을 두고 있다. 그러나 본 논문의 접근 방법은 SORION과 기본 보안 성질면에서 유사하며, 기본 키, 다항 관련성과 같은 무결성 제약조건을 포함하여 다단계 객체 모델을 서술함으로써 다단계 응용 영역의 요구사항들을 잘 표현할 수 있다. 그리고 다단계 객체 모델을 다단계 보안 객체 지향 스키마로 변환하는 규칙을 정의한다. 이 스키마는 여러 가지 상용 다단계 보안 데이터베이스 관리 시스템에 맞는 목표 시스템으로 변환될 수 있다.

### 3. 다단계 객체 모델

객체 모델은 응용의 객체와 그들 관련성에 대한 정적 구조를 서술한다. 즉, 응용 영역의 주요 추상화와 그들의 관련성을 표현하는 표기법이나 개념 집합이다. 보통의 객체 지향 접근방법에서처럼, 클래스(class)나 객체(object)와 같은 개념이 모델링에서 주된 역할을 한다. 응용 영역에 대한 이해는 가장 중요한 객체의 식별, 그리고 동일 종류에 속한 각각의 객체에 퍼져 있는 공통 특징들을 인식함에서부터 시작된다. 내부적 구조(structure)나 행위(behavior)와 같은 객체의 공통 성질들은 객체 클래스로 묶을 수 있다.

IDEA 방법론에서는 객체의 정적 서술(static descri-

ption of object)을 위해 확장된 객체-관련성(extended Entity-Relationship) 모델을 이용한다. 객체는 클래스에 해당되며 관련성은 클래스간의 참조(reference)에 해당된다. 클래스에는 그들의 속성(attribute) 및 메소드(method)가 있다. 클래스 계층구조와 다양한 무결성 제약조건들도 역시 표현된다.

IDEA 방법론이 데이터 집약 시스템에 대해 초점을 두고 있기 때문에, 객체 모델은 객체들 간의 관련성에 대한 구조적 관점을 특히 강조한다. 기존의 객체 지향 방법론과 비교하면, 정보 흐름을 표현하는 기능 모델(functional model)도 없고 객체들간의 메시지 교환을 나타내는 객체 상호작용도(object interaction diagram)도 없다. 필요할 때, IDEA 방법론의 분석 단계에서는 그런 표현을 통합하기 위해서 표준 표기법이나 기법을 이용함으로써 기존의 방법론과 쉽게 통합될 수 있다.

본 절에서는 IDEA의 객체 모델에 보안성을 첨가하는 방법을 논의할 것이다. 그러나, 일반적인 데이터 모델에서 언급하고 있는 의미적 제약조건이나 보안 모델들에서 취급하고 있는 분류등급 제약조건[9, 14, 18, 21, 22, 32, 33]과 같은 사항은 본 논문의 초점이 아니므로, 이들을 상세하게 다루지 않을 것이다.

#### 3.1 객체와 클래스

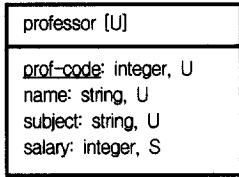
객체(Object)는 응용의 개별적인 개념을 나타낸다. 특정한 사람, 계약, 기업은 객체의 예이다. 데이터베이스에 저장된 객체는 실세계에 존재하는 객체에 해당한다. 그러나, 때때로 객체는 데이터베이스에서 배타적으로 존재한다. 각각의 객체는 객체가 초기에 생성될 때 시스템이 생성한 객체 식별자(object identifier)와 연관된다. 그래서, 데이터베이스 객체(실세계 객체와 같은 방법으로)는 구별되는 정체성(identity)이 있다.

객체는 응용의 개별적인 개념을 나타내며, 객체 O가 보안등급 L이라면, 그것의 객체-식별자가 L이라는 의미이고, 이것은 L 이상의 보안등급에서 볼 수 있다는 것이다.

객체들은 동일 구조를 가진 객체 집합으로 모을 수 있는데, 이들을 객체 클래스(object class)라고 하며 간단히 클래스라고 부른다. 클래스의 보안등급은 그 보안등급 이상인 객체들을 포함한다는 의미이다.

객체의 성질을 모델하지 않고 클래스와 객체를 모델한다는 것은 의미가 없다. 앞에서 언급한 것처럼 유사한 성질들을 가지는 객체들은 클래스로 묶는다. 그러

므로 성질들은 클래스 정의의 일부분으로서 명세되어야 한다. 이런 성질들을 속성이라고 한다. 속성 보안등급은 클래스 보안등급 이상으로 해야 안전하다. 그리고 속성 값의 보안등급은 속성 보안등급 이상이다. 그렇지 않으면, 속성 값을 판독하여 속성이 있다는 것을 추론할 수 있기 때문이다. 클래스의 예는 (그림 1)과 같이 그래픽 표기법으로 나타낼 수 있다.



(그림 1) 클래스의 그래픽 표기법

즉, 클래스 professor의 보안등급은 U이다. 그러므로 클래스 professor는 U, C, S, TS 보안등급의 인스턴스를 둘 수 있다는 의미이다. 속성 name은 U 등급이며, 그의 값 보안등급은 U, C, S TS 등급일 수 있다는 뜻이다.

기본 키(primary key)의 표시는 기본 키를 구성하는 속성 명칭에 밑줄을 친다. 기본 키는 클래스에 있는 각각의 원소들을 유일하게 식별하는 속성들의 집합이다. 본 논문에서는 다단계 관계형 모델에서 언급하고 있는 다단계 개체 무결성[6, 7, 8, 9]를 준수한다.

● 다단계 개체 무결성

릴레이션 R의 기본 키(primary key)를 형성하는 데이터 속성들의 집합을 AK라고 하자. 데이터 속성  $A_i \in AK$ 에 해당하는 모든 속성들의 분류등급  $C_i$ 는 R의 주어진 임의의 튜플내에서 동일 값이고, 이 등급은 데이터 속성  $A_j \notin AK$ 인 각각의 속성  $C_j$ 의 값 이하이다. R의 인스턴스에 있는 어떤 튜플도 임의의 기본 키 속성들에 대해서는 널(null) 값을 가질 수 없다.

