데이터베이스의 보안요구사항 기반 테스트에 관한 연구

김재중, 김기인, 곽은영*, 권호열 [1], 권원일**
강원대학교, *예신정보기술,**STA 컨설팅
e-mail : sesangsari@nate.com, hykwon@kangwon.ac.kr

A Study on Security Requirement based Testing for A Database

J.-J. Kim, G.-I. Kim, E.-Y. Kwak*, H.-Y. Kwon, W. Kwon**
Kangwon National University, *Yeshin Inform. Tech., **STA Consulting Inc.

요 약

IT 기술의 발달로 자료의 대형화, 통신의 초고속 광역화가 이루어짐에 따라 우리 실생활과 비즈니스에 밀접하게 연관되어있을 뿐 만 아니라, 분산서비스거부(DDos)공격과 대규모 개인정보 유출 사례 등은 데이터베이스(DB) 보안의 중요성은 한층 높아지고 있다. 본 논문에서는 대형 개인 정보 유출사고의 가능성을 안고 있는 기업에서 DB 암호화 구축 이후 발생할 수 있는 장애요소를 최소화 할 수 있도록 DB 보안 요구사항에 기반한 점검 항목을 도출하고 테스트 방안을 제시하였다.

1. 서론

IT 기술의 발달로 자료의 대형화, 통신의 초고속 광역화가 이루어짐에 따라 우리 실생활과 비즈니스에 매우 밀접하게 연관되어 정보보안의 중요성은 한층 높아지고 있다. 특히 최근 발생한 분산서비스거부(DDos)공격과 1 천만명 이상의 개인정보 유출사례 등은 데이터베이스(DB) 보안에 대한 관심을 고조시키고 있다. 더욱이 정보유출사고의 60%이상을 차지하는 내부자에 의한 정보유출은 외부 공격에 의한 것보다 더욱 치명적인 특징을 갖는다.

이러한 DB 암호화와 관련된 연구로서, 유두규 등[1]은 교육행정정보시스템(NEIS)의 고객정보를 보호하기 위하여 속성인증서(AC)를 이용한 RBAC 인증과, 사용자의 역할과 역할 DB 의 역할인증서를 검증하여 접근제어를 허가하는 권한기반구조(PMI) 기반의 DB 암호화를 제안하였으며, 이영록 등[2]은 국내외 개인정보보호 관련 법률에 기초한 DB 보안감사로그 항목을 제시한바 있다. 또한 김정욱 등[3]은 데이터베이스 구축사업의 감리지침을 발표하였으며, 김광열[4]은 데이터베이스 보안 감리점검프레임워크를 정의하고 프레임워크를 구성하고 있는 점검영역별로 감리점검항목들을 도출한 바 있다.

또한 법규 측면에서 보면, 고객 개인정보 유출을 막을 수 있는 시스템 구축은 기업 의무 중 하나로서 정보통신망 이용촉진 및 정보보호 등에 관한 법률[5] 제 28 조 제 1 항에 아래와 같이 명시되어 있다.

- 개인정보의 안전한 취급을 위한 내부관리계획의 수립과 시행
- 개인정보 불법 접근 차단을 위한 접근 통제 장치의 설치와 운영
- 접속기록의 위변조 방지 조치
- 개인정보의 안전한 저장과 전송할 수 있는 암호화 기술등을 이용한 보안조치

이와 아울러, 동법 시행령[6] 제 15 조 제 4 항 제 4 호에는 '주민등록번호 및 계좌정보 등 금융정보의 암호화 저장'을 요구하고 있다.

본 논문에서는 대형 개인 정보 유출사고의 가능성을 안고 있는 기업에서 DB 암호화 구축 이후 발생할 수 있는 장애요소를 최소화할 수 있도록 DB 보안 요구사항에 기반한 점검 항목을 도출하고 테스트 방안을 제시하였다.

