데이터베이스 계정분리를 이용한 정보관리 시스템 보안

장영수*, 최진영**
*고려대학교 컴퓨터정보통신대학원 소프트웨어공학과
**고려대학교 컴퓨터정보통신공학과
e-mail : jyskkh@chol.com, choi@formal.korea.ac.kr

A Information Management System Security using separation of Database Identification Numbers

Young Su Jang*, Jin Young Choi**
*Dept. of Software Engineering, Graduate School of Computer & Information Technology, Korea University
**Dept. of Computer Information & Communication, Korea University

요 약

오늘날 공공 및 민간기업의 정보관리 시스템 의존도는 계속 높아지면서 이와 함께 정보보호에 대한 관심 또한 높아 지고 있다. 본 논문에서는 데이터베이스 정보관리 시스템의 계정(ID) 분리를 통해 데이터베이스 시스템의 접근계정을 소유자 계정, 응용서비스 계정, 외부연동 계정, 서비스 계정으로 각각 분리하여 외부 공격으로부터 정보관리 시스템을 보호하고자 하였다. 또한 데이터베이스 관리자에 의해 생성되는 데이터베이스 스키마에 대한 각 계정별 접근정책을 차별화 하여 개발자나 운영자 의 실수로 발생할 수 있는 정보 삭제로부터 데이터베이스 정보관리 시스템의 피해를 최소화 하고자 하였다.

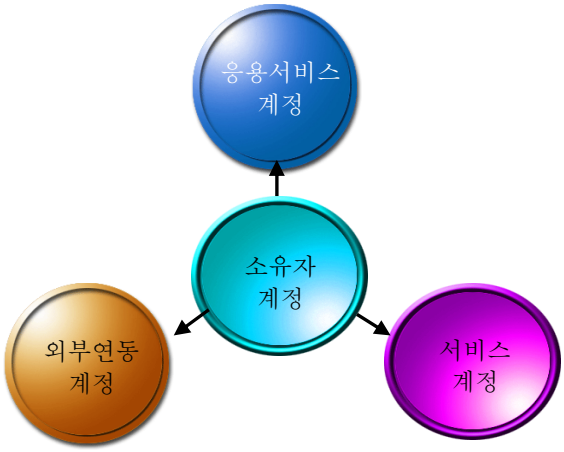
1. 서론

백신과 방화벽으로 일관하던 기존의 보안정책은 네트워크 복잡성 증가, 다양한 외부공격 등으로 새로운 보안 대책과 기술의 도입이 필요하게 되었다. 특히 외부의 공격이 내부 보안프로그램을 무력화 시키고, 공공기관 및 기업의 정보를 유출하는 것은 국가적으로나 기업의 측면에서도 상당한 손실이 아닐 수 없다. 이러한 정보를 관리하는 데이터베이스 정보관리 시스템 또한 업무의 특성에 따라 계정(Identification Number, ID)을 발급, 운영하지 않고 단일계정(Single ID)만을 사용하여 SQL 삽입공격(SQL Injection), 응용프로그램 취약성에 노출되기도 한다[1]. 이를 예방하기 위해 데이터베이스 정보관리 시스템 계정은 시스템 접속 역할 과 함께 외부의 공격으로부터 시스템 피해를 최소화 할 수 있는 정보보호자 역할도 같이 수행하여야 한다[2].

본 연구에서는 데이터베이스 계정을 사용하여, 정보관리에 대해 통합적으로 위험을 관리 할 수 있는 데이터베이스 정보관리 시스템을 모델링 하여 제시한다.

2. 계정분리 모델링 제안

일반적으로 데이터베이스 정보관리 시스템의 계정은 데이터베이스에 접근하기 위한 접속기능과 함께 업무별 서비스 용도에 따라 크게 세가지로 정의 된다. 첫째는 데이터베이스 관리자에 의해 스키마가 생성되는 소유자 계정이다. 일반 사용자들은 접근할 수 없으며, 데이터베이스 관리자만 접근할 수 있다. 이는 데이터베이스 정보관리 시스템의 계정을 통제하여 일반 사용자, 외부의 침입으로부터 물리적으로 스키마들을 보호하기 위함이다. 둘째는 내부 및 외부 사용자를 위한 계정이다. 앞서 기술한 소유자 계정에서 스키마에 대한 접근권한을 부여 받아 사용자 들은 응용프로그램을 통해 스키마에 접근하지만, 물리적으로 스키마에는 접근 할 수 없다. 셋째는 서비스 계정이다. 소유자 계정으로부터 스키마에 대한 조회접근 권한만을 부여 받은 계정으로 통계자료 및 조회 용으로만 사용된다.



