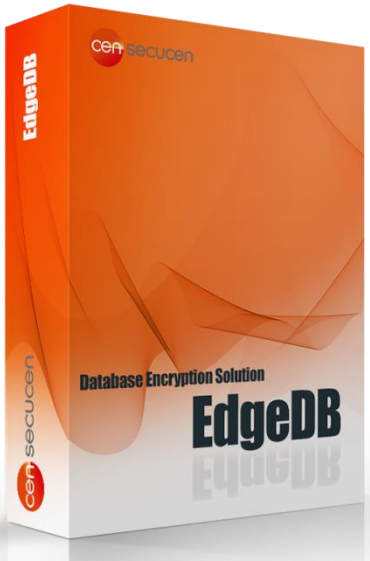
EdgeDB 표준 제안서

DB 암호화 솔루션



Creative | Energy | National Service

secucen
(주)시큐센

Contents

I. 제안 배경

II. EdgeDB 소개

III. 특장점

IV. 주요 기능

V. Reference

VI. ㈜시큐센 소개

Ⅰ. 제안개요

1. 개인 정보 유출 보안 사업의 급증

2. 관련 법규에서 요구하는 개인정보 보호

1. 개인 정보 유출 보안사고의 급증

“ 민감 정보 유출은 내부자 소행이 80% 이상 차지함에 따라
개인/민감 정보의 DB암호화를 수행하여 데이터 자체보호 필요 ”

개인정보 유출 보안 사고

- ‘2016. 07 인터파크 가입자 개인정보유출 사고
- ‘2016. 07 아시아나 항공 고객 개인정보 유출 사고
- ‘2015. 09 봄뿌 회원 개인정보 유출 사고
- ‘2014. 01 KB국민·롯데·농협 3개 카드사 고객 개인정보 및 일부 신용정보 유출 사고
- ’2013. 01 코웨이 가입자 개인정보유출 사고
- ‘2012. 05 EBS 방송국 개인정보유출 사고
- ‘2012. 03 SK텔레콤/KT 개인정보유출 사고

2010년 이후 개인정보 유출 보안사고 급증 !!

