

데이터베이스 보안 기술 동향

이호균* 이승민** 남택웅*** 오진태*** 장중수****

개인정보 유출 사고의 증가와 이에 대응한 개인정보보호법의 시행이 예상됨에 따라 데이터베이스 보안 시장의 급격한 성장이 전망되고 있다. 최근까지 틈새 시장으로 분류되어 써드파티 업체들만이 있던 데이터베이스 보안시장에 시만텍과 같은 대형 보안 업체들도 진입을 예고하고 있다. 지금까지 출시된 데이터 보안 제품들은 아직까지 시장의 요구 사항을 만족할 만한 기술 수준을 보이지 못하고 있고, 기술적인 난제 또한 여러 가지가 남아 있는 상태이지만, 이들 난제를 해결하는 제품 개발에 성공한다면 데이터베이스 보안 시장에서 큰 성공을 기대할 수 있을 것으로 보인다. 본 고에서는 최근 이슈가 되고 있는 데이터베이스 보안 시장의 분석을 위해서, 관련 법규들의 연관성, 관련 특허 및 시장을 선도하고 있는 대표 제품들의 장단점들을 정리하였다.

I. 서론

목	차
I. 서론	
II. 배경	
III. 특허 동향	
IV. 제품 동향	
V. 결론	

데이터베이스 보안이란 정보 보호 관리에 있어서 최종적이고 핵심적 관리 대상인 데이터베이스를 비인가 된 변경, 파괴, 정보 누출을 발생시키는 사건으로부터 보호하기 위한 방법을 말한다. 데이터베이스 보안 방법은 크게 데이터베이스의 입출력 경로를 감시하는 접근제어/감사 제품과 데이터베이스 내부의 데이터 자체를 암호화하는 암호화 제품으로 분류된다. 지금까지의 보안 방법은 주로 접근 경로에 대한 보안이 주류를 차지했지만, 모든 경로에 대한 100% 보안이란 현실적으로 불가능하다. 따라서 이에 대한 해결방안으로 나온 데이터베이스 암호화가 근래 각광 받고 있다. 특히 국내외의 개인정보 유출 사건의 증가와 이에 대한 개인정보보호법 시행 예고 등이 데이터베이스 보안 시장의 확대를 가속화 시키고 있다[1]. 기존의 데이터베이스 보안 시장은 중소기업

* 전자통신연구원 정보보호연구단 /연구원
 ** 전자통신연구원 정보보호연구단 /선임연구원
 *** 전자통신연구원 정보보호연구단 /팀장
 **** 전자통신연구원 정보보호연구단 /그룹장

의 써드파티 업체들이 주류를 이루고 있었으나, 2006년을 기점으로 시만텍과 같은 대기업들이 진입을 예고하고 있다. 우리나라는 DBMS 시장의 90% 이상을 외산 제품이 차지하고 있기 때문에 DB 임베디드 방식의 보안 제품은 개발해도 시장 영향력이 매우 미미할 것이다. 따라서 기존 제품이 풀지 못하는 문제를 해결하는 써드파티 형태의 DB 보안 기술 확보를 통해 외산 제품에 대한 시장 방어력을 강화시켜야 할 것이다. 본고는 2장에서 현재 급격히 성장하고 있는 데이터베이스 보안 시장의 성장 배경과 관계 법령의 연관성 분석 결과를 정리한다. 3장에서는 기존 업체들이 출원한 특허에 대해서 정리하고, 4장에서는 현재 시장에서 수위를 차지하고 있는 제품들의 장, 단점에 대해서 분석한다. 마지막으로 5장에서 결론을 맺는다.

