대학 학사 데이터베이스 통합 보안 모델 설계

정윤수*, 신승수**

Integrative Security Model Design for Academic Affairs Database

Yoon-Su Jeong*, Seung-Soo Shin**

요 약 최근 교육 수월성 제고와 질적 수준 향상을 위해서 대학에서는 정보화를 추진하고 있으나 개인정보를 비롯한 학사행정과 관련된 중요 정보들이 학사 데이터베이스에 집적되어 있어 그에 따른 보호 대책이 필요하다. 이 논문에서는 학사 데이터베이스 구축에 사용되는 DBMS의 접근제어, 기밀성, 무결성 그리고 보안감사 등이 보장되도록 대학의 현실에 적합한 학사 데이터베이스 통합 보안 모델을 제안한다. 제안 모델은 상당 수 대학들이 데이터베이스 보안 제품을 활용하고 있지 못한 여건을 고려하여 DBMS가 제공하는 기능만으로 보안의 가장 핵심 요소인 기밀성 등을 구현하는 세부 방안을 제시하고 있다.

주제어 : 대학 학사, 데이터베이스, 보안 모델

Abstract To improve educational excellence and quality, academies carry forward integrative security model related to academic affairs including personal information. This paper proposes an integrative security model for academic affairs database, which guarantees DBMS access control, confidentiality, integrity, and security inspection. This proposed model considered that most academies can't make good use of data security product and suggests a detailed measure to realize the confidentiality based on the function of DBMS.

Key Words : University, Database, Security Model

1. 서론

최근 정보 기술이 대학 학사 데이터에 접목되면서 개인정보 뿐만 아니라 학사 행정과 관련된 중요 정보들이 학사 데이터베이스에 집적되고 있다[1,2]. 그러나 학사 데이터베이스에 집적된 중요 정보들은 안전성 측면에서 보호 대책 수립과 이행 등에서 요구 수준이 미흡한 상황이다[3].

대부분의 대학에서 학사 데이터베이스 시스템은 보안 차원에서 기본적인 방화벽과 침입탐지시스템만을 사용하여 학사 서비스를 보호하고 있는 상태이다[4,5]. 학사 서비스의 특성상 외부에서 접속할 수 있어야 하기 때문에 외부로부터의 위협에 노출되어 있는 상태이며, 더욱이 대부분의 보안 사고가 외부로부터의 공격보다는 내부자의 오·남용으로 인해 일어나고 있어 적극적인 데이터베이스 보안 대책이 요구된다[6,7].

학사 데이터베이스 보안(database security)이 중요한 과제로 인식되면서 교과부의 권장에 따라 일부 대학에서는 데이터베이스 관련 보안 제품을 도입하여 운영하고 있지만 만일 대학에서는 아직도 예산 상의 이유로 데이터베이스 보안 제품을 도입하지 못하고 있는 실정이며, 도입한 대학의 경우에도 성능 문제 등의 이유로 보안 제품이 제공하는 기능을 충분히 활용하지 못하고 있는 상황이다[8,9].

이 논문에서는 학사 데이터베이스 구축에 사용하는 주요 DBMS(데이터베이스관리시스템)의 데이터베이스에 대한 접근제어, 기밀성, 무결성, 보안감사 기능을 현실에 맞게 효율적으로 사용할 수 있는 학사 데이터베이스 통합 보안 모델을 제안한다. 제안 모델은 기밀성과 무결성의 구현 및 보안 감사를 위한 주요 로그의 생성, 보안

*목원대학교 정보통신학과
**동명대학교 정보보호학과 : 교신저자
논문접수: 2012년 5월 4일, 1차 수정을 거쳐, 심사완료: 2012년 5월 21일

대책 및 감사에 관한 체크 리스트 개발 등과 같은 세부 방안을 제시하고 있다. 또한, 대부분의 대학들이 데이터베이스 보안 제품을 활용하고 있지 못한 여건을 고려하여 제안 모델에서는 DBMS가 제공하는 기능만으로 보안의 가장 핵심 요소인 기밀성을 구현하는 세부 방안을 제시한다.

