Journal of The Korea Society of Computer and Information
Vol. 17, No. 12, December 2012
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2012.17.12.169

웹 응용 시스템 개발을 위한 보안을 고려한 통합 분석·설계 방법론 개발 - Oracle11g를 중심으로 -

주경수*, 우정웅*

A Development of the Unified Object-Oriented Analysis and Design Methodology for Security-Critical Web Applications Based on Object-Relational Database - Forcusing on Oracle11g -

Kyung-Soo Joo*, Jung-Woong Woo*

요 약

응용 시스템 개발 과정에 있어서 중요하고 핵심을 이루는 작업은 분석과 설계 작업이며 아울러 대부분의 응용 시스템은 데이터베이스 기반으로 구축된다. 또한, IT 시스템들 간 상호 연결이 증가되면서 응용 시스템들은 외부 공격에 쉽게 노출되어 지고 있기 때문에 보안과 관련된 처리 과정 역시 중요하다.

보안은 시스템에서 많은 부분과 상호작용을 하는 복잡한 비기능적 요구사항이다. 하지만 이러한 보안은 대부분 개발 마지막 과정에서 고려하기 때문에 보안에 취약한 응용 시스템이 개발될 가능성이 매우 높다. 따라서 개발 초기에 보안을 반영한 분석 및 설계 과정이 매우 중요하다.

J2EE는 웹 응용 시스템을 위한 보안 방안을 제공하고, 아울러 객체-관계형 데이터베이스도 보안을 위하여 역할기반 접근제어를 지원하고 있지만 객체-관계형 데이터베이스 및 J2EE의 역할기반 접근제어를 활용하는, 요구사항 수집부터 구현까지 개발 단계 전체에 걸친 보안을 고려한 일관된 개발방법론은 전무한 실정이다.

따라서 본 논문에서는 보안 요구사항을 요구사항 수집부터 분석 및 설계 그리고 마지막 구현 단계까지 반영하여 J2EE 기반의 웹 응용 시스템을 개발하기 위한, 보안을 고려한 일관된 통합 분석·설계 방법론을 제안한다.

▸ Keywords : 객체지향 분석·설계, 객체-관계형 데이터베이스 설계, RBAC, J2EE, 보안

• 제1저자 : 주경수 • 교신저자 : 우정웅
• 투 고 일 : 2012. 9. 11, 심사일 : 2012. 10. 14, 게재확정일 : 2012. 11. 8.
* 순천향대학교 컴퓨터소프트웨어공학과(Dept. of Computer Software Engineering, SoonChunHyang University)

Abstract

In the development process of application systems, the most important works are analysis and design. Most of the application systems are implemented on database system. So, database design is important. Also, IT System are confronted with more and more attacks by an increase interconnections between IT systems. Therefore security-related processes belong to a very important process.

Security is a complex non-functional requirement that can interaction of many parts in the system. But Security is considered in the final stages of development. Therefore, Their increases the potential for the final product to contain vulnerabilities. Accordingly, Early in development related to security analysis and design process is very important.

J2EE gives a solution based on RBAC((Role Based Access Control) for security and object-relational database also has RBAC for security. But there is not a object-oriented analysis and design methodology using RBAC of J2EE and object-relational database for security.

In this paper, the unified object-oriented analysis and design methodology is developed for security-critical web application systems based on J2EE and object-relational database. We used UMLsec and RBAC of object-relational database and J2EE for this methodology.

▸ Keywords : Object-Oriented Analysis Design, Object-Relational Database, RBAC, J2EE, Security

I. 서 론

인터넷의 급속한 발전으로 인해 J2EE(Java 2 Platform, Enterprise Edition) 기반의 웹 응용 시스템이 많이 개발되고 있다. 이러한 응용 시스템을 개발하는 과정은 정보시스템을 비즈니스 요구사항에 맞도록 설계하고 구축하여 사용자에게 배포하는 과정이다[1,2]. 또한, 현재의 웹 응용 시스템들은 복합객체를 갖고 있다는 특징에 따라 관계형 데이터베이스에서 객체-관계형 데이터베이스로 확장되어 구축되고 있다. 그러나 웹 응용 시스템 개발을 위한 객체지향 분석·설계방법론과 객체-관계형 데이터베이스 설계를 위한 방법론들이 따로 존재하여, 일관된 웹 응용 시스템을 개발하기 어렵다.

