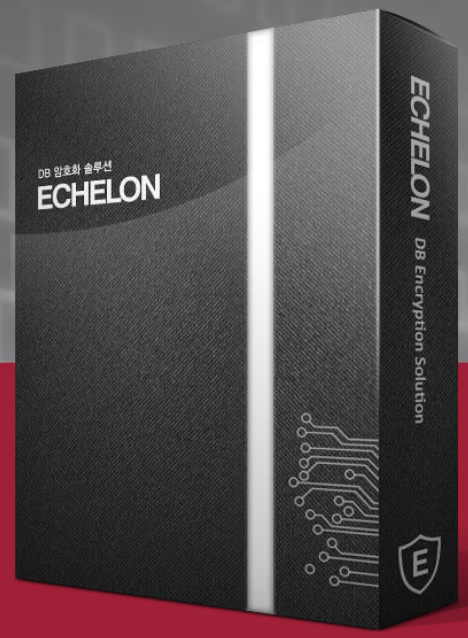
DB암호화 솔루션

애슬론(Echelon)



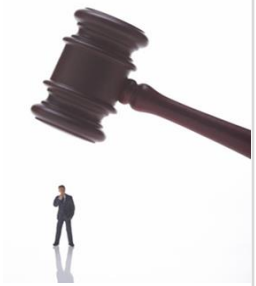
MOXNO SOLUTION

Contents

I. 보안솔루션 도입 필요성

개인정보보호법 시행

개인정보보호법 시행(2011.09.30.)



개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보보호법 제정

개인정보 보호조치

- 관리적 보호조치 ····· 보안 관리자 선임
- 기술적 보호조치 ····· 암호화/ 접근통제 등의 조치
- 물리적 보호조치 ····· 물리적 잠금 장치 설치

※ 공공·민간부문의 모든 개인정보처리자에게 확대 실시

개인정보보호법 위반 벌칙

안전성확보에 필요한 조치를 하지 아니하여 개인정보를 분실,도난,유출,변조 또는 훼손 당한 자
(2년 이하의 징역 또는 1천 만원 이하의 벌금)

※ 해당업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우 면책

해킹 패턴의 변화

개인정보 해킹후 거래

Target: 대기업을 대상으로 해킹
(개인정보가 많은 기업)

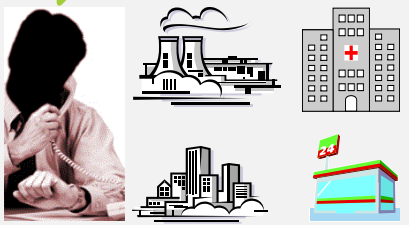
법시행 전

Auction
1,081만명
개인정보유출

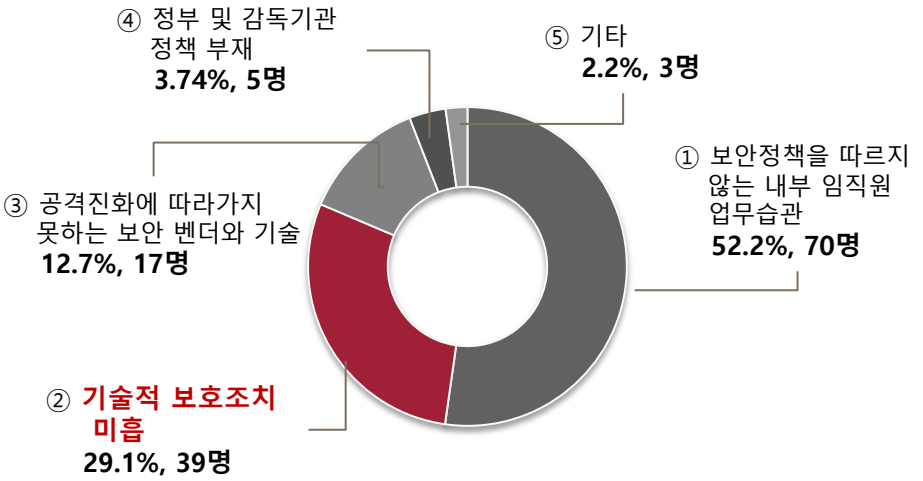
개인정보 해킹후 협박

Target: 보안이 허술한 중/소 기업 대상으로 해킹
(개인정보 수는 의미 없음)

법시행 후



최근 대형 보안사고의 주요 원인



[2012 기업정보보안 가이드 v.7]

I. 보안솔루션 도입 필요성

주민등록번호 암호화 적용시기

1. 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2017년 1월 1일
2. 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2018년 1월 1일

※ 위를 위반 할시 3천만원 이하의 과태료를 부과한다.

개인정보 암호화 조치 안내 (2017.01 개정)

[표] 암호화 방식 선택 시 고려 사항

분류	고려사항
일반적 고려사항	구현 용이성, 구축 비용, 기술지원 및 유지보수 여부
	암호화 성능 및 안전성
	공공기관의 경우, 국가정보원 인증 또는 검증 여부
기술적 고려사항	암복호화 위치(어플리케이션서버, DB 서버, 파일서버 등)
	색인검색 기능 유무, 배치처리 기능 여부

행정자치부 KISA 한국인터넷진흥원

개인정보 보호책임자의 지정

제 31조(개인정보 보호책임자의 지정) ① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다.

② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

…

3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리 감독

…

※ 위를 위반 할시 1천만원 이하의 과태료를 부과한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

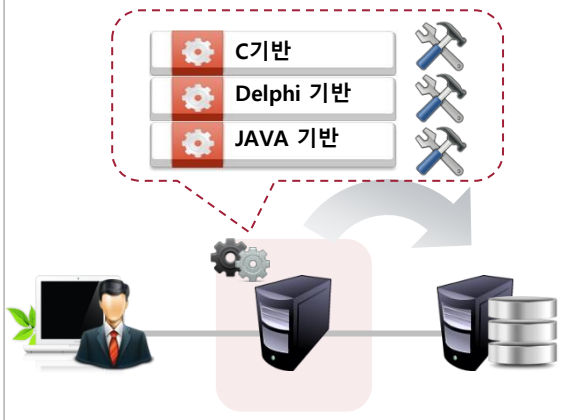
정보통신서비스 제공자등은 개인정보가 안전하게 저장 전송될 수 있도록 보안 조치를 하여야 한다.