DB 암호화 도입 필요성

내부자의 의한 정보유출 및 보안사고 급증

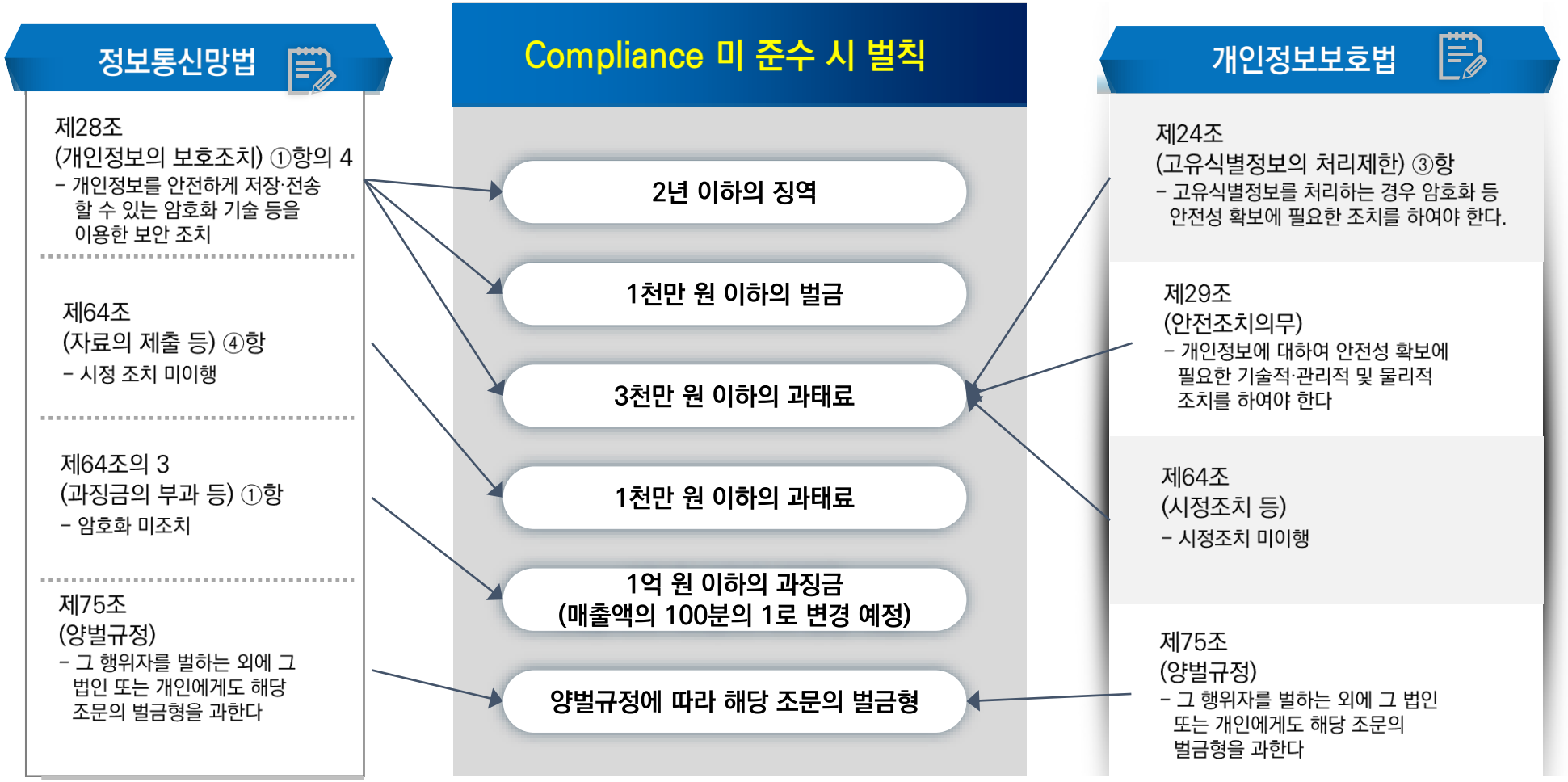
개인정보 유출에 대한 불안감 고조 및 신뢰성 저하

데이터 자산의 가치 증가

DB 정보보호에 대한 국내외 법률 제정

DB 암호화 적용을 통한 DB 유출 위협을 원천 봉쇄

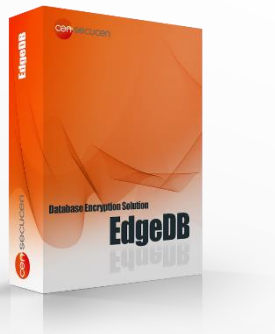
2. 관련 법규에서 요구하는 개인정보 보호



II. EdgeDB 소개

1. EdgeDB 소개
2. EdgeDB 구성도
3. EdgeDB 운영 지원 환경

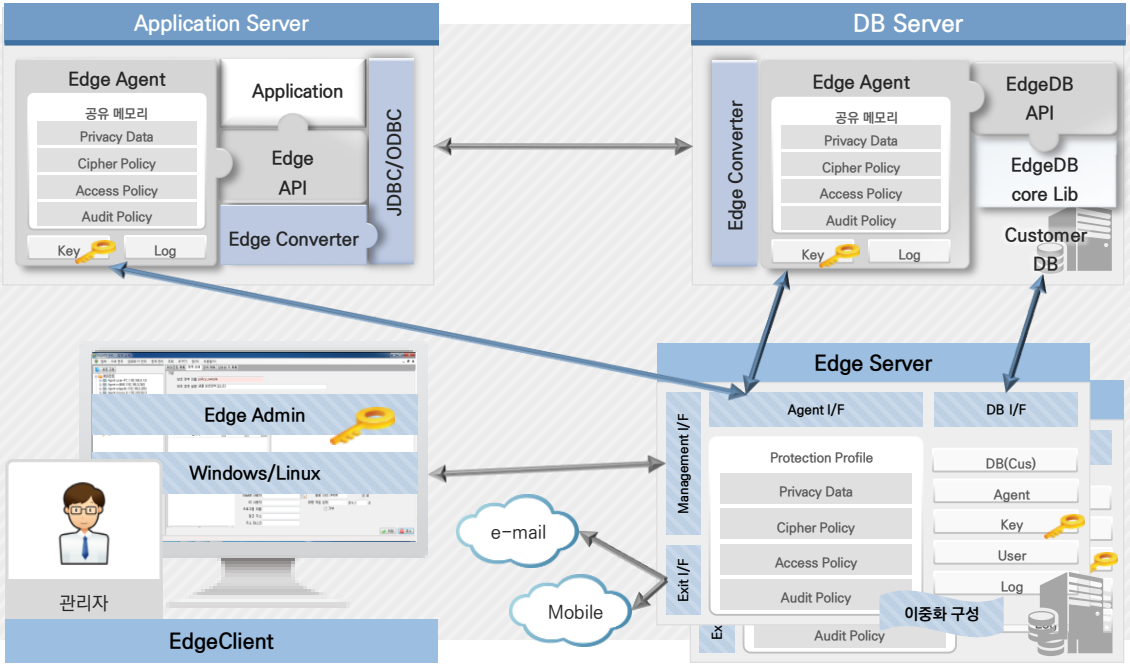
1. EdgeDB 제품 소개



제품명	EdgeDB(엣지디비) V1.0
제조사	㈜시큐센
제품 개요	▪ 국가정보원 국가용 암호모듈 인증 ▪ 컬럼단위 DB 암호화 솔루션 ▪ 다양한 적용 방식 지원 ▪ 공공·금융·기업 등 국내 다수 레퍼런스 보유

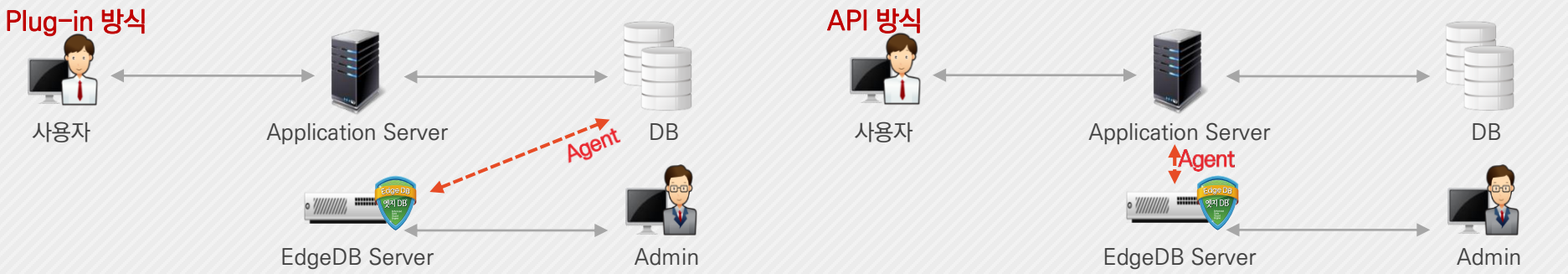
구분	세부 내용
국가정보원 인증	▪ 국가정보원 보안인증사무국 인증 필 (DB암호제품, 라이브러리)
자체암호화 모듈	▪ 자체 국정원 암호 인증 모듈 보유
암/복호화 지원방식	▪ API / Plug-In / SQL Converter
지원알고리즘	▪ ARIA, SEED, AES, SHA256
무중단 암호화	▪ Listener 재기동(Oracle 기준)
구축의 편의성	▪ 기존 운영중인 Application 및 DBMS의 수정을 최소화 ▪ 다양한 OS/DB 지원
운영관리	▪ 암,복호화용 키를 별도 백업 가능 ▪ 다양한 백업 방식에서 데이터에 대한 암호화 유지
권한 제어	▪ 사용자, 사용자 그룹, Application 별 데이터 암,복호화 권한 제어가능

2. EdgeDB 구성도



구분	주요 사양
EdgeDB API	▪ 어플리케이션에서 암.복호화를 수행할 수 있도록 제공되는 다양한 언어의 함수 라이브러리 ▪ API는 Application API와 DB API 두 종류가 제공되며 각각 AP와 DB서버에서 암호화 함수 동작
EdgeDB DB API	▪ DB API 모듈은 DB에 함수를 등록하여 사용하는 모듈로 Application API와 유사하게 DB에서 동작 ▪ View-Trigger를 이용하여 어플리케이션 수정 없이 암.복호화를 DB서버에서 수행
EdgeDB Server	▪ EdgeDB™의 핵심 모듈로 암호화 대상 운영서버의 Edge Agent를 통합 관리 ▪ 암호화 컬럼에 대한 암호화 정책 및 접근제어 정책 관리 ▪ 접근제어 및 암.복호화에 대한 접근로그 및 감사로그 관리
EdgeDB Agent	▪ 암호화 대상 운영서버에서 정책관리, 키 관리, 접근제어, 감사관리를 통합적으로 관리 ▪ 암호화 대상 컬럼의 접근제어 및 감사로그/정책 및 암호화 키에 대한 유효성 관리
EdgeDB Admin	▪ EdgeAdmin을 이용하여 EdgeServer 에 정책관리, 키 관리, 접근제어, 감사관리을 설정함

3. EdgeDB 운영 지원 환경



※ EdgeDB는 Plug-in과 API 간 Hybrid 형태 구성 가능

구분		운영체제	DBMS	암호화 알고리즘	EdgeDB API
EdgeDB	API 방식	▪ Unix – Sun Solaris – HP-UX – IBM AIX ▪ Linux ▪ Windows Server ▪ 기타	▪ DBMS 상관없이 ▪ 모두 지원	▪ SEED ▪ ARIA ▪ AES ▪ TDES ▪ SHA ▪ OPE ▪ FPE	▪ C#, ASP, .NET ▪ JSP, Java ▪ PHP ▪ C/C++ ▪ COBOL ▪ Python ▪ Pro-c ▪ VB
	Plug-In 방식	▪ Unix – Sun Solaris – HP-UX – IBM AIX ▪ Linux ▪ Windows Server ▪ 기타	▪ Oracle ▪ DB2 ▪ MS-SQL ▪ MySQL(Maria) ▪ Informix ▪ Sybase & IQ ▪ Tibero ▪ Altibase		
EdgeServer (Key & Policy Server)		▪ Unix ▪ Window Server			
EdgeClient (EdgeDB Admin)		▪ Windows			

