Journal of The Korea Society of Computer and Information
Vol. 19, No. 12, December 2014
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2014.19.12.143

안정적인 DB보안 시스템 구축을 위한 보안기술요소 분석에 관한 연구

윤 선 희*

Study on the Technical Security Factor for the Implementation of Secure DB System

Sun-Hee Yoon*

요 약

본 논문에서는 기하급수적으로 증가하고 있는 개인 정보 유출로 인한 피해를 방지하기 위해 DB보안 방법을 제안한다. 제안된 보안 방법은 DB접근제어 영역과 DB암호화 영역으로 구분하며 영역별 기술 요소들을 분석하고 안정적인 DB보안 시스템 구축 시 필요한 사항들을 제시한다. 또한 기존의 영역별 DB보안 제품들을 분석하고 성능을 실험하여 결과를 분석한다. 성능을 실험한 결과, DB접근제어 방식은 네트워크 끝점에서 접근통제를 하기 때문에 기존 DBMS의 변경이 거의 필요 없으며 성능저하가 비교적 낮은 장점이 있는 반면 DB암호화 방식은 권한이 없는 경우 데이터 자체의 열람이 불가능하다는 장점이 있다. DB접근제어는 사전 차단이 미약하나 접속 로그 기록을 남겨 사후 추적으로 보완이 가능하다는 단점이 있으며 DB암호화 방식은 적용 가능한 DB종류가 한정적이며 시스템 부하로 성능이 저하될 뿐 아니라 시스템 구축 시 실패율이 높다는 단점이 있다. 따라서 본 논문에서 분석된 영역별 특징들이 향후 기관이나 기업에서 안정적인 DB 보안 시스템을 구축할 때 필요한 참고 자료가 되기를 기대한다.

▸ Keywords : 보안기술요소, DB접근제어, DB암호화

Abstract

This paper introduces Database security to prevent the rapidly increasing issue of private information leakage. The Database security examined in the paper separates into DB access control area and DB encryption area which further leads the paper to analyze the factors of the two areas and suggest necessary elements for creating stable Database security. In addition, the paper examines previous DB security programs by areas and analyzes pros and cons from the tested result. The experiment indicated that while DB access control presents less degradation and reduced the need to modify the existing DBMS

•제1저자 : 윤선희
•투고일: 2014. 11. 19, 심사일:2014. 12. 2, 게재확정일:2014. 12. 10.
*숭의여자대학교 디지털미디어전공(Major in Digital Media, Soong Eui Women's College)
※ 본 논문은 2013년도 숭의여자대학교 교내학술연구비 지원에 의해 연구되었음.

since the access control operates at the end point of the network, DB encryption presented strength in protecting the data from unauthorized access. On the other hand, DB access control is less useful in preventing the attack in advance which leaves the log to enable tracking afterward while DB encryption can only be operated by limited types of Database and causes degradation due to system load and shows higher percentage of failure when creating the system. This paper examines characteristics of Database security areas in order to be used as a reference for institutions or companies seeking stable Database security.

▸ Keywords : Technical Security Factor, DB access control, DB Encryption

I. 서 론

최근 몇 년간 개인정보 유출 사건은 점차 증대되는 추세로 금융기관의 해킹, 신용카드사 내부직원의 개인정보 매매 및 경찰 개인정보를 조회하여 매매하거나, 통신회사의 협력업체 직원이 프로그램을 개발해 개인정보 유출 하는 등 광범위하게 발생하고 있다. 표 1은 주요 개인 정보 유출 사례와 소송관련 자료를 분석한 것으로 최근 보안 침해 사례를 분석해 보면 인터넷 기술의 향상과, 인터넷 비즈니스 기술의 활성화, 해킹 기술 발전 및 도덕적 해이로 인해 과거의 아마추어 수준의 해커들에 의한 자기 과시나 웹사이트 손상, 단순, 웜. 바이러스 유포 또는, 지엽적인 공격에서 벗어나 조직화된 해킹 조직이 결성되고 정보 탈취나 시스템 운영 마비 및 지속적인 위협을 받고 있으며 그 피해 또한 기하급수적으로 증가 하고 있는 실정으로 개인 정보 유출로 집단소송 발생 시 기업은 천문학적 비용을 배상할 수 있다.

공공기관이나 기업에서는 기존의 시스템이나 새로운 시스템을 구축하는데 있어서 개인정보 유출로 인한 침해 사례가 빈번하게 발생하며 그 범위조차 광범위하게 이루어져 개인정보유출을 방지하기 위한 DB보안 정책이 필수요건이 되고 있다. 본 논문에서는 기하급수적으로 증가하고 있는 개인정보유출 피해를 방지하기 위해 DB보안을 위한 기술요소들을 분석하고 기술요소별로 상용화된 제품들을 분석하여 제공함으로써 공공기관이나 기업에서 안정적인 DB보안이 이루어질 수 있는 시스템을 구축할 수 있도록 시스템의 특성 및 규모에 맞게 선택하기 위한 참고 자료로 사용될 수 있도록 한다.

본 논문의 구성은 다음과 같다. 2장에서는 안정적인 DB보안 시스템을 구축하기 위한 기술요소들의 관련 연구 분석에 대해 기술하며 3장에서는 DB보안을 위한 시스템의 구축 시 고려사항들 및 기존의 DB보안관련 제품들의 특성 및 장단점 분석에 관해 기술하며 4장에서는 결론 및 향후 연구 방향에 관하여 서술한다.