또한, J2EE는 웹 응용 시스템들을 위하여 보안을 지원하고 있지만, 이러한 기술들은 대부분 분석·설계의 결과로 사용된 것이 아니기 때문에 일관성이 없어, 보안에 취약한 웹 응용 시스템이 개발될 가능성이 매우 높다[3,4].

이에 따라 본 논문에서는 기존의 객체지향 분석·설계 방법론과 객체-관계형 데이터베이스 설계방법을 기반으로, 보안 요구사항을 요구사항 수집부터 분석·설계 그리고 구현 단계까지, 전 개발단계에 걸쳐 보안에 대한 일관성을 제공하는 통합 객체지향 분석·설계 방법론을 제안한다.

본 논문에서는 J2EE 기반기술 중 JSP와 서블릿을 대상으로 하였고 EJB는 제외하였다.

본 논문의 구성은 다음과 같다. 2장에서는 제안한 방법론의 이해를 돕기 위한 관련 연구들을 소개하고, 3장에서는 제안한 방법론의 적용, 4장에서는 제안한 방법론과 기존 방법론과 비교하고, 5장에서는 결론을 제시한다.

II. 관련연구

1. 객체지향 분석·설계 방법론

객체지향 분석·설계 방법론 중 대표적인 RUP(Rational Unified Process)의 특징은 유스케이스 기반, 아키텍처 중심, 반복 및 점증적이며, 도메인 모델, 유스케이스 모델, 분석 모델, 설계 모델 그리고 구현 모델 등으로 작성된다

[5]. 다만 RUP는 관련된 케이스 툴을 사용하여 관계형 데이터베이스 설계 작업을 부분적으로 지원하고는 있으나 보안에 대한 일관된 분석·설계 방법론은 제시하지 못하고 있다.

2 객체-관계형 데이터베이스 설계 방법론

객체-관계형 데이터베이스 설계 방법론으로는, 확장된 UML 클래스다이어그램을 이용하여 특정 DBMS를 위한 설계 방법론이 존재한다[6]. 이 연구에서는 확장된 UML 클래스다이어그램을 객체-관계형 데이터베이스 스키마로의 변환을 위한 가이드라인을 제시하여 일관된 설계 방법론을 제시하고는 있지만, 기존의 객체지향 분석·설계 방법론과 상호 연관성은 제공하지 못하고 있다.

3 UMLsec을 이용한 보안 유스케이스 모델링

보안과 관련한 분석·설계 방법으로는, 기존의 객체지향 분석·설계 방법론과 보안 요구사항을 통합한 UML 기반의 개발 방법론이 제시되었다[7]. 이 연구에서는 확장된 UMLsec을 이용해서 보안이 중요한 응용소프트웨어시스템 개발을 위한 일관된 객체지향 분석·설계 방법론을 제시하고는 있지만, 객체-관계형 데이터베이스 및 J2EE와의 상호 연관성은 제공하지 못하고 있다.

4 J2EE 기반의 웹 보안

웹 응용소프트웨어들은 다양한 위험에 노출되어 있다. 이러한 위험을 막기 위해 서블릿에서 보안을 설정할 수 있으며, 서블릿 보안의 4요소는 인증, 인가, 비밀보장, 데이터 무결성으로 이뤄진다. J2EE에서의 인증은 BASIC, DIGEST, CLIENT-CERT, FORM과 같이 4가지 인증 방법이 존재한다[8].

한편, 웹 기반의 응용소프트웨어는 MVC 패턴을 주로 사용하여 개발하고 있다.

III. 보안을 고려한 통합 분석·설계 방법론

제안한 통합 객체지향 분석·설계 방법론은, 그림1과 같이 요구사항 정의 단계에서 보안에 대한 요구사항을 추가하였으며, 분석 및 설계 단계에서 UMLsec을 이용한 보안 요구사항을 반영하였고 아울러 객체-관계형 데이터베이스 설계 방법론과 통합하였다. 또한 마지막 구현 단계에서는 보안 요구사항의 설계 결과를 J2EE의 역할기반 접근제어와 객체-관계형 데이터베이스의 역할기반 접근제어를 이용하여 구현하였다.