이 논문의 구성은 다음과 같다. 2장에서는 대학학사 데이터베이스 보안과 학사데이터베이스 구조에 대해서 알아본다. 3장에서는 대학학사 데이터베이스 통합 모델을 제안하고, 4장에서는 학사 성적 무결성 검사 모델을 구현하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 데이터베이스 보안

데이터베이스는 외부의 변화에 맞추어 적절히 저장된 데이터를 변경시킬 수 있어야 하며 새로운 데이터를 저장하거나 기존의 데이터를 삭제, 변경시키는 작업을 통하여 저장된 데이터가 일관성을 유지할 수 있다[8].

데이터베이스 보안은 데이터베이스 환경에 대한 적절한 보안 표준을 생성하고 작성하는 프로세스로부터 시작한다. 이런 표준은 플랫폼간 우수 사례 모음, 그리고 상위 계층 정책 및 규칙에 대한 연결 표준 등 다양한 데이터베이스 플랫폼에 대해 특별한 통제를 포함하고 있다[9,10,11].

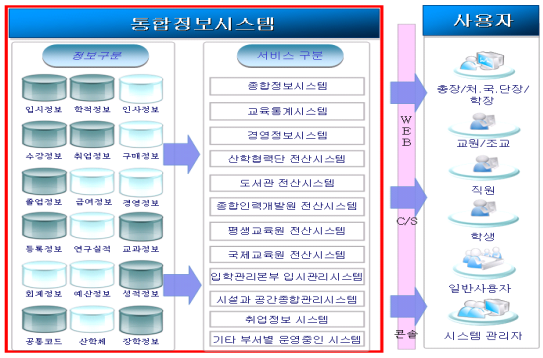
그러나, 데이터베이스 환경에서는 조직체의 다양한 응용과 사용자들이 DBMS를 통해 데이터를 참조하기 때문에 중복성(duplication), 데이터 불일치성(data inconsistency) 혹은 프로그램들과 자료 구조들 사이의 종속성(dependence) 등에서 보안 위협이 존재한다..

데이터베이스에서 정보는 기업체, 교육기관, 공공기관 등에서 중요한 자원으로 사용되고 있으며 기본 운영 기능뿐만 아니라 판매 예측, 예산, 금융 관리 등과 같은 관리 지원 기능들을 자동화하는데도 사용되고 있다. 이 기능들은 조직 내 정보의 중요성을 인식하는 척도로써 나날이 증가하고 있으며 다양한 형태의 보안 위협으로부터 중요한 지적 자산인 정보를 보호하여야 할 필요성이 점점 증가하고 있다[12].

2.2 학사 데이터베이스 구조

학사 데이터베이스 구조는 [그림 1]에서 보는 바와 같이 정보 자체를 저장하고 제공하는 측면(정보구분)과 이들 정보를 사용하는 측면(서비스구분)으로 구분된다[16].

정보구분에서 입시정보, 학사정보, 수강정보, 취업정보, 졸업정보, 등록정보, 교과정보, 성적정보, 장학정보, 공통코드 등이 학사 데이터베이스에 포함되어 있음을 알 수 있으며, 서비스 구분에서는 학사 데이터베이스를 시스템에 활용하여 Web, C/S 및 콘솔을 통하여 사용자가 이용할 수 있다.



[그림 1] 학사 데이터베이스 구조

[그림 1]에서 대학의 학사 데이터베이스가 가지는 주요 특성들은 다음과 같다. 첫째, 입학부터 취업까지 학생의 입시(고교 학생부), 학사, 성적, 등록, 장학, 졸업, 인적사항 등의 개인정보를 포함한 주요 자료들을 관리한다. 둘째, 단위업무별로 여러 시스템에 산재되어 있다. 셋째, 실시간 접속으로 장소에 관계없이 사용한다. 넷째, 다수의 사용자가 Web, C/S, 콘솔 등 다양한 방법으로 동시에 접속하여 사용하며 많은 정보들이 합법적으로 변경된다.

