DOI : 10.5392/JKCA.2011.11.2.061

데이터베이스 규제 준수, 암호화, 접근제어 유형 분류에 따른 체크리스트 구현

Materialize the Checklist through Type of Classification analysis for the Regulatory Compliance and Database Encryption, Access Control

이병엽*, 박준호**, 김미경**, 유재수**
배재대학교 전자상거래학과*, 충북대학교 전기전자컴퓨터공학부***

Byoung-Yup Lee(bylee@pcu.ac.kr)*, Jun-Ho Park(arionfit@naver.com)**,
Mi-Kyoung Kim(mini48minwoo@nate.com), Jae-Soo Yoo(yjs@chungbuk.ac.kr)**

요약

인터넷의 급격한 발달로 인해 수많은 기업에서 다양한 어플리케이션들이 불특정 다수의 사용자에게 개방되어 있는 현재의 비즈니스 환경에서 최근 개인정보의 보안에 대한 이슈가 자주 언급되며, 그 중요도 측면에서 기업의 최우선 과제가 되었다. 얼마 전 정부에서도 정보통신망법 상의 개인정보 보호 강화조치를 법률로 제정하고 이를 다양한 산업군에 적용하고 있다. 기업은 개인정보의 보호를 위해 다양한 방안들을 마련해 이러한 규제를 준수하여, 내부에 관리중인 개인정보에 대해 보안을 강화하기 위해 빠르게 보안 솔루션을 도입하고 있다. 이에 수많은 데이터들이 저장되어 사용되고 있는 DBMS 측면에서 규제를 준수하는 동시에 효과적으로 데이터 보안을 확보하기 위한 방안을 암호화, 접근제어, 감사로 구분하여 각각에 대한 구현방법 및 해당 솔루션들을 비교 및 검토하여 이를 통해 최적의 데이터베이스 보안 방안을 모색할 수 있도록 체크리스트를 구현하였다.

■ 중심어 : | 데이터베이스 보안 | 규제준수 |

Abstract

Due to the rapid development of the Internet, many companies in a variety of applications to users open an unspecified number of the current business environment, security of personal information about recent issues are often mentioned in terms of its importance may be the company's top priority. The government recently on personal information strengthening measures on information communications network law enacted into law which is applicable to various industries. Companies to protect the personal information of various measures to comply with these regulations, and arrange your personal information for internal management to enhance security fast security solution has been introduced. The number of used data is stored in the DBMS in terms of compliance with these regulations at the same time effectively to ensure data security and encryption measures, access control, audit, each separated by an implementation of the solution and how it compares with the best Database security plan allows you to explore as a this paper's security checklist.

■ keyword : | Database Security | Regulatory Compliance |

* 이 논문은 2010년 교육과학기술부"(지역거점연구단육성사업/충북BIT연구중심대학육성사업단)"와 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업의 결과임.(No. 2009-0089128)

접수번호 : #101116-002
접수일자 : 2010년 11월 16일
심사완료일 : 2011년 01월 05일
교신저자 : 유재수, e-mail : yjs@chungbuk.ac.kr

I. 서 론

1. 기업 내 데이터베이스 보안 이슈

1.1 개인정보의 유출

최근 전 국민의 1/5 에 해당하는 모정유사의 개인정보 유출 사례를 기억한다면 최근 들어 빈번하게 발생하고 있는 수많은 데이터 보안 사고들의 핵심은 민감한 개인정보의 유출에 있다는 것을 알 수 있다. 이러한 정보들이 본인의 동의 없이 무단으로 사용되어 불법적인 거래 및 스팸메일에 이용되어 금전적인 혹은 정신적인 피해를 끼치고 있으며 나아가 사회적인 문제까지도 야기하고 있다[1].