다단계 개체 무결성(multilevel entity integrity) 성질이 의미하는 것은 기본 키를 형성하는 속성들에 대한 값은 임의의 튜플내에서 동일한 접근 등급(access class)이어야 한다는 것이며, 기본 키 값의 접근 등급은 튜플에 있는 모든 다른 원소들의 접근 등급 이하이어야 한다는 것이다. 기본 키의 분류등급이 다른 요소

들의 분류등급 이하이어야 한다는 제약조건은 관계형 모델의 개체 무결성 요구조건으로부터 나왔다. 즉, 튜플의 기본 키는 정의가 완전(널이 아니어야)해야 하고 변경되지 않아야 한다.

3.2 일반화와 상속성

일반화(generalization)는 한 클래스와 그 클래스의 정련된 버전(refined version)간의 관련성이다. 이 정련된 버전을 하위 클래스(subclass)라고 한다. 일반화의 개념은 IS-A 계층(hierarchy)이라는 클래스 계층(class hierarchy)을 이룬다. 어떤 클래스는 다중의 하위 클래스를 가질 수도 있다. 만일 C1이 C2의 하위 클래스라면, C2는 C1의 상위 클래스(superclass)가 된다.

어떤 모델에서는 상위 클래스를 하나로 제한하지만, 일반적으로는 다중의 상위 클래스를 가질 수 있다. 한 클래스가 두 개 이상의 상위 클래스를 가질 때 다중 상속성(multiple inheritance)이 발생하며, 단일 상속성(single inheritance)의 것을 자연스럽게 확장하는 의미가 있다. 다중 상속성에서는 하위 클래스가 상속받은 성질들이 동일 명칭(name)일 수 있는데, 그럴 경우 그 명칭에다 상속한 상위 클래스의 명칭을 앞에 덧붙임으로써 명시적으로 모호성을 피할 수 있다.

상위 클래스가 다중의 하위 클래스를 가질 때, 일반화는 상위 클래스 객체들과 하위 클래스 객체들 간의 사상(mapping)을 설정한다. 그 사상은 네 가지 성질로 특징 지을 수 있다.

- ① 상위 클래스의 모든 객체가 한 하위 클래스의 최소한 한 객체에 사상되면, 그 사상은 전체적(total)이다.
- ② 상위 클래스의 어떤 객체가 임의의 하위 클래스의 임의의 객체에 사상되지 않으면, 그 사상은 부분적(partial)이다.
- ③ 상위 클래스의 어떤 객체가 단지 한 하위 클래스의 한 객체에 사상되면, 그 사상은 배타적(exclusive)이다.
- ④ 상위 클래스의 어떤 객체들이 하위 클래스들의 여러 객체들로 사상이 되면, 그 사상은 중복적(overlapping)이다.

상속성의 표기법은 삼각형으로 상위 클래스와 그의 하위 클래스를 연결한다. 만일, 삼각형이 검은 색(▲)으로 채워져 있으면, 일반화는 전체적이면서 배타적인 사상이고 그 밖의 경우에는 빈(empty: △) 삼각형(부분적 사상이나 중복적 사상을 표시함)이다.

보안 관점에서 보면, 일반화는 정련된 메커니즘이기 때문에, 더 기밀한 속성(sensitive attribute)을 보호하는데 사용될 것으로 생각된다. 그러므로 시행할 성질은 하위 클래스 보안등급을 상위 클래스 보안등급 이상으로 하는 것이다. 물론, 하위 클래스들간의 보안등급 관련성은 독립적이다. 그러나 위의 ④번의 경우는 다르다. 왜냐하면, 여러 하위 클래스들로 사상된 객체들의 보안등급이 다르면, 다시 말해서 동일 인스턴스가 각각의 하위 클래스에서 보안등급이 다르다면, 추론 문제가 발생할 수 있다. 그러므로, 사상이 중복적일 때는 하위 클래스들의 보안등급을 동일하게 해야 한다.

다음은 단일 상속에 관한 것이다. 상위 클래스의 속성 보안등급이 하위 클래스 자신의 보안등급보다 낮으면, 하위 클래스로 상속된 속성은 하위 클래스의 보안등급으로 한다. 이것은 속성 및 클래스 보안등급 성질에 따라야 하기 때문이다.

다중 상속에 대한 보안성에 대해서는 본 논문에서 고려하고 있지 않으며, 객체 지향 데이터베이스 시스템에서 보안에 대한 상속성 논의를 위해서는 [26]을 참조하기 바란다.

### 3.3 관련성

관련성(relationship)은 객체들 간의 연관성이며, 그 표기법은 마름모(◇)로 한다. 관련성의 목적은 알려진 의미로 객체들 사이의 연결을 설정하는 것이다. 예를 들면, 사람들이 승용차를 운전하거나 학생들이 시험을 치른다는 같은 것이다. 보통, 관련성은 두 객체들을 연결한다. 이 경우에는 이항 관련성(binary relationship)이라고 부른다. 그러나, 관련성은 두 개 이상의 객체들을 연결할 수 있는데, 이 경우에는 다항 관련성(n-ary relationship)이라고 한다.

관련성은 클래스들 사이를 의미하고, 링크는 인스턴스 사이를 의미한다. 보안등급이 각 관련성에 할당되고, 이 관련성의 보안등급은 관련성에 참여하는 클래스 보안등급 이상이어야 한다. 예를 들어, U 등급의 관련성에 S 등급의 클래스가 연결된다는 것은 의미가 없기 때문이다.

관련성에는 연관될 수 있는 객체의 개수를 제한하는 대응수 제약조건이 있는데, 이는 일대일(one-one), 다대일(many-one), 혹은 다대다(many-many)라는 범주로 묶을 수 있다. 그러나 이들은 보안성에는 영향을 주지 않는다. IDEA 방법론에서 대응수의 표기법은 다

른 설계 방법과 일치하지만, [1] 그리고 Fusion[5]의 제안과는 다르다.

