



Ready for  
**IBM DB2**  
data server software

국가용  
암호제품  
등록필

행정정보  
보호제품  
인증필

# CubeOne™ 제품 소개

## Plug-In, API (V 2.5)

“색인 검색을 지원하는 대용량 DB 전문 암호화 솔루션”

# Contents

---


- ❖ DBMS 암호화 솔루션 개요
- ❖ CubeOne™ 소개
- ❖ CubeOne™ 적용 사례
- ❖ Why CubeOne™



# DBMS 암호화 솔루션 개요

1. (주)이글로벌시스템 소개
2. 개인정보보호 기준
3. DBMS 암호화 어떻게 구성할 것인가?
4. DBMS암호화 솔루션 선택 기준

## 일반 현황 및 연혁

|                 |  |             |     |              |              |
|-----------------|--|-------------|-----|--------------|--------------|
| <b>회사명</b>      | (주)이글로벌 시스템  | <b>대표이사</b> | 강희창 | <b>설립 일자</b> | 2004. 10. 7. |
| <b>주요 사업 내용</b> | (주)이글로벌시스템은 데이터베이스에 대한 보안, 관리, 튜닝에 대한 많은 경험 및 Know-How를 바탕으로 최고 성능의 DB 암호화 솔루션을 개발 공급하는 DBMS 보안 전문 회사입니다.<br>제품 목표는 소중한 DB Data를 암호화 하여 Data 유출을 원천 방지 함으로써 고객사의 피해를 최소화함은 물론, Downtime 없이 업무를 처리 (무 중단) 할 수 있도록 하는데 있습니다. |             |     |              |              |
| <b>주요 개발 제품</b> |  <p>Column Level Encryption Solution for Index Searching</p>  |             |     |              |              |

- 2014**
  - 2014. 12 : 금융결제원 주택청약/납부자료이체(시범사업) DB암호화 구축완료
  - 2014. 12 : 동부화재 차세대 및 정보계시스템 DB암호화 구축완료
  - 2014. 11 : 한국예탁결제원 개인정보보호강화사업 DB암호화 구축 완료
  - 2014. 04 : 통계청 행정자료 DW DB암호화 분리발주 구축
  - 2014. 03 : 관세청 4세대 국가관세종합정보망 구축 2단계 DB암호화 수주
- 2013**
  - 2013. 12 : 대법원 채권담보/기타등기 DB암호화 구축완료
  - 2013. 06 : 전국 25개 의료원 OCS/EMR시스템 DB암호화 구축완료
  - 2013. 05 : 한국철도공사(KORAIL) 예약발권시스템/영업관리시스템 DB 암호화 구축완료
  - 2013. 04 : 국세청 차세대 국세행정시스템 전면 개편 2단계 사업 수주
- 2012 ~ 2010**
  - 2012. 07 : 대법원 가족관계등록정보시스템(내.외부) DB암호화 구축완료
  - 2012. 12 : 대법원 2012년 유관기관연계, 인증시스템 DB암호화 구축완료
  - 2011. 06 : 현대/기아자동차 DB암호화 계약(DB서버 100여대)
  - 2011. 06 : 통계청 행정자료 DW DB암호화 분리발주 구축
  - 2011. 11 : 대법원 2011년 등기정보시스템 DB암호화 분리발주 구축완료
  - 2011. 12 : 조달청 나라장터 DB암호화 구축
  - 2010. 04 : 교육부 NEIS 통합 DB 암호화 선정 (140대)
  - 2010. 04 : 국방부 자료전달체계 사업 구축
  - 2010. 07 : 행안부 G4C 및 통합인증GW 사업 구축
  - 2010. 07 : 현대/기아자동차 (표준 선정)
  - 2010. 07 : 현대 백화점/홈쇼핑 그룹 수주 (29대, 표준 선정)
  - 2010. 07 : 국가용 암호제품 재 검증 완료 (4/21 보안 요건 기준)
  - 2010. 08 : 행정안전부 행정정보 보호제품 등록
  - 2010. 09 : 대법원 등기정보 시스템 DB암호화 구축
- 2009 ~ 2004**
  - 2009. 06 : SKT DB암호화 사업 수주 (160대)
  - 2009. 11 : 신세계그룹 DB암호화 사업 구축
  - 2009. 12 : 국가용 암호제품 등록 (지정번호 NCPL-2009-030)
  - 2008. 06 : 2008 상반기 히트상품 선정 (전자신문, 디지털타임즈)
  - 2008. 08 : 국정원 암호모듈검증
  - 2008. 09 : 대법원 등기정보 시스템 DB암호화 구축
  - 2007. 01 : TTA GS 인증
  - 2006. 12 : NEP 인증 (산업자원부 기술표준원)
  - 2005. 12 : DB암호화 제품 CubeOne Plug-In V1.0 출시
  - 2004. 10 : 주식회사 이글로벌시스템 설립**



# 1. (주)이글로벌시스템 소개



## 제품의 인지도 및 고객 증가율

CubeOne™은 경쟁제품들에 비해 다음과 같은 면에서 절대 우위에 있습니다.

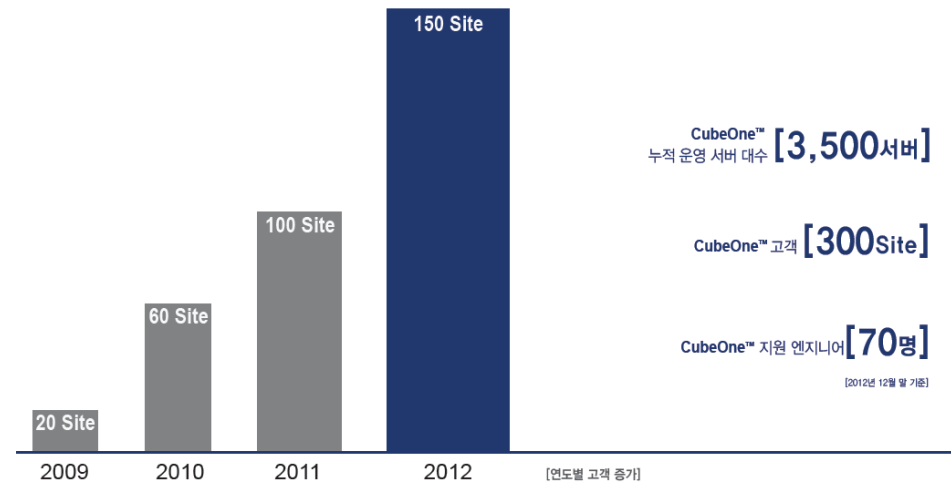
CubeOne™은 대용량 DB암호화 분야에서 절대 강자로 인식되고 있습니다. 이것은 기술력과 안정성이 없이는 불가능한 일입니다. 이러한 고성능/고품질로 인해 고객 선호도 면에서는 자타가 공인하는 국내 1위의 제품입니다.

## 시장 인지도



## 고객 증가율

안정성과 성능을 중요한 경쟁력으로 하는 대용량 DB 암호화 시장에서는 월등한 우위를 점유하고 있습니다.