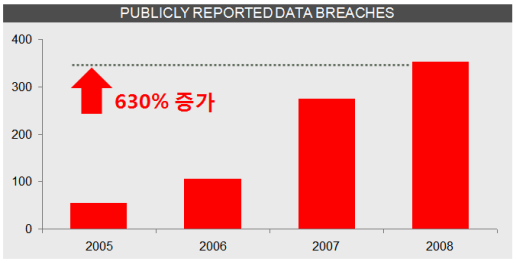

그림 1. 실제 유출된 개인정보 레코드 수(백만건)

개인정보 유출 문제는 비단 국내만의 문제는 아니며, 전세계적으로 관심이 집중되는 이슈 중 하나라 할 수 있다. [그림 2]와 같이 미국의 오픈 시큐리티 파운데이션(Open Security Foundation)에 따르면 유출된 개인정보가 08년 86,311,058개에서 09년 218,756,349개로 전년대비 153%로 상당히 증가 하였다. 유출된 개인정보는 상당히 증가한 것과 달리 공개적으로 보고된 개인정보 유출 사건 건수는 08년 717건에서 09년 436건으로 줄어들었다. 이는 개인정보 유출 사건의 피해 규모가 대형화되고 있다는 것을 의미 한다[9][10]. 따라서 이러한 개인정보의 유출이 개인 에게만 피해를 발생하는 것뿐 만은 아니다. 현재 미션 크리티컬한 비즈니스를 영위하고 있는 수많은 온라인, 오프라인 기업들에게 기업 이미지 혹은 브랜드 이미지라는 것은 이미 단순한 이름 그 이상의 것을 제공하고 있다.

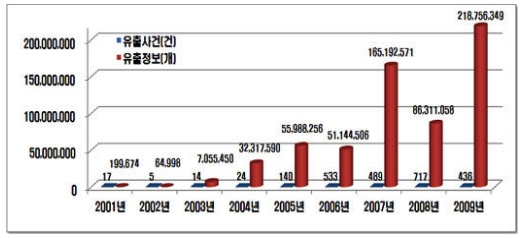

그림 2. 2001~09까지 개인정보 유출 및 레코드 현황

따라서 해당 기업의 정성적 가치를 대변하는 이러한 이미지에 조금의 상처도 용납하지 않는 것이 현 비즈니스 상황이며 더구나 다양한 보안이슈가 발생하고 있는 현 시점에서 모든 기업들은 개인정보의 유출이라는 심각한 보안이슈가 발생하지 않도록 많은 노력을 하고 있다. 한편 개인정보 유출 사고의 발생 원인을 살펴보면 금전적 이익을 얻기 위해 해킹 등 외부 침입에 의해 개인 정보가 유출되거나 내부자의 도용에 의해 누출되는 것으로 파악된다. 09년 국내에서 발생한 주요 개인 정보 유출 및 도용 관련 사건의 경우 대부분 [표 1]과 같이 금전적인 이익과 관련되어 있다[11].

표 1. 2009년 인터넷 개인정보 유출 및 도용사건

사건명	주요내용	발생시기
N포털 이용자 9만명ID, 비밀번호 도용사건	9만명의 ID 등을 광고에 도용해 1억3천만원의 수익을 올리고 다시 ID 등을 팔아 1천만원 챙김	09년 4월
A쇼핑몰 이용자 'e머니' 탈취사건	유출된 주민번호, 이름, ID 등을 조합해 다른 사람의 'e머니(현금과 같은 포인트)'를 사용	09년 7월
G쇼핑몰 고객 ID 도용	ID와 마일리지를 도박 사이트 광고 스팸문자 메시지 2100통을 보내는데 사용	09년 8월
N포털카페 '중고나라'게시판 ID 도용사건	4,900개 ID를 도용해 2만4천개 광고성 글을 카페에 게시,또 '중고나라' 운영자로 로그인해 회원 450만명에게 메일을 보내는 수법으로 1억4천 만원 챙김	09년 10월
219개 중소쇼핑몰 해킹	사이트를 해킹해 결제 계좌번호를 바꾸는 수법으로 500여명에게서 2천5백만원을 가로챔	09년 11월
N게임사 게임아이템 해킹	계정도용으로 아이템, 게임머니 털려, 4,700명 정도가 피해 소송 준비 중	09년 12월