관련성에 보안등급을 부여할 때 중요한 논점 중의 하나는 발생할 수 있는 추론 문제이다. 예를 들어, 클래스 aircraft, destination, mission 간의 S 등급 삼항 관련성 flies를 보자. aircraft와 destination, destination과 mission, aircraft와 mission 간에 U 등급인 이항 관련성이 존재할 때, 이들 U 등급 관련성으로부터 S 등급 관련성 flies를 추론 할 수 있다. 또한, flies가 U 등급이고 aircraft와 destination 사이의 관련성이 S 등급이면, 불일치가 발생할 수 있다. 그래서 관련성에 보안등급을 부여할 때, 다음 사항을 고려해야 한다.

- C1, C2, ... , Cn 사이의 관련성이 L 이면, 클래스의 집합 {C1, C2, ... , Cn}의 부분 집합 사이의 어떤 관련성의 보안등급도 L 이하이어야 한다.
- 클래스의 집합 {C1, C2, ... , Cn}의 부분 집합 사이의 관련성 중 최소한 하나는 L이어야 한다.

모델링과 분석단계 동안, 이들 규칙 위반을 발견하면, 설계자는 잠재적 추론 문제에 주의해야 한다. 위의 방법은 [20]과 유사하다.

## 4. 다단계 객체 모델을 다단계 보안 객체 지향 스키마로 사상

앞 장에서는 IDEA 방법론의 객체 모델에 보안성을 첨가하는 방법을 논의하였다. 본 장에서는 이 객체 모델을 다단계 보안 객체 지향 스키마로 변환하는 방법론을 설명한다. 주요 논점은 보안이 유지되고 추론을 방지하는 기법으로 사상하는 것이다. Elmasri와 Navathe[10]은 객체 지향 접근방법의 단점 중 하나가 의미 모델들에서 일반적으로 표현할 수 있는 관련성을 직접 지원하지 않는다고 설명했다. 명시적으로 표현하는 것이 아니라, 그 관련성은 객체 참조로 해서 간접적으로 표현된다. 본 논문에서도 이런 객체 참조 방법으로 변환을 하며, 보안성이 첨가된다.

본 논문에서 객체 지향 스키마를 명세하는 준정형식은 MKDL(multilevel knowledge data language)[14]와 유사하다(그림 2). 스키마 명세어의 형식은 CLASS라는 하나의 구성체로 이루어지며, CLASS 명세에는 상위 클래스, 하위 클래스 속성(성질), 제약조건 등이 명시된다.

```

CLASS class-name[security-level]
SUPERCLASSES { (class-name-1[security-level]), ... }
ATTRIBUTES
{ (attribute-name-1: type, [security-level]),
  (attribute-name-2: type, [security-level]), ... }
KEY {(attribute-name-1), ... }
SUBCLASSES { (class-name-1[security-level]), ... }
INTEGRITY-CONSTRAINT { (logical formula), ... }
SECURITY-CONSTRAINTS { (logical formula[security-level]),
                        ... }
END class-name
    
```

(그림 2) 스키마 명세어

(그림 3)은 클래스 employee에 대한 명세이다. 속성은 name[U], address[C], salary[C]이고, 하위 클래스는 student-employee[C]이며, 상위 클래스는 people[U]이다. 그리고 기본 키는 name이다. 일반 데이터 모델에서도 언급되는 “직원의 봉급은 800000이상이어야 한다”는 무결성 제약조건이 있다. 그리고 “salary가 3000000 이상이면 salary의 보안등급은 S이다”라는 보안 제약조건에 보안등급은 S이다. 여러 가지 보안등급 제약조건이 있으며, 이에 대한 문헌은 [9, 14, 18, 21, 22, 32, 33] 등이다.

```

CLASS employee[U]
SUPERCLASSES { people[U] }
ATTRIBUTES
{ (name: string, [U]),
  (address: string, [C]),
  (salary: integer, [C]) }
SUBCLASSES { student-employee[C] }
KEY { name }
INTEGRITY-CONSTRAINTS { salary ≥ 800000 }
SECURITY-CONSTRAINTS { (IF(salary≥3000000) THEN
                        security-level(salary)=S)[S] }
END employee
    
```

(그림 3) employee에 대한 스키마 예제

개체-관련성 모델을 객체 지향 스키마로 사상하는 방법에는 최소한 두 가지가 있다[23]. 첫 번째 유형은 각각의 개체와 관련성을 객체로 변환하는 것이고[15], 두 번째 유형은 참조를 사용하여 관련성을 객체 클래스로 통합하고 삼항 관련성에 대해서는 하나의 객체 클래스를 생성하는 것이다[13].

본 논문에서는 IDEA 방법론[3]의 설계와 유사하지만 보안등급이 추가됨으로써 그 변환 방법이 달라진다.

#### 4.1 일반화 설계

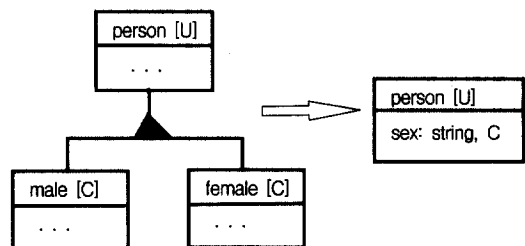
객체 모델에서 일반화 계층구조에 대한 초기의 정의가 여전히 유효한가를 검증할 목적으로 일반화 계층구조를 검토해보기로 한다. 일반화 계층구조를 만들기 위한 어떤 기준이 있어야 한다. 임의의 하위 클래스는 다음 목적 중 하나를 주로 제공한다.

- ① 상위 클래스의 정적 상태에 대해서, 부가적인 정보를 저장할 수 있도록 적절히 확장될 정적 상태(static state)를 가져야 한다.
- ② 직접적으로 하위 클래스의 객체에 적용되지만 상위 클래스가 지원하지 못 하는 어떤 연산(operation)이나 제약조건(constraint)이 있어야 한다.

만일 위의 조건 중 어느 것도 갖추지 않으면, 하위 클래스는 연관된 의미(semantics)가 없다. 클래스의 원소(element)를 표시할 명칭을 도입하는 것이 여전히 편리하지만, 실제로 하위 클래스가 자율적으로 도입하는 부가적인 구조적 정보는 없다. 그러므로, 이 단계에서 하위 클래스를 제거할 수 있다.