표 1. 개인정보유출침해사례
Table 1. Sample of Personal Information Leakage Infringement

회사	원인	규모	경로	법률적 판단
A 캐피탈	해킹	280만명	웹서버에 보관된 개인정보 해킹/유출	기관경고,대표주의/임원 감봉 3개월
B 카드사	내부직원(개인정보취급자)	9만7천건	이메일로 고객정보를 분양대행업체에 유출	
C 증권사	해킹	?만건	1일 1-2건씩 조회하는 방식으로 몇만건 유출	
S 텔레콤	내부직원(개인정보취급자)	1만8993건	동의받지 않은 개인정보를 제3자에게 유출	37억5770만원배상판결(1심)
S포털	해킹(APT 공격)	3500만명	PC를 악성코드에 감염시킨후 DB에 접속한 후 개인정보파일을 생성한 후 FTP로 유출	6억원배상(3천명 대상 개인당 20만원씩 배상)
K통신	웹 애플리케이션 인증	880만건	앱애플리케이션으로 한번에 1-2건씩 6개월간 800만건 조회	관리소홀로 기소

II. 관련 연구기술

1. DB보안기술요소

DB보안을 위협하는 요소로는 데이터노출, 부적절한 변경이나 접근, 접근 차단 또는 거부, 시스템의 보안 취약점 노출, DB 서비스 실패나 물리적 손상 및 개인정보보호에 관한 법률 등이 포함된다. 표 2는 보안의 요소인 기밀성, 무결성 및 가용성을 기반으로 DB 보안의 위협요소들을 분석한 결과이며 표 3은 DB보안 통제 방법에 따른 DB보안 위협 요소를 분석한 결과이다[2].

표 2. DB보안 위협요소와 보안요소간의 관계분석
Table 2. Analysis of Security Factor vs DB Security Threat Factor

DB보안 위협요소	보안 요소		
	무결성	기밀성	가용성
데이터노출	○		
부적절한 변경	○	○	○
부적절한 접근		○	○
접근 차단/거부			○
보안취약점 노출	○	○	○
DB서비스 실패			○
DB 물리적 손상	○		○
개인정보보호에 관한 법률	○	○	○

표 3. DB보안 위협요소와 DB보안 통제방법간의 관계분석
Table 3. Analysis of Security Factor vs DB Security Cobtrol Method

DB보안 위협요소	DB보안 통제방법							
	접근제어	감사/모니터링	사용자 인증	권한 관리	암호화	작업 승인	취약점 분석	백업
데이터노출	○				○			
부적절한 변경	○				○	○	○	
부적절한 접근	○	○	○	○	○	○		
접근 차단/거부	○	○	○	○			○	
보안취약점 노출							○	
DB서비스 실패	○						○	○
DB 물리적 손상	○							○
개인정보보호에관한 법률	○	○			○	○		

DB보안 기술요소는 접근제어 영역과 DB암호화 영역으로 분류할 수 있다〈그림 1〉[2]. 접근제어 영역에서는 DBMS로 그인 및 SQL을 실행 할 때 보안 규칙에 따른 권한 통제가 이루어져야 하며 사용자 수행 SQL과 관련된 정보저장을 통한 부당한 조작 여부를 판단해야 한다. 또한 DB 해킹 보다는 DB접근 권한을 가진 사용자의 권한 남용에 의한 정보 유출 또는 변조를 방지하는 데 주력해야 한다. DB암호화 영역에서는 DBMS에 저장되는 데이터를 암호화하여 저장하고, 복호화 권한을 가진 사용자 또는 서버만 복호화 할 수 있게 해야 하며 접근제어와 병행하는 경우, 시너지효과를 가져올 수 있다. 법률적으로 보호되어야 할 데이터, 업무상 중요한 데이터를 선별하여 적용하며 암호화키에 대한 보안성을 확보할 필요가 있으며 서비스 성능의 영향도를 고려하여 암호화 방식에 대한 선택이 필요하다. 그림 2는 영향도 분석 프로세스를 도출한 것이며 표 4는 DB접근제어와 암호화 방식의 장단점을 분석한 것이다[3].

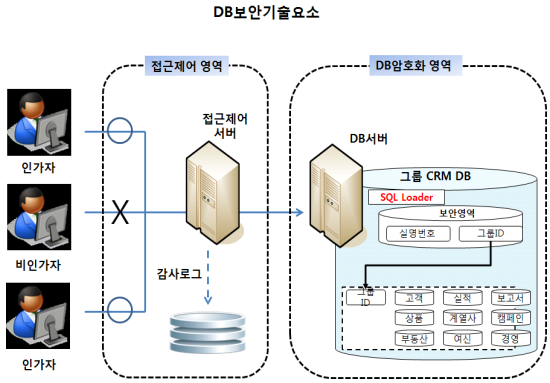


그림 1. DB 보안기술 요소
Fig. 1. DB Security Technique Component

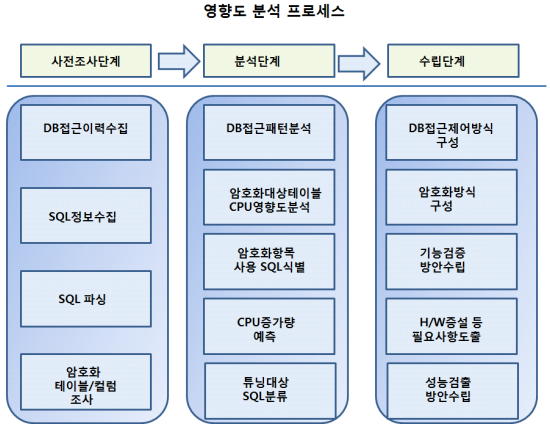


그림 2. 영향도 분석프로세스
Fig. 2. Process of Impact of Degree

표 4. DB접근제어 vs DB 암호화방식 장.단점
Table 4. Advantage and Disadvantage of DB Access Control vs. DB Encryption