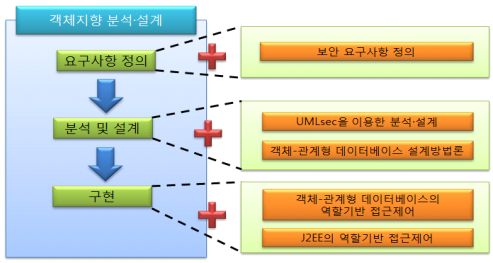

그림 1. 통합 객체지향 분석·설계 방법론 과정
Fig. 1. Process of Integrated Object-Oriented Analysis and Design Methodology

1. 통합 객체지향 분석·설계 방법론

1. 요구사항 정의

1.1 요구사항 리스트 작성

요구사항 정의 단계는 사용자로부터 요구사항을 도출하고 이를 분석하고 요구사항 리스트를 작성하는 활동으로 구성된다[1]. 다음 표1은 가로세로 퍼즐 시스템의 요구사항 리스트에 해당한다. 아울러 퍼즐의 생성은 학생이 아닌 교수만이 생성을 할 수 있기 때문에 퍼즐 생성과 관련된 접근권한은 교수만이 가지고 있다. 따라서 보안에 대한 요구사항은 표1의 9번 항목에 해당한다.

표 1. 가로세로 퍼즐 시스템을 위한 요구사항 리스트
Table 1. Requirement list of 'Horizontal and Vertical Puzzle System'

1. 학생은 원하는 챕터의 퍼즐을 선택 할 수 있어야 한다.
2. 학생은 챕터 선택으로 되돌아 갈수 있어야 한다.
3. 학생은 원하는 챕터의 퍼즐이 보여야 한다.
4. 학생은 퍼즐의 한 칸을 선택하면 문제를 볼 수 있어야 한다.
5. 학생은 문제에 답을 쓸 수 있어야 한다.
6. 학생에게 힌트를 제공해야 한다.
7. 학생은 문제를 풀지 않을 수 도 있다.
8. 퍼즐은 학생이 답을 맞추면 답을 보여줘야 한다.
9. 교수만 새로운 챕터의 퍼즐을 만들 수 있어야 한다.

1.2 유스케이스 작성

유스케이스는 시스템이 어떤 일을 수행하기 위해 거쳐야 하는 단계들을 말하며, 또한 새로 만들 시스템이나 소프트웨어 변경사항에 대한 요구사항을 찾아내는 방법이다[1].

표1에서 작성된 사용자 요구사항 리스트를 기반으로, 보안이 고려된 유스케이스를 작성한다. 이에 따라 보안이 요구되는 유스케이스의 경우에는 유스케이스를 확장해야 된다. 다음

표2는 보안이 요구되는 '사용신청'에 대한 유스케이스이며, 표 3은 '가로세로 퍼즐 시스템'에 대한 일반적인 유스케이스 중 하나이다.

표 2. '사용신청'을 위한 유스케이스
Table 2. Usecase of 'Request'

Use Case : 사용신청

Actor와 관련된 위험성
- 별도의 계정구분이 없기 때문에 학생 계정을 가지고 있는 사용자가 교수로 위장하여 접근할 수 있다.

Security-Critical과 uncritical 입·출력 데이터

Security-Critical I/O	uncritical I/O
아이디	-
패스워드	-

변경된 시스템의 행동
- 교수와 학생은 사용신청 시 신분이 구분될 수 있도록 별도의 계정으로 가입된다. 즉, 사용허가 유스케이스 를 포함하여 시스템으로부터 사용자 구분에 맞는 인 증을 받게 되며, 사용신청 결과 화면을 보여준다.

표 3. '로그인'을 위한 유스케이스
Table 3. Usecase of 'Login'

1. 로그인 버튼을 누른다.
2. 등록된 아이디와 패스워드를 입력한다.
   2.1 교수는 교수 버튼을 선택한다.
   2.2 학생은 학생 버튼을 선택한다.
   2.3 되돌아가기 버튼을 누른다.
3. 확인 버튼을 누른다.
4. 계정 확인 유스케이스를 포함한다.
5. 로그인 결과 화면을 보여준다.

1.3 유스케이스 모델 상세화

유스케이스 상세화 활동에서는 직전 활동에서 도출된 각 유스케이스별로 개요, 관련 액터, 우선순위, 선행/수행 조건, 시나리오 비기능적 요구사항을 정의한다[9]. 또한 보안이 요구되는 유스케이스의 경우에는 비기능적 항목에서 보안에 대한 정의를 명확하게 정의해야 한다. 다음 표4는 보안이 필요한 사용신청 유스케이스 명세서에 해당하며, 유스케이스 명세서를 통한 사용신청 유스케이스의 기본 시나리오는 표 5와 같다.