1.2 다양한 규제의 강화

IT에 의존한 비즈니스 프로세스는 사용자 계정의 급

속한 증가를 가져오고 있으며, 기업 운영환경은 신속한 시장의 유동성, 서비스의 다양성 그리고 정보 및 서비스에 대한 즉각적인 고객의 반응을 특성으로 변화하고 있다. 또한 고객, 협력사 등 내, 외부 정보 이용자에게 기업의 정보자산을 직접 제공하는 경우가 증가 하고 있다. 이러한 비즈니스적 상황에 기인하여 기업 내 데이터 보안을 강화하고자 하는 노력은 이제 더 이상 각 기업의 자발적인 권고사항의 수준을 넘어 다양한 법적 규제를 통해 이를 해결하고자 하는 노력으로 발전하게 되었다. 최근 규제 준수에 따른 즉, 미국의 SOX(Sarbanes-oxley), HIPPA(Health Insurance Portability and Accountability Act), PCI(Payment Card Industry) DSS(Data Security Standard)와 같은 전자상거래 상의 데이터 보안 표준 와 같은 다양한 규제들이 전 세계적으로 강화되고 있으며, 이미 국내에서도 정보통신망법상 개인정보보호 강화조치가 시행되어 수많은 기업에서 민감한 개인정보를 안전하게 관리할 수 있도록 보안 시스템을 구축, 운영해야만 한다[6].

대부분의 기업들이 이러한 규제준수 대상에 포함되어 있으며, 이를 준수하기 위한 시스템 도입 및 인력확보에 높은 우선순위를 부여하고 빠른 시간 안에 이를 해결하고자 노력하고 있다.

IT 전문 조사기관인 포레스터에선 최근 IT Security Priorities 보고서에서 “기업의 정보 자산을 보호하는 것은 이제 보안 프로그램의 가장 큰 이슈이며. 특히, 데이터 보안(90%)은 IT 보안 조직들의 중요한 또는, 가장 중요한 이슈로서 언급되고 있다.”[2] 와 같이 기업 내 데이터 보안의 당위성을 강조하고 있다.

1.3 기업 내 데이터 보안 확보 방안

그렇다면 기업은 어떠한 방법으로 데이터, 특히 이슈가 되고 있는 개인정보에 대한 보안을 확보하는 동시에 강화된 규제들을 손쉽게 준수하는 것과 같은 효율적인 보안 확보방안에 대하여, 데이터가 저장되어 있는 DBMS 측면에서 3가지로 분류하여 각각의 데이터 보안확보 유형 및 구현 방법에 대해 알아보고 본 논문에서는 데이터베이스 보안 솔루션 및 구현을 위한 체크리스트를 구체화 하여 제시 하고자 한다.

II. 본 론

1. 기업 내 데이터베이스 보안확보 유형

1.1 국내 보안 솔루션 현황

대부분의 기업들은 개인정보의 보호를 위해 다양한 보안 솔루션들을 채택해 적용해 오고 있다. 이러한 솔루션들은 해당 기업의 보안 우선순위에 의해 선택적으로 사용되고 있으며 이를 데이터 암호화, 접근제어, 감사와 같은 3가지 유형으로 나누어 보고 이에 속하는 솔루션을 분류해 보면 다음 [표 2]과 같다.

표 2. 국내 보안 솔루션의 분류

분류	국내 솔루션
암호화	Penta Security D'Amo eGlobal system CubeOne
접근제어	WareValley Chakra PnPsecure DB Safer
감사	각 DBMS 벤더의 기술을 적용

그렇다면 이러한 솔루션들은 어떻게 데이터베이스 내 데이터에 대한 암호화 및 접근제어를 구현하고 있는지 기술 구조를 살펴보면 [그림 3]과 같다. 국내 암호화 솔루션들은 원천 기술을 보유하고 있는 DBMS 벤더에서 제공하는 공개된 기술을 사용하여 데이터 암호화를 수행하고 있다.

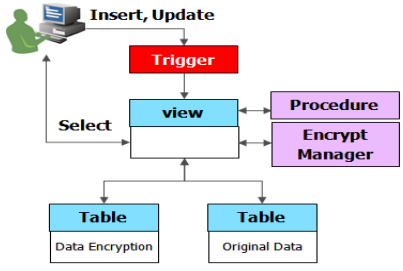

그림 3. 국내 암호화 솔루션 구현방법

일반적으로 공개된 기술을 이용하면 원천적인 DBMS 내부 커널을 이용하지 않고도 암호화 기능을 구현할 수 있다는 장점이 있다. 하지만 그에 따른 성능 부하 및 데이터 변경이라는 위험이 있고 이를 감수하고 도입한 사례가 있으며 대표적으로 국내 솔루션 도입에 앞장섰

던 다수의 공공기관에 적용되어 있다.

