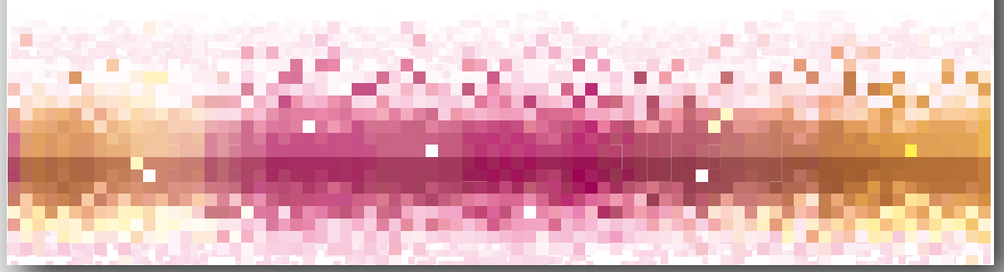
귀사의 데이터베이스 시스템은 안전한가요?

저자 – **박형도** 수석 컨설턴트, 한국 오라클 DB 사업부 (hyungdo.park@oracle.com)

곧 다가올 개인정보보호법의 시행과, 최근에 발생한 금융권 보안 사고로 인하여 정보시스템의 보안은 더 이상 미룰 수 있는 문제가 아니다. 물론 데이터베이스 보안은 전체 정보시스템의 포괄적 보안의 일부이다. 그럼에도 불구하고 데이터베이스 보안은 데이터베이스가 대다수 업무의 핵심 인프라이고 다량의 기업자산의 보관소라는 측면에서 정보시스템 보안의 중추라고 할 수 있다.



들어가며

개인정보보호법의 제정

개인정보보호법이 2011년 3월 제정되어 오는 9월부터 시행될 예정이다. 정보사회의 발전과 신용거래의 고도화로 인해 개인정보의 수집과 이용이 보편화되었고, 이에 따라 개인정보의 보호원칙과 명확한 처리기준에 대한 국가적 차원의 제도화가 필요하게 되었는데 이것이 개인정보보호법의 제정 배경이다.

개인정보 보호법 제정 이전에는 '공공기관의 개인정보보호에 관한 법률', '정보통신망이용촉진 및 정보보호 등에 관한 법률', ' 신용정보의 이용 및 보호에 관한 법률' 등 산업부문별로 개인정보 보호 관련 법체계가 마련되어 있었다. 즉 국가사회 전반을 규율하는 법체계의 미비로 개인정보보호의 사각지대가 여전히 존재하였고 개인정보의 유출 · 오용 · 남용 등의 침해 사례는 끊이지 않았다.

개인정보보호법은 이러한 문제를 해소하기 위하여 공공기관과 민간기업을 망라하여 약 350만개 이상의 단체를 대상으로 온라인/오프라인에 상관없이 포괄적으로 적용하여 개인정보에 대한 권리와 이익을 보장하려는 목적으로 제정되었다.

분야	주요 법률		관련 법률
공공행정	헌법	공공기관의 개인정보보호에 관한 법률	공공기관의 정보공개에 관한 법률
			전자정부법
			주민등록법
			국정감사 및 조사에 관한 법률
정보통신		정보통신망이용촉진 및 정보보호 등에 관한 법률	통신비밀 보호법
			위치정보의 보호 및 이용 등에 관한 법률
			국가정보화 기본법
			정보통신기반 보호법
금융신용		신용정보의 이용 및 보호에 관한 법률	금융실명거래 및 비밀보장에 관한 법률
			방문판매 등에 관한 법률
			전자상거래 등에서의 소비자보호에 관한 법률
			전자거래기본법
			보험업법
			자본시장과 금융투자업에 관한 법률
의료		보건의료기본법 의료법	장기 등 이식에 관한 법률
			생명윤리 및 안전에 관한 법률
			인체조직 안전 및 관리 등에 관한 법률
교육		교육기본법	초중등교육법
			교육정보시스템의 운영 등에 관한 규칙 등

<표 1> 국내 개인정보보호 관련 법체계

자료: 국회 행정안전위원회 , '개인정보보호법안, 공공기관의 개인정보보호에 관한 법률 일부 개정 법률안', 검토보고서

개인정보보호법의 주요 내용은 다음과 같다.