표 4. '사용신청'을 위한 유스케이스 명세서
Table 4. Usecase Specification of 'Request'

항 목	설 명		
이름	사용신청		
개요	학생과 교수는 계정에 대한 사용신청을 한다.		
관련 액터	주액터	학생, 교수	
우선 순위	1	중요도	1(상)
		난이도	3(하)
선행 조건	학생과 교수는 아이디와 패스워드를 입력하고 확인 버튼을 누른 상태이어야 한다.		
후행 조건	사용신청 확인 결과를 보여준다.		
시나리오	기본 시나리오	학생 및 교수는 아이디를 입력한다.	
	대안 시나리오	조건에 맞지 않는 아이디 및 패스워드를 입력했을 경우에 대한 경고문을 확인한다.	
비기능적 요구사항	교수만이 퍼즐을 생성할 수 있다.		

표 5. '사용신청'을 위한 기본 시나리오
Table 5. Basic Scenario of 'Request'

1.사용자는 사용신청 버튼을 누른다.
2.아이디와 패스워드를 입력한다.
   2.1 조건에 맞지 않는 데이터를 입력하지 않을 경우 경고문 확인 후 다시 입력한다.
   2.2 되돌아가기 버튼을 누른다.
3.확인 버튼을 누른다.
4.사용신청 결과를 화면에 보여준다.

1.4 유스케이스 모델 작성

유스케이스 모델 작성은 시스템이 제공할 개별 기능을 유스케이스로 표현하고, 유스케이스와 상호작용을 하는 시스템 외부의 존재를 액터로 표현한다. 그리고 유스케이스 모델의 시각적인 표현을 위해 UML의 유스케이스 다이어그램을 사용하며, 액터와 유스케이스 간의 연관 관계를 표현함으로써 어떤 액터가 어떤 유스케이스를 이용하는지를 기술한다[9]. 다음 그림2는 가로세로 퍼즐 시스템의 유스케이스 모델 작성을 보여준다.

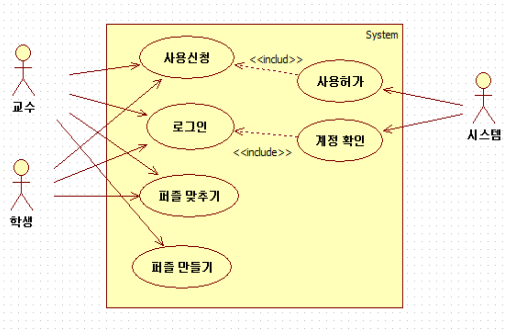

그림 2. '가로세로 퍼즐 시스템'을 위한 유스케이스 모델
Fig. 2. Usecase Model of 'Horizontal and Vertical Puzzle System'

2. 보안을 고려한 분석·설계 단계

분석 단계는 요구사항을 충족시킬 수 있도록 시스템의 구성 요소를 파악하는 것을 목표로 하며, 요구사항 모델을 바탕으로 수행되어야 한다[9].

2.1 유스케이스 본문 분석

유스케이스 본문 분석은 사용자 또는 고객으로부터 얻은 요구사항 정보들을 토대로 그 내용을 분석하여 소프트웨어 시스템에 필요한 클래스들을 추출해 내는 작업을 말한다[1]. 다음 그림3은 보안이 고려된 '사용신청' 유스케이스의 본문 분석에 해당한다.

2.2 접근정책 작성

다음은 접근정책 작성 활동으로, 각 액터들이 각각의 유스케이스에 대한 접근권한에 대해 작성해야 한다[7]. 다음 표6은 가로세로 퍼즐 시스템의 모든 유스케이스에 대한 각 액터의 접근정책을 정의한 것이다.

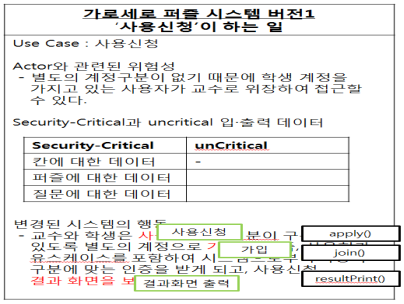

그림 3. '사용신청'을 위한 본문 분석
Fig. 3. Text Analysis of 'Request'

표 6. 액터에 따른 유스케이스 접근정책
Table 6. UseCase Access policies Based on the Actor

	교수	학생	시스템
등록	X	X	X
로그인	X	X	X
계정확인	-	-	X
사용허가	-	-	X
퍼즐 맞추기	X	X	X
퍼즐 만들기	X	-	X
범례 : 모든 권한(X), 일부 권한(P), 권한 없음(-)			