2. DB 암호화 기법

2.1 DB 암호화 요구사항

DB 암호화란 DB 에 저장된 정보(데이터)를 컬럼/테이블/테이블스페이스 단위로 암호화하여 비인가자에 의한 데이터 유출이 불가능하도록 하는 보안 방법으로서, 가장 보안강도가 강하며 최종 보안이라고 할 수 있다. 이 때, 암호화에 요구되는 필수적 요소[7]는 표 1 과 같다.

DB 암호화는 보안성과 DB 운영성이 모두 요구되는 속성을 가지므로 보안 기능과 함께 다양한 DB 환경을 지원하는 기능을 제공해야 한다.

[1] 교신저자

표 1. DB 암호화의 필수적 요소

기능요소	내용
안전한 알고리즘 (ARIA,SEED,AES,TDES,DES)	안전한 알고리즘으로 최고의 보안성 보장
안전한 키관리	암호모듈검증기준이 요구하는 안전한 키관리 (불법접근불가,키제로화)
인덱스 암호화 및 검색	인덱스도 암호화되어야 하며 암호화 인덱스를 통한 색인 검색 지원.
성능	구축성능 및 검색성능의 저하가 최소일 것
가용성	장시간이 소요되는 DB 암호화 작업으로 인한 서비스 무중단 또는 최소화
최소의 제약사항	제약사항이 가능한 적을 것

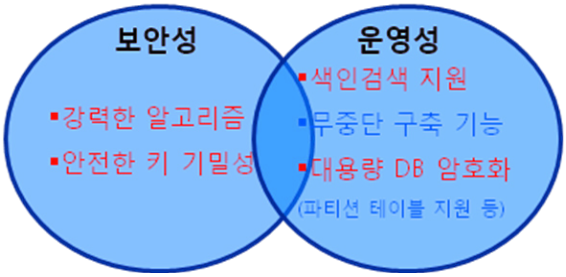

그림 1. DB 암호화의 두 가지 특성

2.2 DB 암호화 방식

DB 암호화는 암호화 기능을 제공하여 데이터 유출을 차단하는 기술로서 플러그인 방식과 API 방식으로 나눌 수 있다. 먼저, 플러그인 방식은 그림 2 와 같이 암호화 제품이 DB 내에 설치되며 암복호화 과정이 DB 내부에서 수행된다. 기존 어플리케이션이나 DB 테이블의 수정이 거의 발생하지 않는 장점이 있으나 DB 서버에 부하를 발생할 수도 있다.

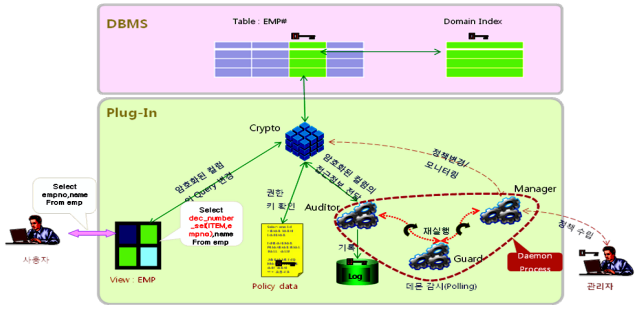

그림 2. 플러그인 방식의 DB 암호화 구성도[8]

API 방식은 그림 3 과 같이 외부 어플리케이션서버에 제품이 설치되어 DB 외부에서 암복호화가 수행된다. DB 서버에 부하를 발생하지 않지만 기존 어플리케이션이나 DB 테이블의 변경이 선행되어야 하는 단점이 있다.

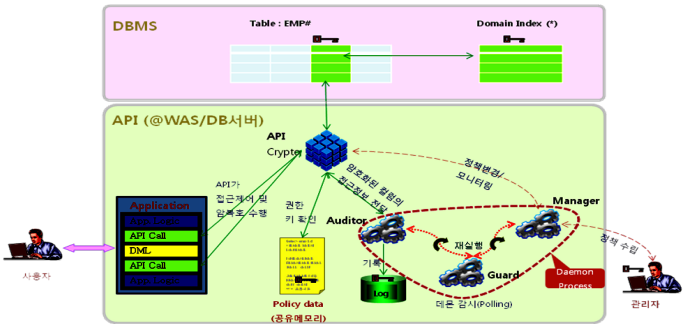

그림 3. API 방식의 DB 암호화 구성도[8]

산업계에서 널리 사용되는 DB 암호화 구조는 그림 4 와 같이 원시 테이블을 다른 테이블 명으로 변경하고 원시 테이블명으로된 뷰를 생성한 후 해당 뷰에 DML 이 가능하도록 트리거(Trigger)를 설정함으로써 암복호화를 수행하는 구조이다.