1) 개인정보 보호법안의 적용대상 확대 – 공공 · 민간부문의 모든 개인정보처리자(제2조)
2) 개인정보보호위원회 설치(제7~8조)
3) 개인정보의 수집, 이용, 제공 등 단계별 보호기준 마련(제15~22조)
4) 고유식별정보의 처리제한 강화(제24조)
5) 영상정보처리기기의 설치제한근거 마련(제25조)
6) 개인정보 영향평가제도 도입(제33조)
7) 개인정보 유출사실의 통지/신고제도 도입(제34조)
8) 정보주체의 권리 보장(제35~39조)
9) 개인정보 분쟁조정위원회 설치 및 집단분쟁조정제도의 도입(제40~50조)
10) 단체소송의 도입(제51~57조)
11) 개인정보 침해사실의 신고(제62조)

개인정보 보호법안(대안)의 세부 내용은 대한민국국회 정보광장에서 확인할 수 있다.

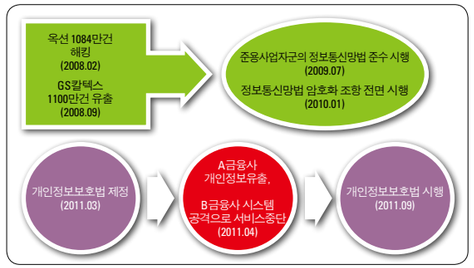
본론

최근 금융권 보안 사고의 유형 (공격과 유출)

개인정보보호법 제정 이전에 정보통신망이용촉진 및 정보보호 등에 관한 법률 (이하 정보통신망법)은 정보통신서비스 제공자 이외에 준용사업자라 하여 다양한 산업군에 걸쳐 개인정보보호를 위한 법적 규제를 제시하였다. 2008년 발생한 옥션 해킹 및 GS칼텍스 고객정보 유출사고 이후 2008년 12월 31일 정보통신망법 시행규칙 일부개정을 통하여 20여 개가 넘는 사업군이 동법을 준수하도록 강제되었다.

이에 따라 2009년 7월부터 백화점,여행업,의료업 및 석유정제업등 20여 개가 넘는 준용 사업자군이 동법의 적용을 받게 되고(시행), 2010년 1월부터는 개인정보를 반드시 암호화하여 저장하여야 하는 등의 조치를 준수해야만 했다.

한가지 흥미로운 사실은 정보통신망법의 준수가 강제되기 직전 옥션 해킹 및 GS칼텍스 고객정보 유출사고와 같은 대형 사고가 발생했던 것처럼, 개인정보보호법이 제정되고 시행되기 이전 시점에 국내 대형 금융기관 두 곳에서 각각 서비스 불능과 고객정보 유출이라는 대형 사고가 발생했다.



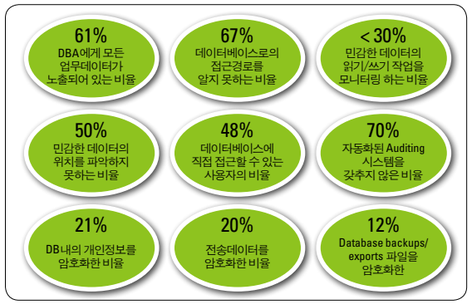
<그림1> 보안 사고 발생 시기와 Compliance 시행 시기

그런데 이전 사건과는 달리 최근에 발생한 금융기관의 사고는 해당 금융기관을 이용하는 국민들의 불편과 금융정보의 유출이라는 점에서 매우 큰 사회적 경제적 파장을 불러일으켰음은 물론 정보시스템의 보안이 절실하다는 사회분위기를 만들어 주었다. 이러한 사회분위기는 9월에 시행될 개인정보보호법과 맞물려 대부분의 산업군에서 그들의 보안실태를 점검하는 계기가 되었고, 지금보다 철저한 장치가 필요하다는 인식을 가지게 해 주었다.