### 개인정보 보호 관련 여건 변화

개인정보보호법안 및 정보통신망법에 따른 개인정보의 기술적·관리적 보호조치 개정안(방통위 고시)이 2010년 1월 29일부터 시행됨에 따라 법규 위반 시 사안에 따라 시정명령, 과태료, 대표이사의 형사처벌 등의 제재를 받게 됩니다.  
이에 따라 주요 개인정보에 대하여 **DBMS 암호화**를 적용하여 DBMS 보안 기능을 갖추어야 합니다.

#### ● 개인정보 취급자의 한정

- 개인정보 취급자 및 관리책임자만이 개인정보시스템에 접근 가능함.

#### ● 개인 정보 암호화 보관(법정 암호화 대상)

- **개인정보보호법** : 주민번호, 운전면허번호, 여권번호, 외국인등록번호
- **정통망법** : 주민번호, 신용카드번호, 계좌번호 3대 정보는 반드시 암호화하여 보관하여야 함.
- 고객 비밀번호 및 생체 정보는 복호화가 불가능한 일방향 암호화 알고리즘을 적용 하여 보관하여야 함.

#### ● 개인정보 처리시스템에 대한 접근통제

- 불법 접근 및 개인정보이상 유출징후에 대하여 접근 통제를 하여야 함.

#### ● 개인정보시스템 접근 로그 저장 및 위변조 방지 규정

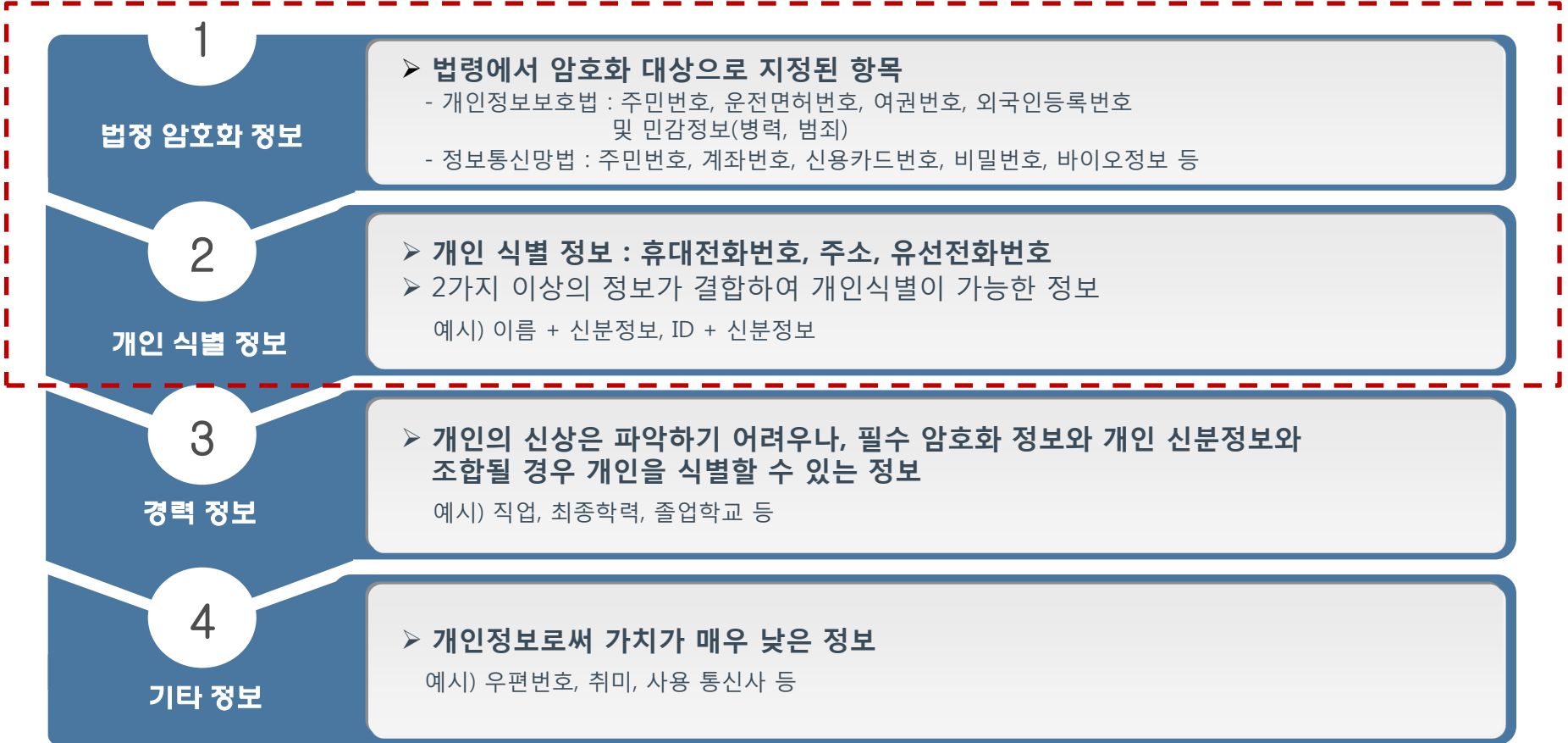
- 기간 통신사업자는 2년, 사업자는 최소 6개월 이상 접근 로그를 보관 하여야 함.

❖ CubeOne™은 관련 법규에서 요구하는 기술적보호조치 기준을 만족하는 구조를 제공 합니다.

## 암호화 대상 개인정보 정의 및 분류 기준

- ❖ 개인정보 취급자(개인정보를 취급하는 사용자) 추출 및 최소화
- ❖ 개인정보 구분 : 각 개인정보의 성격에 따라 보호 우선순위를 책정하여 관리(외부 고객 & 내부 직원 정보)

### 암호화 대상





# 3. DBMS 암호화 어떻게 구성해야 할 것인가?

## 국정원 인증

국가사이버안전센터  
National Cyber Security Center

센터소개 | 사이버위기관리 | **검증** | 자료실 | 신고 및 상담

보안적합성 검증 | 암호모듈검증

"국가사이버안전센터는 IT보안성 확보를 위해 보안적합성 검증 및 암호모듈 검증 업무를 수행하고 있습니다."  
IT Security Certification Center

Home > 검증 > 암호모듈검증 > 검증필 암호모듈 목록

검증필 암호모듈 목록

모듈 명칭: CubeOne

| 암호모듈명        | 검증번호          | 개발사         | 모듈형태      | 검증일      | 호적번호일    |
|--------------|---------------|-------------|-----------|----------|----------|
| CubeOne V2.5 | NCPL-2011-004 | (주)이글로비스시스템 | S/W(DB암호) | 20110223 | 20160601 |
| CubeOne V2.5 | NCPL-2009-030 | (주)이글로비스시스템 | S/W(DB암호) | 20091230 | 20160601 |

전체목록인쇄

국가사이버안전센터  
IT Security Certification Center

센터소개 | 사이버위기관리 | **검증** | 자료실 | 신고 및 상담

보안적합성 검증 | 암호모듈검증

"국가사이버안전센터는 IT보안성 확보를 위해 보안적합성 검증 및 암호모듈 검증 업무를 수행하고 있습니다."  
IT Security Certification Center