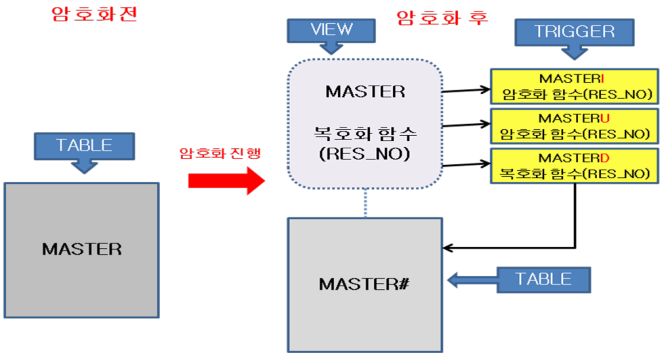

그림-4. DB 테이블 암호화 구조

한편, 인덱스는 그림 5 와 같이 암호화 전/후에 대한 Ordering 상실로 인해 발생할 수 있는 문제를 Domain Index 를 활용하여 해결한다.

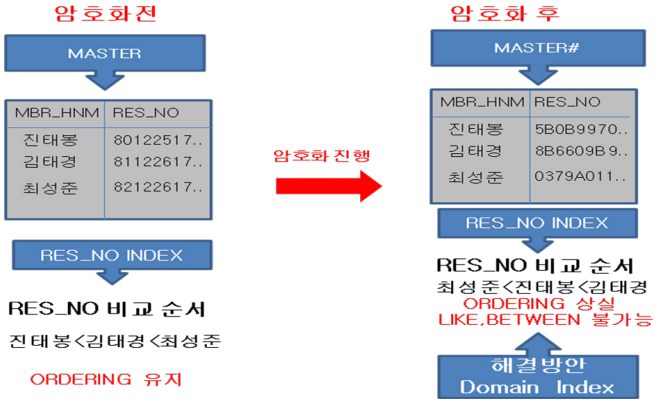

그림 5. DB 인덱스 암호화 구조

이처럼 DB 보안을 위한 암호화가 수행되면, 테이블 구조가 뷰(View)형태로 변경되고 일반 인덱스가 도메인(Momain) 인덱스로 변경되어 기존 질의문에 대한 PLAN 에 변경이 발생되어 수행 속도가 기존보다 느려질 수 있는 문제점이 있다.

3. DB 암호화 구축에 대한 점검 항목

앞에서 살펴본 방식의 DB 암호화 구축에서 실무적

으로 반드시 점검할 항목과 테스트 방안은 다음과 같다.