11. 배 경

본 절에서는 데이터베이스 보안 시장이 성장하게 된 사회적, 법률적인 배경에 대해서 알아본다. 사회의 급속한 정보화에 따라 개인 정보의 가치가 빠르게 상승하고 있고, 개인 정보가 대량으로 수집 활용됨에 따라, 수집된 개인 정보의 불법적인 접근 및 유출 등에 대한 우려가 증가하고 있다. 하지만 현재의 개인정보 이용 환경은 데이터 접근 시에 사용자의 질의 내용과 그에 대한 결과가 관리자에게 그대로 노출되어 사용자의 프라이버시가 침해되는 치명적인 문제로 지적되고 있다. 실제로 최근 인터넷상에서 노무현 대통령의 주민등록번호가 총 416 회 사용되었고 280 회의 성인인증을 받았으며, 한명숙 총리와 함께 여러 게임 사이트에도 가입되는 등 무분별하게 개인정보가 도용되어 심각한 사회적 문제로 대두되었다[2]. 또한 엔씨소프트는 2004년 5월 11일 ‘리니지2’를 업데이트하면서 사용자의 게임정보를 담은 로그 파일을 암호화하지 않아 8,500 명의 게임 이용자의 개인정보가 노출되어 소송이 진행 중이며, 2005년 리니지 게임 대규모 명의 도용사건과 관련해 28만 명의 명의가 도용되어 사고 책임자가 입건되었다[3]. 이와 같이 급증하는 개인정보 유출사고에 대비하기 위해서 세계 각국에서는 관계 법령 정비에 박차를 가하고 있다. 이들 법령이 실효성을 갖게 되면 개인정보를 취급하는 모든 관련 기업들은 개인정보의 보안 관리를 위한 시스템을 필수적으로 갖추어야 한다. 다음은 세계 각국에서 발령 중인 개인정보 보호 관련 법안의 직접 관련 조항들을 정리하고 있다.

1) 일본의 개인 정보 보호 법령 [4]

- 일본의 개인정보보호 법령은 개인 정보를 취급하는 정부 및 사업자의 의무 사항에 대해

서 기술

- 법령 중 제 1 장 2 조에서는 개인정보 데이터베이스에 대한 정의를 규정
- 법령 중 제 4 장 20~22 조는 개인 정보를 취급하는 사업자의 의무 사항을 명시
 - 특히, 20 조에서는 개인 정보에 대한 보안과 기밀성을 보장하기 위한 규정
 - 데이터 암호화, 접근제어, 감사 등이 대표적인 대응 방법

제 1 장 총칙

[제 2 조] ‘개인정보 데이터베이스’란 개인정보를 포함하는 정보의 집합물로, 특 정의 개인정보를 전자계산기를 이용하여 검색할 수 있도록 체계적으로 구성한 것. 전호 에서 든 것 이외에 특정의 개인정보를 용이하게 검색할 수 있도록 체계적으로 구성한 것으로 정령에서 정한 것을 말한다

제 4 장 개인정보 취급 사업자의 의무 등

제 1 절 개인정보 취급 사업자의 의무

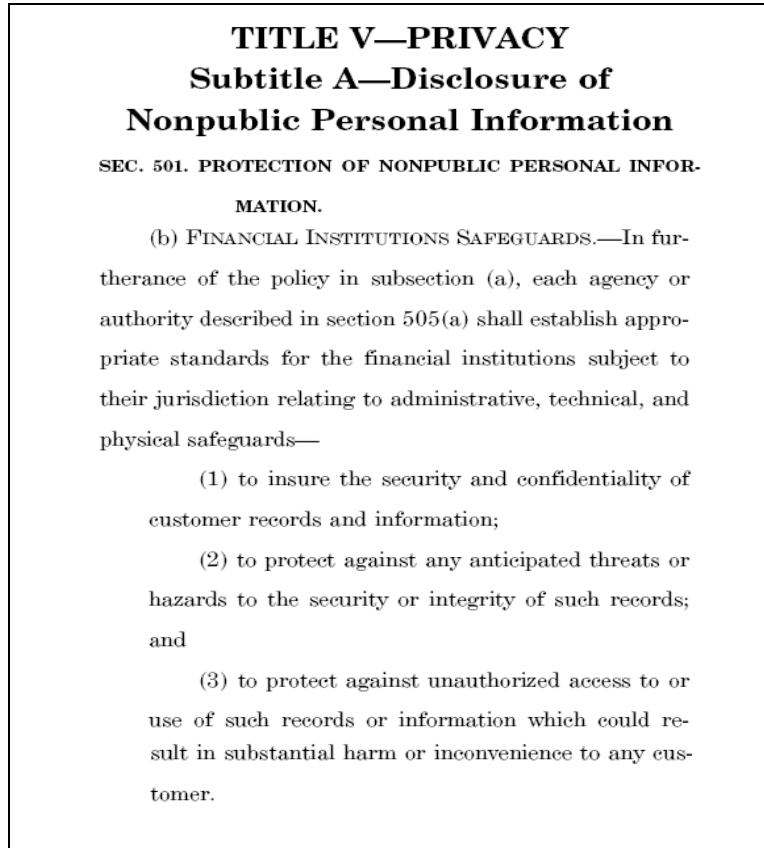
(안전 관리 조치)

[제 20 조] 개인정보 취급 사업자는, 그 취급하는 개인 데이터의 누설, 멸실 또 손 해의 방지 외의 개인 데이터의 안전 관리를 위해서 필요하고 적절한 조치를 강구하지 않으면 안 된다.