Home > 검증 > 암호모듈검증 > 검증필 암호모듈 목록

검증필 암호모듈 목록

모듈 명칭: Klib

| 암호모듈명          | 검증번호          | 개발사   | 모듈형태       | 검증일      | 호적번호일    |
|----------------|---------------|-------|------------|----------|----------|
| KLIB_SQL v1.0  | CM-95-2019.10 | 고려대학교 | S/W(라이브러리) | 20141017 | 20191017 |
| KLIB_lite V2.0 | CM-06-2019.1  | 고려대학교 | S/W(라이브러리) | 20140123 | 20190123 |

Home > IT보안인증사무국 > 암호모듈검증 > 검증필 암호모듈 목록

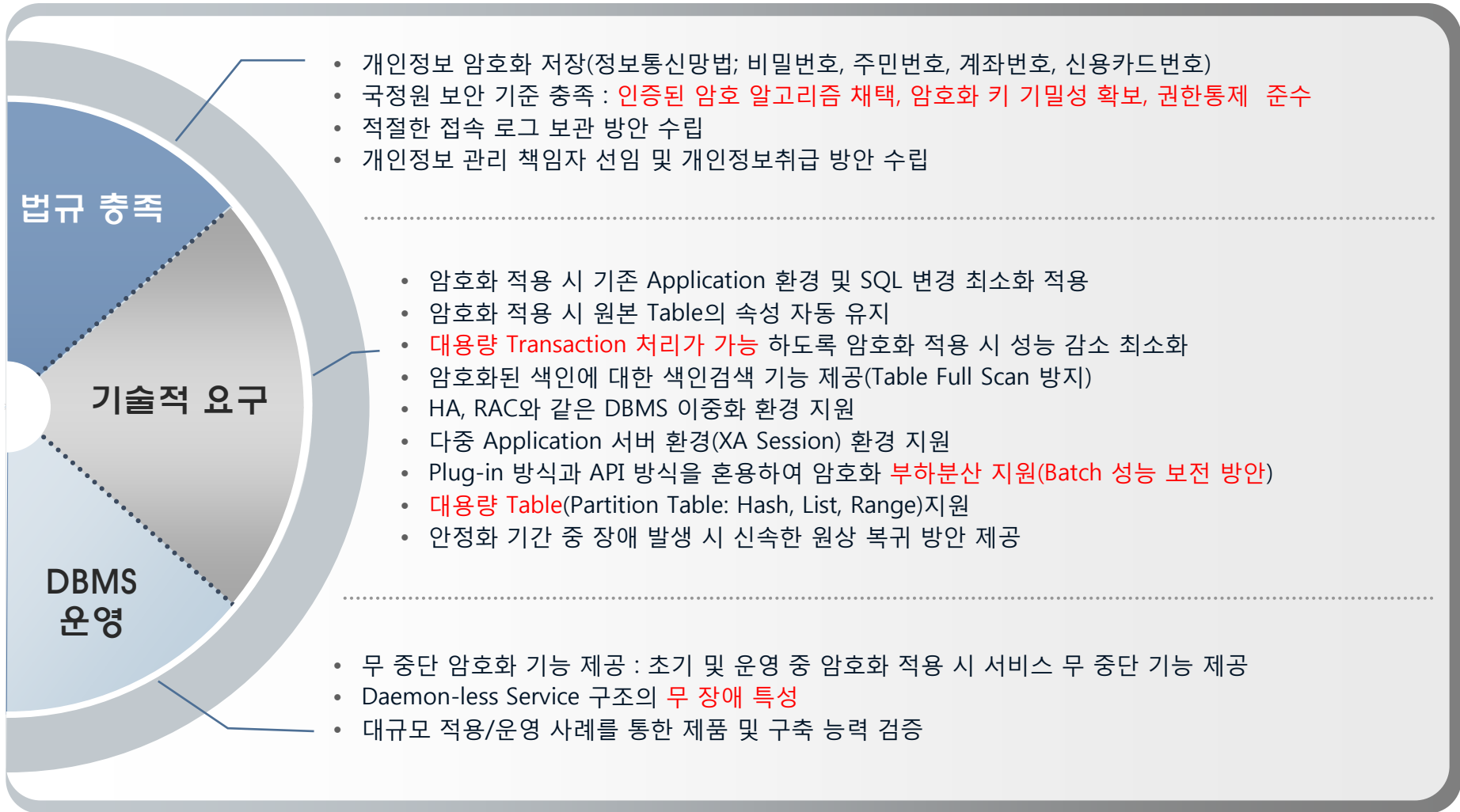
검증필 암호모듈 목록

| 암호모듈 명칭     | CubeOne V2.5  |
|-------------|---|
| 적용기준        | (구)국가공 암호제품 시험기준  |
| 타 암호모듈 적용현황 |   |
| 보안등급        | 보안등급 1  |
| 비고          | DB 암호모듈<br>라이브러리형 암호모듈 탑재후 정합 및 추가시험 완료<br>2015.1 암호안전성 강화 완료 |

※ 국가정보원 발행 검증서는 라이브러리 최초 검증시에만 문서로 발행하며 이후에는 IT보안인증사무국의 홈페이지 "검증필 암호모듈 목록"에 등록 게시로 대체합니다.



## DBMS 암호화 프로젝트 진행 시 고려사항



# 4. DBMS암호화 솔루션 선택 기준

## DBMS 암호화 솔루션 선택 시 필수 고려사항

| 기능 요소        | 내 용   | 미 지원 시 문제점   |
|--------------|---|--|
| 안전한 알고리즘     | <u>안전한 알고리즘</u> 으로 최고의 보안성 보장                           | <u>보안성 미비</u>  |
| 안전한 키 관리     | 암호모듈검증기준이 요구하는 <u>안전한 키관리 (불법접근 불가, 키 제로화)</u>          | <u>보안성 상실</u> (대문 열쇠를 벽에 걸어둔것과 같음)   |
| 인덱스 암호화 및 검색 | 인덱스도 암호화 되어야 하며 <u>암호화된 인덱스를 통한 색인검색이 지원될 것</u>         | 인덱스를 통한 색인검색이 안되면 수백 배나 더 시간이 걸리는 <u>Full Table Scan이 발생함</u> . (결국 비밀번호 정도만 암호화할 수 있음.) |
| 성능           | 구축성능 및 <u>검색성능의 저하가 최소일 것</u>                           | 구축성능이 느리면 작업시간을 잡기가 어려워지며, 구축 후 검색성능이 느리면 <u>고객 서비스에 지장을 줌</u> .                         |
| 가용성          | 장시간이 소요되는 DB암호화 작업으로 인한 <u>서비스중단이 없거나 최소일 것</u>         | 수 십 시간 이상 DB가 정지 하므로 <u>서비스 중단을 초래</u> (24x365 서비스 업무에서는 도입자체가 불가능해짐)                    |
| 최소의 제약사항     | <u>제약사항이 가능한 한 적을 것 (NULL 데이터 암호화, PK/UK 암호화 가능할 것)</u> | 암호화 적용 자체가 이러한 제약사항들로 인해 원래 목적인대로 구축이 불가능해짐.   |

※ 참고자료 : \* 논문, "개인정보 침해사례를 통한 데이터베이스 보호에 관한 연구 - 김정상",  
 \* ISEC 세미나자료, "DB보안 기술의 현황과 문제점 분석 - 김정상",  
 \* 분석보고서, "금융권 DB암호화 솔루션 도입 시 고려사항 검토 - 금융보안연구원",  
 "금융권 정보보호 이슈분석 - 금융결제원"