구분	장점	단점(취약점)
접근제어 방식	네트워크끝점에서의 접근통제 DB변경 불필요 성능저하 미비	원격지에서 일반적인 DB접속통신을 이용하여 DBMS 접속하는 것이 아닌 경우(콘솔 또는 텔넷) 일반적인 SQL전송이 아닌 경우
DB 암호화방식	DB내부 데이터 직접 암호화 해킹을 통해 DBMS에 접근하더라도 암호 해독을 못하는 경우 데이터 열람 불가	적용가능 DBMS가 한정적 시스템의 부하로 성능저하 시스템구축 시 실패율이 높음

2. DB 접근제어

그림 3은 DB접근제어 구축방식을 나타낸 것으로 프록시 게이트웨이방식, 에이전트 방식, 스니핑 방식 및 네트워크 차단 방식 등이 있다[1][2].

DB접근제어 구축방식은 우회 접근방지를 기본으로 하며 특히 프록시 게이트웨이 방식은 DB접속 시 프록시 서버를 강제적으로 경유하도록 내부 사용자 단말기에 전용 프로그램을 설치하거나 접속정보가 저장된 파일을 변경하여 프록시 서버를 경유하도록 해야 한다.

에이전트방식으로 구축된 경우, 콘솔을 이용하여 DB 서버에 접근하더라도 차단할 수 있으나 에이전트 방식의 경우 DB서버에 직접 설치하여 운영하므로 기존 서버에 대한 영향을 최소화해야 한다. 애플리케이션 서버 IP에서 내부사용자가 접속하는 경우, 우회할 수 있는 통로가 될 수 있으므로 애플리케이션서버에서 DB서버로 접속할 수 있는 환경을 제거해야 한다.

스니핑 방식의 경우, 기본적으로는 DB서버에 대한 영향 없이 패킷을 복사하여 로그인하는 기능을 제공한다. 로그인된 세션이 권한이 없거나 권한이 없는 SQL을 수행할 경우, 세션을 종료시키는 기능을 제공한다, 또한 스니핑 방식에 의한 차단을 이용하여 우회접근을 방지할 수 있다. 스니핑 방식에서 프록시 게이트웨이 서버를 경유하지 않고 DB서버에 로그인한 것에 대해 차단하도록 설정을 하는 경우, 우회하여 로그인한 세션을 차단할 수 있다.

네트워크 장치에 의한 차단 방식은 DB서버에 대한 접근 시에 네트워크 접근을 통제할 수 있는 방화벽 같은 통제 장치를 경유하는 경우에는 출발지 IP, 포트정보와 목적지 IP, 등을 통하여 직접 DB서버로 접근을 시도하는 세션을 통제할 수 있다. 내부 사용자와 DB서버가 동일 건물 안에 존재할 경우, 별도의 통제방법을 사용해야 한다[1].

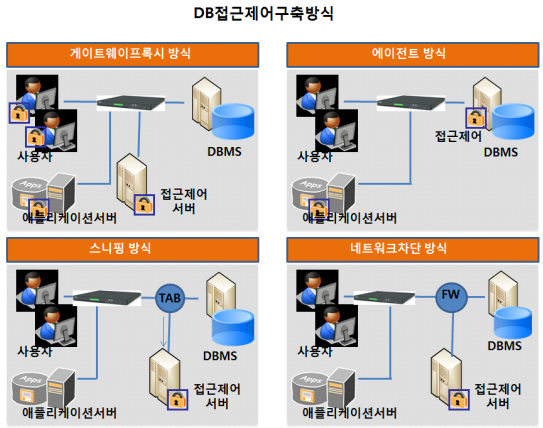


그림 3. 접근제어구축방식
Fig. 3. Implementation Method of DB Acess Control

표 5. DB접근제어 특징 및 장단점
Table 5. Advantage and Disadvantage of DB Access Control

DB접근제어구축방식	특징	장.단점
Gateway Proxy 방식	· 모든 트래픽 대상 이상 없을시 DB서버로 전달 · 우회방지 정책수립 필요	· DB접근 불가 · Dummy서버 접근 불가 · 서버 부하
Agent 방식	· DB서버에 직접 설치하여 운영하므로 기존 서버에 대한 영향을 최소화하여야 함 · 응용서버에서 DB서버에 접속할 수 있는 환경을 제거해야 함	· 콘솔 등에 의한 DB접근 차단 가능 · 접속자 개별 관리 에이전트 설치 필요
Sniffing 방식	· 서버전달 트래픽은 보안 서버에서 모니터링	· 로그만 기록 가능 · 스니핑 서버에 차단 기능을 제공을 제공하면 작동 이상으로 장애 발생 가능 · 패킷 유실에대한 위험
N/W 차단 방식	· 방화벽 등과 같은 통제 장치를 경유하여 네트워크 접근 통제 · IP, 포트 정보 등을 통하여 DB서버로의 접근 시도 차단	· 내부 사용자와 DB서버가 동인 건물내에 있어 방화벽 등의 장치 부재시 통제 방법 필요

3. DB 암호화

DB 암호화는 디스크 전체 또는 테이블 단위를 암호화하거나 암호화 대상이 되는 기밀정보를 담고 있는 컬럼 단위로 암호화하는 경우가 있다. 컬럼 단위 암호화의 경우 기존 애플리케이션의 변경이 필요 없는 플러그인 방식과 애플리케이션의

변경이 필요한 API 방식이 널리 사용되고 있다[1].