1. 비밀번호의 일방향 암호화 저장
2. 주민등록번호 계좌번호 및 바이오정보 등 방송통신위원회가 정하여 고시하는 정보의 암호화 저장
3. 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송수신하는 경우 보안서버 구축 등의 조치
4. 그 밖에 암호화 기술을 이용한 보안 조치

DB암호화 솔루션 방식 별 비교

API방식

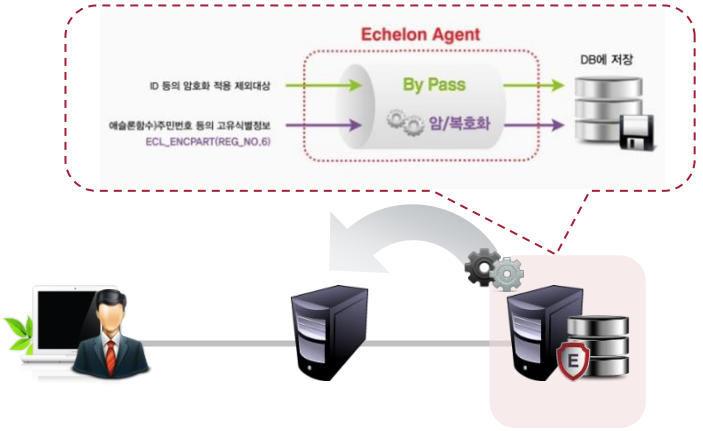
어플리케이션에서 암/복호화



- DB서버의 성능저하 없이 구축가능
- **OS및 개발언어별 라이브러리 제공에 따른 도입 및 구축의 복잡성**
- Toad, Orange 등 사용 툴 사용 불가
- 향후 응용시스템 신규/변경 등에 따른 관리 효율성 저하
- 접근제어 솔루션 추가 도입에 따른 비용 발생

Secure Proxy방식(Echelon)

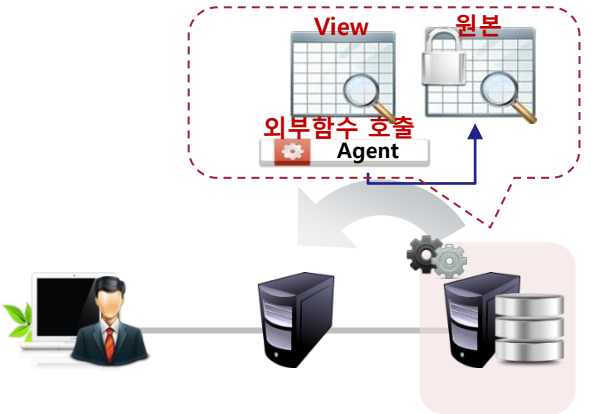
DB내부에서 **독립적** 암/복호화



- **Java 기반 독립프로세스** 암/복호화 처리로 DB서버의 성능저하 최소화
- **기존 DB의 Plan 변경 및 Object(View 등) 추가가 없음** – 성능 극대화 및 DB 무결성 보장
- 독립프로세스 운영으로 부하분산처리 매우 용이 – **다중화 부하분산 가능(어플라이언스)**
- **Multi-Thred 방식으로 암/복호화 다중 및 병렬 처리 가능** – 대용량 작업 시 최상의 성능 제공
- Java 기반으로 DB서버 OS 및 H/W에 뛰어난 **호환성 제공**

Plug-in방식

DB내부에서 암/복호화



- DB에서 제공하는 외부함수 사용
- DB오브젝트 추가(View 생성)로 DB Plan 변경 발생
- **DB 프로세스 종속에 따른 성능 저하**
- 소스 수정 없으나, 쿼리 최적화 시 소스 수정 필요
- **DBA와 개인정보처리책임자의 구분이 모호**

Ⅱ. DB암호화 솔루션 방식 별 비교

구 분	API 방식	Secure Proxy 방식 (애슬론)	Plug-In 방식
보 안	▪ DB에서 Application에게 암호화하여 전달 ▪ WAS에서 DB계정과 비밀번호가 탈취되어도 안전	▪ DB에서 Application에 평문으로 전달 ▪ WAS에서 DB계정과 비밀번호가 탈취되어도 안전	▪ DB에서 Application에 평문으로 전달 ▪ WAS에서 DB계정이 탈취되는 경우 **평문 데이터 유출**
성 능	▪ 암복호화 연산 처리에 최적화 모듈을 사용하며 Application을 통한 분산 효과	▪ DB내부에 독립프로세스 운영으로 DBMS 자원의 최소사용 ▪ 이중화 구성을 통한 부하분산 처리용이	▪ 모든 암복호화 연산과 외부 암복호화 모듈 사용 시 **DBMS 자원 사용** ▪ 다량의 트랜잭션 처리와 배치 작업 처리 불가
가용성	▪ 암복호화 장애시 다른 Application 및 DB에 영향 없음	▪ Agent 이중화 구성을 통해 장애시 고가용성 보장	▪ 암복호화 장애 시 암호화 사용 **모든 업무 마비 가능**
변경성	▪ Application의 암복호화 호출을 기존 로직에 반영 필요	▪ Application의 수정 최소화 ▪ DB테이블 구조 및 스키마 변경 필요 없음	▪ Application의 수정 최소화 ▪ **DB테이블 구조 및 스키마 변경 필요**
사용성	▪ **SQL툴을 사용하여 암복호화 사용불가**	▪ SQL 툴 사용 가능	▪ SQL툴 사용 가능
적용기준	▪ 해킹 위험과 취약서의 위협에 보안강화가 필요한 업무 ▪ 높은 성능이 요구되고 트랜잭션이 많은 업무	▪ 업무의 편리성과 높은 성능이 요구되는 경우	▪ 소스 일부의 변경이 불가하고 업무의 편리성이 필요한 경우
관리성	▪ OS업그레이드 및 소프트웨어 패치시 암호화모듈의 재적용에 따른 **인력투입및 비용 발생**	▪ 암호화 컬럼 추가시 관리자 툴을 사용하여 간단한 적용	▪ 신규테이블 생성시 **Object 추가에 따른 DB구조 변경 발생**

국내 최초 Secure Proxy 방식!!

DB암호화 솔루션 애슬론 (Echelon)

- 강력한 암호화 및 성능 최적화로 안전하게 보호


CC인증


국정원인증


국정원검증필 암호모듈


GS인증

구 분	설 명
개 요	• DB의 개인정보 유출에 대비 고유식별정보 및 주요정보를 컬럼 단위로 암호화(DB암호화)
인 증	• IT보안인증사무국 인증(CC) 암호제품 : 인증번호(CISS-0784-2017) / 보안등급 EAL4 • 국정원 국가용 암호제품 : 검증번호(NCPL-2010-007) • 국정원 검증필 자체 암호모듈(검증번호 : CM-98-2020.1) • GS(Good Software)인증
방 식	• Secure Proxy 방식(국내 최초) – 고성능 암/복호화 처리 구조
암호화	• 선택 **컬럼 단위 주요 정보 암호화**/ 이중보호모드 • 다양한 암호 알고리즘 지원(ARIA, AES, SHA-256) • 관리도구 마법사를 통한 초기 컬럼별 암/복호화 수행 • 기존 DB플랜 변경 없이 암/복호화 • DB성능 저하 시 부하분산 가능(Appliance 사용) • DB프로시저/ 패키지 활용 시 파라미터 값에 대한 암/복호화 가능 • 질의어 추출 기능을 이용한 Application 수정 최소화 (Echelon SQL분석도구) • 보안관리자가 수립한 보안정책에 따른 사용자 접근제어
접근통제	• 보안관리자가 수립한 보안정책에 따른 사용자 접근제어 • 사용자 IP, 응용프로그램, 기간, 시간, 요일 별 접근 제어/ 실시간 접근제어
감사이력	• 질의어(SQL문)요청 내역, 암/복호화 이력 정보, 감사이력 자동백업 • 사용자 IP, 기간, 질의어 별 이력 정보 검색
지원 DBMS	• SAP ERP 지원 • Oracle-8i, 9i, 10g, 11g / MS-SQL-2000, 2005,2008, 2008R2, 2012 • DB2-v8.2, v9.2 / Sybase : ASE(15), IQ(15) / My-SQL / PostgreSQL