2) GLB (Gramm-Leach-Bliley) [5]

- GLB는 금융 기관이 보유하고 있는 개인 정보와 고객 기록 보호를 의무화하고 있음
- Title V는 Privacy에 대해 기술하고 있으며, 특히 Sec. 501(b)에서는 금융 서비스 업 체들이 "관리, 기술 및 물리적인 안전 장치"를 구축하도록 요구하고 있음
 - 501(b)-(1)은 고객 기록과 정보에 대한 보안과 기밀성을 보장하기 위한 규정
 - DB, 데이터 암호화가 대표적인 대응 방법
 - 501(b)-(2)는 이러한 정보를 대한 외부의 위협으로 보호하기 위한 규정
 - DB 침입탐지가 대표적인 대응 방법

- 501(b)-(3)은 고객정보에 대한 비인가된 사용자로부터 접근제어를 통한 보호 규정
-DB 접근제어가 대표적인 대응 방법



(그림 1) GLB (Gramm-Leach-Bliley) 관련 조항

- 3) HIPAA (Health Insurance Portability and Accountability Act) [6]
 - 건강 보험 이전 가능성 및 책임에 관한 법
 - 직장을 바꾸거나 직업을 잃은 사람이 건강 보험을 가질 수 있게 하는 것이 주요 목적인 법안이나 포함된 강령에 개인 의료정보 보안에 대한 내용을 포함
 - 법령 중 SEC. 264 조항은 개인의료정보의 비밀 유지에 대한 의무 사항을 명시
 - 개인정보로 분류될 수 있는 의료 정보에 대한 컴퓨터 저장이나 네트워크 전송은 정보 누출을 막기 위해서 인증 받은 절차에 의해서 수행되어야 함

SEC. 264. RECOMMENDATIONS WITH RESPECT TO PRIVACY OF CERTAIN HEALTH INFORMATION.

(a) IN GENERAL.--Not later than the date that is 12 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall submit to the Committee on Labor and Human Resources and the Committee on Finance of the Senate and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives detailed recommendations on standards with respect to the privacy of individually identifiable health information.

(b) SUBJECTS FOR RECOMMENDATIONS.--The recommendations under subsection (a) shall address at least the following:

- (1) The rights that an individual who is a subject of individually identifiable health information should have.
- (2) The procedures that should be established for the exercise of such rights.
- (3) The uses and disclosures of such information that should be authorized or required.

(c) REGULATIONS.--

(1) IN GENERAL.--If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by section 262) is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act. Such regulations shall address at least the subjects described in subsection (b).

(그림 2) HIPAA (Health Insurance Portability and Accountability Act) 관련 조항

4) SOX(Sarbanes-Oxley) [7]

- SOX는 미국 정부가 기업 지배 구조 개선과 재무 정보 공개, 회계 보고/감사 강화를 목적으로 도입
- 특히, Section 404 조항은 감사인이 반드시 내부적인 제어나 프로세스에 대해 인증하도록 규정
 - 법률 전문가들은 금융 데이터를 관리하는 DB 시스템이 안전하지 못할 경우 경영진은 데이터의 유효성과 내부 제어의 건전성을 입증하는 문제로 인해 어려움을 겪게 될 것임을 지적

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.