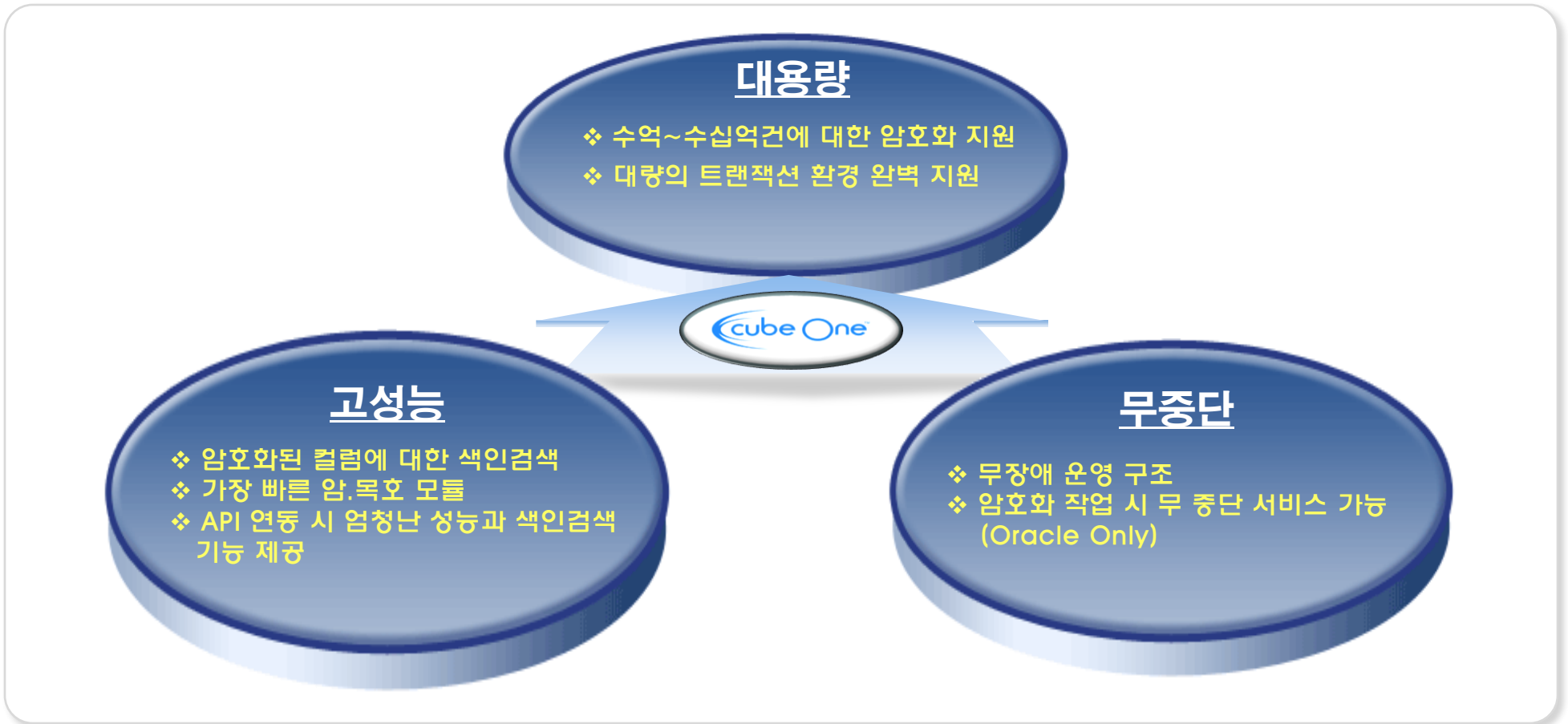
# CubeOne™ 소개

1. CubeOne™ 구성
2. CubeOne™ 주요 특징점
3. CubeOne™ 성능
4. Reference & Success Story
5. Why CubeOne™




## CubeOne™ 제품 개요

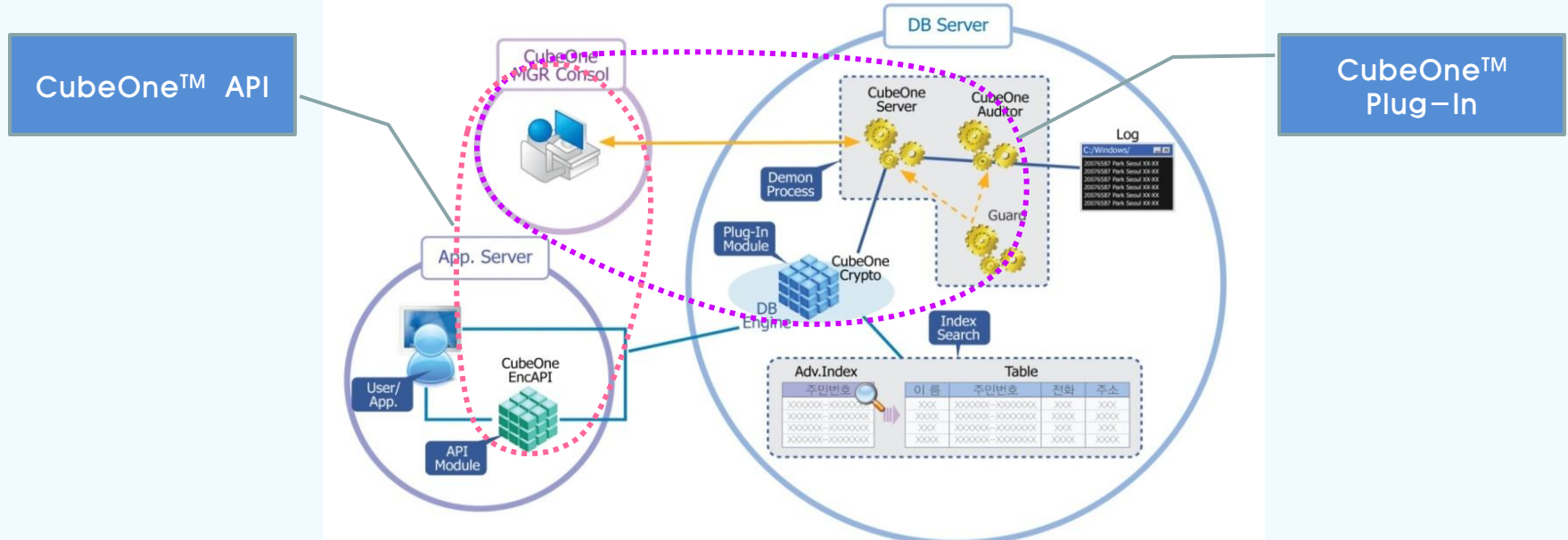
- ❖ CubeOne™은 대용량 DB암호화 전문 제품입니다.
- ❖ 암호화된 인덱스를 이용하여 검색을 가능하게 한 기술로 기술표준원 으로부터 우수신제품인증(NEP)를 받은바 있으며, 또한 300여 사이트를 완벽히 구축.운영을 성공 시킨 세계적으로 유례가 없는 고성능의 대용량, 무중단 DB보안제품입니다.