2.3 분석 클래스 모델 작성

접근정책 작성 활동 이후, 분석 클래스 모델의 작성 활동은 유스케이스의 명세서를 분석해 클래스 다이어그램을 작성하는 활동이다[9]. 즉, 클래스들을 도출하고 클래스 간의 관계를 정의하는 활동이다. 또한 유스케이스 명세서의 분석뿐만 아니라, 표6을 참고하여 보안이 요구되는 클래스들을 구별할 수 있다. 그림4는 각 유스케이스와 기본 시나리오로 도출된 분석 클래스 다이어그램이다. 또한 보안이 요구되는 클래스들은 <<secre-cy>> 스테레오 타입을 사용한다.

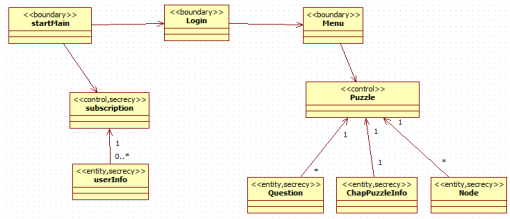

그림 4. 기본 시나리오 분석 클래스 모델
Fig. 4. Basic Scenario Analysis Class Model

2.4 분석 클래스 모델의 상세화

다음은 위에서 작성된 분석 클래스 모델의 상세화 활동이다. 이전 활동에서 도출된 분석 클래스 모델을 바탕으로 유스케이스 명세서의 시나리오를 분석해 각 분석 클래스의 속성과 연산을 정의한다. 그리고 상세화된 분석 클래스 모델의 완전성을 점검하기 위해 각 유스케이스별로 실현 모델을 작성한다[9]. 도출된 분석 클래스들을 바탕으로 각 유스케이스의 기본 시나리오에 대한 실현 모델은 순차 다이어그램으로 작성하도록 한다. 이 과정을 통하여 상세화된 분석 클래스 모델이 필요한 속성과 연산을 정의하고 있는지를 확인할 수 있다[1]. 다음 그림5는 사용신청 유스케이스의 기본 시나리오 실현 모델에 해당한다.

또한 상세화된 분석 클래스 모델은 기존의 분석 클래스 모델에 각 클래스별로 속성과 연산을 추가함으로써 완성된 분석 클래스 모델을 의미하며, 그림6은 가로세로 퍼즐 시스템의 상세화된 분석 클래스 모델을 보여준다.

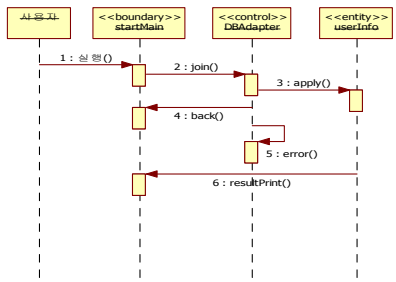

그림 5. '사용신청'을 위한 시나리오 모델
Fig. 5. Scenario Model of 'Request'

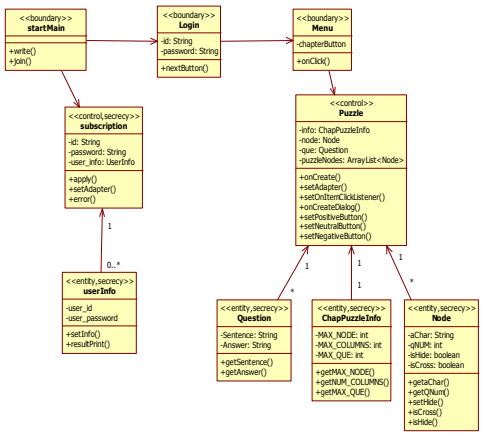

그림 6. '가로세로 퍼즐 시스템'의 상세화된 분석 클래스 모델
Fig. 6. Detailed Analysis Class Model of 'Horizontal and Vertical Puzzle System'

3. 구현

3.1 J2EE의 역할기반 접근제어

웹 기반의 응용소프트웨어 개발을 위해 상세화된 분석 클래스 다이어그램에 MVC 패턴을 적용한다. 따라서 그림6의 상세화된 클래스 다이어그램은 각 스테레오 타입에 따라 다음과 같은 조건을 따른다.