접근제어 솔루션들 역시 [그림 4]와 같이 크게 다를 바가 없다.

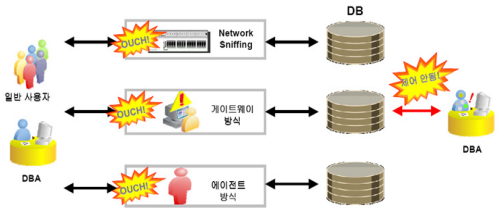

그림 4. 국내 접근제어 솔루션의 리스크

이 역시 DBMS 내부에서 제어할 수 없기에 중간에 게이트웨이나 네트워크 패킷의 스니핑, 에이전트 방식을 채택함으로써 우회 접근에 대한 위험 및 복잡한 업무에 적용할 수 없는 단점을 보유하게 된다.

1.2 DBMS 벤더의 데이터 암호화

데이터 암호화란 데이터 보안확보 유형 중 가장 일반화되어 있는 방식으로 기업 내 저장되어 관리되고 있는 데이터를 인증 받은 암호화 알고리즘을 통해 암호화하여 허가받지 않은 사용자에 의한 데이터 미디어(Disk) 및 백업본이 유출되더라고 이를 이용해 민감한 개인정보를 도용하지 못하도록 할 뿐만 아니라 네트워크를 통해 전송되는 데이터 패킷까지도 암호화하여 스니핑과 같은 해킹 기술을 이용하더라도 [그림 5]와 같이 데이터를 안전하게 관리할 수 있도록 한다 하지만, 이러한 데이터 암호화를 구현 시 고려해야 되는 사항은 어떠한 것들이 있는지 이에 대한 고찰이 필요하다.

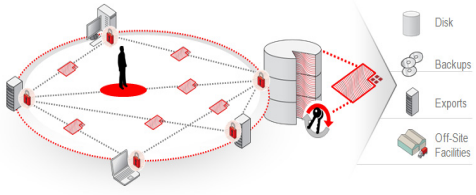

그림 5. 데이터 암호화 유형

첫째, 어플리케이션의 수정이 필요한지의 여부다. 대부분의 경우 데이터를 암호화하는 시스템들은 지금까지 잘 사용해 오던 시스템일 경우가 많으며, 이러한 경우에 잘 사용해오던 수많은 어플리케이션 코드의 수정이 동반되어야 한다면 보안확보에 소요되는 경비가 지나치게 많이 소모될 뿐만 아니라 너무 번거롭기까지 하게 된다. 따라서 보안의 도입시 어플리케이션의 도입 여부는 반드시 점검해 보아야 할 사항이다.

둘째, 성능을 유지할 수 있느냐의 여부다. 데이터를 암호화한다는 것은 특정 알고리즘에 의해 해당 데이터를 변환하고 이를 필요시 다시 원래의 데이터로 복호화해야 하기 때문에 이에 소모되는 리소스 (CPU 파워와 같은)가 더 많이 소비되기 때문에 시스템 성능의 하락을 수반하는 경우가 많다. 이를 얼마나 최소화할 수 있는 것이 데이터 암호화의 또 다른 관건이며 O사와 같은 DBMS 벤더들은 이러한 암/복호화를 커널 내부에서 수행케 함으로서 성능 하락을 최소화 할 수 있는 메커니즘을 제공한다[3].

1.3 DBMS 벤더의 접근제어

데이터 유출 사례 중 가장 많은 사례는 대부분의 경우 해킹에 의한 데이터 유출을 생각하겠지만 현실은 그렇지 않다. 오히려 내부자에 의한 데이터 유출이 가장 심각하며 이에 대한 대처방안 역시 기업 내 데이터 보안확보의 중요한 화두이다. 이를 해결하기 위한 방안으로 데이터 접근제어가 있다.

접근제어란 외부에서 인가받지 않은 장비 혹은 IP의 DBMS 접근을 원천적으로 차단할 뿐만 아니라 사용자 혹은 어플리케이션의 권한에 따라 접근할 수 있는 데이터를 정의하고 이에 위반할 경우 해당 데이터에 접근할 수 없도록 한다.