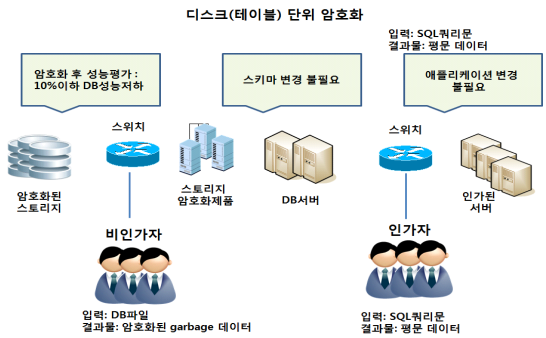


그림 4. 디스크(테이블) 단위 암호화
Fig. 4. Disk(Table) Level Encryption

그림 4는 디스크(테이블)단위의 암호화 방식을 나타낸 것으로 디스크 전체 또는 테이블 단위를 암호화 하는 것은 DB 파일을 보호하고 비인가 사용자에 의한 불법적인 파일 열람을 제한하는 것이다. 인가된 서버만이 정상적인 암호화된 데이터를 해독 하고 열람할 수 있게 하는 것으로 DB 암호화 중 가장 편한 방식 중 하나이다. 하지만 DB 파일을 암호화하는 것은 인가된 DB 호스트 서버에 접속하는 다양한 시스템들과 사용자들을 식별하지 못하므로 이를 위해 컬럼(Column) 단위의 암호화가 요구된다. 그림 5는 컬럼 단위의 암호화 방식을 나태낸 것으로 컬럼 단위의 암호화는 개인정보나 기업의 민감한 정보를 담고 있는 특정 테이블의 컬럼만을 암호화 하는 것으로 DB 서버에 접속하는 사용자들을 구분하고 정의된 암복호화 정책에 따라 데이터를 제공하므로 DB 암호화 제품 중에 현장에서 가장 널리 쓰이는 방식이다[9].

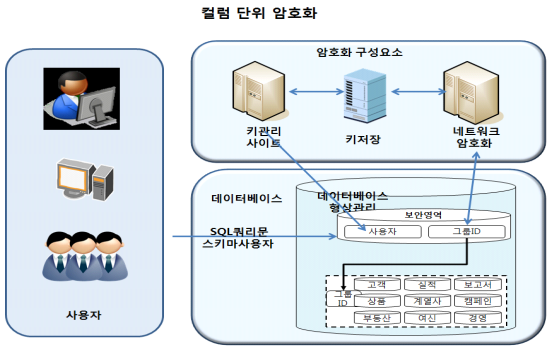


그림 5. 컬럼 단위 암호화
Fig. 5. Colum Level Encryption

그림 6은 컬럼 단위의 암호화방식을 나타낸 것으로 컬럼 단위의 암호화는 DB 서버내의 플러그인을 장착하여 암복호화를 수행하는 방식과 애플리케이션 서버가 암복호화를 위한 API을 호출하여 수행하는 방식으로 분류되는데, 선택 시에 고려사항은 DB서버의 자원 사용량, 속도 개선 그리고 기존 애플리케이션의 변정 여부 등이다.

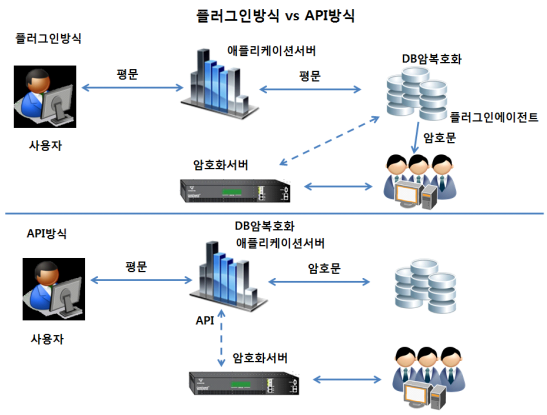


그림 6. 플러그인 방식 vs API방식
Fig. 6. Plug-In Method vs API Method

III. DB 보안 제품 분석 및 실험

1. DB보안 시스템 구축을 위한 고려사항

안정적인 DB보안 시스템을 구축하기 위해서는 법적 규제 준수 및 비용감소를 위한 효율성이 높아야 하며, 기존의 DB 운용환경의 보장을 위해 안정성을 확보해야 한다. 또한 기존 서비스로의 완벽한 호환성을 유지하기 위해 확장성이 제공되어야 하며 서비스 중단 방지 및 안정성을 확보하기 위해 규제가 준수 되어야 한다. 효율성을 제공하기 위해서는 용이하고 신속한 암호화와 기존 DB의 성능이 보장되어야 하며, 적용 비용의 최소화 및 관리 비용의 최소화를 위한 환경이 고려되어져야 한다. 안정성 측면에서는 업계 표준의 알고리즘이 채택되어져야 할 뿐만 아니라 완벽한 보안키 관리가 이루어져야 하며 데이터 정합성이 유지되어야 한다. 확장성을 제공하기 위해서는 기존에 사용되어지고 있는 응용프로그램의 변경이 최소화되도록 해야 하며 효율적인 관리 및 인터페이스가 원활하게 이루어져야 할 뿐만 아니라 플랫폼 호환성이 고려되어야 한다. 규제준수를 위해서는 개인정보보호법을 준수해야 하며 정보통신망 이용촉진 및 정보보호 등에 관한 법률을 준수해야 한다[12].