① 〈〈entity〉〉 타입을 사용한 클래스는 Model로서 데이터베이스의 스키마로 변환시킨다.
② 〈〈boundary〉〉 타입을 사용한 클래스는 View로서 JSP 등으로 구현한다.
③ 〈〈control〉〉 타입을 사용한 클래스는 Con-troller로서 서블릿 등으로 구현한다.
④ 〈〈secrecy〉〉 타입을 사용한 클래스는 보안이 고려되어야만 하는 클래스이며, 〈〈entity〉〉 타입과 같이 사용되었다면 데이터베이스의 역할기반 접근제어를 이용하여 보안을 적용한다. 또한 〈〈control〉〉 타입과 같이 사용되었다면 J2EE의 보안 매커니즘을 적용한다.

본 논문에서 사용된 예에서는 subscription 클래스 다이어그램이 〈〈control〉〉과 〈〈secrecy〉〉가 적용되어 있기 때문에 J2EE 기반의 보안 매커니즘을 적용하기 위해 role을 정의한다. 다음 표 7, 8, 9와 같이 인증과 인가를 통해 J2EE 기반의 보안 매커니즘을 적용할 수 있다.

표 7. 1단계 : Role 정의
Table 7. Step 1: Role Definition

```
- Tomcat-user.xml
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
<role rolename="professor"/>
<role rolename="manager"/>
<user username="professor"
password="1234"
roles="professor manager"/>
</tomcat-users>
- web.xml
<security-role>
<role-name>professor</role-name>
</security-role>
```

위의 표7과 같이 특정 보안 역할을 가진 사용자만 특정 서블릿에 요청을 할 수 있도록 Role을 지정하고, 배포서술자에 그에 맞는 Role을 사상(Mapping) 해주어야 한다.

Role을 지정한 후, 접근 가능한 자원 및 사용이 가능한 HTTP 메소드를 배포서술자에 지정해야 하며 다음 표8과 같다.

표 8. 2단계 : 자원 및 메소드 제약 정의
Table 8. Step 2: Constraints Defined of Methods

```
- web.xml
<security-constraint>
<web-resource-collection>
<!-- 사용하는 이름 -->
<web-resource-name>test web resource
</web-resource-name>
<!-- 제약을 걸 자원 -->
<url-pattern>/*</url-pattern>
<!-- 제약을 걸 HTTP 메소드 -->
<http-method>GET</http-method>
<http-method>POST</http-method>
</web-resource-collection>
<!-- 정의된 자원을 호출할 수 있는 역할 -->
<auth-constraint>
<role-name>professor</role-name>
</auth-constraint>
```

다음 표9는 Role과 자원에 대한 인증의 구현이다. 표9에서 "〈auth-method〉" 란에는 앞서 기술한 J2EE 기반의 4가지 인증 방식 중 FORM으로 작성하고, "〈form-login-page〉" 와 "〈form-error-page〉"에서는 인증이 Form 방식일 때 개발자가 작성한 html page를 띄워주도록 정의한다.

표 9. 3단계 : 인증의 구현 및 정의
Table 9. Step 3: Implementation and Definition of Certification

```
- web.xml
<login-config>
<auth-method>FORM</auth-method>
<form-login-config>
<form-login-page>/login.jsp</form-login-page>
<form-error-page>/loginerror.html</form-error-page>
</form-login-config>
</login-config>
```

4. 객체-관계형 데이터베이스 설계

4.1 객체-관계형 데이터베이스 설계방법론

관계형 데이터베이스 설계 방법론에서 개념 스키마를 물리적 스키마로 변환시키는 일부 규칙을 제안하는데[10], 유사한 방법으로 본 논문에서 제시하는 객체-관계형 데이터베이스 설계 방법론은 특정 제품인 Oracle11g 스키마로 변환시키는 방법을 제안한다[11,12,13,14]. 이 방법은 다음 표10에서 요약한다.

4.2 객체-관계형 데이터베이스의 역할기반 접근제어

그림7은 그림6의 상세화된 분석 클래스 모델에서 엔티티 클래스들이 표10의 변환 방법으로 적용된 클래스 다이어그램이며, 적용된 클래스 다이어그램을 바탕으로 그림7의 ChapPuzzleinfo 클래스는 표11과 같이 객체-관계형 데이터베이스 스키마로 변환할 수 있다.

또한 그림7에서 보안이 요구되는 엔티티 클래스들은, 표6에 따라 각 액터에 대한 접근권한을 역할기반 접근제어를 통해 설정할 수 있다[15]. 표12는 보안이 적용된 교수에 대한 접근 권한이며, 표13은 학생 역할에 대한 접근권한이다.