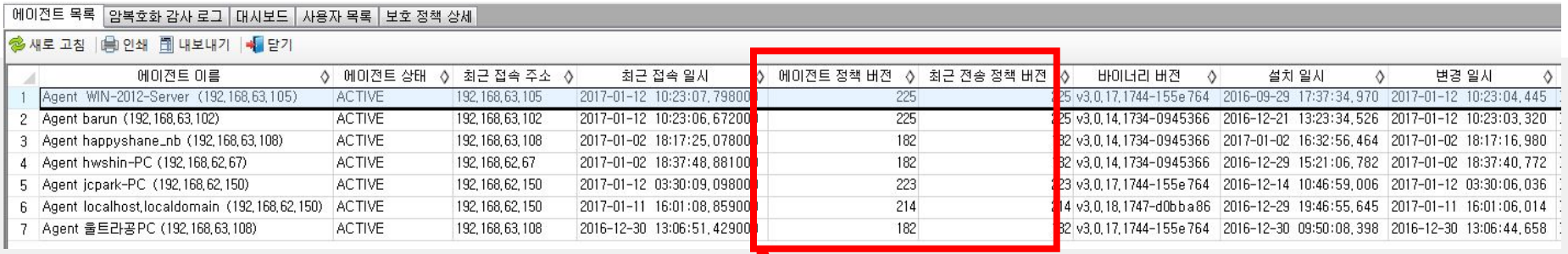
Ⅲ. 특장점

1. 정책 버전 관리

2. 다중 암호화 키 동시 적용

1. 정책 버전 관리

정책 생성 / 수정 / 삭제에 대한 버전 관리



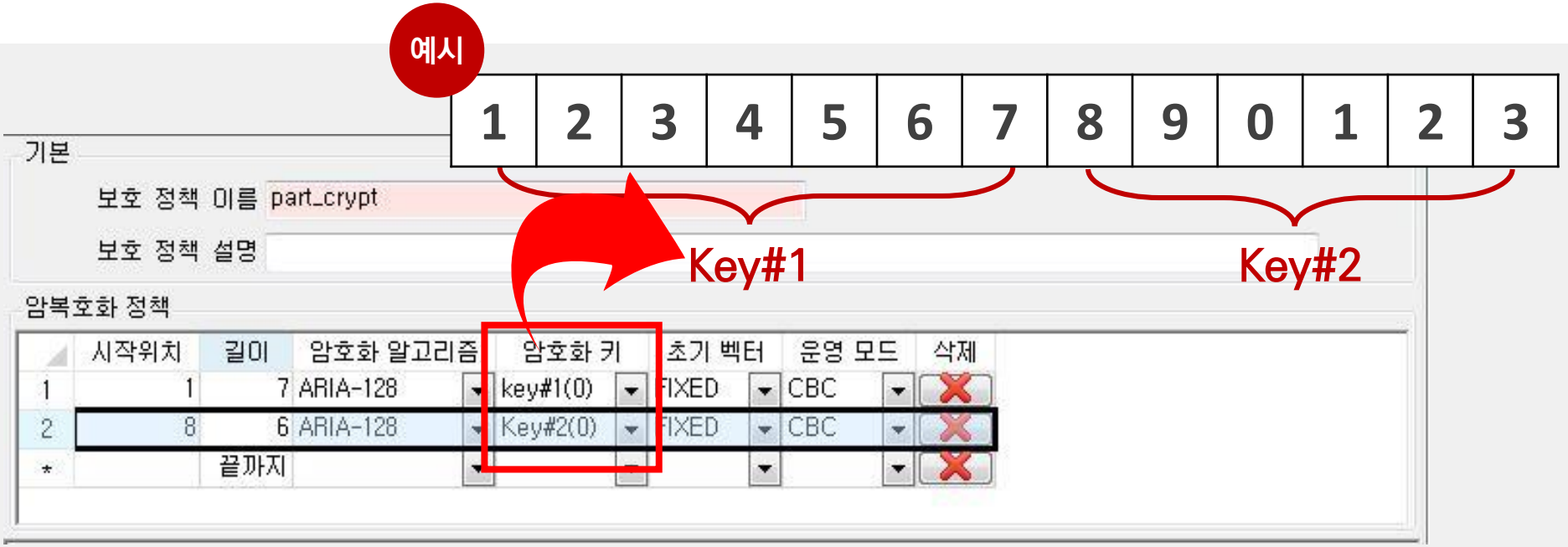
	에이전트 이름	에이전트 상태	최근 접속 주소	최근 접속 일시	에이전트 정책 버전	최근 전송 정책 버전	바이너리 버전	설치 일시	변경 일시
1	Agent WIN-2012-Server (192.168.63.105)	ACTIVE	192.168.63.105	2017-01-12 10:23:07.79800	225	225	v3.0.17.1744-155e764	2016-09-29 17:37:34.970	2017-01-12 10:23:04.445
2	Agent barun (192.168.63.102)	ACTIVE	192.168.63.102	2017-01-12 10:23:06.67200	225	225	v3.0.14.1734-0945366	2016-12-21 13:23:34.526	2017-01-12 10:23:03.320
3	Agent happyshane_nb (192.168.63.108)	ACTIVE	192.168.63.108	2017-01-02 18:17:25.07800	182	182	v3.0.14.1734-0945366	2017-01-02 16:32:56.464	2017-01-02 18:17:16.980
4	Agent hwshin-PC (192.168.62.67)	ACTIVE	192.168.62.67	2017-01-02 18:37:48.88100	182	182	v3.0.14.1734-0945366	2016-12-29 15:21:06.782	2017-01-02 18:37:40.772
5	Agent jcpark-PC (192.168.62.150)	ACTIVE	192.168.62.150	2017-01-12 03:30:09.09800	223	223	v3.0.17.1744-155e764	2016-12-14 10:46:59.006	2017-01-12 03:30:06.036
6	Agent localhost.localdomain (192.168.62.150)	ACTIVE	192.168.62.150	2017-01-11 16:01:08.85900	214	214	v3.0.18.1747-d0bba86	2016-12-29 19:46:55.645	2017-01-11 16:01:06.014
7	Agent 홀트라공PC (192.168.63.108)	ACTIVE	192.168.63.108	2016-12-30 13:06:51.42900	182	182	v3.0.17.1744-155e764	2016-12-30 09:50:08.398	2016-12-30 13:06:44.658

에이전트 정책 버전	최근 전송 정책 버전	버전	설치 일시	변경 일시
225	225	v3.0.17.1744-155e764	2016-09-29 17:37:34.970	2017-01-12 10:23:04.445
225	225	v3.0.14.1734-0945366	2016-12-21 13:23:34.526	2017-01-12 10:23:03.320
182	182	v3.0.14.1734-0945366	2017-01-02 16:32:56.464	2017-01-02 18:17:16.980
182	182	v3.0.14.1734-0945366	2016-12-29 15:21:06.782	2017-01-02 18:37:40.772
223	223	v3.0.17.1744-155e764	2016-12-14 10:46:59.006	2017-01-12 03:30:06.036
214	214	v3.0.18.1747-d0bba86	2016-12-29 19:46:55.645	2017-01-11 16:01:06.014
182	182	v3.0.17.1744-155e764	2016-12-30 09:50:08.398	2016-12-30 13:06:44.658

+ 정책이 생성, 수정, 삭제 될 경우 자동으로 버전이 갱신
+ 설정된 정책이 Agent에 반영 되었는지 확인 가능하며 이를 통해서 오용 방지 가능