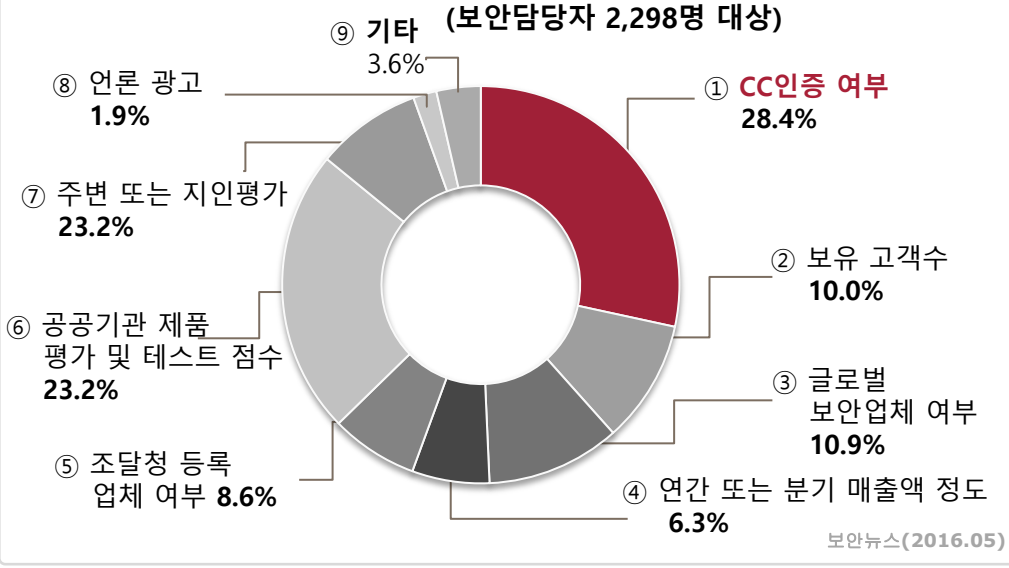
제품소개

IT보안인증사무국 인증(CC) 제품

인증제품명	Echelon V2.5		
인증일	20170419		
만료일	20200418		
제품유형	DB 암호화		
보증등급	EAL4		
인증보고서 번호	CR-17-20		
인증 번호	CISS-0784-2017		
공통평가기준 버전	CC V3.1R2		
준수 보호프로파일	N/A		
평가기관	TTA	개발사/신청기관	(주)유비엠정보

EAL4

정보보호솔루션 도입시 최우선 선정 기준
(보안담당자 2,298명 대상)



보안뉴스(2016.05)

CC(Common Criteria) 인증은 정보보호제품에 대한 평가 기준이 각 국가별로 서로 달라 하나의 제품이 수출되는 국가별로 서로 다른 인증을 받아야 하는 불편을 없애기 위해 평가·인증 결과를 회원국간에 공유하는 **국제상호인정협정(CCRA)**에 따라 우리 나라의 경우 평가기관의 평가를 통과한 제품에 대해 **국가정보원 IT보안인증사무국에서 수여하는 인증**입니다.

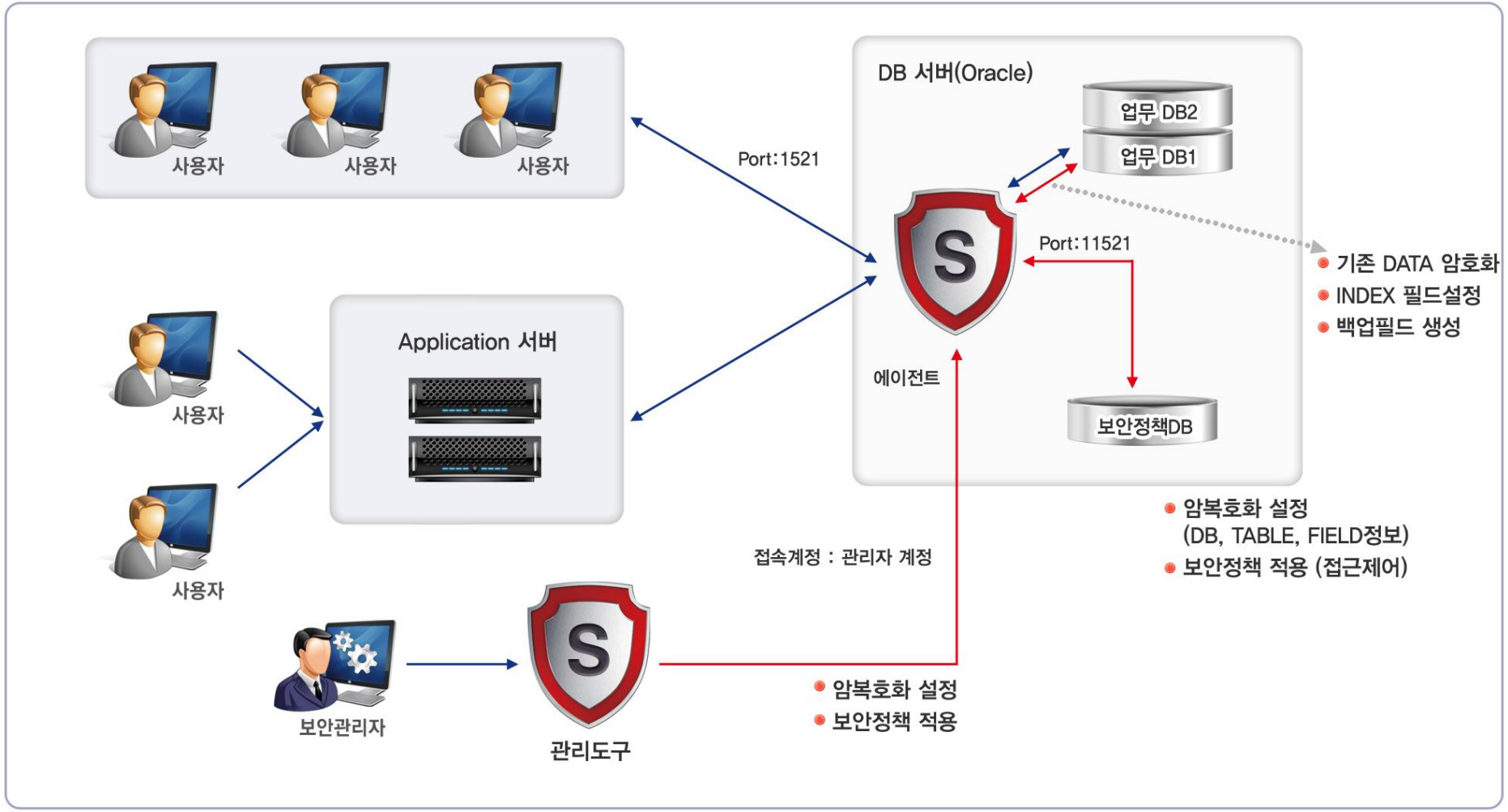
CC인증은 EAL 등급으로 나뉘게 됩니다.