정보시스템 보안의 관점에서 두 곳 금융기관의 사건은 각각 공격과 유출이라는 용어로 설명된다. 정보시스템에 대한 공격은 분산서비스거부 공격(DDoS), Malware 주입 및 계정 정보의 획득 후 정보시스템 구성요소에 대한 파괴(Shutdown, Drop, Delete)등의 형태로 나타난다. 이에 반해 정보유출의 경우는 대부분 그 표적이 데이터베이스일 확률이 높다. 고객정보와 같은 개인정보를 포함하여 기업의 중요 정보를 저장하고 있는 데이터베이스의 유출은 데이터베이스 관리시스템(DBMS) 내에서 적절한 권한을 가지고 있거나, 데이터베이스가 설치된 운영체제(OS) 내에서 데이터베이스 파일을 이용(읽기, 쓰기)할 수 있는 권한 혹은 그 이상의 권한을 가진 사용자에 의해 발생될 소지가 높다. 즉 데이터베이스에 대한 보호는 데이터베이스 시스템 계정정보의 보호는 물론이고, 이미 적절한 계정정보와 데이터베이스에 대한 접근권한을 가지고 있는 내부자에 대한 보안 위협(공격 혹은 실수, 정보 유출)에 초점을 맞추어야 한다.

내부자에 의한 보안 위협

기업이 데이터베이스 시스템에 접근할 권한이 있는 내부자의 보안 위협에 대해 취하고 있는 조치 실태를 IOUG(Independent Oracle Users Group)의 2009년

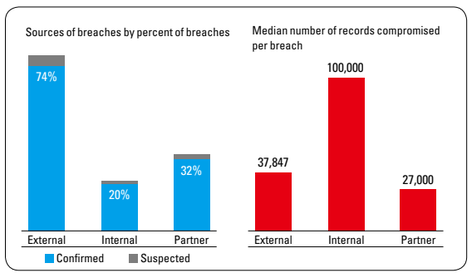


<그림2> 보안 장치 실태 – IOUG Data Security Report 2009

Data Security Report 를 통해 확인할 수 있다.

데이터베이스 파일이나 백업파일의 유출로 인한 피해를 차단하기 위한 DB 암호화 비율은 20% 정도를 넘지 않으며, 60% 이상의 기업에서 데이터베이스 시스템에 대한 접근 경로를 인식하지 못하고 있고, 업무와 무관한 DB관리자(DBA)에게 업무데이터가 노출되어 있는 경우도 매우 많음을 알 수 있다. 물론 정보시스템을 운영함에 있어 내부직원에 대한 기업의 신뢰가 바탕이 되어야 함은 기본이다. 하지만 정보시스템의 가장 중심에 있는(중요성이건, 물리적 위치이건) 데이터베이스 보안의 핵심은 내부자(적법한 내부자이건, 계정도용을 통한 침입자이건)에 대한 보안임에도 데이터베이스를 위한 보안 장치는 매우 미흡함을 알 수 있다.

내부자에 의한 데이터 유출 시도는 해킹등의 방법을 통해 시스템에 침입한 외부자에 의한 시도보다 그 횟수는 적을지라도 유출되는 데이터의 양이나 파급효과 측면에서 영향도가 훨씬 강하다. 내부자는 기업이 보유하고 있는 대량데이터를 비교적 쉽게 접근할 수 있을 뿐 아니라, 대량 데이터 중에서 개인정보와 회사의 기밀정보와 같은 알짜 정보의 위치를 이미 파악하고 있기 때문이다.



<그림3> 내부자 보안 위협의 심각성

본 기고는 정보시스템의 핵심이자 다양한 보안 위협(공격과 유출)의 최종 타깃이라 할 수 있는 데이터베이스를 안전하게 보호하고 운영하기 위한 몇 가지 방법들과 그에 따른 고려사항들을 독자 여러분들께 제시하고자 한다.

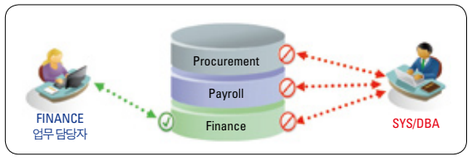
귀사의 데이터베이스 시스템은 안전한가요?

본 기고의 제목은 "귀사의 데이터베이스 시스템은 안전한가요?" 이다. 데이터베이스를 대상으로 하는 보안 위협요소 중 주요 내용을 정리하면 다음과 같다.

▶ 내부 관리자에 의한 권한 오용 대비책은?
▶ 인가된 사용자에 의한 실수 및 의도적인 위협 대비책은?
▶ DB 파일 유출 사고 대책을 준비하고 계신가요?
▶ 데이터 암호화 구현으로 인한 성능저하와 비용으로 고민하고 계신가요?
▶ DBMS 관련 보안사고 발생 시 사후 분석이 가능한가요?
▶ 항상 가용한, 안전한 DR 환경을 구축하고 있습니까?