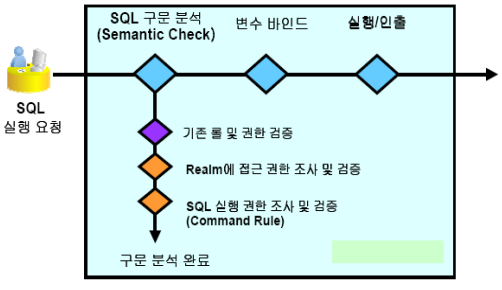

그림 6. O사 접근제어 구현

데이터에 접근하는 방법이 다양하기 때문에 이를 제어해야하는 접근제어 역시 다양한 제어 방식을 지원해야 한다. 또한 우회 접근을 원천적으로 차단하여 보안상의 취약점이 발생할 수 없도록 해야 한다. 대표적인 DBMS 업체인 O사의 경우 [그림 6]과 같이 수많은 접근제어 펙터를 제공하며 이러한 펙터들을 서로 조합하여 사용할 수 있게 하여 다양한 접근방식을 모두 만족시킬 수 있는 제어 기능을 제공할 뿐만 아니라 SQL Parsing 시 접근제어를 수행하기 때문에 우회 접근을 원천적으로 차단하여 최상의 접근제어를 통한 데이터 보안을 가능케 한다[4].

1.4 DBMS 벤더의 감사

최근 몇 년 사이 금융이나 대기업, 정부투자기관 등에서는 다양한 시스템의 도입과 전자 금융 등의 활용이 증대되고 있다. 이에 정보기술에 기초한 효율적이고 효과적인 데이터 감사 업무 수행이 주요 과제로 대두되기 시작했다[8]. 따라서 기업 내에서의 데이터 유출을 원천적으로 차단하는 것만큼 중요한 보안 이슈가 데이터에 대한 감사 기능의 활용이다. 지금까지의 데이터에 감사는 단순히 DBMS 내 모든 혹은 특정 활동들에 대한 내역을 저장하고 이를 문제가 발생했을 때 이용하는 경우가 대부분 이었지만 최근 감사가 설정된 이벤트가 발생하면, 해당 이벤트를 포함하여 이벤트를 발생시킨 사용자와 이벤트를 발생시킨 사용자의 클라이언트 컴퓨터에 대한 다양한 정보를 수집 한다. 이제 강화된 보안규제를 준수하기 위해선 그 이상의 효율적인 관리 및 통제를 필요로 하게 된다.

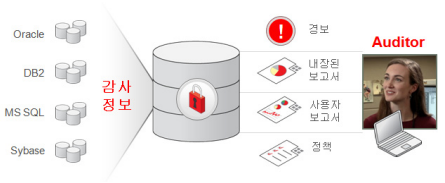

그림 7. 감사 솔루션의 유형

기업 내 분산되어 있는 다양한 시스템의 감사정보를 통합관리하고 이러한 데이터에 대한 인위적인 위/변조를 원천적으로 제어하며 실시간 경보를 통한 효율적인 관리 및 다양한 보고서를 작성할 수 있도록 그 기능의 확대가 필요한 시점이다. 이러한 다양한 요구사항을 모두 충족할 수 있는 솔루션의 도입이 기업 내에서는 매우 필요하게 대두 되었다[5].

2. 기업 내 데이터 보안확보 유형과 규제 준수

2.1 정보통신망법 상 개인정보보호 강화조치

인터넷의 급격한 확산으로 인해 수많은 어플리케이션들이 불특정 다수의 사용자에게 개방되어 있고 사용자 인증을 위해 개인 정보를 필요로 함에 따라 대부분의 기업들이 개인 정보를 자체 관리함으로서 개인정보보호를 강화하기 위한 조치가 국내에서 방송통신위원회 주도로 대통령령으로 시행하게 되었으며 2009년 적용 대상 업체의 확대로 인해 국내 대부분의 기업에서는 이를 반드시 준수해야 하며 위반 시 벌금 및 처벌을 받게 된다[6].

2.2 개인정보의 기술적 관리적 보호조치 기준

정보통신망법 상 강화된 개인정보보호 기준에 맞는 기술적 관리적인 보호조치를 구분해 각 항목별로 살펴보면 [표 3]과 같다[7].