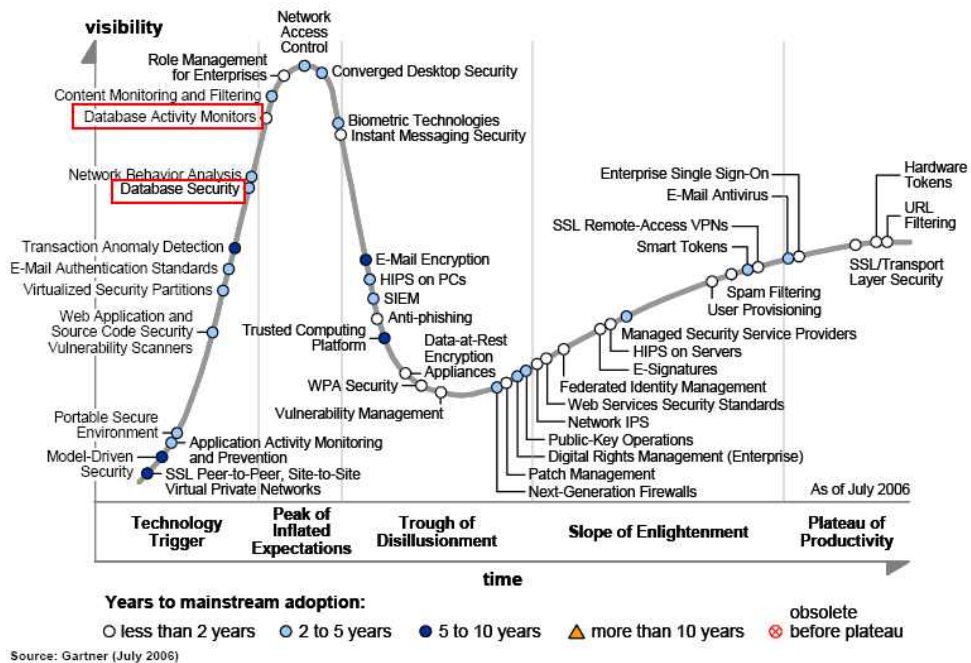
(a) **RULES REQUIRED.**—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) **INTERNAL CONTROL EVALUATION AND REPORTING.**—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

(그림 3) SOX (Sarbanes-Oxley) 관련 조항



(그림 4) 정보 보안 기술의 Hype Cycle (가트너 2006)

이와 같은 사회적, 법률적 배경을 바탕으로 데이터베이스 보안 시장은 빠르게 성장하고 있다. 그림 4는 2006년 가트너에서 발표한 정보 보안 기술의 Hype Cycle이다[8]. 그림에서 보듯이 데이터 베이스 보안 제품은 2~5년 이내에 시장 고점에 다다를 것이며 기술적인 면에서는 성장기에 접어들었다. 데이터베이스 활동 감시 제품은 2년 이내에 시장 고점이 예상되며 기술적으로는 성장기에 있음을 알 수 있다.

III. 특허 동향

데이터베이스 보안관련 제품들은 크게 암호화 제품과 접근제어/감사 제품으로 구분될 수 있다. 본 절에서는 특허 동향을 제품 군에 따라서 구분해서 정리한다.

1) 데이터베이스 암호화 관련 특허

데이터베이스 암호화 제품은 크게 DBMS 자체에 포함된 암호화 기능과 써드 파티에서 제공하는 암호화 기능으로 구분된다. 써드 파티 제품은 다시 제품 구현 형태에 따라서 DBMS 시스템에 소프트웨어 에이전트 형식으로 장착되는 방식과 별도의 하드웨어 어플라이언스 형태의 제품으로 구분된다. 소프트웨어 방식으로 유명한 국외 업체로는 Protegrity 와 nCipher 가 있다. 특히 Protegrity 는 데이터베이스 보안과 관련된 논문과 특허를 매우 활발하게 발표하고 있다. 표 1 의 1,2,4,5 번이 소프트웨어 방식과 관련된 특허이다. 특허 특허 1 은 소프트웨어 방식의 암호화 제품이 키 관리를 위해서 하드웨어 방식의 HSM(Hardware Security Module) 장비와 혼용되는 형태를 고안하고 있는데 Protegrity 는 이 형태를 이용한 영업으로 국내외에서 수위의 시장 매출을 보이고 있다. 하드웨어 어플라이언스 형태의 제품으로 국외 제품 평가에서 1 위를 차지하고 있는 Ingrian 또한 여러 개의 관련 특허를 보유하고 있다 (표 1 의 3 번 특허).

표 1) 데이터 암호화 제품 관련 특허

번호	국가	출원일자	출원인	출원명
1	US	2000-11-16	Protegrity Corporation	Combined hardware and software based encryption of databases

2	US	2003-11-27	nCipher Corporation Ltd.	Biometric key generation for secure storage
3	WO	2005-05-18	Ingrian Networks, Inc.	Encrypted Table Indexes and Searching Encrypted Tables
4	WO	2000-11-27	Protegrity Corporation	Method for Reencryption of a Database
5	EP	2004-12-02	Protegrity Corporation	Database system with second preprocessor and method for accessing a database

2) 데이터베이스 접근제어/감사 관련 특허

데이터베이스 접근제어/감사 제품 관련 특허는 표 2 와 같다. 표 2 는 국내의 데이터베이스 접근제어/감사 제품을 출시한 회사들의 대표 특허를 정리하고 있다. 시장 조사 전문 기관인 Forrester 에서는 DB 접근제어/감사 전문 업체로 Application Security, IPLocks, Quest Software 등을 선정하였다[9]. 이들 회사의 제품 및 특허는 데이터베이스의 접속 선로를 통과 하는 트래픽을 감시하고 사용자 질의 및 명령어들을 분석함으로써 보안 사고를 예방, 탐지하는 방법과 관련이 있다.