DB보안 시스템 구축 시 제외될 수 없는 사항으로 개인정보보호법 제 33조의 사항인 개인정보영향평가를 실시해야한다. 개인정보영향 평가란 개인정보를 활용하는 새로운 정보시스템의 도입이나 개인정보 취급이 수반되는 기존 정보시스템의 중대한 변경을 할 경우 시스템의 구축. 응용. 변경 등이 프라이버시에 미치는 영향에 대해 사전에 조사 예측, 검토하여 개선 방안을 도출하는 체계적인 절차를 말하며 정부가 인정하는 개인정보 영향평가 대상 기관이 실시해야 한다.

DB접근제어 정책을 수립하는데 있어서 고려해야 할 사항은 첫째 암호화된 컬럼에 관련된 암복호화 보안 정책 수립을 위한 암복호화 권한 설정, 둘째, 복호화 권한이 부여 되지 않은 사용자의 조회 요청 시 응답할 내용, 즉 암호화된 데이터나 마스킹, 오류처리 등을 운영 환경에 적합하게 수립하기 위한 비인가자의 요청에 대한 처리, 셋째, 암호화 데이터에 접근하는 경로에 대해 허용 및 차단에 대한 우선순위 정책 수립 및 다수 클라이언트에 대해 일괄적인 접근 통제 정책 수립을 위한 우선순위 정책, WAS 또는 DB관리자, 개발자 등 클라이언트의 IP/MAC주소, 애플리케이션별, 시간대별 암호화 데이터에 대한 접근 통제 수립을 위한 클라이언트 접근 통제 등이 있다[13].

2. DB보안 제품 분석

DB 암호화 정책수립 시 고려해야할 부분은 크게 암호화 대상 및 암호화 방안으로 구분할 수 있다. 암호화대상은 관련 법규에서 암호화하도록 지정한 개인정보와 고유 살별정보를 선정하는 것으로 암호화 대상 컬럼수는 최소화하여야 하며 법규정을 충족해야 한다. 또한 암호화대상 정보는 모든 DB에 적용하여 암호화하도록 해야 한다. 암호화 방안으로는 패스워드에 대해서는 해쉬알고리즘을 사용한 단방향 암호화를 적용해야 하며 나머지 암호화 대상 항목은 양방향 암호화를 적용해야 한다. 해쉬알고리즘은 SHA-256이상, HAS-160 등의 보안성이 검증된 알고리즘을 사용해야 하며 양방향 알고리즘은 ARIA-128이상, SEED 등의 보안성이 검증된 알고리즘을 사용해야 한다. 표 6은 국가정보원 IT보안인증사무국에서 발표한 DB보안제품의 핵심 보안 요구사항이다.

표 6. DB보안제품 핵심요구사항(IT보안인증사무국)
Table 6, Mandatory Requirement of DB Security Solution (IT Security Certification Bureau)

구분	보안요구사항	요구기능	설명
암호 지원	안정성이 검증된 암호 모듈/알고리즘 등 사용	· ARIA 128/192/256, SEED · SHA 256이상, has-150	· 국정원 암호 모듈 검증필
암호키 관리	암호키 생성, 접근, 갱신, 파기 등의 안전성 확보	· 암호키 유도는 검증된 국제표준 알고리즘 · 공유메모리에 로드된 암호키는 평문불가	· 국정원 "DB 암호제품 보안 요 구 사 항 " (2010.10.04)
DB 데이터 암복호화	암호문, 인덱스 등 중요 데이터의 안전성 확보	· 안전한 암호모듈을 통하여 암. 복호화 원본데이터는 암호화 후 삭제	· 암호모듈 검증 제도에 검증받은 암호모듈
접근 제어	암호키, 암호문 등에 대한 비인가자의 접근 차단	· DB계정, IP, 애플리케이션, 접속기간 등 조견별 제한	· 국정원 "DB 암호제품 보안 요구사항" (2010.10.04.)
암호 통신	전송 데이터의 기밀성, 무결성 유지	· 제품 구성 요소간 안전한 전송	
식별 및 인증	인증 제품 사용자의 신원 확인 및 검증	사용자의 연속된 인증 실패 후 초기화인증 데이터 재사용 공격 방지	
보안 감사	제품관련 중요 이벤트에 대한 감사 기록	감사 데이터는 인증된 사용자만 접근DB테이블 명, DB컬럼명, 쿼리 유형에 따라 검토	
보안 관리	보안정책, 감사기록 등의 효율적인 관리	암호키 및 보안 정책 등 중요데이터에 대한 백업 및 복구 기능 제공	

표 7과 표 8은 국가 정보원 IT보안인증사무국에서 요구하는 보안제품 보안요구사항을 기반으로 현재 상용화된 제품들에서 접근제어 제품 및 DB 암호화 제품에서 필수적으로 제공되어져야 하는 기능들을 분석한 것이다.

표 7. DB 접근제어 제품의 기능 분석
Table 7. Requirement Function of DB Access Control

기능	세부기능	내용
일반	지원플랫폼	UNIX(Solaris, AIX, HP-UX, OSF1), Linux, Windows
	접속 애플리케이션	Toad, Orange, Golden, SQL-Gate 등
	지원DB	Oracle, MS-SQL, Sybase, Altibase, DB2 등
	외부기관인증	GS인증 및 국정원 보안 적합성 검증필
접근 제어	사용자인증	ID/PWD+PKI, OTP, Two-Factor 인증
	통제대상 DB	Oracle, MS-SQL, Sybase 등 모든 DBMS 접근제어
	시스템계정 접근제어	시스템접속계정 통제
	DBMS계정 접근제어	DB접속 계정 통제
	사용자 제어	사용자 IP, 접속 애플리케이션 통제
	서버접속	DB서버에 대한 telnet ssh, ftp, sftp