내부 관리자에 의한 권한 오용 대비책은?

데이터베이스를 통한 정보 유출 사고 중 내부자에 의한 소행으로 밝혀진 비율은 약 50%에 육박하는 것으로 알려져 있다. 이는 많은 기업의 데이터베이스 관리 체계가 적절한 역할 분리 (Separation of Duties)를 구현하고 있지 않음에 기인한다. 예를 들어 데이터베이스 관리자(DBA)라 할지라도 업무데이터에 대한 직접적인 Ownership이 없다면 내부 정보 및 불필요한 데이터에 대한 무분별한 접근을 통제 해야만 한다.



<그림4> Super-User(내부관리자)에 대한 접근 통제

인가된 사용자에 의한 실수 및 의도적인 위협 대비책은?

위의 경우는 업무담당자 이외의 강력한 권한을 가진 내부자 (DBA Role을 가진 자)가 지금까지와는 달리 업무 데이터를 자유롭게 접근하는 것을 통제해야 함을 의미한다. 그렇다면 업무 담당자는 언제 어디서나 업무 데이터를 접근/처리할 수 있도록 해야 할까? 그렇지 않다. 죄송한 말씀이지만 업무담당자도 실수를 할 수도 있고, 또는 악의적인 의도를 가질 수도 있기 때문이다. 따라서 정당한 권한을 가진 업무담당자라 하더라도 인가된 환경에서 데이터베이스를 접근하는지, 적절한 작업을 수행하는 지의 여부가 항상 모니터링 되어 기대되지 않는 작업이나 실수를 미연에 차단할 수 있어야 한다. 예를 들어 업무 담당자가 업무 시간에 중요 테이블이나 인덱스를 실수로 Drop 한다면 이는 심각한 장애를 유발할 것이다.

<그림5> 인가된 사용자에 대한 통제

DB 파일 유출 사고 대책을 준비하고 계신가요?

앞서 설명 드린 바와 같이, 내부자에 의한 데이터 파일의 유출 시도는 고객정보와 같은 개인정보가 한번에 대량으로 유출될 가능성이 있기 때문에 DB파일 암호화와 같은 파일 유출 사고 대책은 필수적이다.

데이터베이스 파일이 이미 암호화 되어 있다면 그것을 처리 (Read, Write)할 수 있는 OS 계정이나 root 계정에 의해 파일이 유출된다 할지라도 이미 읽을 수 없게 조치된 것이므로 대량의 개인정보 유출과 같은 대형 사고를 방지할 수 있다.

그렇다면 이토록 강력한 데이터베이스 보안 수단인 데이터의 암호화 저장을 지금까지 많은 기업이 미루어왔던 이유는 무엇인가? 주로 다음과 같은 이유에 기인한다.

▶ 데이터 암호화로 인한 성능 저하 우려
  -> 서비스 수준 및 기업 경쟁력 저하
▶ 과다한 비용 -> 응용프로그램의 전면 수정으로 인한 시간 및 인력 투입 비용
▶ 암호화 적용에 따르는 데이터 Migration/Upgrade로 인한 Downtime 가능성

▶ 연계시스템 영향도, 관리 포인트 증가, 기존 솔루션에 대한 불신 등등

데이터 암호화를 고려하시는 많은 고객들에게서 필자가 전해 들은 바에 의하면 위의 이유들 중 가장 큰 고려사항은 역시 암호화 구현으로 인해 예상되는 성능저하와 투입비용이다.

데이터 암호화 구현으로 인한 성능저하와 비용으로 고민하고 계신가요?

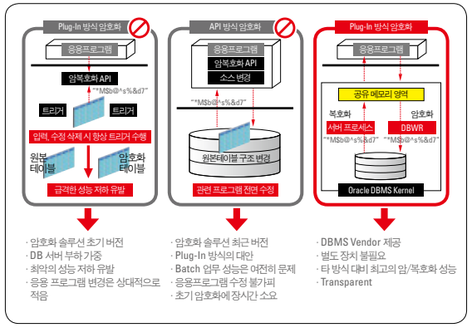
데이터 암호화로 인해 우려되는 성능저하의 정도와 투입비용 (응용프로그램의 수정으로 야기되는)은 암호화 및 복호화를 수행하는 방식에 기인합니다. 암호화 및 복호화를 수행하는 방식은 크게 세가지로 구분할 수 있다.