EAL(평가보증등급) 이란,
평가제품의 보증수준을 나타내는 척도를 나타내는 등급으로서, 등급이 높을수록 보증수준이 높음을 나타냅니다.

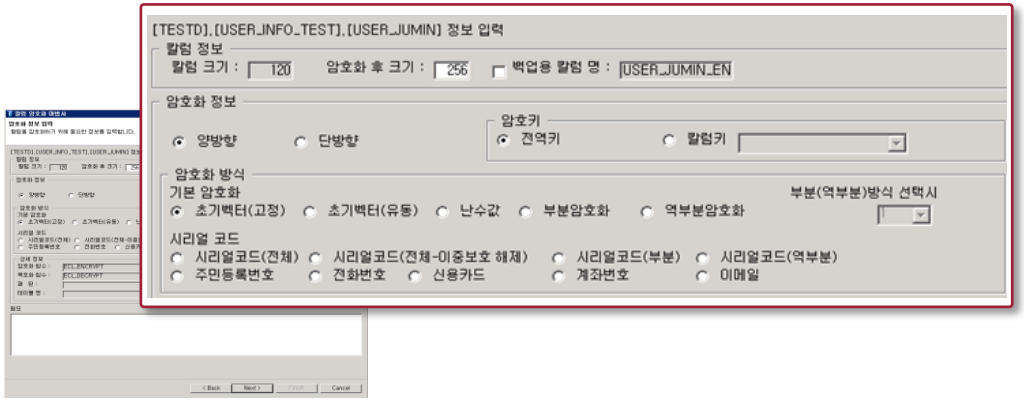
애슬론은 EAL4 등급으로 2017년 4월 19일 인증이 되었으며 국내 암호화 제품 중 가장 높은 등급으로 국정원의 인증을 받아 **안정성과 신뢰성을 보증**합니다.

IT보안인증사무국 http://www.itscc.co.kr

Ⅲ. DB암호화 솔루션 애슬론 - 구성도

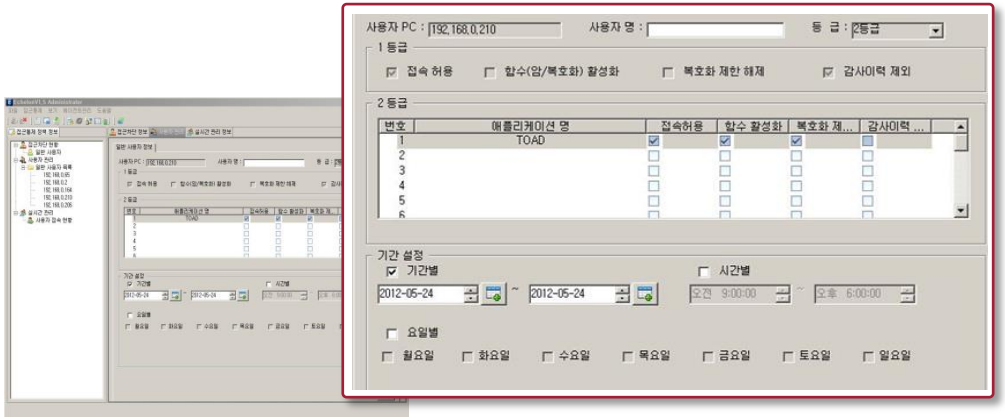


주요기능



1. 암/복호화 기능

- 주요정보 컬럼별 암호화
- 다양한 암호화 알고리즘 지원 (ARIA, AES, SHA-256등)
- 마법사를 통한 암/복호화 수행
- 암호화 수행중 장애로 인한 복구 지원
- 주요정보 암호화 시 사용할 방식 설정: 단방향/양방향
- 초기벡터(고정), 초기벡터(유동), 난수값, 토큰