접근제어/감사 형태의 제품 및 특허 최신 동향은 실시간 감시 및 침입 차단 기능의 도입을 들 수 있다. 감사 기능은 처리해야 할 데이터가 방대하고 분석 모듈의 고 지능화가 필요하기 때문에 실시간 감사를 제공하는 업체가 많지 않았지만, 외국 제품을 시작으로 실시간 감사 기능이 지원되는 추세이다. 그리고 기존 네트워크 침입 탐지 시스템과 유사한 개념으로 데이터베이스 시스템 자체에 대한 크래킹 시도를 차단할 수 있는 DB 침입 탐지 기능을 통합적으로 제공하기 시작하였다.

표 2) 데이터베이스 접근제어/감사 제품 관련 특허

번호	국가	출원일자	출원인	출원명
1	US	2003-2-24	IPLocks, Inc.	Method and Apparatus for Monitoring a database system
2	US	2001-2-12	Quest Software, Inc.	System and Method for reconciling transactions between a replication system and a recovered database
3	KO	2004-4-03	피앤피시큐어	데이터베이스 감시 및 보안 방법 및

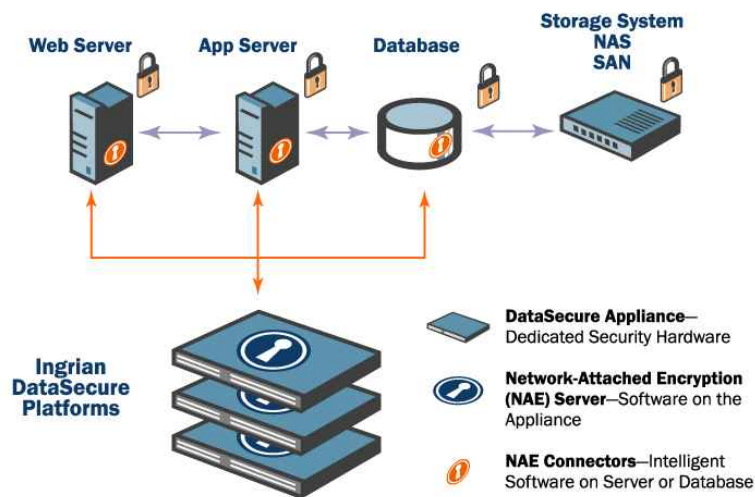
				장치
4	KO	2004-1-09	바넷정보기술	3-Tier 구조 기반의 데이터베이스 접근 통제 시스템 및 방법

IV. 제품 동향

이 절에서는 현재 데이터베이스 보안 시장을 선도하고 있는 제품들의 장단점에 대해서 정리한다. 기존 제품들이 해결하지 못하는 문제점을 정리해 봄으로써 향후 데이터베이스 보안 제품의 진화 방향에 대해서 유추해 볼 수 있을 것이다.

1) 데이터베이스 암호화 제품

1-1) Ingrian[10]