▶ Plug-In 방식 암호화
▶ API 방식 암호화
▶ Kernel 수행 방식 암호화

Plug-In방식 암호화는 암호화 솔루션을 제공하는 업체가 초기에 채택했던 방식으로서 데이터를 입력,수정,삭제 시에 데이터베이스 트리거를 구동시켜 암호화를 수행하고 , 조회 시에는 내장된 복호화 API를 사용하는 방식으로서 급격한 성능 저하를 유발한다. 응용 프로그램의 변경이 비교적 적다는 장점이 있으나 급격한 성능저하라는 치명적 단점으로 인해 대량 데이터를 보유하거나 Mission-Critical 한 업무에 적용이 불가능하다.

API 방식은 Plug-In 방식의 급격한 성능저하를 일부 개선하였으나 데이터를 입력,수정 삭제 시 암호화 모듈을 Call 하고 및 조회 시 복호화 모듈을 Call하는 로직으로, 관련된 응용프로그램을 전면적으로 수정해야 하는 부담이 있다. 뿐만 아니라 성능 측면에서 API 방식이 Plug-in 방식에 비해 개선된 부분은 OLTP Transaction 뿐이고 Batch 처리나 초기 암호화 성능면에서는 여전히 취약점을 가진다.

이에 비해 Kernel 수행 방식의 암호화란 데이터베이스 공급사가 각자의 데이터베이스 제품에 특화하여 제공하는 제품으로 Oracle을 비롯한 대부분의 DBMS 공급사가 각자의 암호화 솔루션을 제공한다. Oracle이 제공하는 암호화 솔루션인 Transparent Data Encryption도 Oracle Kernel 레벨에서 암복호화를 수행함으로써 암호화로 인한 트랜잭션의 성능 저하와 응용프로그램의 변경으로 인한 투입 비용을 최소화 한다. 따라서 암호화 솔루션을 선택해야 하는 경우 특정 제품의 특장점을 파악하기 보다는 암호화를 수행하는 방식이 어떤 것이냐에 초점을 맞추어야 한다.



<그림6> 암호화 방식별 메카니즘 및 특징

DBMS 관련 보안사고 발생 시 사후 분석이 가능한가요?

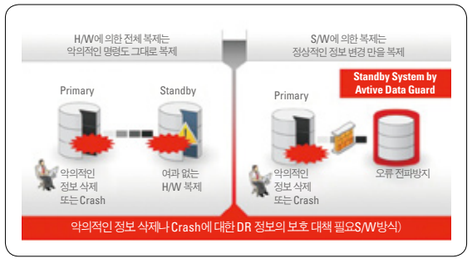
지금까지 언급한 접근통제와 데이터 암호화는 보안 사고에 대처하기 위한 선제적 대응방안이다. 하지만 두 가지 대응방안을 위한 적절한 장치를 갖추었다는 것이 데이터베이스 보안사고로부터 완전히 자유로움을 의미한다고 생각되지는 않는다.

Oracle을 포함한 모든 데이터베이스는 데이터베이스에 대한 접속, 자원의 사용여부 및 객체에 대한 권한 (Privilege), 역할 (Role)등의 기능과 함께 기본적으로 감사 (Audit) 기능을 제공한다. 감사 기능을 통하여 데이터베이스의 사용 현황 모니터링은 물론, DBMS 관련 보안사고 발생 시 사후 분석자료를 확보할 수 있다. (책임 소재의 규명)

또한 데이터베이스의 상시 감사를 통한 통합 모니터링 활동은 데이터베이스를 대상으로 하는 불법행위는 항시 감시되고 있다는 내부 인식을 확립하는 데 도움을 준다.

항상 가용한, 안전한 DR 환경을 구축하고 있습니까?