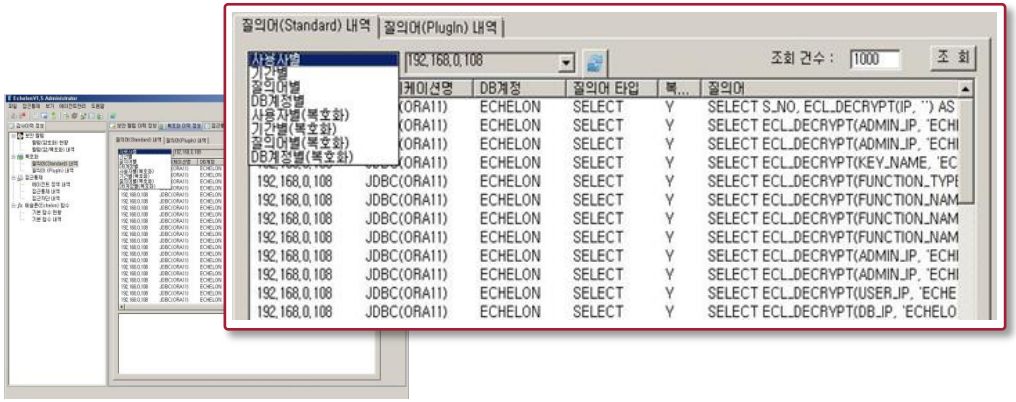


2. 접근 통제

- 세분화된 접근통제 기능

■ 통제정책 : 기간별, 시간별, 요일별 통제 수행 가능

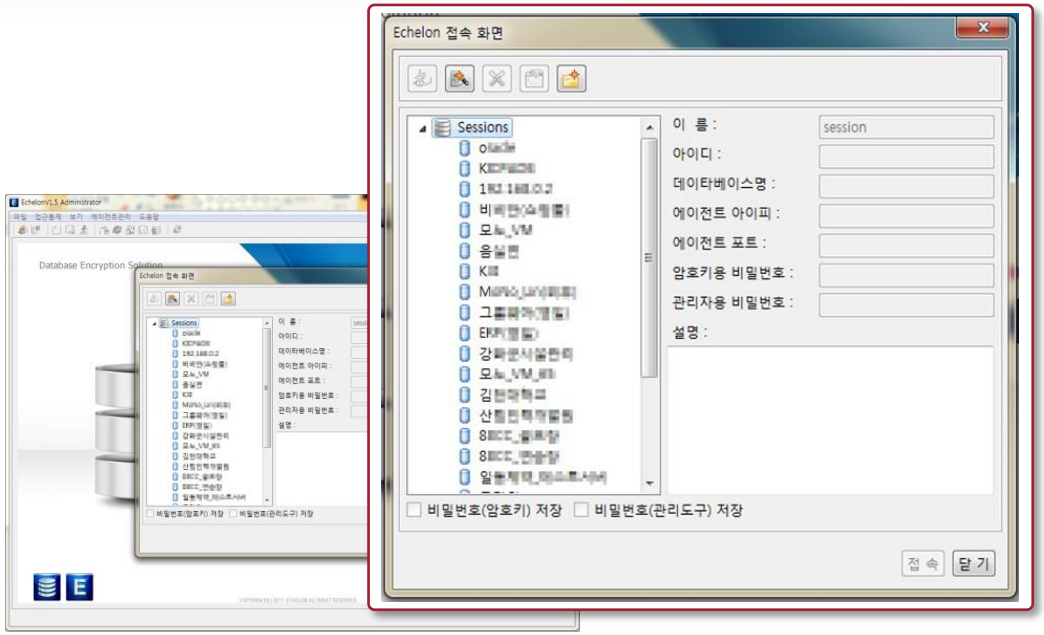
■ 통제방식 : 접근 허용 : 사용자의 DBMS 접근 허용/ 차단
함수(암/복호화) 활성화
사용자가 주요 정보 접근 시 암/복호화 기능 부여



3. 감사이력

- 질의어에 대한 감사이력 (애슬론 만의 특장점)제공
  - ■ 에이전트 정책내역
  - ■ 접근통제 내역
  - ■ 접근차단 내역

주요기능

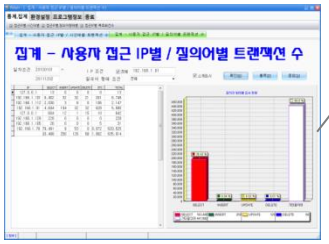


4. 보안정책관리

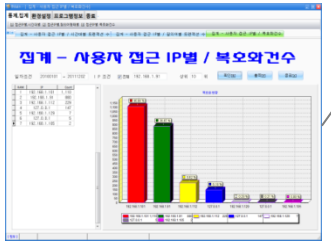
- 안전한 키 백업 및 복구 기능
- 타 기종 DBMS 동시지원 기능
- 하나의 관리도구로 다중 DB서버 관리 기능
- 보안정책 자동백업 기능

5. 통계

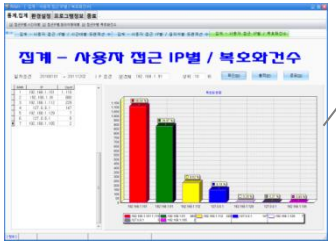
IP 시간대별



IP 질의어별



IP 복호화 건수



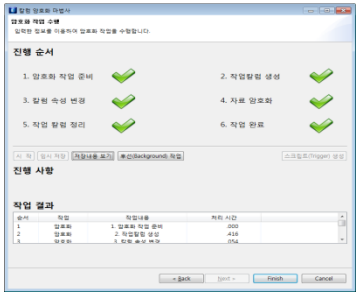
IP 접근이력조회

- 애슬론은 다양한 형태의 통계자료를 생성하며 결과는 Print 출력가능
- IP 시간대별, IP질의어별, IP복호화 건수, IP접근이력조회 통계 출력