2. 다중 암호화 키 동시 적용

한 개의 칼럼에 2개 이상의 암호화 키 적용 가능

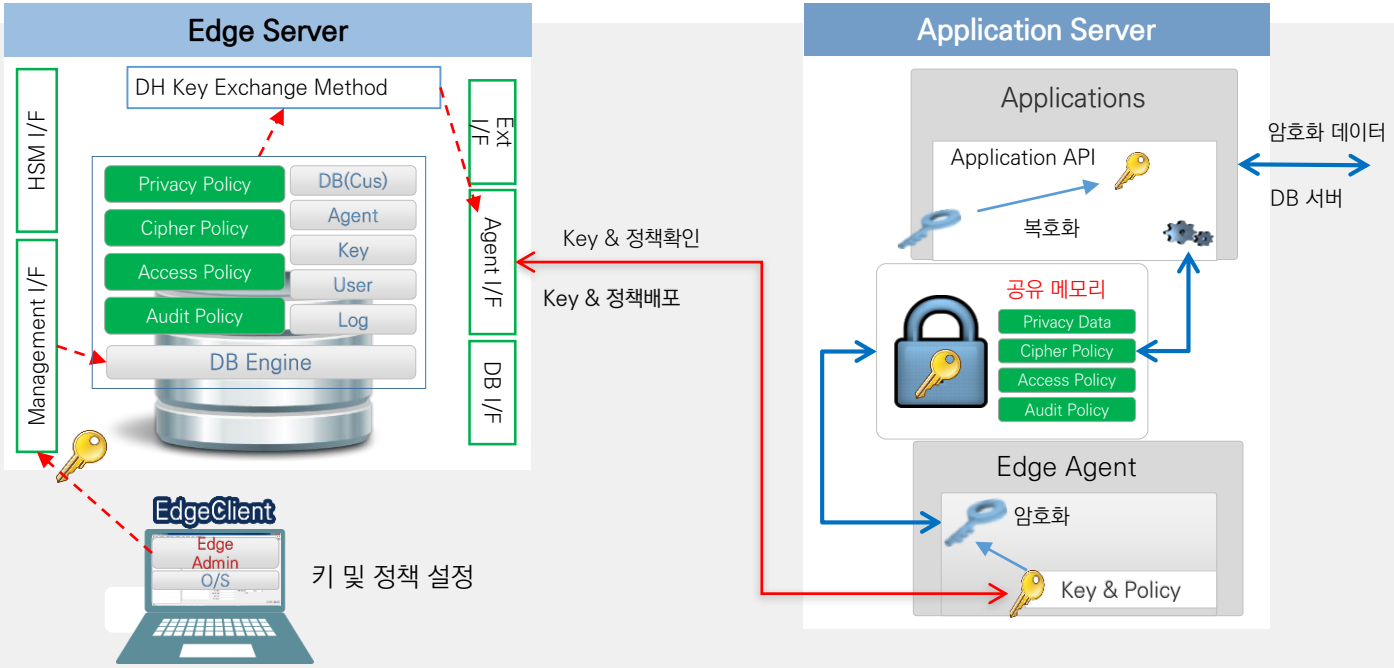


+ 한 개의 칼럼에 2개 이상의 암호화키를 적용하여, 하나의 암호키가 유출되더라도 전체 칼럼의 복호화는 이루어지지 않음
+ 예시: 주민번호 13자리 중 앞 7자리와 뒤 6자리의 암호화 키를 다르게 설정가능
  → 암호 키 하나가 유출되는 경우에도, 주민번호 전체 복호화 불가

Ⅳ. 주요기능

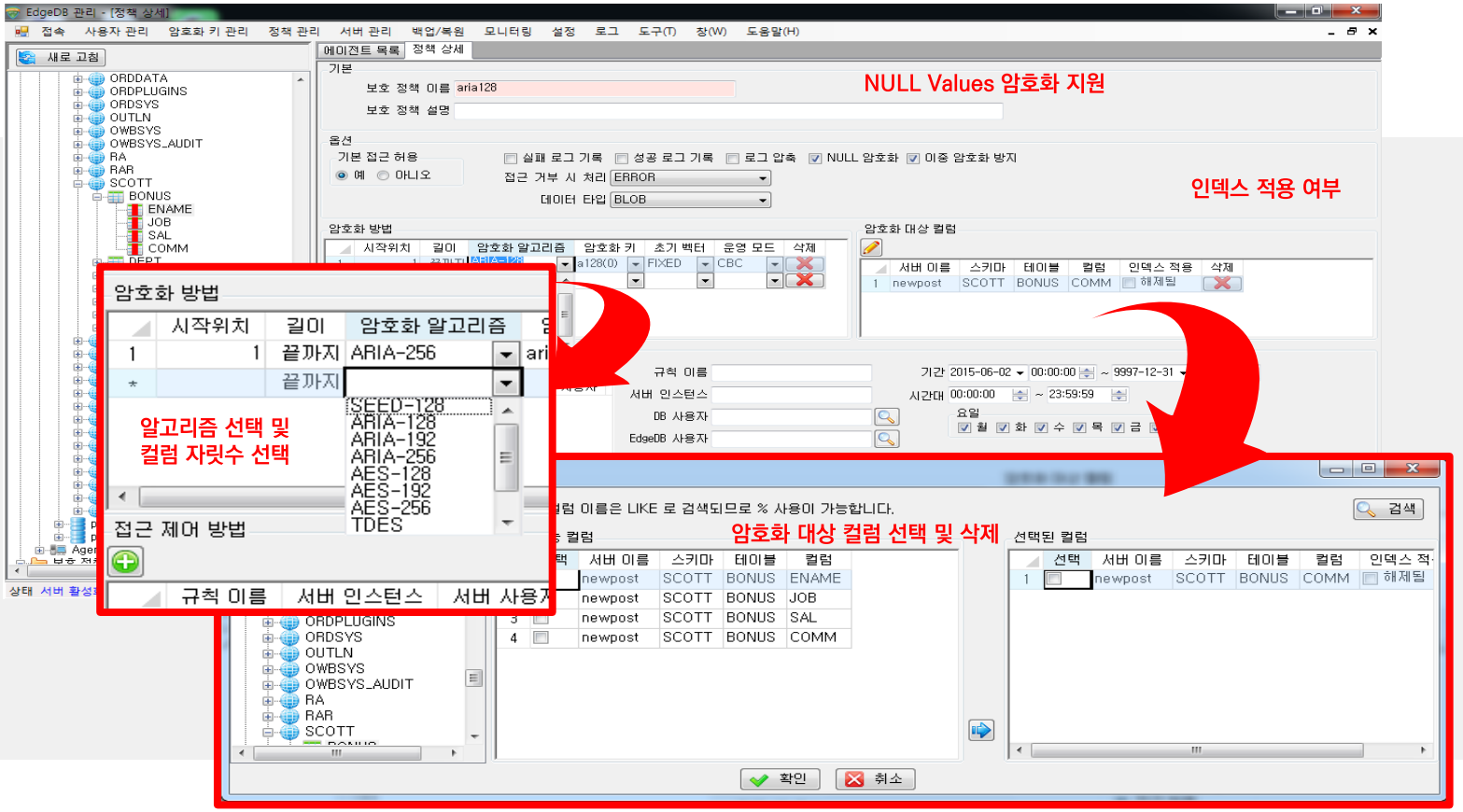
1. 안전한 암호화 Key 관리
2. 컬럼 단위 암호화 지원
3. 다양한 Data Type 암호화 지원
4. 암호화 시 Random IV 적용
5. Data 부분 암호화
6. 인덱스 검색 지원
7. 파일 암호화
8. 장애 감지 및 알림 기능
9. 암호화 컬럼 접근통제 관리
10. 실시간 암·복호화 및 상태 모니터링
11. 비인가 접근 차단 / 통제 및 감사 기능