		접근제어
	세션차단	사용자접속 세션 강제 차단
모니터링	세션모니터링	telnet ssh, ftp, sftp를 통한 DB작업에 대한 모니터링
	SQL모니터링	감시대상 DB에 연결된 세션에 대한 작업내역 모니터링
	DB세션 모니터링	DB에 연결된 세션에 대한 상태 정보 모니터링(SQL쿼리문 요청수, 평균응답시간,데이터조회건수, 네트워크사용량 등)
SQL 파싱	SQL 통제	DDL/DML/DCL SQL 명령어 통제기능
		중요 테이블 및 컬럼 접근제한
	데이터마스킹S	실행 SQL 쿼리문의 경과에 대한 데이터마스킹 기능
	SQL 결제	중요정보시스템의 SQL결제 기능
	SQL 로그 감사	SQL쿼리문에 대한 로깅 및 SQL쿼리문 결과값 로그저장
	로깅 및 감사	접속세션 및 실행 명령어별 이력관리 및 감사데이터생성
구성방식	Proxy 방식	사용자 접근(2-tier)의 DB접속에 대한 보안감사 제공
	에이전트방식	애플리케이션서버 및 DB접속에 대한 보안감사 제공
	Sniffing 방식	WAS, 미들웨어 등(3-tier)접속에 대한 보안 감사 제공
	N/W차단방식	Firewall 등 N/W차단 접속에 대한 보안 감사 제공
계정감사	시스템 계정 감사	DB 서버 로그인 횟수 제한
		DB 서버 주기적 패스워드 변경
이중화	장애대응	Bypass/Active-inactive 기능 제공

표 8. DB 암호화 제품의 기능 분석
Table 8. Requirement Function of DB Encryption

기능	내용
제품 규격	애플리케이션의 변경 여부
	보안 인증
암호화	국내외 표준 암호 알고리즘 사용
	무중단 서비스 암호화
	인덱스 암호화(일치, 범위, 검색 등)
사전 분석	주요 개인정보 컬럼 자동 검색
	사전 암호화 전/후 성능 자동 분석
	암호화 대상 컬럼 관련 쿼리 자동 수집 및 영향도 분석
	DB서버 암호화 부하 분산
접근 제어	DB계정/IP/애플리케이션/시간대별 암호 컬럼 접근제어
보안 감사	선택적 감사 기능
	로그 스케줄링
보안 관리	암호 키 비밀번호 복구
	PKI 기반의 보안 관리자 인증
	지원 DBMS

표 9. DB접근제어제품 구축방식 제품 비교 분석
Table 9. Implementation Analysis of Commercial Solution of DB Access Control

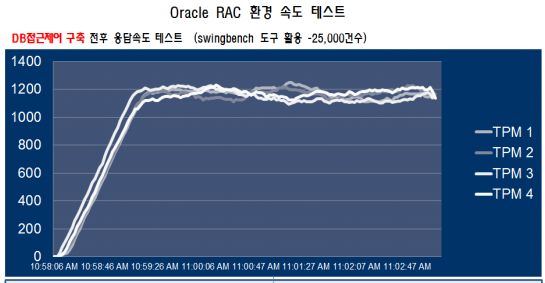
제품	게이트웨이 프락시	에이전트	스니핑	N/W차단
패트라	○	○	○	
DB Safer	○	○	○	
샤크라맥스	○		○	○
DB-I	○			○
IProtector	○		○	○

표 10. DB암호화 제품 비교 분석
Table 10. Analysis of Commercial Solution of DB Encryption

구분	D'amo	XecureDB	VDS
암호화방식	· 컬럼 단위	· API 방식	· 테이블 단위
장점	· 적용 범위에 따른 상대적 적은 비용	· 좋은 성능 · 높은 호환성	· 좋은 성능 · 높은 호환성 · DB이외의 로그파일암호화 가능
단점	· 오랜 구축 기간 소요 · 한정된 OS, DBMS호환 · 유지보수 비용이 큼	· 높은 개발비용 및 오랜 구축 기간 소요 · 유지보수 비용이 매우 큼 · 애플리케이션 변경 시 추가 개발필요	· 높은 개발 비용 및 오랜 구축 기간 소요 · 상대적으로 비싼 S/W
암복호화 성능차이	· 암호화 전• 후의 성능 차이는 약 20~30%정도 발생 · 특정 Query (조건검색, 범위검색 등)에서는 상당히 낮은 성능을 보여줌	· 암호화 전후의 성능차이는 미미 · 별도의 Server에서 암호화를 수행하기 때문에 단기간에 대량의 Data 암복호화 수행시 성능저하 발생	· 암호화 전과 후의 성능 차이는 약 5% 이내로 미미
설치시 DBMS, 애플리케이션변경여부	· DBMS의 환경 변화(뷰트리거 생성) · 애플리케이션 소스코드 수정 필요 (별도의 API 제공)	· Data 수집 및 전송을 위한 API를 제공 · 애플리케 이션 소스코드의 수정과 추가 개발이 필요	· DBMS / 애플리케이션의 환경 변화에 영향 미미
중앙집중관리지원여부	· 기능 없음	· 기능 없음	· Web UI에서 중앙 집중 관리
암호화 시 Data Size 증가여부	· 10~20% Size증가	· 10~20% Size증가	· 10% 이하 Size증가
지원환경	· MS-SQL, Oracle, DB2등을 지원 DBMS의 종류 및 Version에 영향을 받음	· 모든 DBMS를 지원 · 애플리케이션 서버의 개발 환경 및 OS에 영향을 받음 (C, JAVA, PHP등 지원)	· 모든 DBMS 지원 서버의 OS 및 CPU에 영향을 받음(대부분의 OS지원)

3. DB접근제어 및 암호화 전후 성능 실험

그림 7은 Unix 환경의 Oracle 데이터를 DB접근제어 전후의 응답 속도 실험을 한 결과이다. A통신사 B대리점에서 DB접근제어 제품인 DB_I를 사용하여 2500건의 회원데이터를 상대로 실험한 결과, DB접근제어의 경우, 네트워크 단말에서 접근통제를 하는 경우가 대부분으로 애플리케이션의 변경이나 데이터 자체의 암호화 과정이 거의 발생하지 않기 때문에 DB접근제어 전후의 응답속도는 기존의 시스템에 비교하여 큰 영향을 미치지 않는 것으로 나타났다.