## CubeOne™ 제품군

|      |  |   |
|------|--|---|
| 제품명  | CubeOne Plug-In  | 제품모양  |
| 제품버전 | Ver 2.5  |  |
| 제품구성 | <ul style="list-style-type: none"> <li>CubeOne™ Plug-In : Oracle, MS-SQL, DB2, Tiberio, Informix, MySQL, GreenPlum, TeraData, Sybase IQ, PostgreSQL, Altibase 등</li> <li>CubeOne™ API : Any DBMS, SAM/TXT File</li> <li>CubeOne™ for SAP</li> <li>CubeOne™ Options : Security Server, API Handler</li> </ul> |   |

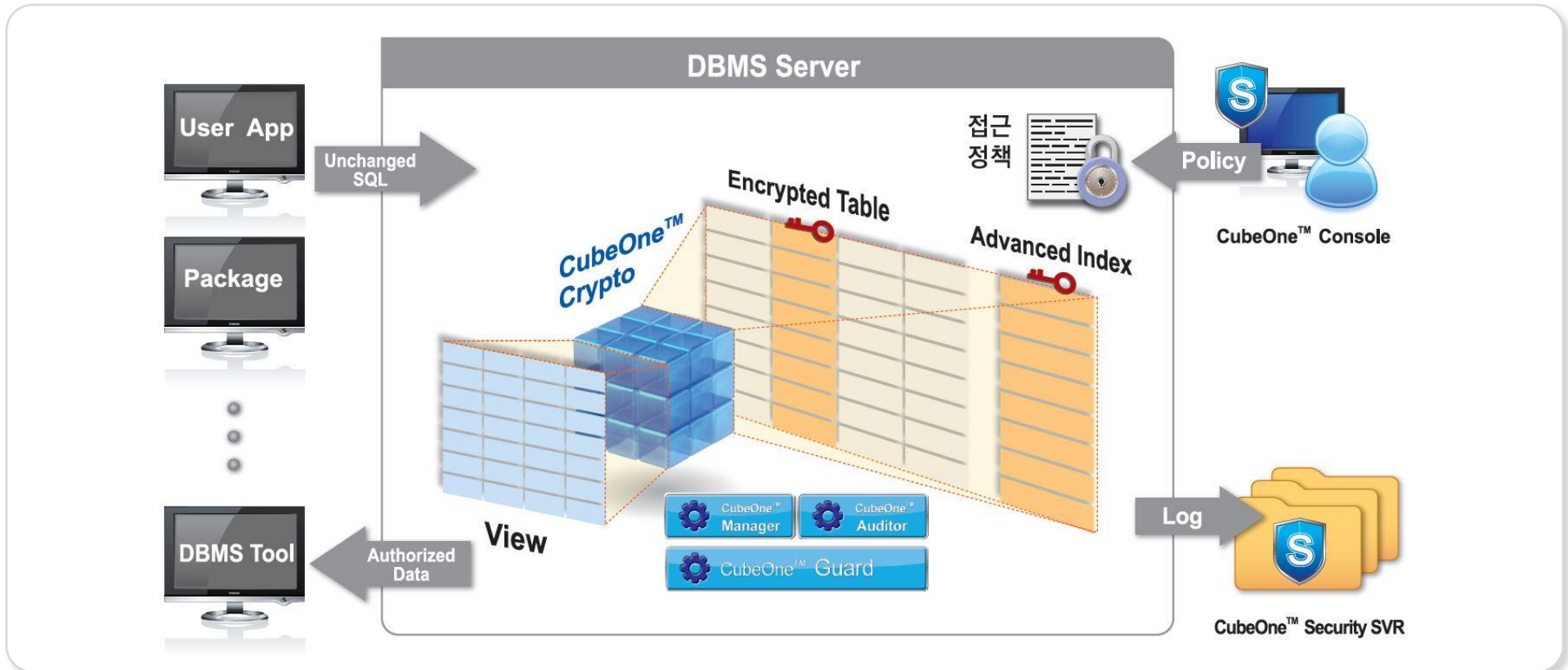
### CubeOne™ 제품군 구성도



※ CubeOne Plug-In과 API간의 Hybrid 형태 구성 지원

## CubeOne™ Plug-In 소개

- ❖ **Application 독립성** : App에서 사용하는 SQL의 수정을 최소한으로 하여 적용 가능
- ❖ **무중단 구축** : 초기 암호화 적용 및 암호화 컬럼 추가 시 무중단 암호화 적용(Oracle Version)
- ❖ **암호화 색인 검색** : 암호화 되어 저장된 Index 검색기능, 암호화 적용 후 Application 성능 보장
- ❖ **빠른 암호화 성능** : 암/복호화 시 시스템 부하를 최소화 하는 구조 (타 제품 대비 2~3배 성능)



## CubeOne™ Plug-In 특징점

### 색인 검색

- ❖ 암호화된 데이터 색인 검색 가능
- ❖ 이점 : 수 많은 운영사이트에서 기능이 검증된 암호화 색인검색 기능을 사용, Table Full Scan 방지
- ❖ 제약 : Oracle 이외의 DB는 수정 필요

### 무 중단 암호화

- ❖ 암호화 구축 중에도 DB 운영 가능 (DB, 리스너 재기동 및 Long time Locking 없음)
- ❖ 이점 : 영업손실 없이 수시로 구축 가능. Re-org 효과 발생

## CubeOne™ Plug-In

- ❖ Application에서 사용하는 SQL의 수정 없이 적용 가능
- ❖ 비정형 SQL Tool 지원(오렌지, Toad)
- ❖ 이점 : API 형태에 비해 거의 수정 없이 적용
- ❖ 제약 : 특정 형태의 문장의 경우 수정 필요