1. 안전한 암호화 Key 관리



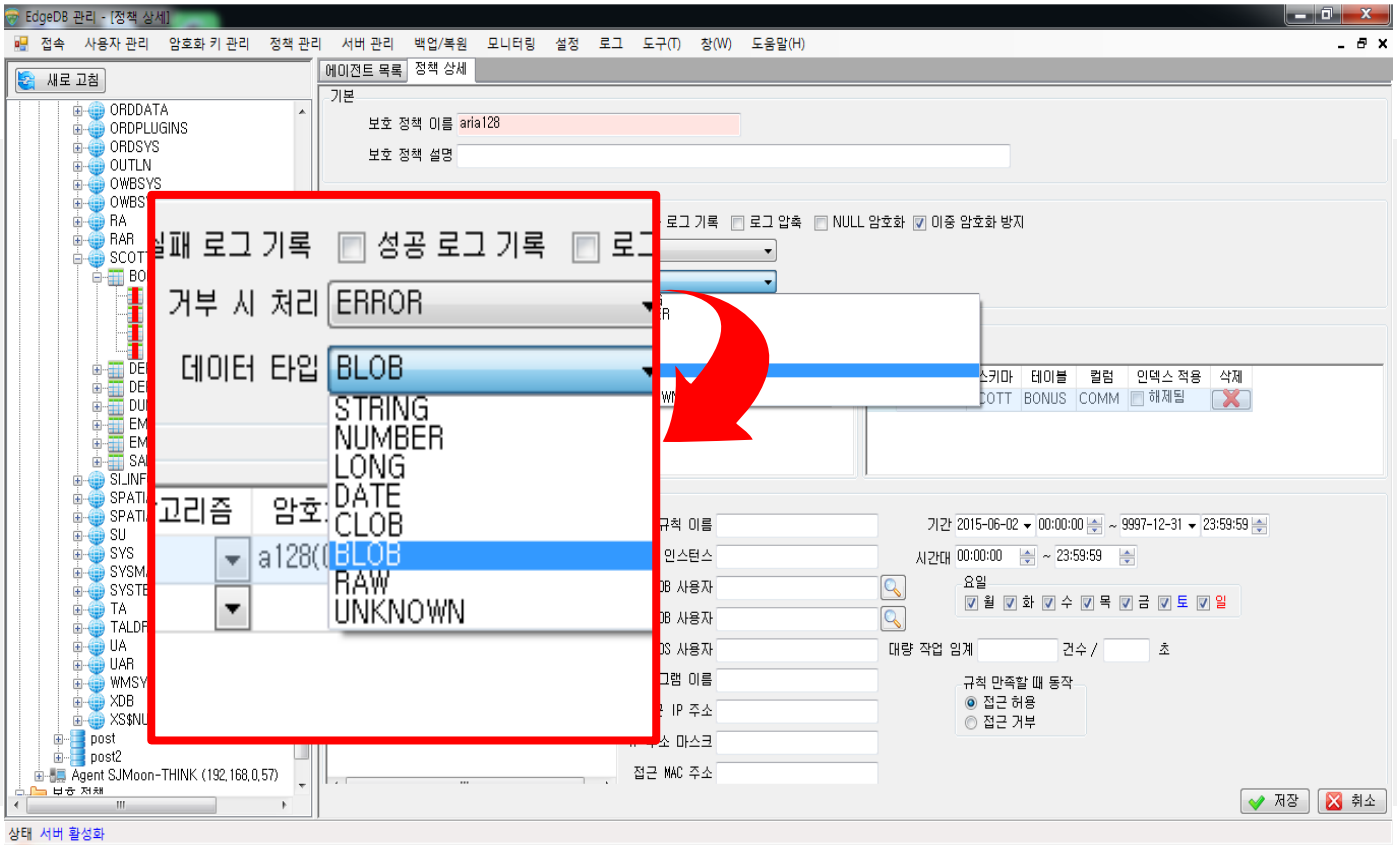
+ EdgeDB의 모듈의 통신은 모두 암호화 통신
+ 공유메모리에 Key와 정책 Load한 후 암/복호화에 이용
+ EdgeDB 장애 시에도, Data 암/복호화는 정상

2. 컬럼 단위 암호화 지원



+ Admin Console(UI 상)에서 암/복호화 대상을 Column 별 선택하여 추가/제거 가능

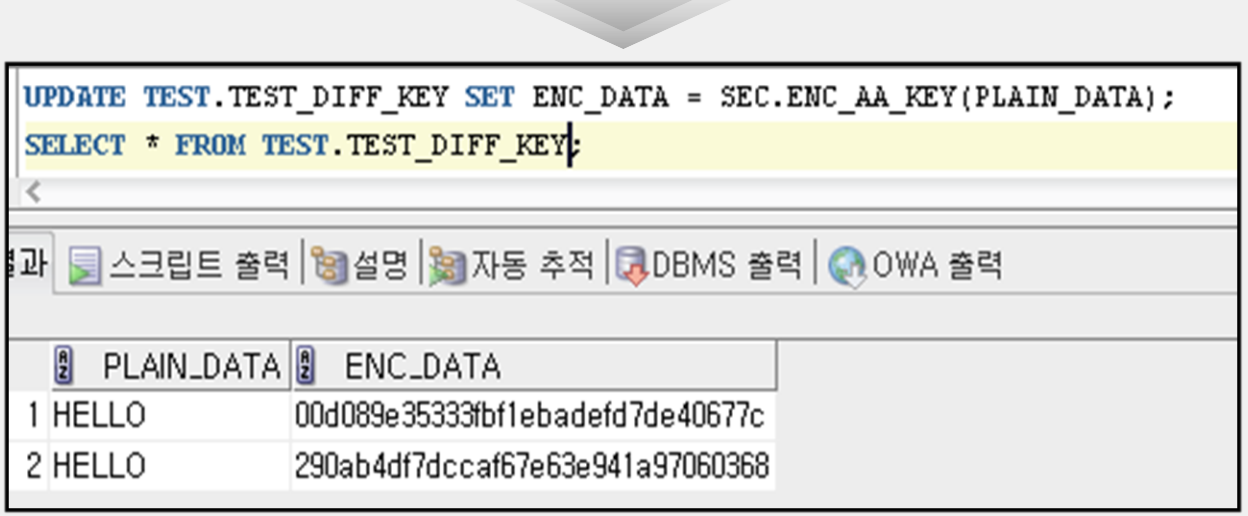
3. 다양한 Data Type 암호화 지원



+ Char, VarChar, String, Number, BLOB, CLOB 등 다양한 Data Type 지원

4. 암호화 시 Random IV 적용

```
UPDATE TEST.TEST_DIFF_KEY SET ENC_DATA = SEC.ENC_AA_KEY(PLAIN_DATA);
SELECT * FROM TEST.TEST_DIFF_KEY;
```