(그림 1) 계정분리 모델 구성체계

3. 계정분리 모델 통제정책

데이터베이스 정보관리 시스템의 계정은 데이터베이스 관리자에 의해 생성된 스키마의 접근권한 및 사용 용도에 따라 물리적 변경 여부, 자원의 통제, 접속권한, 접근통제로 분류 할 수 있으며, 각 계정별 역할은 고유기능 역할 수행과 보완적인 구조로 설계되어야 한다. 특히 업무별 성격에 따른 활용에 관련되는 각각의 계정에 대해서는 정보관리 시스템의 설계단계에서부터 분류 되어야 한다. 계정분리 단계별 통제정책에 대해서는 표 1 과 같이 정의할 수 있다.

<표 1> 계정분리 단계별 통제정책

계정분류	계정 특성
소유자 계정	○ 물리적 변경여부 - 물리적 스키마 생성, 변경 가능 - 데이터베이스 관리자에 의해 최초 모(母) 스키마 생성 - 미공개 계정으로 데이터베이스 관리자가 관리 ○ 자원의 통제 - 스키마에 대한 DDL(Data Definition Language) / DML(Data Manipulation Language) 권한소유 ○ 접속권한 - 데이터베이스 관리자 및 제한된 사용자만 접속가능 ○ 접근통제 - 스키마 접근 시 제약사항 없음
응용서비스 계정	○ 물리적 변경여부 - 물리적 스키마 변경 불가능 ○ 자원의 통제 - 응용서비스 용 계정 접근권한 부여 - 스키마에 대한 DML(Data Manipulation Language) 권한소유 - 동의어, View 에 의해 스키마에 접근 - 다량의 일괄데이터 처리가 불가한 버퍼 사이즈 구성 - 외부연동 계정에서 입력된 자료 처리 ○ 접속권한 - 응용서비스용 접근 계정 ○ 접근통제 - 스키마에 대한 접근통제 제어
외부연동 계정	○ 물리적 변경여부 - 물리적 스키마 변경 불가능 ○ 자원의 통제 - 외부기관 또는 내부 타 데이터베이스 접근 용 계정 접근권한 부여 - 스키마에 대한 DML(Data Manipulation Language) 권한소유 - 동의어, View 에 의해 스키마에 접근불가 - 외부연동 계정에서 입력된 자료는 응용서비스 계정에 서 별도 처리 ○ 접속권한 - 외부 서비스용 접근 계정 ○ 접근통제 - 스키마에 대한 접근통제 제어
서비스 계정	○ 물리적 변경여부 - 물리적 스키마 변경 불가능 ○ 자원의 통제 - 통계자료 및 조회용 계정권한 부여 ○ 접속권한 - 특정서비스 기간 접속을 위한 계정 ○ 접근통제 - 특정 스키마에 대해 조회만 가능

4. 정보관리 시스템 계정 암호 관리 절차

○ 계정 패스워드 변경 : 데이터베이스 정보관리 시스템의 패스워드 관리 정책에 대한 내부 처리 지침을 준수하여, 정기적으로 패스워드를 변경 한다.

○ 계정 패스워드 관리 : 응용서비스 계정, 외부연동 계정, 서비스 계정의 패스워드는 암호화된 파일에 보관되어야 하며, 각 계정의 응용프로그램에서는 암호화 파일에 접근하여 패스워드를 획득하여야 한다.

○ 계정 접근 사용내역 기록 : 전산화된 관리시스템을 통하여 데이터베이스 정보관리 시스템으로의 접근 로그를 저장하고, 주기적으로 분석한다[3].

5. 결론

본 논문은 데이터베이스 정보관리 시스템에서 업무서비스 별 계정의 역할을 구별하고자 하였다. 지금까지 정보관리 시스템의 계정은 정보관리 시스템에 접속하고 업무를 분류하기 위한 용도로만 사용되었다. 계정은 외부에 노출된 정도에 따라 소유자 계정, 응용서비스 계정, 외부연동 계정, 서비스 계정으로 분류되며, 각각의 계정에서 수행하는 역할 또한 계정분리 모델에서의 통제정책에 근거하여 분류하였다.

향후 과제는 본 논문에서 제안하는 데이터베이스 정보관리 시스템 모델이 효율성을 가지고 객관적으로 평가될 수 있도록 실무사례를 중심으로 지속적으로 보완해가며 발전시키는 연구가 요구된다.

참고문헌

[1] Robert C. Seacord. “Secure coding in C and C++”

[2] 정보보호관리체계 인증제도의 발전방향 연구, 한국정보보호진흥원, 2003.12

[3] 국가정보보호백서, nis 국가정보원 · 방송통신위원회, 2008