표 2. DB 암호화 구축의 점검항목과 테스트방안

No	점검 항목	테스트방안
1	암호화 알고리즘 지원	-필수 알고리즘(ARIA, SHA) 지원 여부 -기타 알고리즘(AES,DES, SEED) 지원 여부
2	암호화 키 관리	- 암호화 키에 허가 받지 않은 사용자의 접근 불가여부 - 제품종료 시 키 제로화 여부 - 암호화 키가 안전한 장소에 저장여부 - 암/복호화 키 백업 및 복구 지원
3	접근통제	- 사용자 IP, Mac,어플리케이션, 특정 시간대 암호화 커널에 접근제어 - DB 사용자 패스워드 임의 변경 통제 여부
4	감사 및 로그	- 보안정책의 설정, 변경 또는 배포시 Audit 로깅 기능 제공 - 암호화 컬럼에 대한 다양한 접근 로그기록 - 접근로그, 성공/실패 로그 등 다양한 로그에 대한 검색 기능 확인 다양한 조건 별 보고서 제공 기능
5	암호화 기능	- 인덱스 컬럼에 대한 암호화지원 - 암호화 컬럼에 대한 인덱스지원을 위한 어떠한 형태의 복호화한 데이터 존재 여부 - 암호화 이후 원본 테이블의 제약조건 유지여부 - 인덱스 컬럼에 대한 암호화지원 - 인덱스 검색 지원(일치검색, 범위검색) - 다양한 데이터 타입의 암호화 지원(char, varchar, number, date, float, long, clob, blob, null) - 암호화 된 테이블에 컬럼 추가/삭제 등 구조 변경 지원 - PK, FK 조건이 설정된 컬럼 암호화 가능 - Trigger 설정된 테이블의 컬럼 암호화 가능 - 파티션 테이블 암호화 지원 - 부분암호화 지원 - RAC 또는 분산 환경 지원 - 암호화 컬럼 상호간 또는 일반 - 암호화된 테이블에 대한 export /import 시 암호화 유지 여부 -암호화 설정 해제시 원래 테이블 구조로 복원 가능 지원 여부
6	성능부분	- 암호화 성능 측정:대량의 데이터 암호화 소요시간 및 CPU 점유율 - 복호화 성능 측정:대량의 데이터 암호화 소요시간 및 CPU 점유율 - 암호화 후 테이블 및 인덱스의 데이터량 증가 정정성 - 일치검색의 응답시간 - 범위검색 응답시간
7	이식성 및 유지보수성	- Multi-Instance 지원 유무 - 제품관리자 설명서 및 사용자 설명서 지원 - 암호화 각종 작업에 대한 GUI 지원 - 다수의 DB 서버에 대한 보안관리 와 DB 운영의 통합관리 지원 - OS DBMS, N/W 등의 파라미터 변경 여부 - 암호화 진행시 서비스 무중단 지원 - 초기암호화 도중 해당 테이블에 대한 DML 수행 가능 여부 - 초기암호화 도중 발생하는 DML 이 암호화 종료 후 암호화된 테이블에 반영되어 있는지 여부 암호화 진행 중 오류 발생시 자동 복구 기능제공 여부

위 점검 항목에 대한 테스팅 절차를 통해 DB 암호화 적용에 따른 장애요소를 용이하게 식별할 수 있다.

4. 결론

본 논문에서는 DB 암호화가 필요한 타당성과 구축 방안, 구축 시 발생할 수 있는 장애요소를 미연에 찾아내기 위한 점검 항목과 테스트 방안을 제시하였다.

향후 연구되어야 할 주제는 첫째, DB 암호화에 따른 DB 구조변경으로 야기되는 성능 문제 최소화 방안, 둘째 기술적인 보안과 함께 내부 관계자의 교육을 통한 관리적 보안이 최적의 조합을 이루어 병행하는 방법 등이다.

참고문헌

[1] 유두규, 문봉근, 전문석, PMI 기반의 RBAC 를 이용한 NEIS 의 DB 보안 구현, 정보보호학회논문지 Vol.14 No.6, pp. 31-45, 2004. 12.

[2] 이영록, 이형효, 박해룡, 전길수, 개인정보보호를 위한 DB 보안감사로그 설계, 한국인터넷정보학회 2008 정기총회 및 추계학술발표대회 제 9 권 제 2 호, pp. 119-124, 2008. 11.

[3] 김정욱 외, 데이터베이스 구축사업에 대한 감리지침, 한국전산원, 2004. 11.

[4] 김광열, 데이터 안전성 확보를 위한 데이터베이스 보안 감리점검 프레임워크 연구, 석사 학위논문, 건국대학교, 2007.11

[5] 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 법률 제 10138 호, 방송통신위원회, 2010.3.17

[6] 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령, 방송통신위원회/행정안전부, 2009. 1.28

[7] 금융권 DB 암호화 솔루션 도입시 고려사항 검토-금융보안연구원

[8] 신상윤, CubeOne™ 제품 소개 - 색인 검색을 지원하는 대용량 DB 전문 암호화 솔루션, eGlobal, 2009. 8.