2.3 데이터베이스 보안 제품 비교분석

데이터베이스 보안 제품을 접근제어 방식과 암호화 방식으로 구분하여 장·단점을 정리한 결과는 <표 1>과 같다[13,14,15]. <표 1>에서 데이터베이스 접근제어/감사는 네트워크 단에서 데이터베이스에 대한 접근 통제를 수행하기 때문에 DBMS에 대한 변경이 없고 성능 저하가 발생하지 않는다는 점에서 장점을 가지고 있다. 데이터베이스 접근제어/감사는 네트워크상에서 데이터베이스 접속 SQL이나 원격통신을 이용한 접속을 통제하기 때문에 경우에 따라서는 완벽하지 않을 수 있다. 잘못된 접근제어 정책 설정에 의한 정보 유출 가능성이 높으며, 데이터베이스 보안 솔루션에서 장애가 발생할 경우 네트

〈표 1〉 데이터베이스 보안 제품의 비교분석

종류	개요	장점	단점
데이터베이스 접근제어 / 감사	-사용자별 권한을 할당하고 SQL 제어를 통해 불법적인 접근을 차단 -접속세션에 대한모니터링 수행	-부여된 접근권한에 따른 다양한 접근 제어 가능 -해당 세션에 대한 모니터링 가능 -허가되지 않은 외부 침입에 대한 효과적 대응	-데이터베이스 자체 유출 후 해당 데이터 악용에 무방비
데이터베이스 암호화	-데이터베이스 테이블 암호화 -컬럼별로 암호화적용 가능 -권한이 있는 자만 복호화 수행	-DB 내의 데이터 파일 및 기 타 물리적 방법으로 인한 불법 유출 방지 -데이터베이스 내 모든 데이터에 접근할 수 있는 데이터베이스 관리자로부터 민감한 정보보호에 효과적	-기 구축된 데이터베이스에 적용 어려움 -인덱스 컬럼 암호화로 인한 성능저하 우려

워크 장애로까지 확대될 수 있으므로 접근제어 관련 정책을 설정하기 위해 관리자들의 시간과 노력이 훨씬 더 요구된다.

암호화 방식은 DBMS 내부에서 데이터를 직접 암호화하는 방식을 사용한다. 따라서 해킹을 통하여 DBMS 내부에 접근한다고 하더라도 암호화된 데이터를 복호화하지 못한다면 아무런 의미가 없게 된다. 따라서 권한을 제한 받을 경우에 데이터 자체를 열람할 수 없다는 장점을 가진다. 그러나 데이터베이스를 암호화하는 것은 해당 데이터에 직접적인 변경을 가한다는 것을 의미한다. 이럴 경우, 적용 가능한 DBMS가 한정적일 수 있고 시스템에 계산 시간 부담을 주어 질의에 대한 응답 시간 등의 측면에서 서비스 질이 떨어질 수 있는 문제점이 있다.

3. 대학 학사 데이터베이스 통합 보안 모델 설계

이 절에서는 대학 학사 데이터베이스의 효율적인 보안 관리를 위한 대학 학사 데이터베이스 통합 보안 모델을 제안한다.

3.1 개요

학사 데이터베이스에는 교직원 신상정보, 급여정보를 비롯하여 학생들의 신상정보, 성적 정보 및 대학의 중요 정보들이 데이터베이스에 저장되어 인터넷을 통하여 시간과 공간을 초월하여 서비스되고 있다. 만약 학사 데이터베이스가 악의적으로 이용되어 보안 사고가 발생할 경우 그 피해는 매우 심각해질 수 있다.

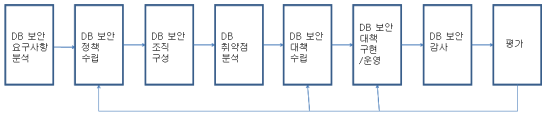
학사 데이터베이스의 효율적인 운용을 위해서는 관련 보안 지침을 기반으로 인가된 내부 사용자의 오·남용 방지, 개인정보보호 등을 위하여 접근 통제 체계 및 정보 유출 방지, 데이터베이스 접근에 대한 기록의 유지와 로그 분석, 보안 감사 등과 같은 보안 대책의 체계적 실시가 필요하며 데이터베이스 관리자와 데이터베이스 보안 관리자에게 상호 독립적 역할 배정을 통하여 보다 안전한 데이터베이스 보안을 담보하는 방안이 필요하다.