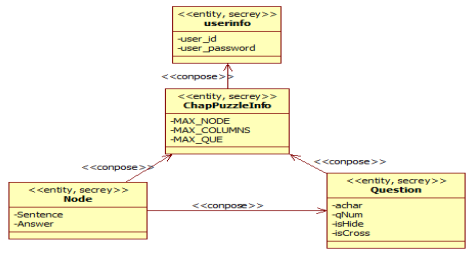

그림 7. '가로세로 퍼즐 시스템'을 위한 클래스 다이어그램
Fig. 7. Class Diagram of 'Horizontal and Vertical Puzzle System'

표 11. '퍼즐정보' 테이블 스키마
Table 11. 'Puzzle Info' Table Schema

```
CREATE OR REPLACE TYPE puzzle_info AS OBJECT (
pid NUMBER,
totalcellnum NUMBER,
colcellnum NUMBER,
quizn NUBBER,
quiznum REF puzzle_quiz,
qnum REF puzzle_node,
)
/* 테이블 생성 */
CREATE TABLE info OF puzzle_info
(PRIMARY KEY (pid))
```

표 10. 객체-관계형 데이터베이스 스키마로의 변환 방법
Table 10. Conversion Method of Object-Relational Database Schema

UML	SQL:2008	Oracle11g
Class	Structured Type	Object Type
Class extension	Typed table	Table of Object Type
Attribute	Attribute	Attribute
Multivalued	ARRAY	VARRY
Composed	ROW / Structured Type in column	Object Type in column
Calculated	Trigger/Method	Trigger/Method
Association		
One-To-One	REF/REF	REF/REF
One-To-Many	REF/ARRAY	REF/Nested Table
Many-To-Many	ARRAY/ARRAY	Nested Table/Nested Table
Aggregation	ARRAY	Nested Table
Generalisation	Types/Typed Tables	Oracle cannot directly represent The generalization concept

표 12. '교수'에 대한 접근 권한 스키마
Table 12. Access policies Schema of 'Professor'

```
CREATE ROLE pro_entry;
GRANT pro_entry TO user_id;
GRANT ALL ON
puzzle_info TO pro_entry;
GRANT ALL ON
puzzle_node TO pro_entry;
GRANT ALL ON
puzzle_quiz TO pro_entry;
```

표 13. '학생'에 대한 접근 권한 스키마
Table 13. Access policies Schema of 'Student'

```
CREATE ROLE st_entry;
GRANT st_entry TO user_id;
GRANT SELECT ON
puzzle_info TO st_entry;
GRANT SELECT ON
puzzle_node TO st_entry;
GRANT SELECT ON
puzzle_quiz TO st_entry;
```

V. 설계방법론 비교

기존의 객체지향 분석·설계 방법론과 UMLsec, 그리고 본 논문에서 제안한 통합 분석·설계 방법론에 대한 비교는 표14와 같다. 표14에서 알 수 있듯이, 기존의 객체지향 분석·설계 방법론은 객체-관계형 데이터베이스에 대한 지원이 전무한 실정이며, 보안에 대한 고려도 되지 않고 있다. 또한 UMLsec을 활용한 분석·설계 방법론은 보안을 고려하고 있지만, 객체-관계형 데이터베이스와 상호 연관성은 지원하지 않고 있다. 하지만 본 논문에서 제안한 설계방법론은 기존의 객체지향 분석·설계 방법론과 UMLsec에서 제시하지 못했던 객체-관계형 데이터베이스와의 상호 연관성을 지원하고 있으며, 역할기반 접근제어 설정을 통해 J2EE 기반의 보안과 객체-관계형 데이터베이스의 보안을 지원하고 있다.

표 14. 설계방법론 비교
Table 14. The Comparison of Design Methodology

	객체지향 분석·설계 방법론 지원	객체-관계형 데이터베이스 지원	보안 지원
기존의 객체지향 분석·설계 방법론	O	X	X
UMLsec	O	X	O
제안한 통합 객체지향 분석·설계 방법론	O	O	O

V. 결 론

본 논문에서는 객체-관계형 데이터베이스를 이용한 J2EE 기반의 웹 응용 시스템 개발을 위한, 보안을 고려한 통합 객체지향 분석·설계 방법론을 개발하였다. 이를 위하여 보안에 대한 요구사항을 수집하고, 수집된 요구사항을 UMLsec을 이용하여 분석·설계 과정에 반영하였으며 아울러 그 수행결과를 객체-관계형 데이터베이스 설계방법론과 통합하여 J2EE 및 객체-관계형 데이터베이스의 역할기반 접근제어를 이용하여 구현하였다.