Ⅲ. DB암호화 솔루션 애슬론 - GUI

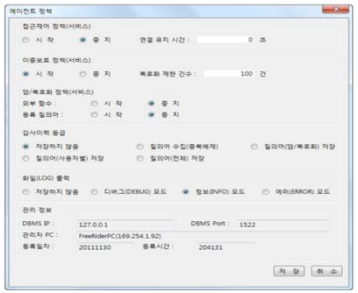
관리도구

보안관리자의 PC에 설치 하나의 관리 Tool로 여러 개의 Agent를 감시/통제



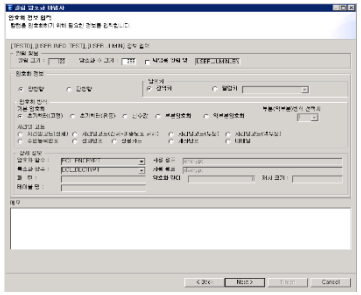
초기 암호화

암호화 진행상태 확인. 작업완료 후 관리도구의 데이터 뷰를 이용하여 암호화 상태 확인



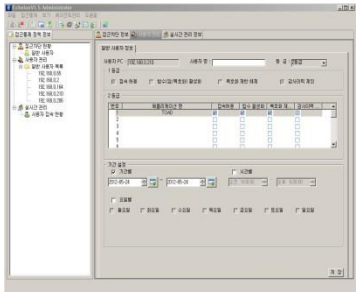
Agent 정책관리 화면

접근제어, 이중보호정책, 암/복호화 정책 등 관리정보로 구성



컬럼별 암호화 설정

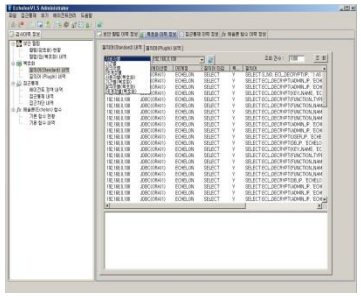
주요정보 컬럼 단위별 암/복호화 기능을 제공
양방향/단방향 등 설정



접근통제 설정

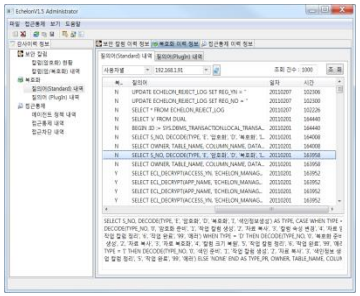
접근통제 정책에 의한 세분화된 접근통제 기능 설정

Echelon 주요 기능 및 편의성을 고려한 Graphic User Interface



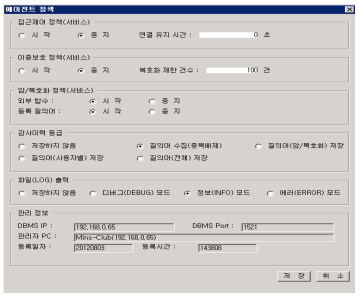
감사이력

사용자별/기간별/질의어별 및 복호화 함수 사용 여부에 대한 조건별 검색기능 제공



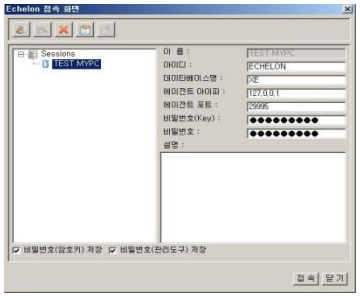
질의어별 감사이력

DBMS에 접근하여 사용자가 요청한 질의어에 대한 접근제어/감사이력을 저장



이중보호모드 설정화면

주요 정보 복호화 요청 시 제공 정보 제한 설정 기능 내부 유출의 위험으로부터 보호



암호키 관리 화면

암호키 유출 및 비인가자의 접근을 원천적으로 차단

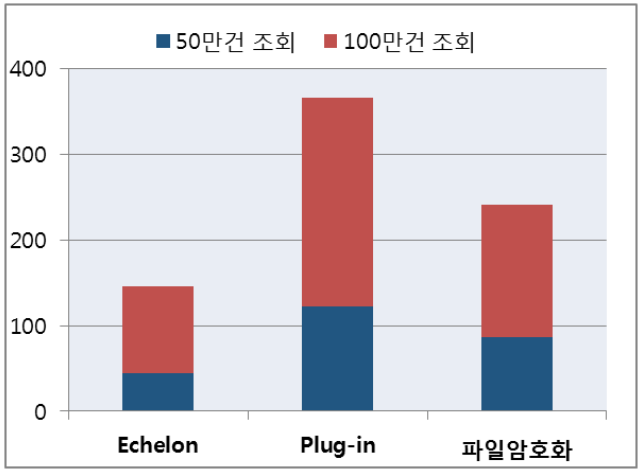
통계 화면

다양한 형태의 통계자료를 생성하며 결과는 프린터로 출력 가능

1. 애슬론 V2.5의 고성능 암/복호화 처리 아키텍처

- 애슬론(Echelon) v2.5의 Secure Proxy방식은 대용량 처리 시 최상의 성능을 보장합니다.
- 암/복호화 고속화 구조
- 초당 7,000건~12,000건 암/복호화 처리 능력

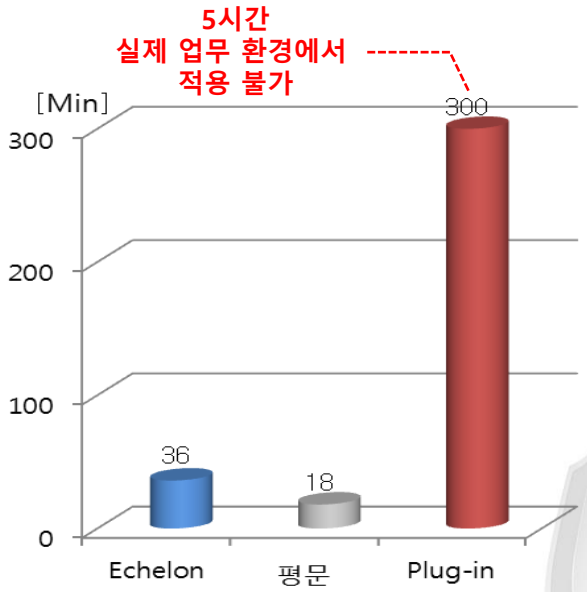
OLTP(실시간) – 암호문 조회 성능



[sec]	Echelon	Plug-in	파일암호화
50만 건 조회	**45.06**	121.98	86.33
100만 건 조회	**101.03**	243.86	154.11

- **K사 DB암호화 솔루션 성능테스트 결과**
- **실시간 대용량 정보 조회**
- **100만 건 조회 시 Plug-in 방식 대비 약 2.5배의 성능차이**

Batch(일괄)- 배치성 업로드 성능



- **배치 일괄 정보 2,800만 건 업로드(저장)**

2. 커스터마이징 최소화

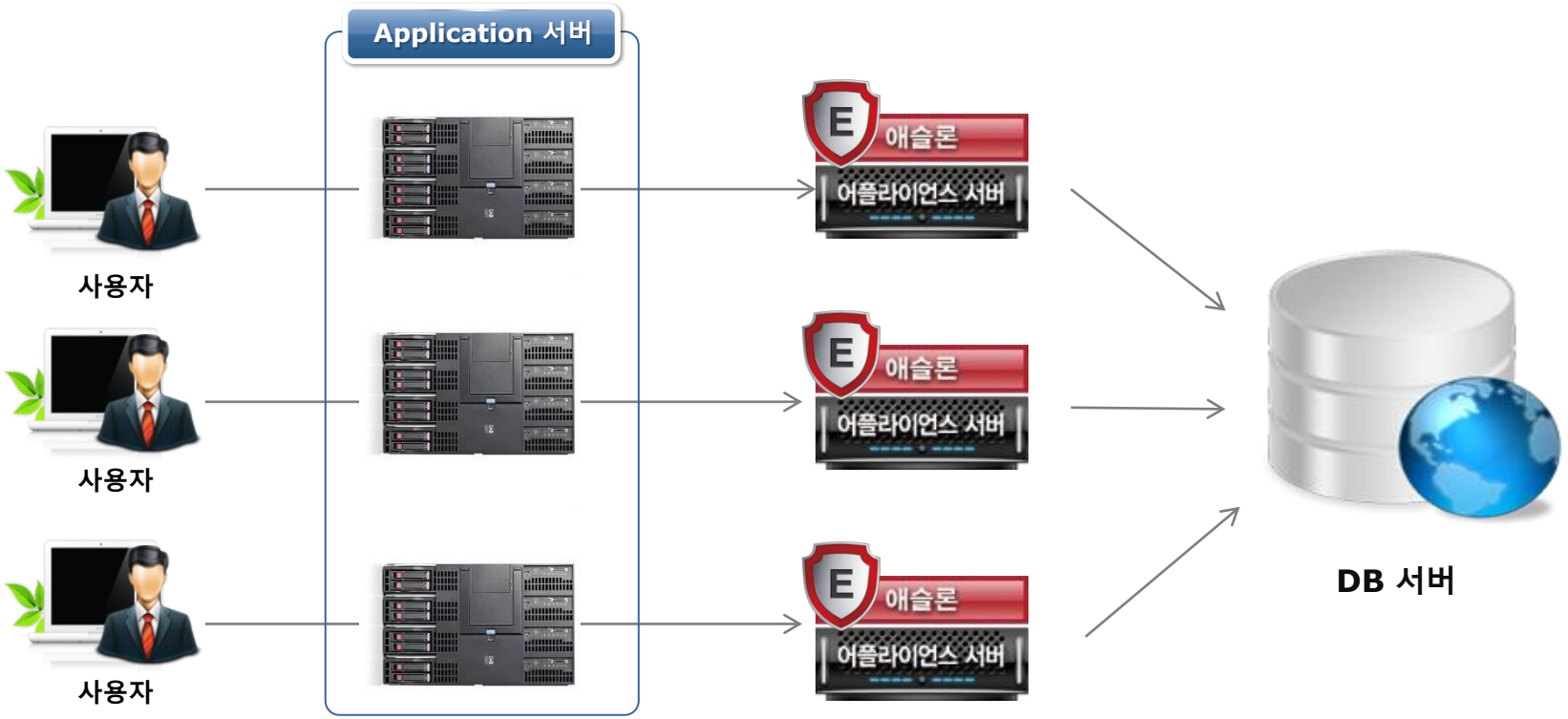
- 애슬론 적용함수를 질의어에 단순 적용하여 Application 수정 최소화
- 애슬론 Agent에서 데이터를 함수로 선별 고속 암/복호화 처리