'hello' 라는 동일 값의 암호화 수행 시 서로 다른 암호화 데이터 결과

+ 동일한 Data 암호화 시 서로 다른 암호화 결과 값이 나오도록 IV 적용

※ IV (Initialization Vector) : 첫 블록을 암호화할 때 사용되는 초기값

5. Data 부분 암호화

```
select SEC.ENC_OE_ID7('1234561234567') FROM DUAL;
```

주민번호 뒷자리에 대하여 부분 암호화 수행

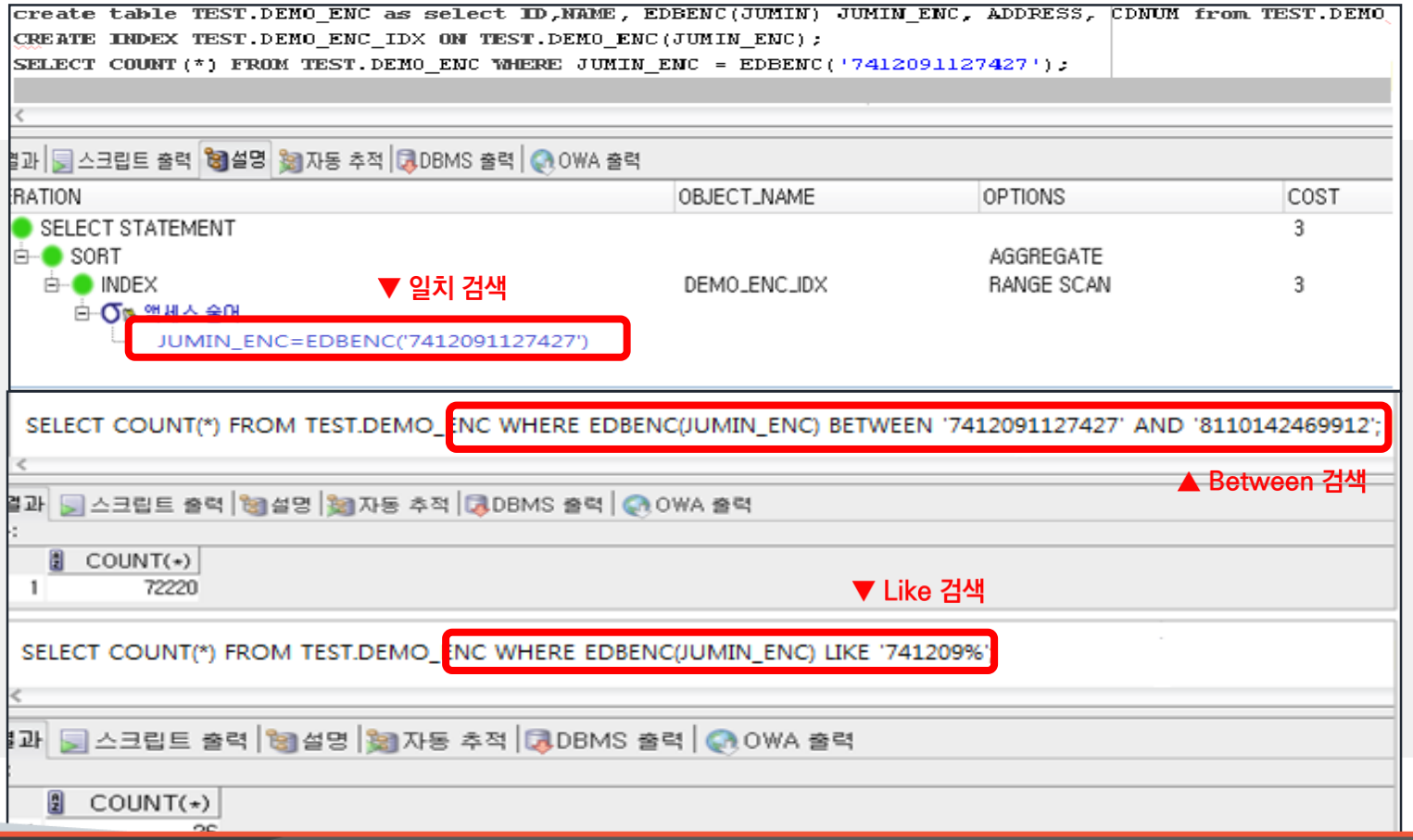
```
select SEC.ENC_OE_ID7('1234561234567') FROM DUAL;
```

과 스크립트 출력 | 설명 | 자동 추적 | DBMS 출력 | OWA 출력

	SEC.ENC_OE_ID7('1234561234567')
1	12345619f748efd73bd0b0b7c98aecbd6...

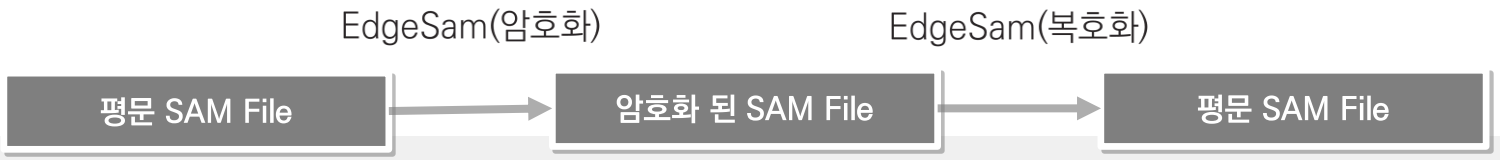
+ 컬럼 Data에서 원하는 부분만 선택하여 암호화 적용 기능 지원

6. 인덱스 검색 지원



+ 인덱스 암호화 시에도 일치 검색, 전방 일치 검색, 범위 검색 등 다양한 검색기능 지원

7. 파일 암호화



▪ 구분자 기반 SAM 파일

```
./EdgeSam {-e|-d} Src_File Tar_file -c '컬럼 구분자' -r '레코드 구분자'
   -Column_Position1 Encryption_Algorithm1
   [-Column_PositionN Encryption_AlgorithmN]
```

▪ (-e : 암호화 수행 /-d : 복호화 수행

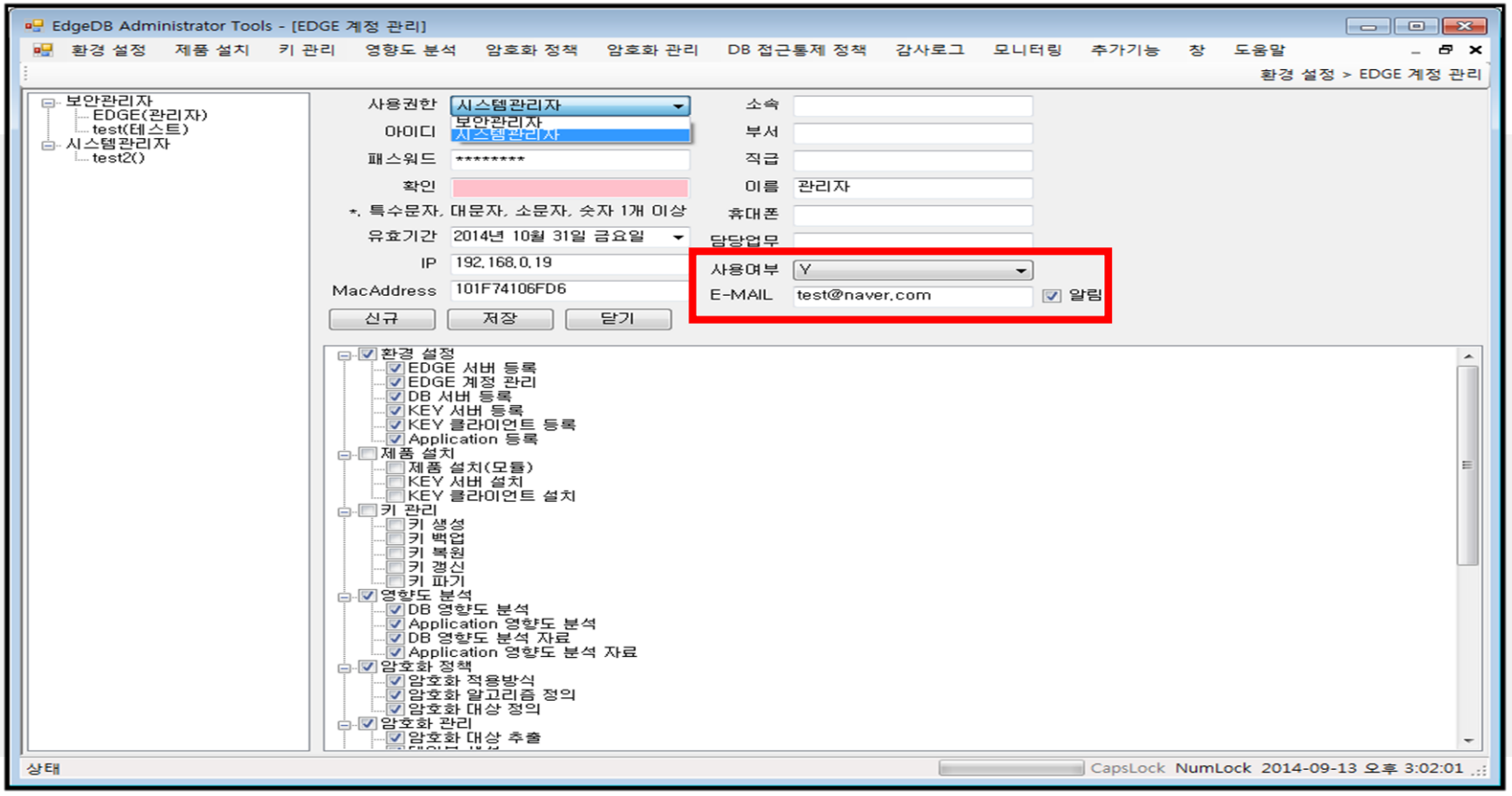
▪ 길이 기반 SAM 파일

```
./EdgeSam {-le|-ld} Src_File Tar_file -c 'Column_Start_Position1
   Column_End_Position1 Encryption_Algorithm1 [-Column_Start_Position_N
   Column_End_Position_N Encryption_Algorithm_N]
```