그러나 위의 두 조건이 충족되지 않아도 보안 관점에서는 유효하다. 즉, 하위 클래스들의 보안등급이 서로 다를 때는 위의 사항에 따라 일반화를 제거할 수 없다. 그렇지만 하위 클래스들의 보안 등급이 동일할 때는 상위 클래스의 정적 상태에 제거될 하위 클래스를 모델하는 하나 이상의 부가적인 속성을 첨가해야 한다. 물론 부가적으로 첨가된 속성의 보안등급은 제거된 하위 클래스의 보안등급을 그대로 따른다.

예를 들어, U 등급의 클래스 person에 C 등급의 sex 속성을 간단히 첨가함으로써 person 일반화에서 male과 female을 제거한다(그림 4). 물론, sex 속성에 적당한 값을 줌으로써 특정 하위 클래스에 있는 멤버십(membership)을 모델한다.



(그림 4) 일반화 계층구조의 제거

4.2 관련성 설계

객체 지향 모델에서 관련성은 객체-값(object-valued) 속성(한 클래스에서 다른 클래스로의 포인팅)으로 보통 표현된다. 예를 들면, employee와 department 사이의 관련성 worksIn은 employee에 객체-값 속성(그의 타입은 department)을 첨가함으로써 모델된다. employee에서 department로의 관련성 순회(traversal)는 employee 정적 상태 내에 저장된 특정 부서 객체의 객체 식별자를 접근함으로써 이루어진다.

객체-값 속성으로 모델될 관련성을 객체 모델에서 제거하고, 제거된 관련성에 해당하는 객체-값 속성을 어떤 클래스에 포함시킨다. 이 과정에서 몇 가지 설계 방안이 있다. 대부분의 경우는 각각의 관련성에 대하여 하나의 포인터를 저장하면 충분하다. 그러나 어떤 경우에는 각 클래스에 한 쌍의 포인터를 저장하는 것이 편리하다. 이것은 관련성에 대한 대칭적인 순회가 가능하지만, 중복(redundancy)이나 어떤 관련된 부담(overhead)이 있을 수 있다. 또 어떤 경우에는 보조 클래스를 도입할 수 있다.

보안성을 고려할 때, 관련성의 보안등급은 이에 참여하는 클래스 보안등급 이상이어야 한다고 3.3절에서 설명하였다. 그런데 관련성에 참여하는 클래스 중에서 더 낮은 클래스에다 이 관련성에 해당하는 객체-값 속성을 첨가한다면, 이것은 더 낮은 객체에서 더 높은 객체를 참조한다는 뜻이 된다. 이렇게 된다면, 보안성을 보장할 수 없으며, 아래에서 설명할 다단계 관계형 모델의 다단계 참조 무결성[6, 7, 8, 9]를 위반한다. 여기서, 다단계 참조 무결성(multilevel referential integrity)을 언급한 것은 다단계 보안 객체 지향 모델에서도 참조한다는 의미가 유사하기 때문이다.

• 다단계 참조 무결성

참조될 릴레이션에 대응하는 기본 키를 가진 튜플이 없다면, 한 릴레이션에 있는 어떤 튜플도 널이 아닌 이차 키(secondary key)를 가질 수 없다. 한 튜플 내에서 이차 키를 구성하는 각각의 원소(element)의 접근 등급은 동일해야 하고(즉, 2차 키 속성들은 일정한 접근 등급이어야 한다), 참조될 튜플에 있는 기본 키 요소들의 접근 등급 이상이어야 한다.

다단계 참조 무결성 성질이 의미하는 것은, 만일 주어진 접근 등급에서 외래 키(foreign key)가 보인다면, 참조될 기본 키를 포함하고 있는 튜플도 역시 그 접근

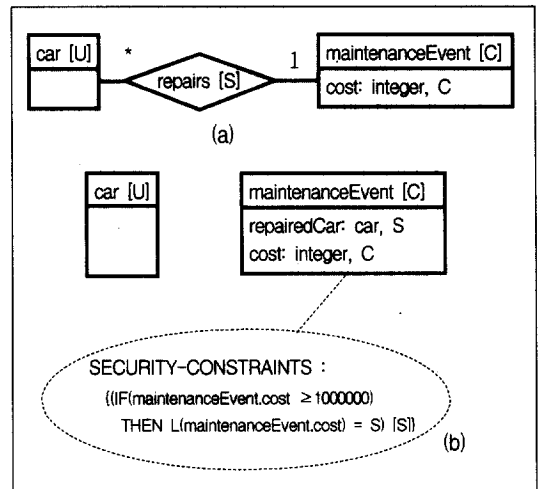
등급에서 보여야 한다는 것을 뜻하며, 또한 외래 키 원소의 보안등급은 참조될 기본 키의 보안등급 이상이어야 한다는 것이다. 즉, 모든 참조는 접근 등급에서 하향적이어야 한다.

(1) 단방향 참조

대부분의 경우는 각각의 관련성에 대한 단방향의 객체-값 속성으로 사상한다. 이런 방법을 단방향 참조(single reference)라고 한다. 보안등급  $L(C_1)$ 인 클래스  $C_1$ 과 보안등급  $L(C_2)$ 인 클래스  $C_2$ 를 연결하는 관련성  $R$ 의 보안등급을  $L(R)$ 이라고 하자. 그러면,  $L(C_1) \geq L(C_2)$ 일 때, 클래스  $C_2$ 로의 참조를 클래스  $C_1$ 에 첨가할 수 있다. 더 낮은 보안등급의 객체가 높은 보안등급의 객체를 참조한다는 것은 보안 유출이 발생할 수 있기 때문이다. 그 과정은 (그림 5)와 같다.

- ① 객체 모델에서 관련성  $R$ 을 제거한다.
- ②  $R$ 이라는 새로운 속성을 클래스  $C_1$ 에 도입한다.  $R$ 의 타입은  $C_2$ (클래스  $C_1$ 이  $R$ 에서 대응수가 일(one)일 때)이거나, 혹은 set-of( $C_2$ )(대응수가 다(many)일 때)이다.
- ③ 새로운 객체-값 속성의 보안등급은  $L(R)$ 로 한다.