테스트	평균
TPM1 (접근제어 전 Test 1)	1014.424 tpmc
TPM2 (접근제어 전 Test 2	1016.480 tpmc
TPM3 (접근제어 후 Test 1)	1025.278 tpmc
TPM4 (접근제어 후 Test 2)	1020.768 tpmc

그림 7 DB접근제어 전후의 시스템 성능 실험
Fig. 7. System Performance Test of DB Access Control

표 11은 Unix환경에서 Oracle데이터의 DB암호화 전후의 응답시간을 측정한 것이다. 측정 대상은 C시청에서 사용하는 Oracle 데이터를 상대로 기존의 시스템과 DB암호화 시스템, DB암호화를 한 후 튜닝을 한 시스템의 경우를 비교 분석한 것이다[15]. DB암호화를 할 경우, 기존의 시스템과 비교했을 때 시스템의 성능 부하가 10% 이상 증가되었으나 DBMS 튜닝을 통해 물리적인 I/O를 줄이고 논리적 I/O를 높일수록 전체 응답시간은 감소되는 것으로 나타났다.

표 11. DB 암호화 성능 시험 결과 - I
Table 11. Test Result of DB Encryption -I

구분		응답시간(초)		TPS 평균	총 처리 건수	CPU (DB서버)	
		평균	최대			평균	최대
AS-IS	회원 조회	19.0	25.8	10.4	5920	440	510
	회선 조회	19.1	26.5	10.4	5940		
	청약	84.0	101.4	2.1	1190		
DB 암호화	회원 조회	21.6	23.8	12.1	5890	470	510
	회선 조회	21.8	34.0	12.3	5910		
	청약	89.0	115.3	2.8	1300		
DB 암호화 + 튜닝	회원 조회	10.5	12.1	29.8	5900	500	530
	회선 조회	10.1	11.8	18.9	5880		
	청약	42.0	47.8	7.5	1220		

표 12는 B은행을 실험 대상으로 하여 Unix 환경의 Oracle 데이터를 암호화하여 측정한 결과이다[15]. 측정대상은 평상시 CPU운용환경에서의 암호화 전/후의 성능 실험, CPU부하가 50% 상태에서 암호화 전/후의 성능 실험 및 Index Join후 암호화 전/후의 성능 실험한 결과를 비교 분석한 것이다. 분석 결과, 평상시의 경우 암호화 전후 10% 안팎의 성능부하가 발생하였으나 CPU를 50%부하를 부여한 경우 성능차이는 크게 발생하지 않았으며 Index Join후와 같은 DB를 논리적 튜닝 했을 경우에도 암호화 전후의 성능 차이를 감소할 수 있는 것으로 나타났다.

표 12. DB 암호화 성능 시험 결과 - II
Table 12. Test Result of DB Encryption - II

구분 (단위:건)		암호화전			암호화후		
		test 1	test 2	test 3	test 1	test 2	test 3
평상시	1	0.18	0.17	0.19	0.21	0.19	0.20
	50,000	1.58	1.58	1.59	1.82	1.82	1.81
	100,000	3.18	3.18	3.19	3.66	3.64	3.67
	CPU부하율 (%)	25.0	25.1	25.0	26.5	27.1	27.4
50% CPU 부하	1	0.31	0.21	0.29	0.34	0.37	0.35
	50,000	2.11	1.95	2.07	1.91	2.40	2.15
	100,000	3.76	3.71	3.74	3.53	3.89	3.75
	CPU부하율 (%)	62.3	62.2	62.4	64.5	63.9	63.7
Index join후	1	0.18	0.15	0.14	0.17	0.19	0.18
	50,000	0.57	0.53	0.52	0.65	0.71	0.69
	100,000	1.08	1.05	1.02	1.23	1.27	1.24
	CPU부하율 (%)	22.5	22.7	22.6	23.5	24.0	23.9

그림 8은 위의 DB접근제어와 DB암호화 제품들을 대상으로 실험한 결과를 가지고 Unix환경과 Oracle데이터의 동일한 환경에서 동일한 시간동안의 처리량을 시뮬레이션한 결과이다.

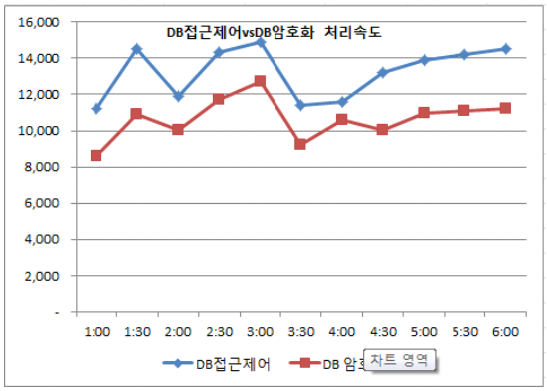


그림 8. DB접근제어 vs DB암호화 제품 처리량 비교
Fig. 8. Process Performance of DB Access Control vs DB Encryption

본 실험 결과, DB 접근제어 전후의 경우 DB 자체의 암복호화가 발생하지 않기 때문에 기존 시스템과 비교했을 때 성능의 차이는 거의 없었으나 DB암호화 전후의 경우 데이터 크기가 증가할 뿐만 아니라 데이터 암복호화에 따르는 속도 때문에 10% 안팎의 성능 차이가 발생하는 것을 알 수 있다. 따라서 대부분 온라인 대상의 네트워크 단말에서 처리속도에 민감한 시스템에는 DB접근제어 제품 등이 적합할 것으로 나타났으며 금융권 등 처리속도 보다는 데이터 보안이 민감한 분야는 또는 오프라인의 배치 처리가 가능한 시스템에는 DB보안 제품이 적합할 수 있다.