▪ (-e : 암호화 수행 /-d : 복호화 수행

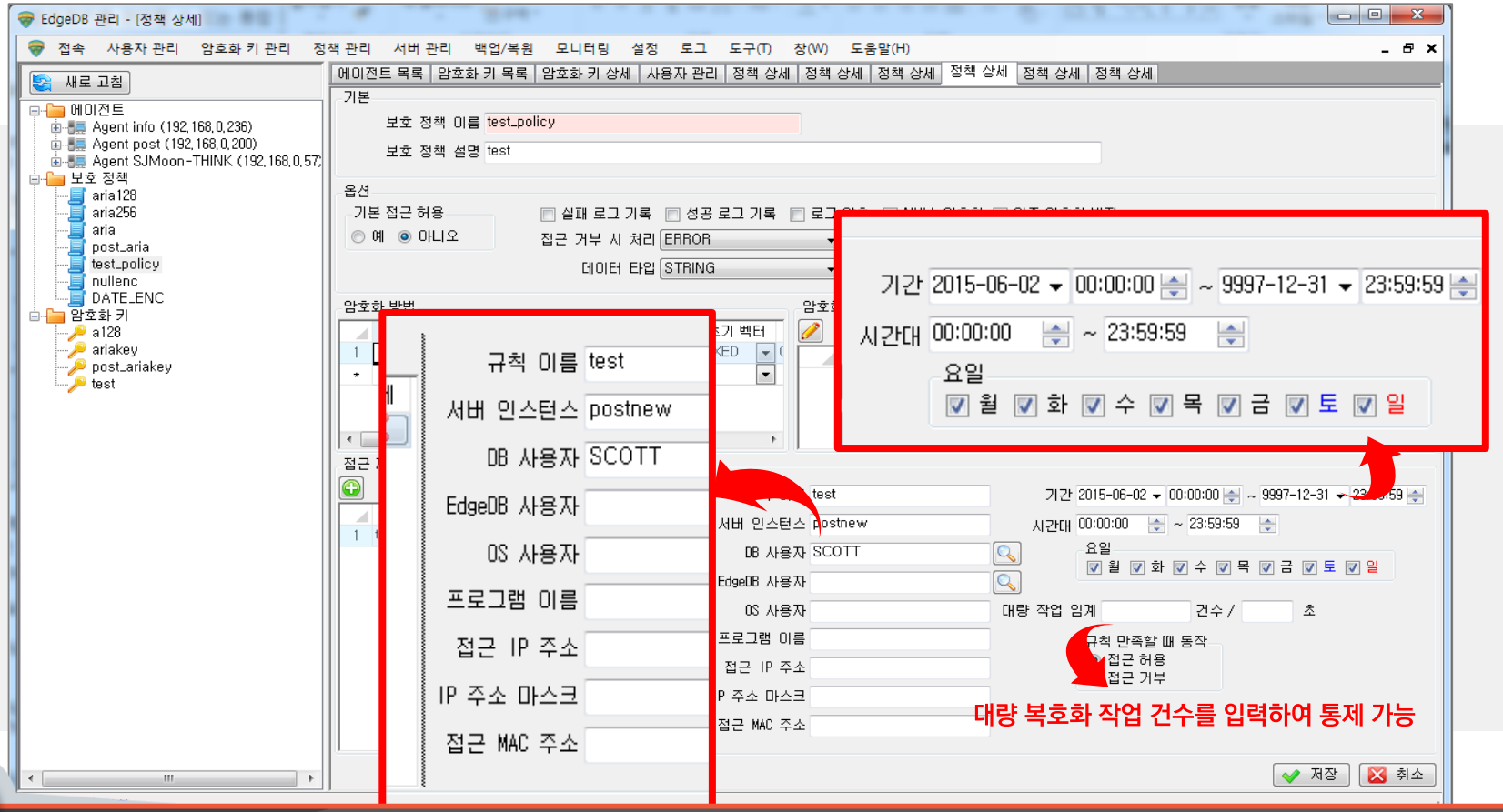
+ Log File, Upload File, Export File 등의 암호화 칼럼 또는 File 전체 암/복호화 제공

8. 장애 감지 및 알림 기능



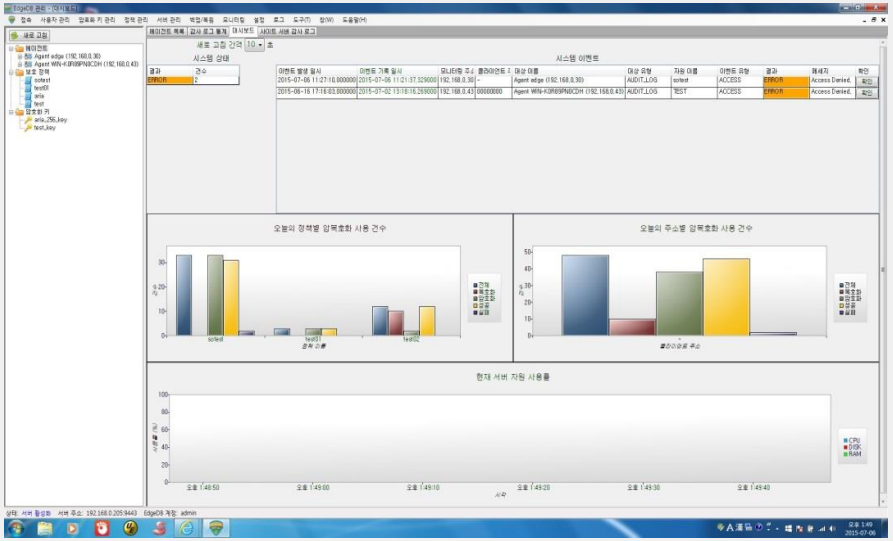
+ 모니터링 기능을 통하여 사전 장애 가능성을 감지해 e-mail을 이용해 정책관리자에게 알림 메일/내용 전달