(그림 5) 관련성을 단방향 참조로 변환



(그림 6) 관련성을 단일 참조로 변환하는 예제

예를 들어, (그림 6(a))에 나타난 car로부터 maintenanceEvent로의 관련성 repairs를 고려해 보자. 이것은 일대다(one-many) 관련성이다. 이 관련성은 (그림 6(b))에 나타난 것처럼 maintenanceEvent 클래스에 타입 car의 속성 repairedCar을 첨가함으로써 모델된다. 여기에서, 보안 제약조건의 의미는 maintenanceEvent 클래스의 cost 값이 1,000,000 이상이면, 그 cost 속성의 보안등급을 S 등급으로 하는 내용-종속 제약조건이며, 이 보안 제약조건 자체의 보안등급도 S 등급이라는 뜻이다.

(2) 양방향 참조

대부분의 응용에서는 양방향(대칭 순회)으로 관련성을 이용한다. 이 경우, 속성 쌍으로서 관련성을 모델할 수 있다. 각각은 하나의 순회 방향(traversal direction)을 모델링한다.

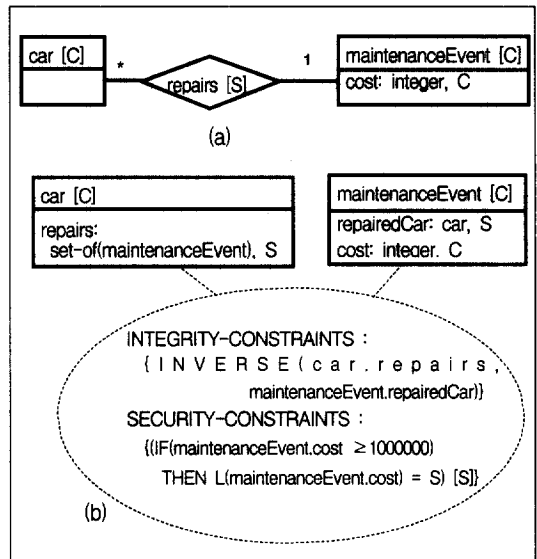
보안등급  $L(C_1)$ 인 클래스  $C_1$ 과 보안등급  $L(C_2)$ 인 클래스  $C_2$ 를 연결하는 관련성  $R$ 의 보안등급을  $L(R)$ 이라고 하자. 여기서는  $L(C_1)=L(C_2)$ 이고,  $L(R) \geq \text{least upper bound}(L(C_1), L(C_2))$ 이어야 한다.  $L(C_1) \neq L(C_2)$  이라면, 양방향 참조는 다단계 참조 무결성에 위배된다. 그리고  $A_1$ 은  $C_1$ 로부터  $C_2$ 로의 순회를 위한 명칭이고,  $A_2$ 는 역방향의 순회를 위한 명칭이라고 하자. 그러면 변환과정은 (그림 7)과 같다.

- ① 객체 모델에서 관련성  $R$ 을 제거한다.
- ②  $A_1$ 이라는 새로운 속성을 클래스  $C_1$ 에 도입한다.  $A_1$ 의 타입은  $C_2$ (클래스  $C_1$ 이  $R$ 에서 대응수가 일(one)일 때)이거나 set-of( $C_2$ )(대응수가 다(many)일 때)이다.
- ③  $A_2$ 라는 새로운 속성을 클래스  $C_2$ 에 도입한다.  $A_2$ 의 타입은  $C_1$ (클래스  $C_2$ 가  $R$ 에서 대응수 일(one)일 때)이거나 set-of( $C_1$ )(대응수가 다(many)일 때)이다.
- ④ 클래스  $C_1$ 에 포함될 속성  $A_1$ 의 보안등급  $L(A_1)$ 과 클래스  $C_2$ 에 포함될 속성  $A_2$ 의 보안등급  $L(A_2)$ 는 관련성  $R$ 의 보안등급  $L(R)$ 로 한다.  $A_1$ 과  $A_2$ 는 역 관련성을 나타낸다.

(그림 7) 관련성을 양방향 참조로 변환

예로서, (그림 8(a))의 car에서 maintenanceEvent로의 관련성 repairs를 양방향 참조(coupled reference)로 표현해 보자. 물론, 관련성에 참여하는 클래스들의 보

안등급은 같아야 한다. (그림 8(b))에 나타난 것처럼 두 개의 외연 속성 repairs와 repairedCar를 도입하여 관련성을 변환한다. 그리고 클래스 car의 속성 repairs와 클래스 maintenanceEvent의 속성 repairedCar는 역 관련성이라는 무결성 제약조건을 표현한다. (그림 8(b))에서의 보안 제약조건은 (그림 6(b))에 나타난 보안 제약조건과 동일하다.



(그림 8) 관련성을 양방향 참조로 변환하는 예제

(3) 가교 클래스

관련성이 상태(속성)를 갖거나 혹은 두 개 이상의 클래스와 연결될 때, 관련성의 사상에서는 가교 클래스(bridge class)라는 보조 클래스를 도입한다.  $R$ 을 위의 특징을 가진 관련성이라고 하고,  $C_i$ 는  $R$ 과 연계된 클래스라고 하자. 그리고  $C_i$ 와  $R$ 의 보안등급은 각각  $L(C_i)$ 와  $L(R)$ 이라고 하자. 이 때의 변환 과정은 (그림 9)와 같다.

- ① 관련성  $R$ 을 가교 클래스  $B$ 로 변환한다. 그리고  $R$ 을 제거한다.
- ② 처음의  $R$ 에 연결된 각각의 클래스  $C_i$ 에 대하여,  $B$ 의 상태에 객체-값 속성  $R_i$ (타입  $C_i$ )를 포함시킨다.  $B$ 의 모든 속성  $R_i$  집합은 보통  $B$ 의 기본 키(primary key)이다. 그러나,  $B$ 의 슈퍼 키(super key)일 수도 있다. 즉,  $B$ 의 객체들을 식별하기 위해 엄밀하게 필요하지



않는 어떤 속성들을 포함할 수 있다. 예를 들어, 만일, 담당 교수(professor)가 주어진 강의실(classroom)에서 각각의 과목(course)을 강의하면, lecture 가교 클래스에서는 (course, class) 쌍을 키(key)로 할 수 있다.