(그림 5) 인그리안 데이터베이스 암호화 제품의 구성도

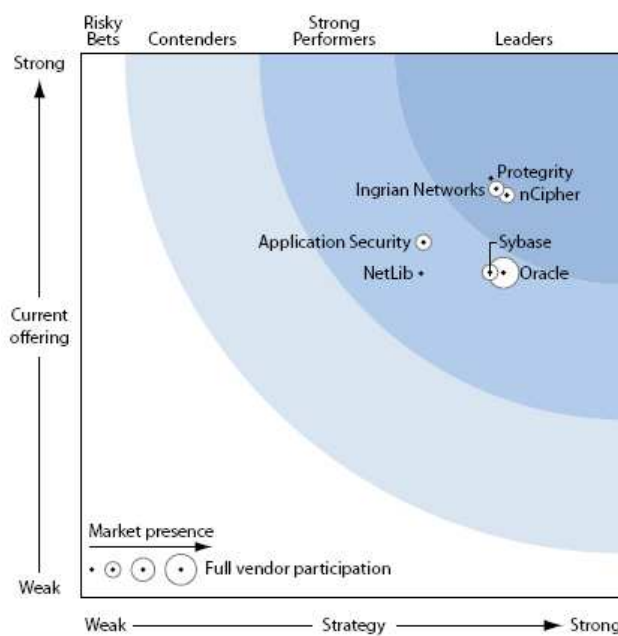
인그리안은 Forrester 시장 보고서에서 하드웨어 어플라이언스 형태의 제품 중 평가 1 위 업체로서 데이터베이스 암호화 제품들의 공통된 단점인 속도 문제를 어플라이언스 형태의 제품 개발로 해결하고자 하고 있다. 즉 기존 제품을 사이트에 적용했을 때 전체적인 DB 운용 속도가

저하되는 원인이 암호화에 걸리는 부하에 있다고 보고, 암호화 전용 고속 하드웨어를 개발함으로써 해법을 제시하였다. 그러나 실제 제품을 비교해 보면 비약적인 성능 향상을 보이지 못하는 것으로 보고되고 있다. DB 운용 속도의 저하는 암호화에 걸리는 부하뿐만 아니라 다른 요소들도 있는데, 이들 요소의 개선은 이루어지지 않았기 때문이다. 그러나 국외 시장에서 이 제품은 타 제품에 비해서 비싼 가격에도 불구하고 시장 평가에서 수위를 차지하고 있다. 이는 어플라이언스 형태가 주는 신뢰감뿐만 아니라, DB 운영자들이 DB 시스템 자체에 소프트웨어 에이전트 형태의 써드파티 모듈을 추가하는데 거부감을 갖고 있다는 데서 원인을 찾을 수 있다. 소프트웨어 에이전트 형태의 제품은 DB 시스템 자체에 소프트웨어 모듈을 추가해야 하지만, 어플라이언스 형태의 제품은 별도의 시스템에서 운용되기 때문에 DB 운용에 영향이 최소화된다. 그림 5는 인그리안의 제품 구성도를 보이고 있다.

1-2) Protegrity [11]

Protegrity는 소프트웨어 에이전트 방식의 데이터베이스 암호화 업체 중에서 국외 시장 평가 1위인 업체이다. 소프트웨어 에이전트 방식은 국내 대부분의 DB 암호화 업체들이 채택한 방식으로 초기 진입은 쉽지만 어플라이언스 형태에 비해서 사용자에게 주는 신뢰감이 떨어질 수 있는 단점이 있다. Protegrity는 이를 보완하기 위해서 키 관리 기능은 별도의 하드웨어 제품(Hardware Security Module)으로 보완하고 있다. 앞서 언급한 것처럼 DB 암호화 제품의 평가 요소 중에서 암호화 성능뿐만 아니라 그 이외의 요소들이 차지하는 비중도 상당히 큰데, 그 중 하나가 키 관리 기능이다. 특히 키 관리 기능은 DB 암호화에 적용할 때, 컬럼 별 적용, 사용자 별 적용과 같이, 고려해야 할 요소가 많기 때문에 복잡도가 높아질 수 밖에 없고, Protegrity는 이를 별도의 하드웨어 제품으로 해결하고 있다. DB 암호화 제품 적용 시 언급되는 난제 중 또 하나는 암호화된 컬럼에 대한 검색 속도 개선 문제이다. 암호화된 상태에서는 사용자의 질의와 데이터를 비교할 수 없기 때문에 복호화 과정을 거쳐야 하고 이 때문에 검색 성능이 비약적으로 저하되게 된다. 이를 해결하기 위해서 암호문 자체에 대한 비교가 가능하게 하는 수학적 접근 방법과 인덱스를 추가하는 응용 프로그램 계층에서의 해결 방법이 있다. Protegrity는 검색 속도 개선 문제와 같은 제품의 시장 적용 시 발생하는 난제에 대해서 많은 특허와 논문을 발표하고 있다. 이를 바탕으로 Protegrity는 같은 소프트웨어 에이전트 방식의 제품 중에서 가장 우수한 성능을 보이고 있다.