함수명	함수사용방식	함수설명
ECL_ENCRYPT( )	**ECL_ENCRYPT(REG_NO)**	전체 암호화
ECL_DECRYPT( )	**ECL_DECRYPT(REG_NO)**	전체 복호화
ECL_ENCPART( )	**ECL_ENCPART(REG_NO,6)**	앞자리 6자리 이후 부분암호화
ECL_DECPART( )	**ECL_DECPART(REG_NO,6)**	앞자리 6자리 이후 부분 복호화
ENC_DIGEST( )	**ENC_DIGEST(REG_NO)**	단방향 암호화 (복호화 불가능)

구분		함수적용예시
단순	적용 전	SELECT NAME, REG_NO FROM CUSTOMER WHERE REG_NO = '1234567890123' ;
	적용 후	SELECT NAME, ECL_DECRYPT(REG_NO) FROM CUSTOMER WHERE REG_NO = ECL_ENCRYPT('1234567890123');
JOIN	적용 전	SELECT NAME, REG_NO FROM CUSTOMER a, visit b WHERE a. REG_NO = '1234567890123' AND a. REG_NO= b. REG_NO;
	적용 후	SELECT NAME, ECL_DECRYPT(REG_NO) FROM CUSTOMER a, visit b WHERE a. REG_NO = ECL_ENCRYPT('1234567890123') AND a. REG_NO= b. REG_NO;

3. 대량의 트랙잭션(Transaction) 암/복호화 처리

- 고객식별정보에 대한 암/복호화는 CPU자원 많이 사용
- 애슬론은 DBMS와 별도 프로세스로 동작
- 부하분산 기능 제공. 암/복호화 처리에 따른 서비스 시간을 최소화



4. 효율적 자원사용

- 자체 프로세스 동작으로 DBMS 부하 최소화
- 암/복호화 Agent 자원사용
- **평균 CPU 사용율 : 3%~5% , 평균 Memory 300MB 이하**

1. 테스트 조건

- **주민등록번호 - 13자리 암호화**
- **동시 사용자 수 – 100명 동시 조회**
- **사용자당 100건의 주민등록 번호 및 성명 조회**

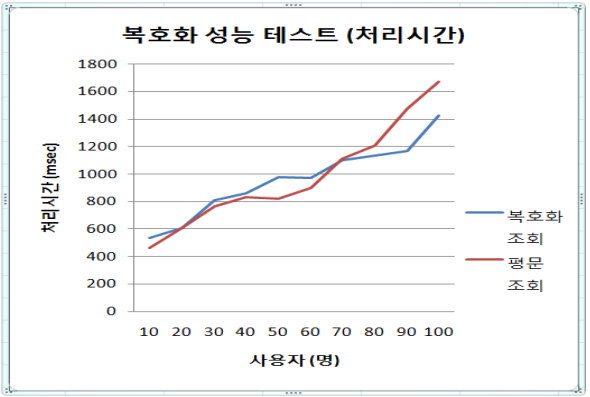
2. 테스트 결과

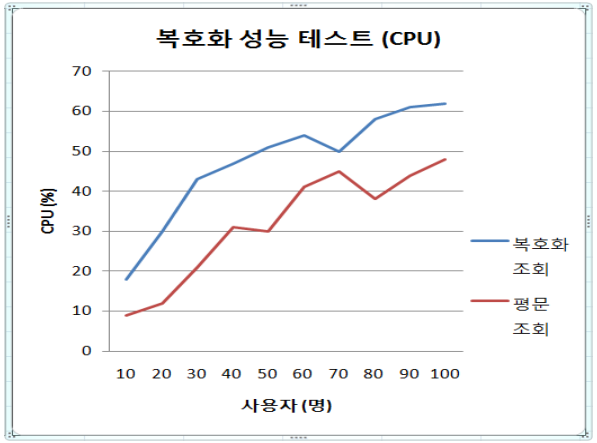
[처리시간]

- **평문 조회 – 약 2분 20초**
- **복호화 조회 – 약 2분 40초**

[CPU 점유율]

- **동시10명 100건 조회 시**
  평문조회 vs 복호화조회 : CPU 성능차이 8%
- **동시 100명 100건의 조회 시**
  평문조회 vs 복호화조회 : CPU 성능차이 12%

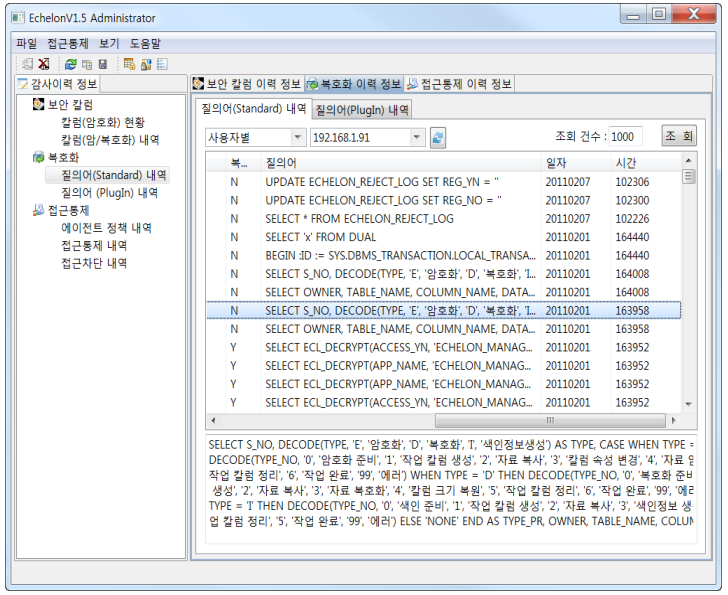




5. 질의어별 감사이력

- DBMS에 접근하여 사용자가 요청한 질의어에 대한 접근제어 및 감사이력 저장
- 감사이력은 질의어 별, 사용자 별, 기간별 및 복호화 함수 사용 여부에 대한 조건 별 검색 기능을 제공합니다.