3.2 학사 데이터베이스 통합 모델

이 절에서는 학사 데이터베이스 보안을 위한 프로세스 모델을 제시하고, 구체적 운영을 위하여 DBMS 단독 사용 시 운영 모델과 데이터베이스 보안 제품 활용 시 운영 모델로 구분하여 특징을 기술한다.

3.2.1 프로세스 모델

학사 데이터베이스 보안을 위한 프로세스 모델은 경영 시스템(management system)의 기본 개념인 PDCA 사이클을 기반으로 설계한다.



[그림 2] 학사 데이터베이스 보안 프로세스

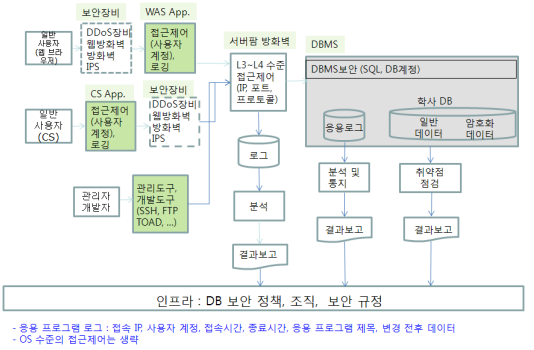
[그림 2]처럼 데이터베이스 보안 요구사항 분석, 데이터베이스 보안 정책 수립, 데이터베이스 보안 조직 구성, 데이터베이스 취약점 분석, 데이터베이스 보안 대책 수립, 데이터베이스 보안 대책 구현 및 운영, 데이터베이스 보안 감사, 평가 등의 8단계로 구성된다.

학사 데이터베이스 보안 프로세스는 평가 단계에서 도출된 문제점들을 바탕으로 데이터베이스 보안 정책 수립, 데이터베이스 보안 대책 수립, 데이터베이스 보안 대책 구현 및 운영 등에 반영하여 해당 프로세스를 개선하

는 것을 주요 특징으로 함으로써 각 대학의 보안 프로세스가 지속적으로 개선됨을 보장하게 된다.

3.2.2 DBMS 단독 사용 시 운영 모델

[그림 3]은 DBMS 단독 사용할 경우의 학사 데이터베이스 통합 보안 모델을 나타내고 있다. [그림 3]에서 일반 사용자는 교수, 학생 등을 의미하며, 웹 브라우저와 C/S를 이용하여 각각 보안장비와 WAS app.를 통하여 데이터베이스로 접근하게 된다. 이 과정에서 IP, 포트, 프로토콜 등의 정보를 기반으로 서버팜 방화벽을 통과하게 된다. 데이터베이스 관리자나 개발자는 개발도구나 관리도구를 통하여 서버 팜을 거쳐 데이터베이스에 접근하게 된다. 서버 팜 방화벽은 모든 접근에 대해 접근 제어 처리 과정에서의 주요 사건들에 대한 로그를 남겨 추후 분석에 이용하도록 한다.



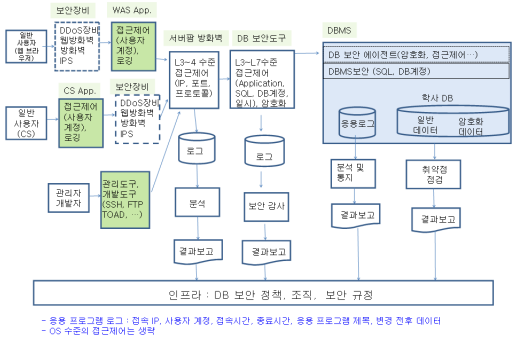
[그림 3] DBMS 단독 사용 시 운영 모델

[그림 3]에서 L3~L4 수준의 서버팜 방화벽의 접근제어를 통과하면 구현된 DBMS가 제공하는 보안 기능이 동작되며, 그 과정에서 응용 로그를 생성하여 추후 보안 감사 등에 활용한다. 물론 데이터베이스 보안 담당자는 이 기록을 분석하여 결과를 보고하고 대책을 강구하여야 한다. 또한 데이터베이스가 설치된 시스템의 보안 취약점을 주기적으로 점검하고 이를 보고하고, 취약점을 해소하도록 조치하여야 한다.