그림 6은 Forrester 에서 발표한 데이터 암호화 제품 평가이다[12]. 그림에서 보듯이 중소 벤더인 Protegrity, Ingrian, nCipher 가 선두 업체 영역을 차지하고 있는 반면, DBMS 전문업체인 오라클은 아직 그 수준에는 미치지 못하고 있음을 알 수 있다. 즉 데이터베이스 보안 시장은 아직까지 대기업이 관심을 갖지 않았던 틈새 시장의 영역이었으나, 2006 년을 기점으로 시장에 급속히 확대될 것으로 예상되고 있다.



(그림 6) 데이터베이스 암호화 업체 비교

데이터베이스 암호화는 포괄적인 데이터 보안 전략의 한 구성요소로서 효과적인 도구이다. 하지만 DB 암호화가 유일한 보안 수단은 아니다. DB 암호화를 위해서는 심각한 성능의 저하나 시스템 재구성 부하가 요구될 수도 있다. 또한 DB 암호화 이외에 보안이 뛰어난 시스템과 네트워크 보안 체계, DB 접근 제어 만으로도 효과적인 보안 체계를 구축할 수 있다. DB 암호화 기능은 궁극적인 DB 보안 솔루션이 아니라, 다음과 같은 경우에 효과적으로 이용될 수 있는 보안 구성 요소이다[17].

- 기밀 데이터에 대한 불법 접근 방지, DB 파일 도난 예방

- 신용카드번호, 주민번호 등의 보안
- 내부 관리자의 기밀 데이터 접근 제한
- 정부 규제 법안의 요구 사항 만족

DB 암호화는 다음과 같은 단점이 있다. 첫째, 인덱스나 키 필드를 암호화 하는 경우 성능에 큰 악영향을 미치게 된다. 둘째, 응용 계층에서 수정 비용이 추가될 수 있다. 셋째, 접근 권한 체계를 변경해야 한다(관리자와 보안 관리자가 분리되어야 한다). 넷째, 범위나 부분 검색을 요청하는 경우, 모든 암호 데이터가 복호화 되어야 하기 때문에 심각한 성능 저하가 생기게 된다. 결국, 기존 DB 시스템에 컬럼 기반 암호화를 적용하는 것은 생각하는 것보다 더 많은 부하가 걸릴 수 있다.

따라서 더욱 개선된 새로운 컬럼 기반 암호화 제품이 나오기 전까지는 데이터베이스 접근제어/감사 제품과 미디어 암호화 제품을 함께 사용하는 것이 효과적인 데이터 보안 체계가 될 수 있다 (미디어 암호화 제품은 컬럼 기반 암호화 제품과는 달리 DB의 데이터 저장 장치 내부에서 데이터 모두를 암호화 시키는 장비임).

다음절에서는 효과적인 DB 보안을 위하여 DB 암호화와 함께 사용할 수 있는 데이터베이스 접근제어/감사 제품에 대해서 알아보도록 한다[14].

2) 데이터베이스 접근제어 및 감사 제품

2-1) Application Security [15]

어플리케이션 시큐리티에서 출시한 AppRadar 는 실시간 모니터링 및 감사 기능과 기업용 데이터베이스 보안을 결합한 실시간 데이터베이스 활동 감시 솔루션이다. 일반적인 네트워크 또는 운영 체제 로그 시스템과 달리, AppRadar 는 데이터베이스에 특화된 감사와 위협 감시를 수행하기 때문에 실시간으로 보안 이벤트들을 경고 할 뿐만 아니라 또한 사용자 활동에 의해 정의된 감사 사건을 표시한다. 데이터베이스의 보안 위협들에 대해 축적된, 방대한 지식을 바탕으로 정의된 정책을 기반으로 실시간 감시가 운영된다. AppRadar 는 계층화된 방어가 가능하며 개인 정보 보호 및 관련 정책에 부합하는 정보 시스템 운영이 가능하도록 도와준다. 하지만 가격이 매우 고가이고, 보고 기능이 미흡하기 때문에 보고서 생성 시간이 느리다는 단점이 있다.