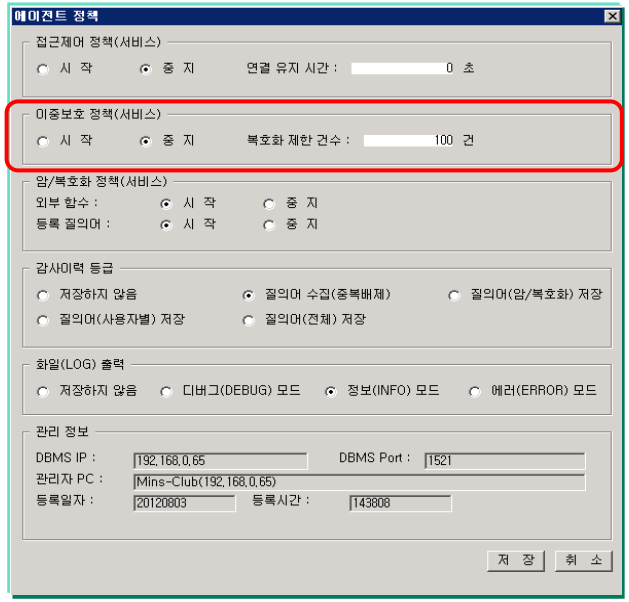
감사이력 – 사용자 별/기간 별/질의어 별



6. 이중보호모드 제공

- 내부 및 외부로부터 대량의 데이터가 한번에 유출되는 것을 방지하는 강력한 보호기능 탑재
- 관리도구를 이용하여 보고화 데이터의 수량 통제 가능
- 인가된 사용자도 DB에 접속하여 주요 정보에 대한 데이터 검색 시 지정된 건수만 복호화 조회 가능 그 외의 데이터 암호화 출력

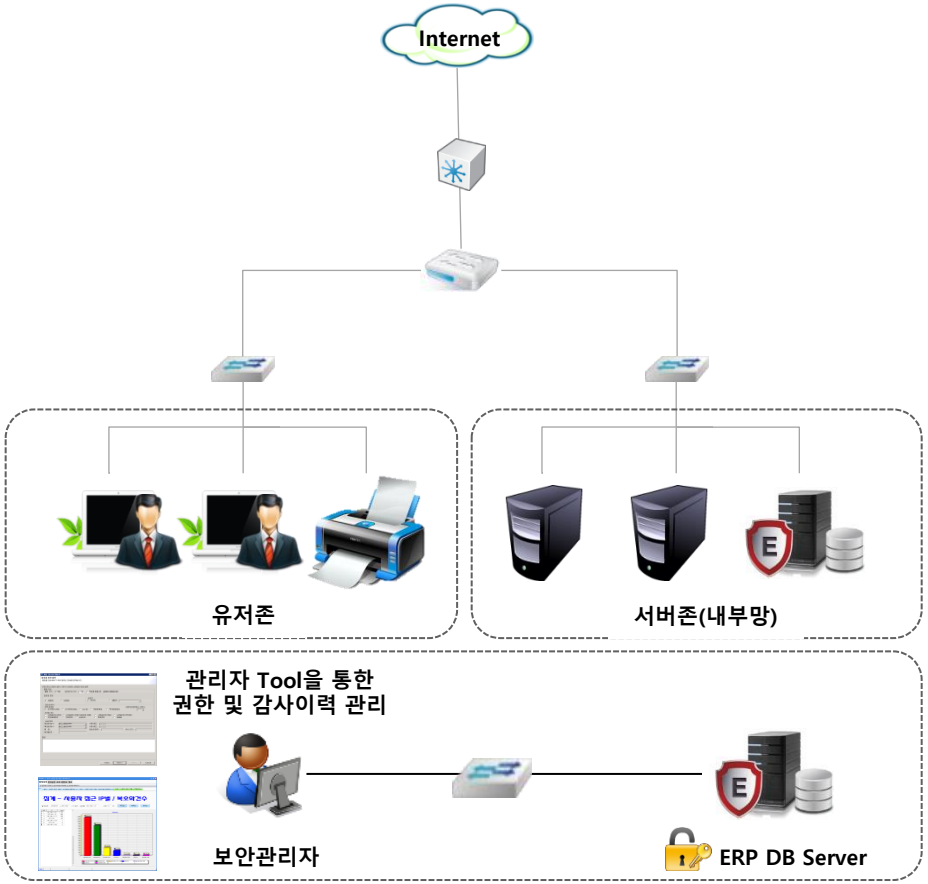
이중보호모드 – 복호화 건수의 제한으로 대량의 데이터 유출 방지



구축사례

고객사 환경

- 직원수 : 약 100여명/ 상조회사
- 적용 시스템 : ERP 시스템
- 개인정보보호법 기술적 보호조치를 위한 DB암호화 조치 필요
- 정보보호체계를 강화하며 사이버 테러 위협에 대비한 예방대책 필요



제안상품 및 도입효과

DB암호화

모델명	DB서버	CPU
애슬론(Echleon)	1	2

- 보안관리자 PC : 통합관리자 Tool
- DB Server : ERP DB서버 Agent설치
- Secure Proxy방식
- 국정원 인증, 국정원 검증필 자체암호모듈, GS인증
- 칼럼 단위 별 암/복호화 처리
- 다양한 암호화 알고리즘 제공
  : ARIA, AES, SHA-256 등

- DBMS 정보 선택적 암호화, 사용자별 인증 및 접근 제어 및 감사이력 제공
- DBMS 운영 관리자와 DB 보안 관리자 역할 분리를 통한 DBMS 보안 강화
- GUI 기반의 다양한 통계, 모니터링 기능 제공
- Oracle DBMS지원
- 도입효과
  - ERP시스템의 개인정보 및 금융정보의 암호화를 통한 개인정보 및 기업내부자산 정보보호 조치 완료
  - DB암호화 구축 후 성능저하 최소화로 업무부하에 영향을 최소화 함
  - 접속이력 관리를 위한 감사이력(SQL문)을 제공하여 법적 요건사항 충족
  - 개인정보보호 및 정보보호 관리체계를 강화하여 고객사의 대외 신뢰도를 향상
  - 추후 동종업계 바이럴 마케팅을 통한 2건의 동종업계 수주 사례 확보

V. 주요 고객사

2000여 개 레퍼런스!!

- **기업** – 후지제록스, 매리어트호텔 서울, KT기술연구소, 남양산업, 현대종합상조 등
- **교육** – 부산외국어대학교, 웨스트민스터신학대학원대학교 등
- **공공** – 경찰박물관, 우체국금융개발원, 신용보증재단중앙회, 국토해양부철도사법경찰대 등

”고객감동”을 넘어 “고객행복”을 드리고자

“최선”을 다하겠습니다!