데이터베이스 내의 주요 항목에 대해 기밀성을 제공하기 위해서 DBMS에서 기본적으로 제공하는 암호화 기능을 사용하여야 하며, 주요 사건에 대한 로그를 기록하여야 한다. 예를 들어 Oracle의 경우 DBMS_CRYPTO 패키지를 이용하여 암호화, 로그 기록을 위하여 audit 명령을 사용한다.

3.2.3 데이터베이스 보안 제품 활용 시 운영 모델

데이터베이스 보안 제품 활용 시 운영 모델은 [그림 4]와 같다. [그림 4]는 [그림 3]의 모델 기능에 데이터베이스 보안 제품 기능을 통합한 결과이다. 따라서 데이터베이스 자체에 대한 보안 기능의 동작이 “DB 보안 에이전트”에 의하여 제공되므로, 데이터베이스를 이용하는 응용 프로그램에서 암호화/복호화 함수를 호출하지 않으며, 보안 감사 기록 생성을 위한 별도의 코드를 작성하지 않는다.



[그림 4] 데이터베이스 보안 제품 활용 시 운영모델

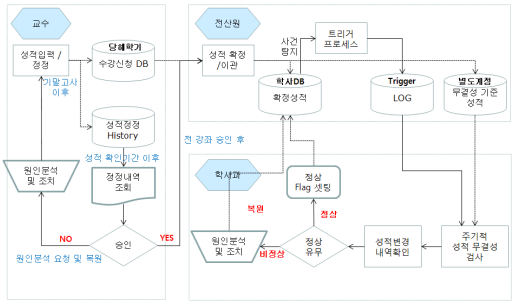
서버팜을 통과한 모든 데이터베이스에 대한 접근은 반드시(in-line 방식으로) DB 보안도구(제품)을 거치게 되며 이 과정에서 주요 정보가 로그로 기록되어 분석된다.

4. 학사 성적 무결성 검사 모델 구현

이 절에서는 제안 모델을 이용하여 학사 데이터베이스의 성적 무결성 검사를 위한 프로세스를 구현하여 구현된 모델의 성적 정정내역 조회, 트리거(trigger)를 통한 성적 트리거 활용, 로그 생성 트리거 및 로그 활용 등 세부 구성 요소에 대하여 기술한다.

4.1 성적 무결성 모델 설계

[그림 5]은 학사 데이터베이스의 성적 무결성 검사의 전체 흐름도를 나타내고 있다. [그림 5]의 성적 무결성 검사는 당해 학기 성적 입력, 입력 성적의 확인, 트리거 기능을 기반으로 효율적으로 동작하는 정정 기간 중 발생 가능한 위·변조 가능성의 검사 및 성적 확정 후 성적 변동에 대한 주기적인 검사 실시 등으로 구성된다.

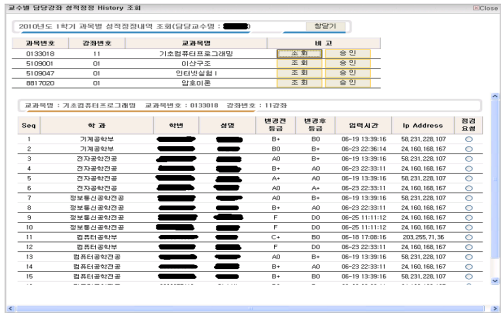


[그림 5] 성적 무결성 검사

4.2 모델 적용 사례

4.2.1 성적정정 History 조회

[그림 6]은 교수별 담당강좌별 성적정정 History의 조회 결과를 나타내고 있다.



[그림 6] 성적 정정 내역조회

[그림 6]처럼 조회 버튼을 클릭할 경우 1회 이상 성적이 변경된 수강 학생들의 학과, 학번, 성명, 변경 전 등급, 변경 후 등급, 입력시간, IP 주소 등의 정보를 제공하며, 위·변조 가능성이 있는 경우 점검 요청 라디오 버튼을 클릭하여 해당 성적 정정에 대해서 점검을 요청한다. 당해 강좌의 정정내역이 모두 정상적일 경우 승인버튼을 클릭한다.