- ③ 만일, 관련성 R이 처음에 가진 속성이 있다면, R의 모든 속성들은 B의 속성이 된다.
- ④ 가교 클래스 B의 보안등급 L(B)는 관련성 R의 보안등급 L(R)로 설정하고, B의 상태에 포함된 객체-값 속성 R<sub>i</sub>의 보안등급 L(R<sub>i</sub>)도 관련성 R의 보안등급 L(R)로 한다. 가교 클래스 B의 보안등급을 관련성 R의 보안등급으로 하는 것은 당연하다. 그리고, 객체-값 속성 R<sub>i</sub>의 보안등급을 관련성 R의 보안등급으로 해야 하는 이유는 3.1절에서 설명한 다단계 개체 무결성을 위반하지 않아야 하기 때문이다.

속성에 해당한다. 그리고, 다단계 참조 무결성 성질을 준수해야 하므로, L(R<sub>i</sub>)와 L(B)가 동일할 때만이, 임의의 클래스 C<sub>i</sub>와 B 사이의 양방향 참조를 첨가할 수 있다. 양방향 참조를 첨가하기 위해서는 (그림 10)과 같은 과정이 더 필요하다.

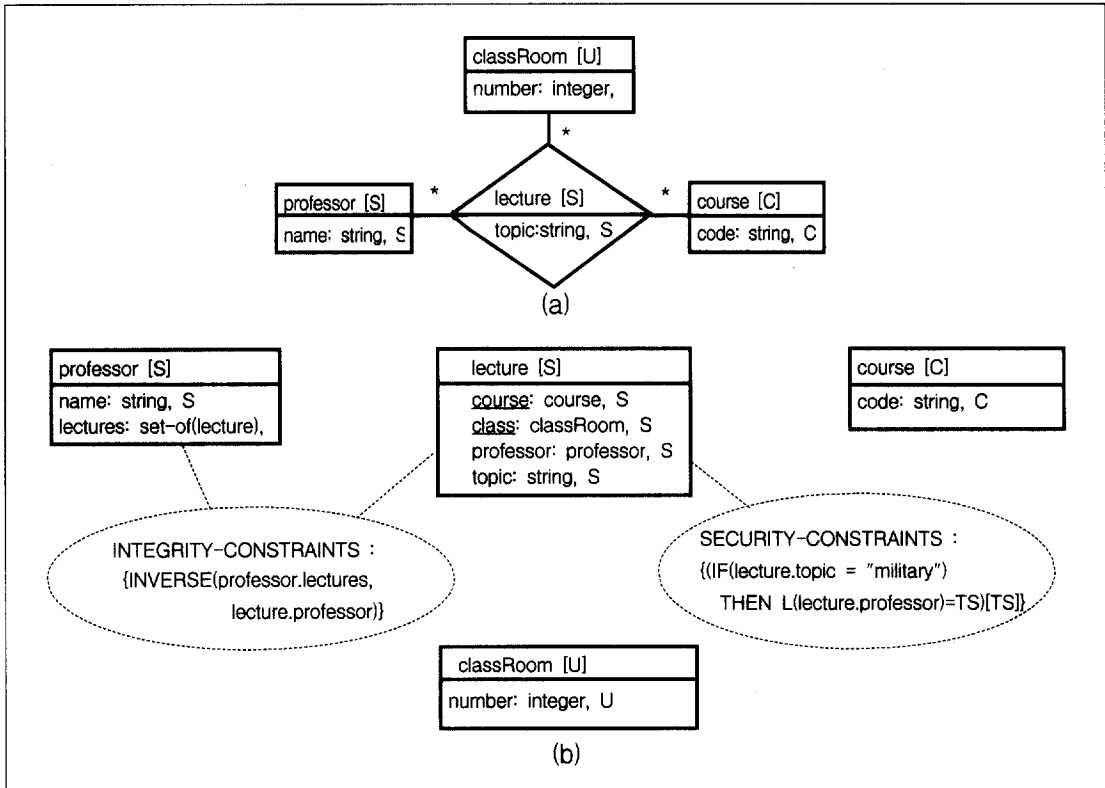
- ① 새로운 속성 A<sub>i</sub>를 C<sub>i</sub>에 덧붙인다. A<sub>i</sub>의 타입은 B(R에서 C<sub>i</sub>의 최대 대용수가 일(one)일 때)이거나 set-of(B)(R에서 C<sub>i</sub>의 대용수가 다(many)일 때)이다.
- ② 속성 A<sub>i</sub>의 보안등급 L(A<sub>i</sub>)는 B의 보안등급 L(B)와 동일하게 한다. 이것도 다단계 참조 무결성 때문이다.

(그림 9) 관련성을 가교 클래스로 변환

위의 방법은 여러 개의 단방향 참조가 나온다. 이들 각각은 가교 클래스 B에서 여러 클래스 C<sub>i</sub>로의 포인터

(그림 10) 가교 클래스로의 변환에서 양방향 참조 첨가

클래스 professor, course, 그리고 classRoom을 연결하는 삼항 관련성(ternary relationship) lecture를 고려해 보자. 강의는 주제()라는 속성이 있다. (그림 11(b))



(그림 11) 관련성을 가교 클래스로 변환하는 예제

는 관련성을 모델링하기 위해 가교 클래스를 도입하여 속성을 만든 후의 객체 모델을 설명하고 있다. 예제에서, professor에서 lecture로의 참조를 양방향(couple)으로서 모델하지만, lecture에서 course와 classRoom으로 단방향 참조이다.