표 3. 개인정보의 기술적 관리적 보호조치 기준

구분	항	내용
제3조		개인정보관리계획 수립 및 이행 (관리 책임자 및 취급자의 지정과 교육)
제4조 접근통제	1	최소인원에만 접근권한 부여
	2,3	접근권한 변경/말소 관리 및 부여/변경/말소 내역 기록 (최소 5년 보관)
	4	외부에서 정보통신망으로 접속 시 안전한 인증 수단의 적용
	5	접속권한 제한을 통한 불법적인 접근 및 침해사고 방지
	6,7	패스워드 작성규칙 수립/이행
	8	처리시스템/취급자PC 설정(인터넷,P2P,공유설정 차단)
제5조 접속기록 위,변조 방지	1,2	접속기록(처리일시, 내역 등) 저장 및 월 1회 확인/감독 및 최소 보존기간 규정
	3	접속기록 별도 저장 및 백업 보관(위변조 방지)
제6조 암호화	1	본인 인증정보(패스워드, 생체정보) 일방향 암호화 저장
	2,3	주민등록번호, 신용카드번호 및 계좌번호의 암호화 저장 및 인증정보 송/수신 시 암호화
	4	개인정보 PC 저장 시 암호화
제7조 악성프로그램	1	백신 S/W 설치(악성프로그램 점검/치료)
	2	백신 S/W 월 1회 갱신/점검(최신 업데이트)
제8조 출력 및 복사 시 보호조치	1	출력시(인쇄,화면,파일생성 등) 용도 특정 및 항목 최소화
	2	인쇄/이동매체복사 시 기록/사전승인(재복사 포함)
	3	명칭 및 일련번호 표시
	4	2항 위법여부 확인 및 유출 시 법적 책임 주지

지금가지 언급했던 데이터 암호화, 접근제어, 감사를 통해 이러한 규제를 준수할 뿐만 아니라 개인정보 유출을 통한 기업 이미지의 하락과 같은 치명적인 위험에서

벗어나 다양한 비즈니스 환경에서 빠르게 적응할 수 있는 기업으로 체질개선을 했다고 볼 수 있다.

2.3 데이터베이스 보안구현

본 논문은 다양한 보안 솔루션들에 대한 고찰을 하였고, 이에 따른 데이터베이스 보안을 구현하기 위한 체크리스트를 제언하고자 한다. 데이터베이스의 보안을 구현하기 위해서는 [표 4]에서와 체크 항목의 분류와 분류항목에 대한 다양한 부분들의 검증이 필요하다. 또한 Infra의 성능 적인 측면에서 반드시 테스트가 진행되어야 한다. 이는 암호화 관련 디스크의 성능 개선의 측면에서 살펴보면 암호화, 복호화에 따른 디스크 I/O가 발생하기 때문에 디스크 I/O성능이 개선되면, 선형적인 응답 속도를 향상시킬 수 있다. CPU의 처리속도 측면에서도 블록 싸이퍼 암호화 알고리즘의 특성상 암호화 성능을 개선할 수 있는 방법으로 CPU의 클럭 스피드 개선이 필수이고, OLTP와 같이 병렬 처리가 불가능한 작업의 응답속도 개선에 매우 효과적인 개선을 할 수 있다. 또한 병렬처리를 통한 개선방법은 디스크 IO를 많이 사용하는 배치 작업의 경우, 병렬처리를 통해 CPU 개수의 증가에 따라 선형적인 성능향상을 구현해야 하고, 배치 작업의 경우에도 암호화에 따른 비용 보정은 디스크 I/O속도 및 CPU클럭 스피드 개선이 동일하게 적용 되어야 한다.