2-1) IPLocks [16]

IPLocks 는 취약성 평가, 감시 기능, 감사 및 분석 기능을 수행하는 데이터베이스 보안 제품을 출시하고 있다. 취약성 평가 기능은 접근권한, 메타데이터, 서버, OS 환경 설정 측면에서 외부 침입 가능성 또는 취약성을 탐지하여 보여줌으로써 즉각적으로 보안 문제를 확인할 수 있게 한다. 또한 사용자, 테이블 기본 정보, Public 접근권한, 관리자 옵션, 감사 테이블, 시스템 접근권한, 원격 로그인, 암호 관리, 적용 패치 버전 등의 정보를 평가한다. 실시간 감시 기능은 불법 접근과 권한 변경, 비인가 사용자의 데이터베이스 스키마 변경, 그리고 비정상적이거나 의심스러운 접근 패턴에 대한 감시 및 경고 발생을 수행한다. 그리고 사용자, 세션, 객체 각각에 대한 접근 패턴에 대한 학습을 수행하고, 학습에 따른 임계치 값을 넘어서는 의심스러운 접근패턴을 통보한다. 감사 및 분석 기능은 모든 변경사항과 실패한 시도에 대해서 감사를 수행한다. 그림 7은 국외 데이터베이스 보안 제품이 제공하고 있는 기능들을 비교, 정리한 것이다.

Vendor	Authentication	Authorization	Security patch deployment	Vulnerability assessment	Data-at-rest encryption	Data-in-motion encryption	Database auditing	Intrusion detection
Application Security				✓	✓		✓	✓
BMC Software	✓	✓					✓	✓
Computer Associates	✓	✓					✓	
Guardium							✓	✓
IBM	✓	✓	✓		✓	✓	✓	
IPLocks				✓			✓	✓
Lumigent Technologies							✓	✓
Microsoft	✓	✓	✓			✓	✓	
nCipher					✓			
NetLib					✓			
Next Generation Security Software				✓				
Oracle	✓	✓	✓		✓	✓	✓	
Quest Software	✓	✓						
Protegrity					✓			
Sybase	✓	✓	✓			✓	✓	
Symantec	✓	✓		✓				✓
Vormetric					✓			

Source: Forrester Research, Inc.

(그림 7) 국외 데이터베이스 보안 제품 기능 비교

VI. 결 론

지금까지 최근 각광 받고 있는 데이터베이스 보안 제품과 특허에 대해서 알아보았다. 데이터베이스 보안 분야는 개인정보보호법의 발효로 인해서 급속한 시장 확대가 예상되는 분야이다. 또한 기존 제품들이 아직 시장의 요구를 만족시키지 못하고 있기 때문에 많은 시장 가능성이 남아 있는 분야이기도 하다. 암호화 기능 적용 시 기존 데이터베이스 운용 속도 저하 문제와 같은 제품 개발 관련 기술뿐만 아니라 검색이 가능한 암호 기술과 같은 학술적인 난제 또한 많이 남아 있기 때문에 향후 국내외 학계와 산업계에서 많은 연구와 제품 개발이 요구되는 바이다.

<참 고 문 헌>

- [1] Rich Mogull, Ray Wagner, "Data Security Enters the Spotlight", Gartner, 24 Oct 2005
- [2] 매일경제신문, "盧대통령 주민번호 인터넷 떠돈다", 2006년 6월 27일
- [3] 전자신문, "리니지 명의로용으로 부당이득 취한 9명 입건", 2006년 6월 31일
- [4] "개인정보보호 관계 법률", <http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/index.html>
- [5] HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 ,
<http://www.cms.hhs.gov/HIPAAgenInfo/Downloads/HIPAAlawdetail.pdf>
- [6] Information Regarding the Gramm-Leach-Bliley Act of 1999,
<http://banking.senate.gov/conf/titlev.pdf>
- [7] Sarbanes-Oxley Act of 2002, <http://www.energysolve.com/sarbanesoxley072302.pdf>
- [8] Rich Mogull, Ray Wagner, John Girard and Vic Wheatman, "Hype Cycle for Data Security, 2005", Gartner, 12 Jul 2005
- [9] Noel Yuhanna, "Comprehensive Database Security Requires Native DBMS Features And Third-Party Tools", Forrester, March 29, 2005
- [10] Ingrian, <http://www.ingrian.com>, 2006
- [11] Protegrity, <http://www.protegrity.com>, 2006
- [12] Noel Yuhanna, "The Forrester Wave : Database Encryption Solutions, Q3 2005", Forrester, August 8, 2005
- [13] Rich Mogull, "When and How to Use Database Encryption", Gartner, 6 Feb 2004
- [14] Rich Mogull, "Database Activity Monitoring Is a Viable Stopgap to Database Encryption for the Payment Card Industry Data Security Standard (and Beyond)", Gartner, 3 Jul 2006
- [15] Application Security, <http://www.appsecinc.com/>, 2006
- [16] IPLocks, <http://www.iplocks.com/>, 2006