4.2.2 성적 트리거 활용

Oracle에서의 트리거란 특정 사건에 의해 자동으로 실행되는 PL/SQL(procedure laznguage/structured Query language)을 의미한다. 특정 사건이란 데이터베이스 테이블에 DML(data manipulation language) 문이 실행될 때 발생되는데, 예를 들어 insert, update, delete 문이 사용되는 경우 트리거링 사건을 정의할 수 있으며, 이들이 실행될 때 트리거가 자동으로 실행되는 것을 트리거링이라 한다.

학사 데이터베이스의 확정 성적 테이블에서 성적 정정(추가, 삭제 등도 포함)이 발생하면 트리거링이 되도록 트리거 프로그램을 작성하여, 해당 사건이 발생하면 자동으로 이 트리거가 기동하여 로그가 생성된다. 그리고, 무결성 기준 성적 테이블을 이용하여 주기적인 무결성 검사를 통해 위변조 유무를 분석하고 조치를 취한다. 여기서 정상적인 변경일 경우 별도의 C/S 프로그램을 실행하여 정상 Flag임을 처리한다. [표 2]은 성적 트리거 활용 방법을 기술하고 있다.

4.2.3 로그 생성 트리거

[표 3]는 특정 사건 발생 시 로그를 생성하는 트리거의 예제를 나타내고 있다. 4.2.2절과 같이 Oracle 시스템에서 동작하는 트리거 프로시저는 데이터베이스 테이블에 발생하는 모든 사항(추가, 수정, 삭제 등)을 일시적으로 'redo 로그 버퍼'에 저장한다. 'redo 로그 버퍼'는 테이블의 내용이 수정된 경우에는 변경 전 데이터는 'redo 로그 버퍼'의 'old' 영역에, 변경 후 데이터는 'new' 영역에 각각 저장한다.

[표 3]에서는 성적 정정에 대한 로그를 생성하는 것을 주 목적으로 트리거 생성 방법을 기술하고 있다. [표 3]에서는. 따라서 트리거 프로세스를 작성할 때, Oracle이 생성한 'redo 로그 버퍼'의 내용을 기준으로 로그를 생성할 것인지를 결정하게 된다. 즉, 사용자 정의 트리거의 작성 시 변경 전 데이터는 'old'를 컬럼명 앞에 붙여 참조하고 변경 후 데이터는 'new'를 붙여 참조한다.

트리거 프로세스에 의하여 생성된 로그 데이터는 성적 테이블과 다른 공간의 데이터베이스에 저장하여 보안을 유지하도록 한다.

〈표 2〉 성적 트리거 활용 방법

- 대상 성적 테이블에 대해 Insert/Update/Delete 등과 같은 SQL 문이 실행되면 Oracle 내부적으로 실행되어지는 시스템 프로시저인 트리거에 의하여 성적 테이블의 변경 전(old)/변경 후(new) 내역이 자동으로 임시 메모리 성격의 'redo 로그 버퍼'에 기록됨 - 보안 담당자는 SQL 문이나 PL/SQL 문을 이용하여 성적 테이블의 변경 등의 사건 발생 시 동작할 사용자 정의 트리거(성적 트리거)를 작성하여 로그를 생성

〈표 3〉 로그 생성 트리거

```
-- 성적 테이블 수정 시 자동으로 기동되는 Oracle 시스템 트리거가 생성하는 'redo 로그 버퍼'를 이용하여 작성
TRIGGER Update_Sngj205

-- 테이블 내용이 수정되는 경우 Update(삭제 : Delete, 추가 : Insert) 사용
   After Update on Sngj205
For Each Row

Begin
-- 'redo 로그 버퍼' 상의 변경 전 데이터는 old를 컬럼명 앞에 붙여 참조, 변경 후 데이터는 new를 붙여 참조
   if (:old.rec_grd <> :new.rec_grd) then -- 'redo 로그 버퍼'의 변경 전 성적 등급과 변경 후 성적 등급을 비교(같은 경우 확정 성적 등급에
   변경이 발생 한 경우임)

-- 성적테이블과 다른 데이터베이스에 트리거 로그를 저장
      Insert into etchjdb.sngj_trigger
      (yy, shtm, std_no, sbjt_no, clss_no, inpt_dt, bf_rec_grd,  af_rec_grd, flag)
      values
      (:old.yy,  :old.shtm, :old.std_no, :old.sbjt_no, :old.clss_no, to_char(sysdate,'yyyy-mm-dd hh24:mi:ss'), :old.rec_grd,
      :new.rec_grd, 'A');
   end if;

end;
```