IV. 결론

DB접근제어는 네트워크 끝점에서 접근통제를 하기 때문에 기존 DBMS의 변경이 거의 필요 없으며 성능저하가 비교적 낮은 장점이 있는 반면 DB암호화방식은 권한이 없는 경우 데이터 자체의 열람이 불가능하다는 장점이 있다. DB접근제어는 사전 차단이 미약하나 접속 로그 기록을 남겨 사후 추적으로 보완이 가능하다는 단점이 있으며 DB암호화 방식은 적용 가능한 DB종류가 한정적이며 시스템부하로 성능이 저하될 뿐 아니라 시스템 구축 시 실패율이 높다는 단점이 있다. 현재는 암호화보다는 접근제어 방식이 시장에서 더 선호되는 방식이라고 할 수 있지만, 사실 두 방식은 상호 보완적인 관계라고 할 수 있다. 정보시스템을 구축할 때 가장 기본적이며 핵심은 중요 데이터가 있는 DB에 대해 접근제어 DB보안 시스템을 구축하되, 암호화 제품의 추가적인 도입여부는 상황에 따라 신중히 선택하고, 2차적인 정보유출 방지 시스템을 구축하는 것이다. 안정적인 DB보안 시스템을 구축하기 위해 각각 시스템의 구성 요건 및 특성을 고려해 접근제어 방식과 DB암호화 방식을 각각 또는 상호 보완하여 선택하는 데 있어서 본 논문이 참조될 수 있기를 기대한다.

참고문헌

[1] http://www.dbguide.net/db.db?cmd=view&boardUid=152806&boardConfigUid=9&categoryUid=216&boardIdx=146&boardStep=1

[2] Eong-Jun Kang, "Sucessful DB Security System Implmentation Method", Technical paper, Softforum,, 2012

[3] Joo Kyung-Soo, Woo Jung-Woong, "An Object-Oriented Analysis and Design Methodology for Secure Database Design -focused on Role Based Access Control", Journal of the Korea Society of Computer and Information, vol.18, no. 6, pp.63-70, June. 2013.

[3] DatabaseSecurity(Common-sensePrinciples), http://www.governmentsecurity. org/articles/DatabaseSecurityCommon-sensePrinciples.php

[4] http://www.kdb.or.kr/info/info_05_.php

[5] http://cafe.naver.com/volthee/120

[6] http://redkite777.tistory.com/315

[7] Jong-Il, Pak, Dae-Woo Park, "A Study on DB Security Problem Improvement of DB Masking by Security Grade", Journal of the Korea Society of Computer and Information, vol.14, no. 4, pp.101-109, April. 2009.

[8] Analysis Report of New Trend of DB Encryption and Security Technology, Financial Security Agency, September, 2012.

[9] Tae-Hee Park, "Database Encryption Police-Introduction of DataSecure", KSCI Review, vol.16, no 1, pp.61 -72, Jan. 2008.

[10] Young-Dae Ko, Sang-Jin Lee, "Proposal of Personal Information DB Encryption Assurance Framework", Journal of the Korea Institute of Information Security and Cryptology, vol.24, no. 2, pp.397-409, April, 2014

〔11〕 Seong-Yoon Shin, "A Study on Definitions of Security Requirements for Identification and Authentication on the Step of Analysis ", Journal of the Korea Society of Computer and Information, vol.19, no. 7, pp.87-93, July. 2014.
〔12〕 Joo Kyung-Soo, Woo Jung-Woong, "An Object-Oriented Analysis and Design Methodology for Secure Database Design -focused on Role Based Access Control", Journal of the Korea Society of Computer and Information, vol.18, no. 6, pp.63-70, June. 2013.
〔13〕 Woo Seok Seo, Jung Oh Park, Moon Seog Jun, "A Design of Policy Treatment Techniques of Access Control Inference based Convergence Security System", Korea Information Science Society Journal:Information Communication, vol.38, no. 6, pp.422-430, June. 2011.
〔14〕 Eui-Kil Lee, "Encrption Solution for Personal Information Security, Vometric Data Security Introduction", Technical Paper, COMAS, 2013
〔15〕 Hyun-A Park, Dong-Hoon Lee, Taek-Young Jeong, Young-Taek, Jeong, "Comprehensive Study on Security and Privacy Requirements for Retrieval System over Encrypted Database", Journal of the Korea Institute of Information Security and Cryptology, vol.22, no. 3, pp.621-635, June, 2012

저 자 소 개

윤 선 희
1983: 숭실대학교
전자계산학과 공학사.
1986: (미)웨인주립대학교
전자계산학과 이학석사.
1994: 성균관대학교
정보공학과 공학박사
현 재: 숭의여자대학교
디지털미디어전공 교수
관심분야: DB보안, 유비쿼터스, LBS, 증강현실, 빅데이터
Email : shyoon@sewc.ac.kr