(그림 11)에서 무결성 제약조건은 클래스 professor의 속성 lectures와 클래스 lecture의 속성 professor가 역 관련성이라는 것을 나타낸다. 그리고 보안 제약조건은 클래스 lecture의 속성 topic 값이 "military" 일 때, 클래스 lecture의 속성 professor의 보안등급을 TS로 하고, 이 보안 제약조건 자체의 보안등급도 TS로 한다는 뜻이다.

다항 관련성(n-ary relationship)은 여러 개의 이항 관련성(binary relationship)으로 분해할 수 있다. 이항 관련성을 이해하기가 더 용이하므로, 이 기법을 사용하는 방법도 연구 가치가 있다. 그러나 이것은 본 논문의 범위를 벗어난다. 이에 대한 더 많은 연구는 [10, 27, 24, 25] 문헌에 잘 제시되어 있다.

## 5. 결 론

다단계 운영 환경에서는 서로 다른 보안등급의 사용자들이 다단계 데이터베이스를 접근하지만, 다단계 보안 데이터베이스 관리 시스템(MLS/DBMS)은 사용자에게 인가되지 않은 데이터를 접근할 수 없도록 다단계 데이터베이스를 관리한다. 현재의 MLS/DBMS들은 SQL 표준을 확장하여 각각 서로 다른 다단계 환경을 구현한다. 결과적으로 다단계 데이터베이스 설계자가 각각의 DBMS를 이해하여 적용해야 한다. 그러므로 어떤 중간 단계의 스키마를 개발하고, 이것을 변환하여 각각의 MLS/DBMS에 대한 SQL을 자동 생성하는 도구를 만든다면, 많은 노력과 비용을 절감할 수 있다.

본 논문은 이런 중간 단계의 스키마(다단계 보안 객체 지향 스키마)를 개발할 목적으로 비보호 데이터베이스 응용 설계를 위한 IDEA 방법론을 활용함으로써 기존의 방법론에서 개발된 여러 기법들을 이용할 수 있다. 다단계 객체 모델에는 객체와 클래스, 다단계 객체 무결성, 일반화와 상속성, 관련성 개념 등이 포함된다.

그리고 다단계 객체 모델을 다단계 보안 객체 지향 스키마로 변환하는 방법을 제시했다. 보안 의미가 첨가됨으로써 IDEA 방법론의 의미가 달라지게 된다. 즉, 한 객체에서 다른 객체로의 참조(reference)는 보안 위

반이 발생하지 않도록, 반드시 높은 보안등급의 객체에서 낮은 보안등급의 객체로 참조되게 했다. 보통의 비보호 객체-관련성 모델을 객체 지향 스키마로 변환하는 연구나 보안 객체 모델을 다단계 보안 관계형 모델로 변환하는 연구도 많지만, 본 논문의 접근방법은 IDEA 방법론에서 동기가 되었으며, 다음과 같은 특징이 있다.

- 다단계 객체 모델에서는 객체 종속성을 더 분명하게 하는 클래스들간의 명시적 연관성(explicit association)을 사용한다. 즉, 일반 객체 지향 모델에서는 관련성을 직접 지원하지 않고, 객체 참조로써 간접적으로 표현한다. 그러나 본 논문에서의 다단계 객체 모델은 개체-관련성 모델과 같은 의미 모델에서처럼 관련성(예, 이항 관련성)을 명시적으로 나타냄으로써, 응용 영역에 대한 보안 요구사항을 직접적으로 표현한다.
- 다단계 보안 객체 지향 스키마 설계에서는 다단계 참조 무결성을 따른다.
- 비정형의 스키마 정의어에서 KEY 정의 부분이 있다. 일반 객체 지향 모델에서는 객체 값 속성으로 클래스간의 관련성을 직접 지원하기 때문에 키의 중요성은 없다. 그러나 다단계 객체 모델을 다단계 보안 관계형 시스템으로 변환할 경우, 빠른 접근 방법을 위해서 기본 키 개념이 필요하기 때문에, 다단계 보안 객체 지향 스키마에 키를 표기하는 것은 매우 중요한 의미가 있다.

본 논문의 결과는 여러 가지의 상용 보안 DBMS로의 사상(mapping)을 자동화시키는 범용 스킵이 되는 기초 자료가 될 것이다. 그러나 추후 연구과제로서 정적 성질 이외의 동적 성질이나 연산과 같은 특성뿐만 아니라 연관성 대응수(association cardinality)[30]나 데이터 종속성(data dependency)[31]을 이용한 추론분석에 대한 연구가 진행되어야 할 것이다.

## 참 고 문 헌

- [1] C. Batini and S. B. Navathe, Conceptual Database Design, an Entity-Relationship Approach, Redwood City, CA, Benjamin Cummings, 1993.
- [2] Burns, R., "ER Approach to Multilevel Database