표 4. 데이터베이스 보안구현 체크리스트

검증 영역	검증 구분	검증 항목	검증 방법
1) 보안	보안 관리	• 암호화 알고리즘 안정성, DMM 지원 여부	Function Test
	암호화 키 관리	• Master Key 관리, 키 관리의 안정성	Function Test
	솔루션 운영 관리	• DB암호화 솔루션 프로세스 control, DB암호화 키 재생성 등	업체 시연
2) Application	DB Object	• 암호화 테이블이 Partition이고 Partition Key에 암호화 항목이 포함되어 있는 경우 사용 가능 여부	SQL 수행
	SQL Pattern	• Query Tool 사용 시 사용자 권한에 의한 암/복호화 여부	SQL 수행
		• SQL 상의 연산자(=, 〈, 〉, Between, Like, IN) 사용	SQL 수행
		• 각종 sql 함수(Substr, Length, Decode, Case, Trim, Translate, Replace 등) 사용 여부와 WHERE 절 사용 시 인덱스 사용 여부	SQL 수행
		•암호화 항목이 포함되어 있는 결합 인덱스의 색인 검색 가능 여부	SQL 수행
		• Outer Join/Sub Query/Order By 사용 가능 여부	SQL 수행
3) Architecture	Architecture	•UKey 아키텍쳐(TmaxSoft ProFrame-C) 적용 가능 및 영향도	프로그램
	Application 운영	•솔루션 자체 Error Message 처리 방식 적용 여부(자체 디버깅 기능 및 Error Message처리 기능 여부)	프로그램
		•데이터 관련 운영 Tool(ETL, SQL Loader, Connect Direct) 지원 여부	프로그램
4) Infra.	적용 환경 관리	•암호화 적용된 테이블 형태 및 환경의 변경 가능 여부 (Alter, drop, reorg 등)	SQL 수행
	Data Migration	• 초기 Data Migration 소요 시간 및 테이블/인덱스 증가 Size	초기 이행
	성능	•암호화 적용후 OLTP 서비스 응답시간 변화률	성능테스트
		•암호화 적용후 DB 응답시간 변화률	성능테스트
		•암호화 적용후 Batch 업무 처리시간 변화률	성능테스트
		•암호화 적용후 System(CPU,Memory,Storage) 사용량 증가율	성능테스트
		•On-Line SQL 발생 I/O 횟수 변화률	성능테스트

따라서 [표 4]에서와 같이 검증영역을 네 가지로 분류하고 각각의 검증영역에서 실제적으로 보안 솔루션 구현을 하기위해 검증 내용을 구체화 하였다. 보안관리를 하기 위한 적용 알고리즘 이라든지, SQL 패턴의 분석, 데이터 보안을 확장 또는 기능적인 향상을 위한 아키텍쳐 측면에서도 점검해야 할 구체적인 진단 리스트를 구현 하였다.

III. 결론

1. 데이터베이스 보안의 향후 과제 및 결론

1.1 현 데이터베이스 보안 솔루션의 과제

수많은 기업들이 보유하고 있는 민감한 데이터의 경우 대부분 DBMS 로 관리되고 있다. 이러한 데이터의 보안은 다수의 보안 솔루션 벤더 및 DBMS 벤더의 솔루션에 의존하고 있으며 이를 통해 상당한 수준의 데이터 보안을 확보할 수 있다. 하지만 비즈니스 환경은 급변하고 있으며 이에 따른 좀 더 강화된 규제 및 새로운 IT 패러다임에 대비할 수 있어야 한다.

암호화, 접근제어, 감사의 세 가지 유형으로 구분한 데이터 보안 확보의 유형은 향후, 모바일 환경의 대두와 클라우딩 컴퓨팅으로 인한 IT 환경의 변화에 따라 지금까지의 보안 솔루션 벤더와 기업 모두에게 새로운 도전이 될 것이며 이러한 변화를 적극적으로 수용하며 지속적인 투자 및 연구개발을 통해 발전시키는 동시에 보다 다양한 기술과의 융합(압축과 같은)을 통해 그 영역을 확대 시키는 것이야 말로 현 보안 솔루션의 과제라 할 수 있다.

1.2 결론

지금까지 데이터베이스 보안 확보 방안들을 살펴보았다. 다양한 보안 솔루션들이 존재하며 각각의 기술을 가지고 수많은 기업에서 사용되고 있는 이러한 솔루션들 중 최상의 선택을 한다는 것은 매우 어려운 일이다. 다만 위에서 언급한 세 가지의 보안유형으로 살펴보면 암호화, 접근제어, 감사의 측면에서 DBMS 벤더의 솔루션들이 가장 기술적으로 앞서 있으며 이는 성능부하

및 우회차단, 통합감사와 같은 요건들을 가장 잘 충족하고 있다고 할 수 있다. 본 논문에서 제시한 체크리스트는 데이터베이스에 보안 솔루션 도입 및 구현을 위한 기본적인 체크 사항 및 검증 항목들을 검증영역의 보안, 어플리케이션, 아키텍처, 인프라의 측면에서 세부적으로 기술 하였다. 이는 기존의 데이터베이스 보안의 약점을 이용한 다양한 해킹 방법 및 보안영역에서 약점에 대한 솔루션의 검증 방법을 구체적으로 제시 하였고, 데이터의 암호화 및 복호화에 따른 데이터베이스의 성능 적인 측면에서도 솔루션 검증 및 테스트 할 수 방법을 제시 하였다.