9. 암호화 컬럼 접근통제 관리

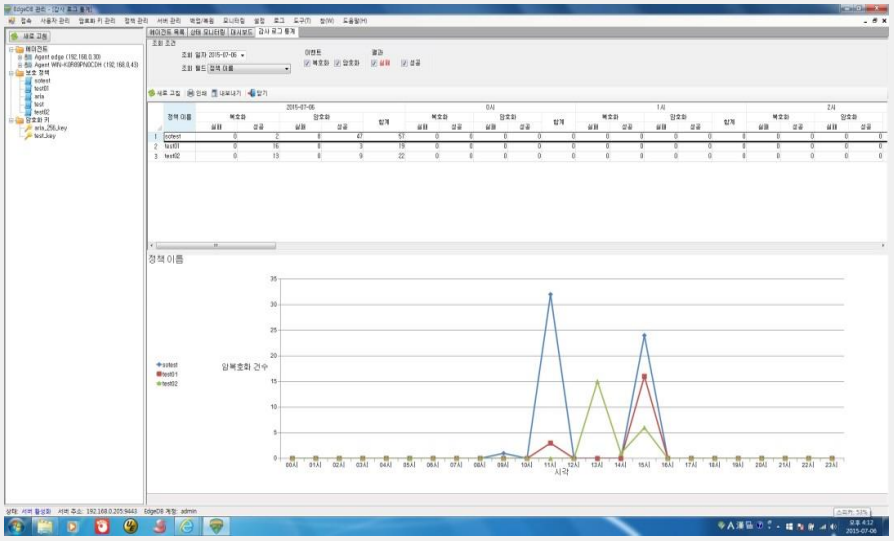


+ 암호화 컬럼에 대한 DB 사용자, IP, 기간, 요일, 시간, 어플리케이션 별 접근통제 가능

10. 실시간 암·복호화 및 상태 모니터링



대시보드

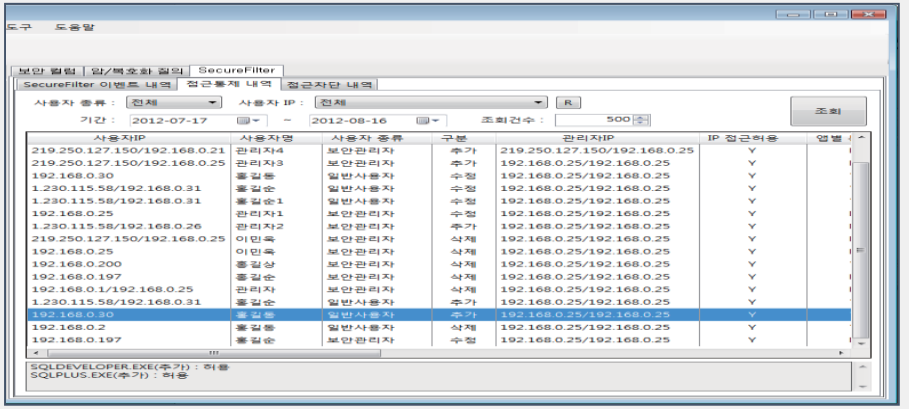


상태 모니터링

+ 관리서버,에이전트의 CPU, DISK, RAM의 사용률과 임계치를 모니터링 하며, 실시간 암/복호화 상태 및 운영서버의 상태 모니터링 제공

11. 비인가 접근 차단 / 통제 및 감사 기능

접근 차단 이력 관리



접근 통제 이력 관리

+ 사용자, IP, Application, 기간, 시간대 별, 요일 별, 접근통제 감사 로그 모니터링 관리
+ 내부자의 악의적인 정보 유출로부터 안전하게 보호

V. Reference

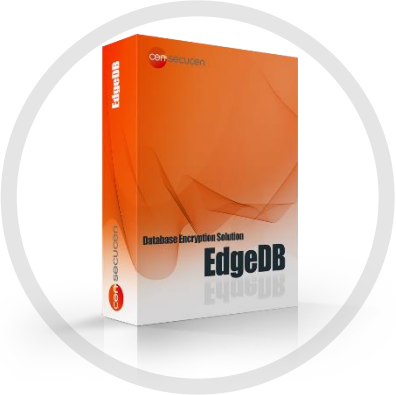
레퍼런스

DB 암호화 솔루션 EdgeDB는 공공 / 금융 / 기업 등 다양한 형태로 구축된 다수의 사례를 보유하고 있는 검증된 솔루션 입니다.

신한금융투자 신협 KLID 한국지역정보개발원 NPS 국민연금공단 National Pension Service ETRI 한국전자통신연구원

우정사업본부 KOREA POST 대구광역시 DAEGU METROPOLITAN CITY 인천광역시 Incheon Metropolitan City NIA 한국정보화진흥원

NFS 국립과학수사연구원 National Forensic Service 국토교통부



대구환경공단 Daegu Environmental Corporation

KATECH 자동차부품연구원 KOREA AUTOMOTIVE TECHNOLOGY INSTITUTE 서울특별시 KITECH 한국생산기술연구원 KIOST 한국해양과학기술원

서울대학교 SEOUL NATIONAL UNIVERSITY h·well 국민건강보험 National Health Insurance Service KRIHS 국토연구원 HIRA 건강보험심사평가원

KIC 한국형사정책연구원 Korean Institute of Criminology SAMSUNG 삼성의료원 국립 한국방송통신대학교 Korea National Open University 여성가족부 Ministry of Gender Equality & Family

VI. ㈜시큐센 소개

6. ㈜시큐센 소개

㈜시큐센 개요

secu cen
(주)시큐센

주식회사 시큐센

대표자 박원규

- '12년 설립 후, 바이오 전자서명 사업을 전개해 온 "㈜시큐센"과, '11년 설립 후, 모바일 보안 솔루션/서비스 사업을 전개해 온 "바른소프트기술㈜"이, '15년 9월 통합 후, 아이티센의 보안부문 전문 계열사로 편입하여, 바이오 전자서명과 모바일 분야의 핀테크 보안 솔루션/서비스 전문기업으로 발전
- '18년 2월1일 아이티센의 금융권 모바일/창구 전자문서 구축분야 전문기업인 "㈜S&TC"를 흡수합병하여 "핀테크 보안기술 전문기업"으로 성장

사업 분야 : 바이오 전자서명, 모바일 보안 솔루션/서비스, 블록체인 기반 융합보안사업

자본금 : 7억 1,562만원

주소 : 서울특별시 영등포구 가마산로 343 콤텍빌딩 3층

전화번호 : 02-3495-0700

팩스 : 02-521-6275

회사설립일시 : 2011년 12월 7일

부문종사기간 : 2011년 12월 ~ 2020년 2월 현재 (8년 2개월)

주 요 연 혁

2011~2020

2020
- 현대카드 블록체인기반 DID APP 구현 사업 수주 및 진행

2019
- 금결원『바이오분산관리 전자서명 기술지원 및 이용기관 연계 협약』체결
- (주)알체라『바이오 전자서명·인증관련 인식기술 제휴계약』체결

2018
- 주식회사 에스엔티씨 합병
- 기술혁신형 중소기업(Inno-Biz)선정

2017
- 라이나 금융 방화벽정책관리 시스템 구축 사업 수주
- 나이스 학교생활기록부 ISP 사업 수주
- 하나금융티아이 '바이오 전자서명' 사업협약 체결

2016
- 국토교통부 '부동산안전거래 통합지원시스템' '바이오 전자서명' 수주
- 공정위 소비자피해구제 종합지원시스템 구축(정보보호시스템) 사업 수주
- 에듀파인시스템 응용SW 유지보수사업 수주(보안컨설팅)
- 기획재정부 국고보조금 통합관리시스템 구축사업 수주(정보보호분야)

2015
- 전북은행FDS(이상거래탐지시스템) 수주 및 구축완료
- LGU+Pay Now FDS 수주 및 구축완료

2015
- 전화번호 안심로그인 서비스 공동사업제휴/런칭('16.1)
- SK그룹사 APT대응솔루션 구축사업 수주
- 금융위원회, 제5차 핀테크 Demo-Day 선정 및 발표
- 아이티센 자회사로 편입

2014
- '바이오 전자서명' 공인인증기술 지정 위한 사전심사 진행
- 외환은행 FDS 프로젝트 수주 및 구축완료
- 롯데카드 안심쇼핑 세이프인증서 부가서비스 런칭

2013
- 안행부 모바일 공통기반 앱보안시스템 구축
- '바이오 전자서명' 특허 3건 등록 및 GS인증 획득
- 스마트폰 도용방지 서비스 출시
- 경남은행 차세대 인터넷 뱅킹 시스템 구축사업 참여

2012
- 외환은행 인터넷뱅킹 앱 위변조방지/난독화 수주/구축

2011
- 법인 설립

서울특별시 서초구 서초동 반포대로 13 아이티센빌딩
ITCEN Bldg., Banpo-daero 13-gil, Seocho-gu, Seoul, Korea
TEL+82-2-3495-0700 FAX+82-2-586-6996

WWW.SECUCEN.COM

시큐센
secucen