최근 국내 대형 금융기관에서, 수일에 걸쳐 정상적인 서비스가 불가능한 최악의 사고가 발생한 바 있다. 운영시스템은 물론 운영 시스템의 장애 시 서비스 연속성을 보장하기 위한 Stand-by DR (Disaster Recovery) 시스템까지 불능 상태가 되었다는 것이 언론 보도의 내용이다. 이로 인해 본 사건은 현재 국내 대다수의 기업들이 취하고 있는 DR 구축 방식인 Storage 복제 방식을 근본적으로 재고하게 하는 계기가 되었다. Storage 복제 방식은 운영시스템의 저장내용을 DR 시스템에 전체적으로 복제하는 방식이기 때문에 악의적인 명령 (Delete , Null-Copy) 도 그대로 전달된다. 즉 강력한 권한을 가진 누군가가 악의적으로 (혹은 실수로) 데이터베이스 파일을 삭제한다면 해당 삭제 명령이 DR 시스템에 그대로 반영되어 운영시스템, DR 시스템 양자가 모두 불능 상태에 빠지게 됨을 의미한다.

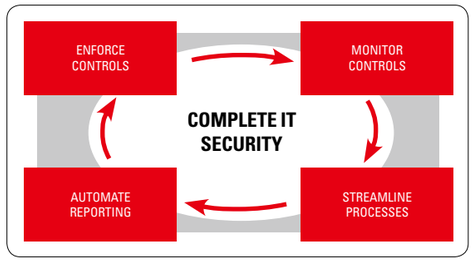


<그림7> DR 구축 방식의 비교 (H/W방식 vs. S/W방식)

Storage 복제 솔루션이 데이터베이스 파일의 복제를 통하여 Standby 시스템을 구성할 수 있게 할 뿐 아니라, 데이터베이스와 무관한 파일들까지도 복제할 수 있게 함으로써 업무적인 효용성이 매우 크다는 것을 부인할 수는 없다. 하지만 이번 사태가 주는 교훈은 Storage 복제 솔루션에만 전적으로 의존할 것이 아니라 S/W적인 복제를 통하여 정상적인 정보 변경만을 복제함으로써 악의적인 파일 삭제나 Crash에 대한 DR 시스템의 보호 대책이 필요하다는 것이다. Storage 복제 솔루션에 의한 DR시스템의 구성과 함께 Database의 변경내역을 저장하는 Redo 파일만의 복제와 적용을 통한 DR 시스템의 구성을 추가하여 3중으로 데이터베이스의 가용성을 확보할 필요가 있다는 것이다.

맺음말

지금까지 데이터베이스에 기반한 보안 위협요소와 그 대응방안에 대해 알아보았다. 곧 다가올 개인정보보호법의 시행과, 최근에 발생한 금융권 보안 사고로 인하여 정보시스템의 보안은 더 이상 미룰 수 있는 문제가 아니다. 물론 데이터베이스 보안은 전체 정보시스템의 포괄적 보안의 일부이다. 그럼에도 불구하고 데이터베이스 보안은 데이터베이스가 대다수 업무의 핵심 인프라이고 다량의 기업자산의 보관소라는 측면에서 정보시스템 보안의 중추라고 할 수 있다. 또한 정보시스템의 보안은 특정 보안 제품의 도입에 의해 해결되는 것이 아니라 정보시스템을 관리하고 운영하는 주체에 의한 프로세스라는 관점에서 이해되어야 한다.



<그림8> 보안은 제품이 아니라 프로세스이다

보안 장치 및 정책을 마련하고 이에 대한 지속적인 모니터링을 통하여 개선된 프로세스를 추가하고, 이에 대한 자동화된 보안 보고서를 통해서 다시 미흡한 부분에 대한 장치와 정책을 마련하는 일련의 활동인 것이다. 이러한 과정을 통하여 정보 시스템의 핵심부터 End-Point까지(DBMS->DBMS Server->Application Server->Web Server -> PC 및 Backup장비) 최선의 보안 환경을 구축해 나갈 수 있으리라 생각한다.

본 기고에서 설명해 드린 보안 장치에 대한 Oracle의 보안 Solution은 다음과 같다.

데이터베이스 보안 환경을 구축해야 하는 이 글의 독자

<그림9> Oracle Database Security Solution Stack

여러분들에게, 최상의 보안 환경을 구성함과 동시에 기존 비즈니스의 영향을 최소화 할 수 있는 최적의 솔루션을 선택함에 있어서, 이 글이 도움이 되었으면 한다.