- Design," The 1st RADC Database Security Workshop Menlo park, CA, May 1988.
- [3] S. Ceri and P. Fraternali, *Designing Database Applications with Objects and Rules*, Addison-Wesley, 1997.
- [4] P. Chen, "The Entity-Relationship Model : Toward a Unified View of Data," *ACM Transaction on Database Systems*, Vo. 11, No. 1, pp.9-36, 1976.
- [5] D. Coleman, P. Arnold, S. Bodoff et. al., *Object-Oriented Development : The Fusion Method*, Englewood Cliffs, NJ, Prentice-Hall International, 1994.
- [6] D. E. Denning et al., *Secure distributed data view : security policy and interpretation for class A1 multilevel secure relational database system*, Technical Report A002 SRI International, 1986.
- [7] D. E. Denning, *Secure distributed data views : the Sea View formal security model*, Technical Report A003 SRI international, 1987.
- [8] D. E. Denning, et. al., "Views for multilevel database security," *IEEE Trans. Software Eng.* 13(2), 1987.
- [9] D. E. Denning et al., "The Sea View security model," *Proc. IEEE Symp. on Security and Privacy*, Oakland, CA, April 1988.
- [10] R. Elmasri and S.B. Navathe, *Fundamentals of Database Systems*, Second edition, Benjamin/Cummings, redwood City, 1994.
- [11] M. Fugini, "Secure Database Development Methodologies," *Database Security : Status and Prospects*, C. E. Landwehr, eds., North Holland(Elsevier), pp.103-130, 1988.
- [12] G. E. Gajnak, "Some Results from the Entity-Relationship Multilevel Secure DBMS Project," *Proc. 4th IEEE Annual Computer Security Application Conference*, 1988
- [13] J. G. Hughes, *Object-Oriented Databases*, Computer Science, Prentice Hall, 1991.
- [14] D. G. Mark et al., "Hypersemantic Data Modelling for Inference Analysis," *DATABASE SECURITY VIII : Status and Prospects*, North-Holland, pp.157-180, 1994.
- [15] S. B. Navathe and M. K. Pillallmarri, "OOER : Toward Making the ER Approach Object Oriented," *Proceedings of the 8th International Conference on Entity-Relationship Approach*, pp.55-76, 1989.
- [16] B. H. Patkau, D. L. Tennenhouse, "The Implementation of Secure Entity-Relationship Databases," *Proc. IEEE Symposium on Security and Privacy*, 1985.
- [17] G. Pernul, A. M. Tjoa, "A View Integration Approach for the Design of MLS Databases," *Proc. 10th Int'l. Conf. on the Entity-Relationship Approach*, San Mateo, CA, Oct. 1991.
- [18] G. Pernul, "Security Constraint Processing During Multilevel Secure Database Design," *Proc. 8th Annual Computer Security Applications Conference*, IEEE Computer Society Associations, pp.75-84, 1992.
- [19] Sell, P., "The SPEAR Data Design Methodology," *Proceedings of the 6th IFIP Database Security Conference*, Vancouver, BC, August 1992.
- [20] P. J. Sell and B. M. Thuraisingham, "Applying OMT for Designing Multilevel Database Applications," *DATABASE SECURITY VII : Status and Prospects*, North-Holland, pp.41-64, 1994.
- [21] Smith, G., "Modelling Security Relevant Data Semantics," *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, 1990.
- [22] G. W. Smith, "The Semantic Data Model for Security : Representing the Security Semantics of an Applications," *Proc. of the 6th Int. Conf. on Data Engineering*, 1990.
- [23] I.Y. Song, "A Survey of Object Oriented Database Design Methodologies," *Proceedings of the International Conference on Information and Knowledge Management*, Baltimore, MD, pp.52-59, 1992.
- [24] I. Y. Song and T. H. Jones, "Analysis of Binary Relationships with Ternary Relationships in ER Modeling," *In Proceedings of 12th International*

Conference on Entity-Relationship Approach, Dallas, TX, December, pp.265-276, 1993.

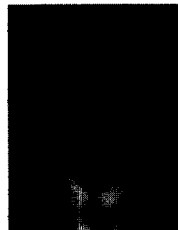
- [25] I. Y. Song, T. H. Jones, and E. K. Park, "Binary Relationship Imposition Rules on Ternary Relationships in ER Modeling," In proceedings of 2nd International Conference on Information and knowledge management, Washington, D.C., October, pp.57-66, 1993.
- [26] D. Spooner, "The Impact of Inheritance on Security in Object-Oriented Database Systems," Database Security II : Status and Prospects, Ed : C. Landwehr) North-Holland, 1989.
- [27] T. J. Teorey, Database Modeling and Design : The Fundamental Principles, 2nd Edition, Morgan-Kauffman, 1994.
- [28] Wiseman, S., "Abstract and Concrete Models for secure Database Applications," Proceedings of the 5th IFIP Working Conference in Database Security, Shepherstown, W. VA, November 1991.
- [29] Thuraisingham, M. B., "Mandatory security in object-oriented database systems," Pro. Conf. on Object-oriented Programming : Systems, Languages, and Applications(OOPSLA), Orlando, October 1989.
- [30] T. H. Hinke, H. S. Delugach and R. Wolf, "A Framework for Inference-Directed Data Mining," DATABASE SECURITY Volume X : Status and Prospects, Chapman & Hall, pp.229-239, 1997.
- [31] K. Zhang, "IRI : A Quantitative Approach to Inference Analysis in Relational Database," DATABASE SECURITY XI : Status and Prospects, Chapman & Hall, pp.279-290, 1998.
- [32] 김영균, 노봉남, "보안 객체 지식 모델에서 보안 제약 조건", 통신정보보호학회논문지, 제3권, 제1호, pp.48-57, 1993.
- [33] 박선주, 노봉남, "다단계 보안 멀티미디어 데이터 모델을 위한 보안 제약조건", 통신정보보호학회논문지, 제3권, 제2호, pp.16-30, 1993.



### 김정중

e-mail : jkim@eros.kyungnam.ac.kr  
 1977년 중앙대학교 전자계산학과 (이학사)  
 1981년 중앙대학교 대학원 전자계산학과(이학석사)  
 1988년 중앙대학교 대학원 전자계산학과(이학박사)

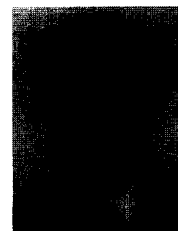
1978년 삼미금융(주)  
 1979년~1980년 금성통신(주) 연구소  
 1981년~현재 경남대학교 컴퓨터공학과 교수  
 관심분야 : 소프트웨어 공학, 객체지향 분석 및 설계



### 박운재

e-mail : wjpark@mail.tpc.ac.kr  
 1989년 경남대학교 전자계산학과 (공학사)  
 1993년 경남대학교 대학원 전자계산학과(공학석사)  
 1997년 경남대학교 대학원 전자계산학과 박사과정 수료

1989년~1994년 한국산업단지공단  
 1995년~현재 한국섬유패션대학 전자계산과 조교수  
 관심분야 : 객체지향 분석과 설계, 데이터베이스 응용 설계



### 심갑식

e-mail : gssim@cjcc.chinju.ac.kr  
 1985년 전남대학교 계산통계학과 (이학사)  
 1987년 전남대학교 대학원 계산통계학과(이학석사)  
 1993년 전남대학교 대학원 전산통계학과(이학박사)

1993년~현재 진주산업대학교 교양과정부 부교수  
 관심분야 : 데이터베이스 보안, 데이터베이스 응용 설계, 컴퓨터와 정보사회