5. 결론

최근 대학의 학내 무선 인터넷 서비스의 확대 및 스마트 폰을 통한 각종 서비스의 개발 등과 같은 학사 서비스의 환경적 변화는 수요자인 교수 및 학생들로부터 긍정적인 반응을 얻고 있는 반면 전산망을 비롯한 보안의 측면에서는 부담이 가중되고 있는 것이 현실이다. 본 논문에서는 대학의 이러한 환경적 여건을 고려하여 한정된 보안 인력과 자원을 최대한 활용하여 학사 데이터베이스의 보안 피해를 사전에 예방하고 최소화하기 위한 학사 데이터베이스 통합 보안 모델을 제안하였다. 제안된 모델은 학사 데이터베이스에 대한 접근 통제, 기밀성과 무결성 및 보안 감사 등의 기능 요소를 가지며, 데이터베이스 보안 제품을 사용하는 경우와 그렇지 못한 경우로 나누어 설계함으로써 각 대학들의 여건에 맞는 모델을 선택하여 활용할 수 있도록 하였다. 향후 연구에서는 제안 모델을 구현하여 각 대학들의 실제 보안 모델을 운영할 계획이다.

참 고 문 헌

[1] KISA(2009), "Database security audit log Specification for Personal Information protection", Korea Informatino Security Agency.

[2] KISA(2009), "Explanation Document about Technology and Management Security Follow-up Measures of Privacy", Korea Internet & Security Agency.

[3] B. S. Kim(2009), "Database Security for Privacy Protection in Education Information System", University of Seoul.

[4] ITFIND(2008), "Report of Cryptography Use Activation", ITFIND.

[5] H. G. Lee, S. M. Lee and T. Y. Nam(2007), "Database Encryption Technology and Current Product Trend", ETRI, Vol. 22, No. 1, pp. 105-113.

[6] NIS(2010), "Security Requirement of DB Security Product", Natinoal Cyber Security Center.

[7] TTAS.KO-12.0064(2007), "A Guide for Database Security", Telecommunications Technology Association.

[8] A. Shulman, "Top Ten database Security Threats", IMPERVA

[9] CPNI(2008), "Understanding Database Security", Next Generation Security Software.

[10] DISA(2004), "Database Security technical Implementation Guide". DoD.

[11] E. Burtescu(2009), "Database security - Attacks and Control Methods", Jounal of Applied Quantitative Methods, Vol. 4, No. 4 pp. 449 - 454.

[12] H. A. Afyouni(2006), Database security and Auditing, Course Technology.
[13] ISACQ, IS Standards(2009), “Guidelines and Procedures for Auditing and Control Professionals″.
[14] Oracle(2008), “Oracle Database Security Checklist”.
[15] V. W. Marek(2007), “Database Security Issues”, University of Kentukey.
[16] Yoon-Su Jeong, Seung-Soo Shin(2012), “Study of Compare Research Analysis of Security Present Condition in University Academic Affairs Database”, The Journal of Digital Policy& Management, vol. 10, no. 3, pp. 113-120.

정 윤 수

・2000년 2월 : 충북대학교 대학원 전자계산학 이학석사
・2008년 2월 : 충북대학교 대학원 전자계산학 박사
・2009년 8월~2012년 2월 : 한남대학교 산업기술연구소 전임연구원
・2012년 3월~현재 : 목원대학교 정보통신공학과 전임교수
・관심분야 : 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안
・E-Mail : bukmunro@mokwon.ac.kr

신 승 수

・2001 충북대학교 수학과(이학박사)
・2004 충북대학교 컴퓨터공학과 (공학박사)
・2005~현재 : 동명대학교 정보보호학과 부교수
・관심분야 : 네트워크보안, USN, 스마트카드.
・E-Mail : shinss@tu.ac.kr