최상의 보안 솔루션은 없다. 다만 항상 데이터 보안에 관심을 갖고 이를 유지 및 발전시킬 수 있는 의지와 이를 도와줄 수 있는 신뢰할 수 있는 솔루션의 결합을 통해 최선을 다하는 것이야 말로 최상의 보안 확보 유형이라 할 수 있다.

참 고 문 헌

[1] http://datalossdb.org/reports
Publicly Reported Data Breaches by DataLossDB 2005~2008

[2] Report on IT Security priorities for 2009 by Forrester Research

[3] http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/asointro.htm#i1008719
Advanced Security Administrator's Guide.

[4] http://download.oracle.com/docs/cd/E11882_01/server.112/e10576/dvintro.htm#CEGBCJCB
Database Vault Administrator's Guide.

[5] http://download.oracle.com/docs/cd/E14472_01/doc.102/e14459/avadm_intro.htm#sthref30
Audit Vault Administrator's Guide.

[6] http://law.go.kr/LSW/lsSc.do?menuId=0&p1=&query=%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D+%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84+%EB%B0%8F+%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8+%EB%93%B1%EC%97%90+%EA%B4%80%ED%95%9C+%EB%B2%95%EB%A5%A0&x=3&y=9
정보통신망 이용촉진 및 정보보호 등에 관한 법률/시행령,/시행규칙

[7] http://www.kisa.or.kr/jsp/public/laws/laws3.jsp
개인정보의 기술적 관리적 보호조치 기준 해설서

[8] http://olv.moazine.com/rviewer/index.asp

[9] http://blog.daum.net/kcc1335/1890

[10] http://datalossdb.org

[11] 사이버 테러대응센터, http://www.netan.go.kr/

저 자 소 개

이 병 엽(Byoung-Yup Lee) 종신회원

- 1991년 2월 : 한국과학기술원 전산학과(공학사)
- 1993년 2월 : 한국과학기술원 전산학과(공학석사)
- 1997년 2월 : 한국과학기술원 경영정보공학(공학박사)
- 1993년 1월 ~ 2003년 2월 : 대우정보시스템 차장
- 2003년 3월 ~ 현재 : 배재대학교 전자상거래학과 부교수

<관심분야> : XML, 지능정보시스템, 데이터베이스시스템, 전자상거래학

박 준 호(Jun-Ho Park) 정회원

- 2008년 2월 : 충북대학교 정보통신공학과(공학사)
- 2010년 2월 : 충북대학교 정보통신공학과(공학석사)
- 2010년 3월 ~ 현재 : 충북대학교 정보통신공학과(박사과정)

<관심분야> : 분산 데이터베이스 시스템, 센서 네트워크, RFID, 차세대 웹, U-Leaning(LMS, LCMS)

김 미 경(Mi-Kyoung Kim) 준회원

- 2009년 2월 : 충북대학교 정보통신공학과(공학사)
- 2009년 9월 ~ 현재 : 충북대학교 정보통신공학과(석사과정)

<관심분야> : DB 시스템, 센서 네트워크, 저장시스템, 파일시스템

유 재 수(Jae-Soo Yoo) 종신회원

- 1989년 : 전북대학교 컴퓨터공학과(공학사)
- 1991년 : 한국과학기술원 전산학과(공학석사)
- 1995년 : 한국과학기술원 전산학과(공학박사)
- 1995년 ~ 1996년 : 목포대학교 전산통계학과 전임강사
- 1996년 ~ 현재 : 충북대학교 전기전자컴퓨터공학부 교수

<관심분야> : 데이터베이스 시스템, XML, 멀티미디어 데이터베이스, 분산 객체 컴퓨팅