본 논문에서 제시한 통합 객체지향 분석·설계 방법론은 기존의 객체지향 분석·설계 방법론이 제시하지 못했던 보안에 대한 일관된 분석·설계 방법을 제공하고 있으며, 아울러 객체-관계형 데이터베이스 설계 방법론과의 연관성도 제공하고 있다. 이에 따라 개발과정 전체에 걸친 보안에 대한 일관성을 제공하게 된다.

본 연구에서 제안한 통합 개발방법론은 객체-관계형 데이터베이스인 Oracle11g를 사용한 J2EE 기반의 보안이 요구되는 웹 응용 시스템을 개발하는데 사용하였다.

참고문헌

[1] Brett D. McLaughlin, Gary Pollice, David West, Head First Object Oriented Analysis & Design, Hanbit Media. Inc, pp. 96-103, 2007.

[2] Han Jeong-Su, Kim Gwi-Jeong, Song Yeong-Jae, Introduction to UML : Object-Oriented Design as in a friendly learning, Hanbit Media. Inc, pp. 58-66, 2009.

[3] Madan, s, "security Standards Perspective to Fortify Web Database Applications From Code Injection Attacks", International Conference on Intelligent Systems, Modelling and Simulation(ISMS), pp. 226-230, Jan 2010.

[4] Iqra Basharat, Farooque Anam, Abdul Wahab Muzaffar, "Database Security and Encryption: A Survey Study", International Journal of Computer Application, Vol. 47, No. 12, June 2012.

[5] Cho Wan-su, "UML 2 & UP Object-Oriented

Analysis&design", pp.189-205, Hongrung Publishing Company, 2005.
〔6〕 Jho Do-hyung, Joo Kyung-Soo, "UML Extension for Object-Relational Database Design - Focusing on Oracle11g-", Korea Society of Internet Infomation, Vol. 12, No. 6, pp.149-159, December 2011.
〔7〕 G.Popp, J. Jurjens, G.Wimmel, R. Breu, "Security-Critical System Development with Extended Use Case", Asia-Pacific Software Engineering Conference, 5-1 self, 2003.
〔8〕 Kathy Sierra, Bert Bates, Bryan Basham, Head First Servlet & JSP, Hanbit Media. Inc, pp. 683-721, 2009.
〔9〕 Chae Heung-Seok, Object-oriented CDB Project for UML and Java as learning, Hanbit Media. Inc, pp. 290-960, 2009.
〔10〕 Jho Do-hyung, Joo Kyung-Soo, "Development of Integrated Design Methodology for Relational Database Application -Focusing on Object-Oriented Analysis and Design Methodology-", Korea Society of Computer Information, Vol. 16, No. 11, 2011.
〔11〕 Oracle Corporation, Oracle 11g SQL Reference Release 2 (11.2), www.oracle.com, 2011.
〔12〕 ISO(International Standardization Organization), ISO/IEC 9075-11:2008, www.iso.org, 2011.
〔13〕 E. Marcos, B. Vela, J. M. Cavero, "A Methodology for Object-Relational Database Design Using UML", 12th International Conference and Workshop on Database and Expert Systems and Applications, 2001.
〔14〕 E. Marcos, B. Vela, J. M. Cavero, "Aggregation and Composition in Object-Relational Database Design", Fifth East European Conference on Advances in Databases and Information Systems, 2001.
〔15〕 Khaleel Ahmad, Jayant Shekhar, Nitesh Kumar, K.P.Yadav, "Policy Levels Concerning Database Security", International Journal of Computer Science & Emerging Technologies, Vol. 2, No. 3, June 2011.

저 자 소 개

주 경 수
1993: 고려대학교 전산학과 공학박사.
현 재: 순천향대학교 컴퓨터소프트웨어공학과 교수
관심분야: Database System, XML, System Integration, Object Oriented System
Email : gsoojoo@sch.ac.kr

우 정 웅
2012: 순천향대학교 컴퓨터학과 공학사.
현 재: 순천향대학교 컴퓨터소프트웨어공학과 석사과정
관심분야: Database System, Object Oriented System, UML
Email : jyone0715@gmail.com