### Application 독립성

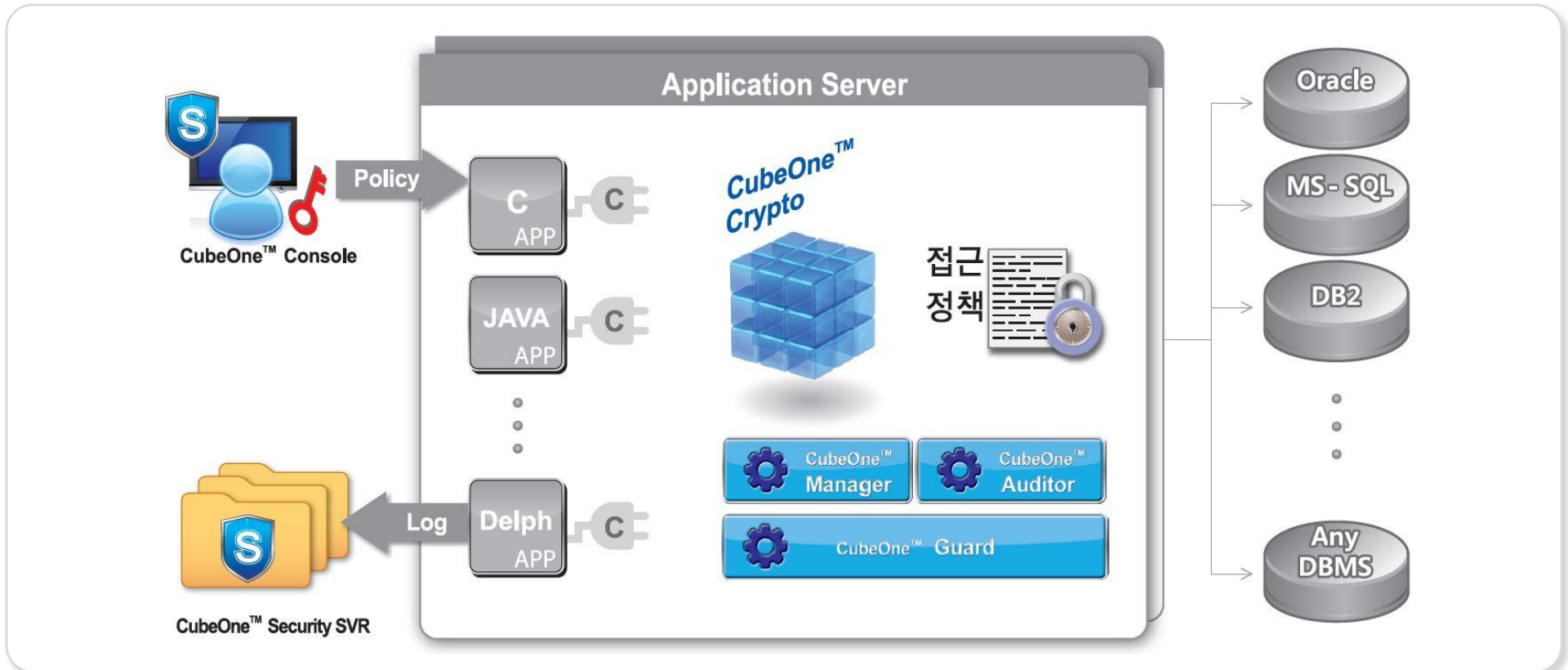
- ❖ 기능 : 2~3배 짧은 구축시간 및 빠른 처리성능
- ❖ 이점 : 시스템 부하시간 최소화

### 빠른 성능



## CubeOne™ API 소개

- ❖ DBMS에 종속적이지 않는 이기종 DBMS간의 암호화 기능 제공
- ❖ 간단한 Daemon-less 서비스 구조로서 **무장애** 구조 및 **고성능** (경쟁제품 대비 약 50% 이상 빠름)
- ❖ DBMS서버에 **Hybrid**(Plug-In & API) 방식 적용 시 **Local 배치** 업무 시 총 수행시간 단축
- ❖ 암호화 필드 색인검색 / 비정형 SQL의 처리 / 초기 무중단 암호화 구축을 위하여 API Handler 별도 제공 (Option)





## CubeOne™ API 특징점

### 색인 검색

- ❖ 암호화된 데이터 색인 검색 가능
- ❖ 이점 : 수 많은 운영사이트에서 기능이 검증된 암호화 색인검색 기능을 사용, Table Full Scan 방지
- ❖ 제약 : API Handler 적용 시 가능 (Oracle, MS-SQL, DB2 등)

### 비정형 SQL 지원

- ❖ API Handler 사용으로 DBMS 관리 Tool을 이용한 DBMS 작업 지원
- ❖ 이점 : 초기 암호화 구축 지원. 비정형 SQL Tool 지원 (오렌지, Toad)
- ❖ 제약 : Plug-In이 지원되는 DBMS만 지원

## CubeOne™ API

- ❖ 간단한 Deamon-less 구조로 처리성능 배가
- ❖ 이점 : 경쟁 제품 대비 약 50% 이상 빠름 (Batch 업무 시 총 수행시간 단축)
- ❖ Plug-In 제품과 Hybrid 구성 시 월등한 Batch 수행 성능 보장

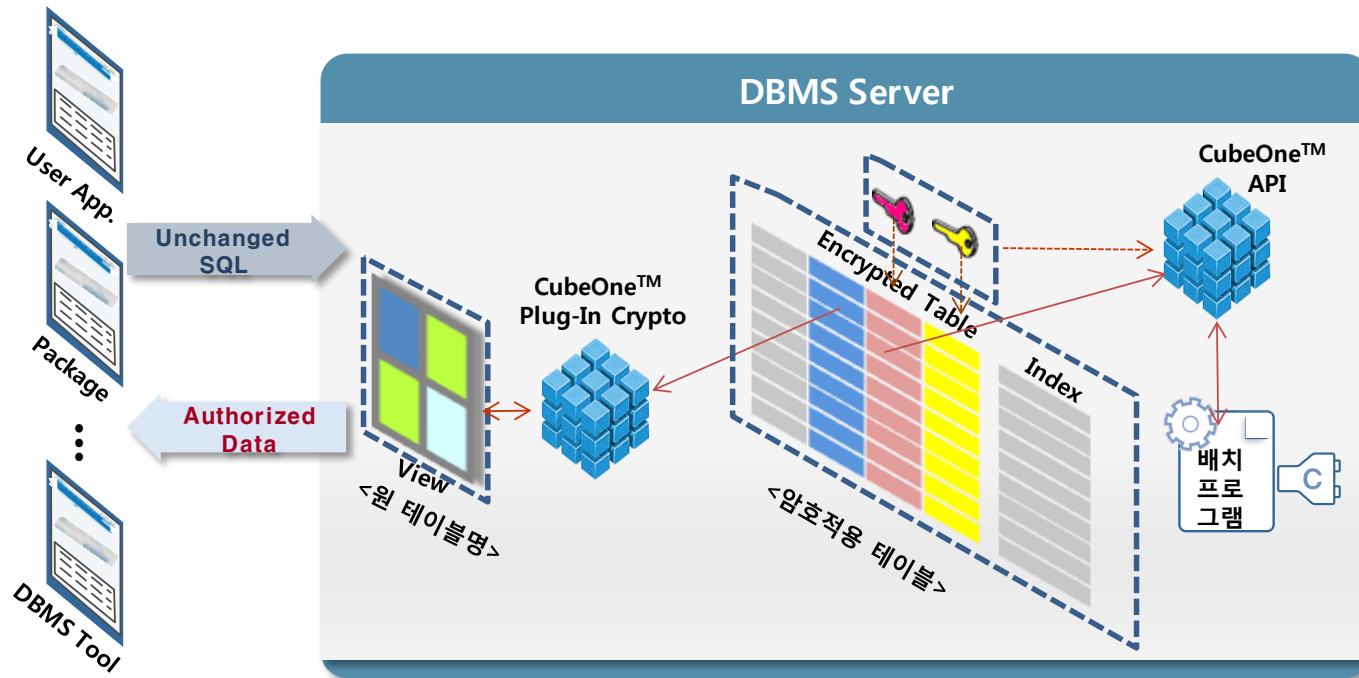
### 뛰어난 성능

- ❖ DBMS 암호화 적용이 어려운 TERADATA, Sybase, Informix등의 이 기종 DBMS 환경 지원
- ❖ 기존 Plug-In 지원 DBMS와 암호화 Key 공유

### 이 기종 DBMS 지원

## 고성능 Hybrid 구성

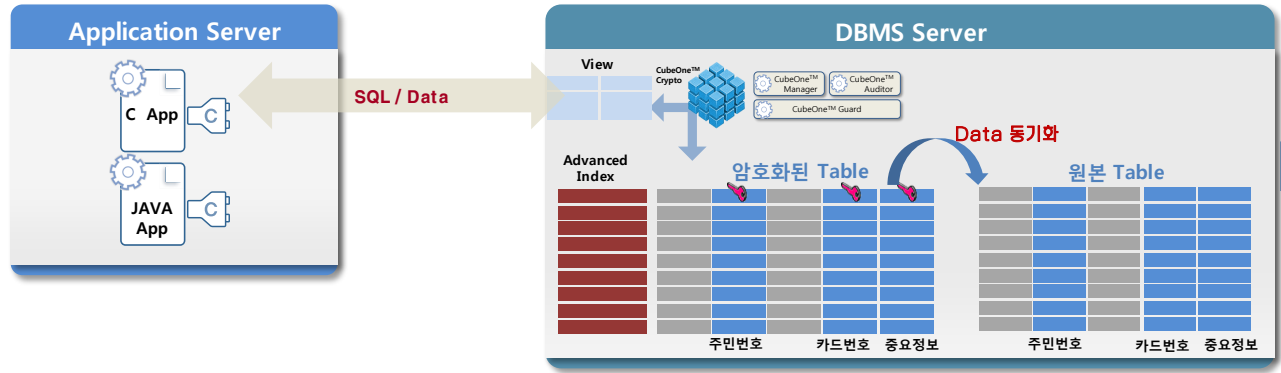
- ❖ CubeOne™은 암호화 적용성이 우수한 Plug-In과 성능이 우수한 API를 동시에 사용할 수 있는 Hybrid 구성을 지원 합니다.
- ❖ 일반적인 OLTP성 업무와 배치 업무에 대하여는 Plug-In으로 처리하고, 응답시간이 중요한 OLAP성 업무에 대하여 한정적으로 API를 적용하면, 암호화 시 가장 문제가 되는 성능 저하를 최소한으로 하여 암호화 서비스를 구축 할 수 있습니다.
- ❖ 본 구성은 [대형 통신사](#)와 [유통사](#)에서 그 안정성과 성능이 입증 되었습니다.



※ 본 구성을 채택할 경우 API 적용에 따른 Application 수정이 필요합니다.

**암호화 적용 후 장애발생 시 신속한 원상복구**

**암호화된 테이블로 서비스 Open**



**서비스 장애 발생 → 원상 복구 결정  
Dual Sync Mode 해제**

**원본(평문) 테이블로 서비스 전환**

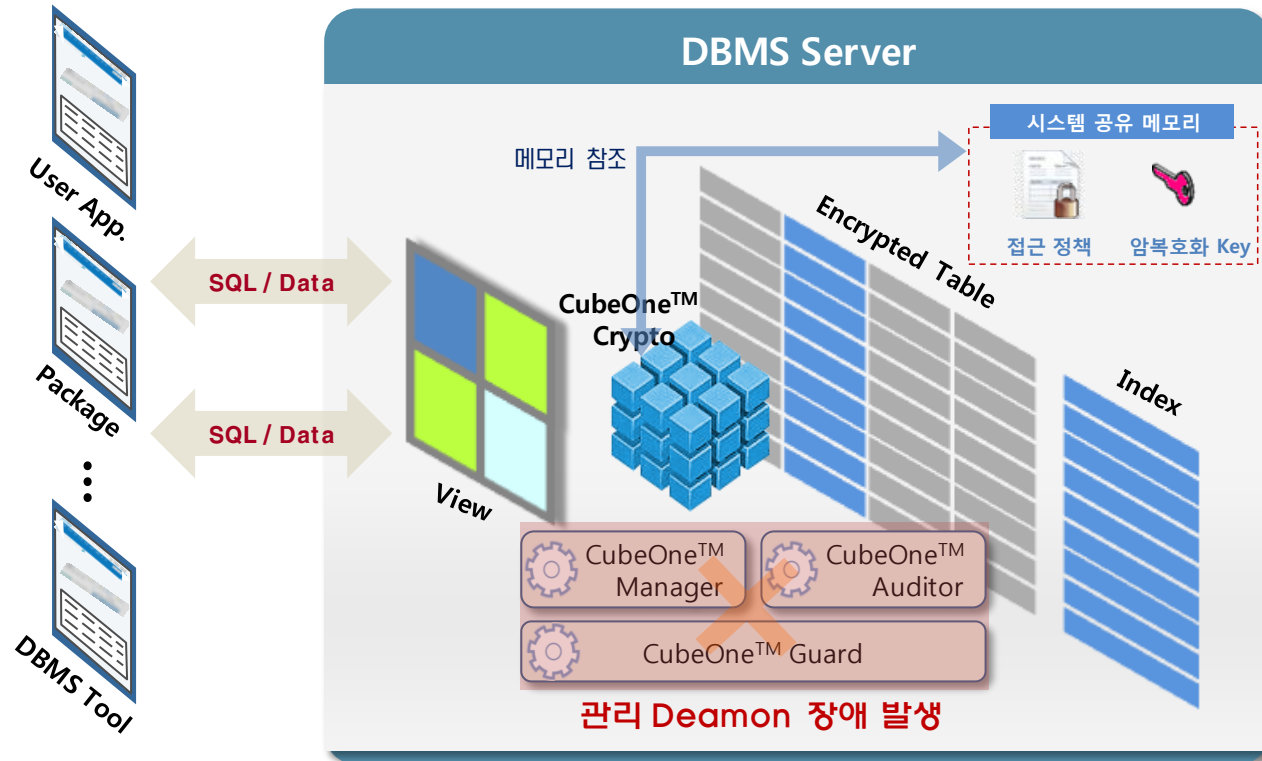
**전환시간:  
수초~수분**



※ 본 구성은 암호화 서비스 안정화기간 중에만 사용하여야 하며, 서비스 안정화 이후 원본(평문) 테이블은 삭제 하여야 합니다

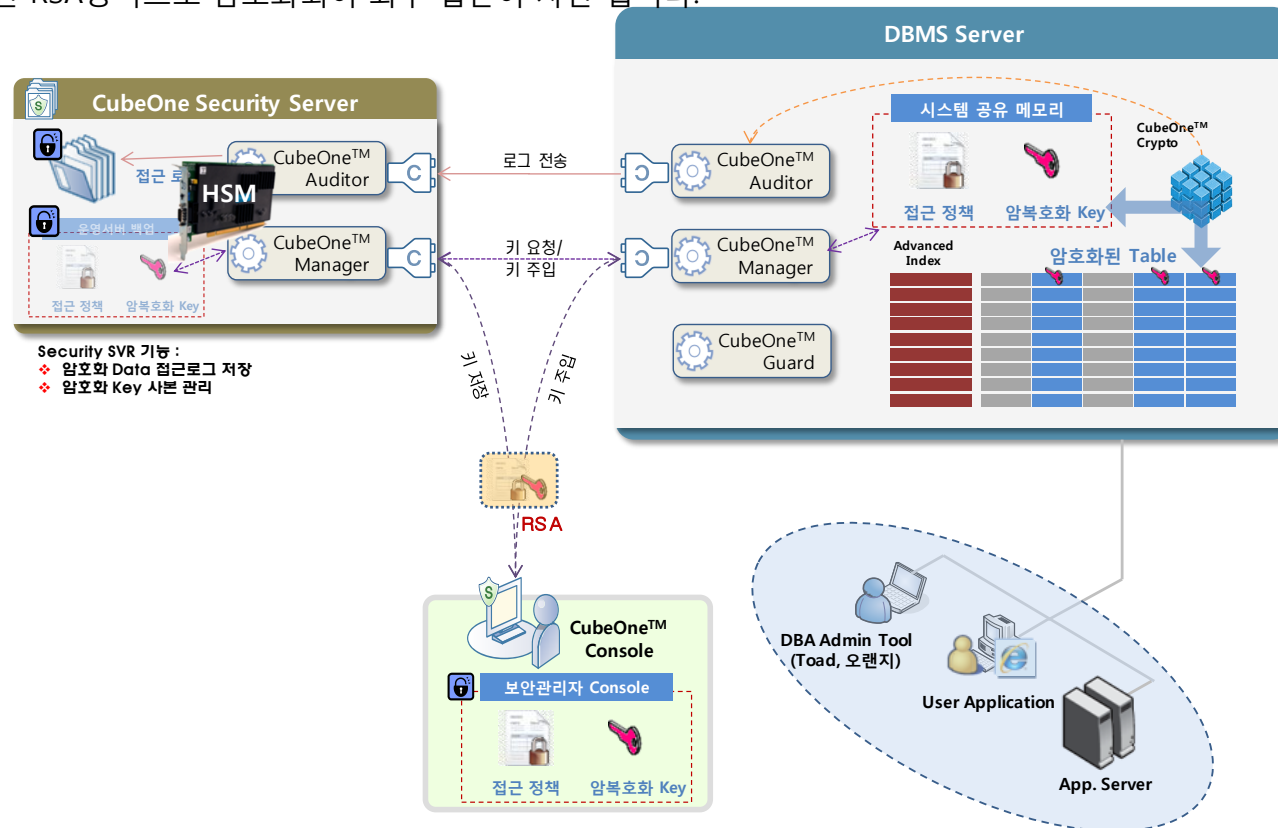
## Daemon-Less 서비스 구조 (무장애 구조)

- ❖ CubeOne™의 암호/복호화 서비스는 관리 Daemon의 도움 없이 CubeOne™ Crypto에 의하여 단독 수행되며, Memory 상에 존재하는 Key와 정책을 참조하여 암호/복호화 작업을 수행 합니다.
- ❖ 단, 관리 Daemon의 장애 발생시 새로운 Key와 정책의 반영(CubeOne™ Manager), 접근 로그 저장(CubeOne™ Auditor)과 같은 작업은 Daemon 재 기동 시까지 정지 됩니다.



## 안전한 암호화 Key 및 접근정책 관리

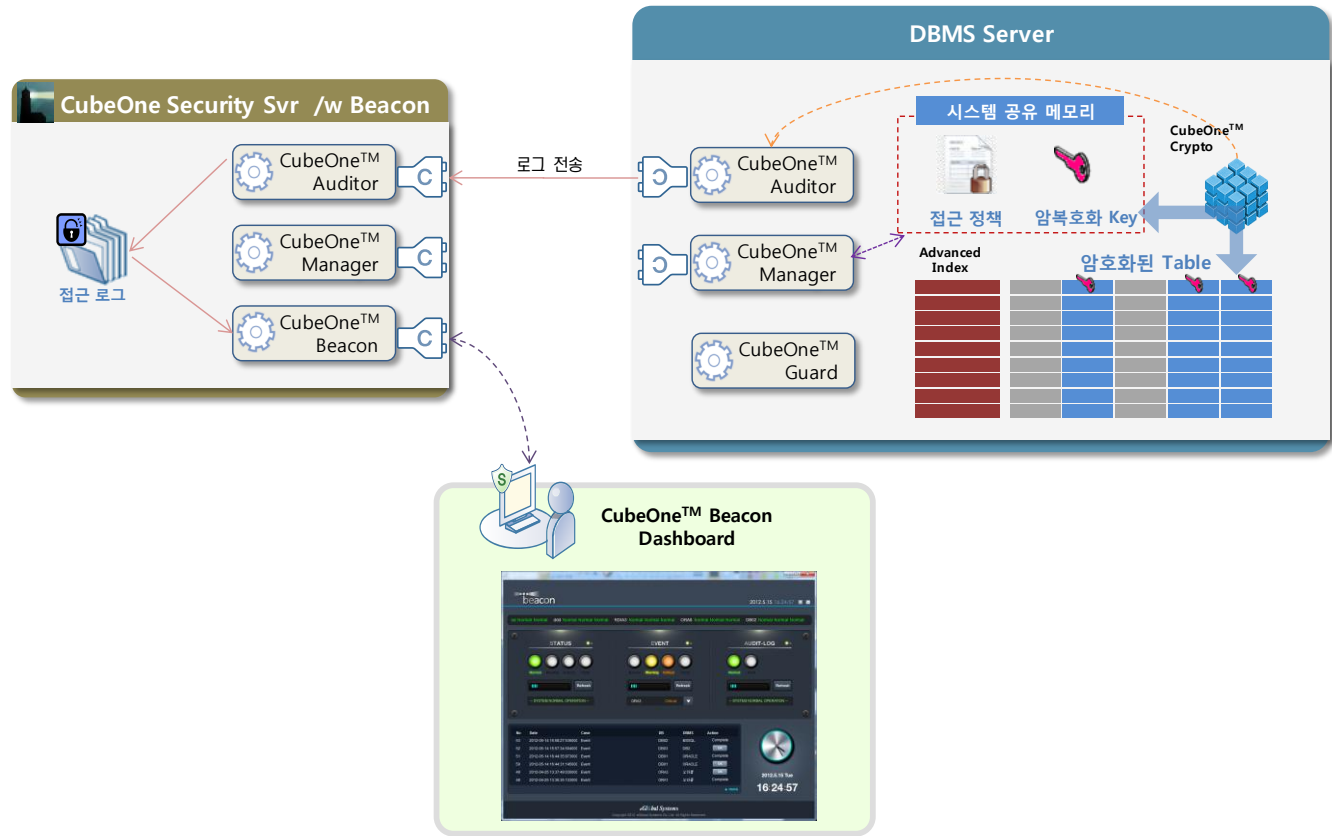
- ❖ 암호화 키와 Master키는 분리되어 HSM에 저장(Optional) 할 수 있으며, 암호화키는 DBMS에 저장하지 않으며, 메모리에 상주시켜, 사용 후 모듈 종료 시 **키 제로화** 됩니다. (암호키를 DB나 파일에 저장한 제품은 실수 또는 고의로 키 컬럼을 Update 또는 Delete하는 경우 서비스가 불가능해 짐.)
- ❖ 키 주입 시 안전한 RSA방식으로 암호화되어 외부 접근이 차단 됩니다.



※ CubeOne Security Server는 Option 입니다.

## 암호화 상태 모니터링 (대량 복호화 방지)

- ❖ CubeOne™ Security Server의 구성에 Add On 하여 Beacon 구성하면 전용 Dashboard를 통하여 CubeOne™이 적용된 시스템의 암호화 처리상태 통합 모니터링을 지원 합니다.
- ❖ 인가된 사용자의 대량 복호화 요청을 효과적으로 제어 할 수 있습니다.

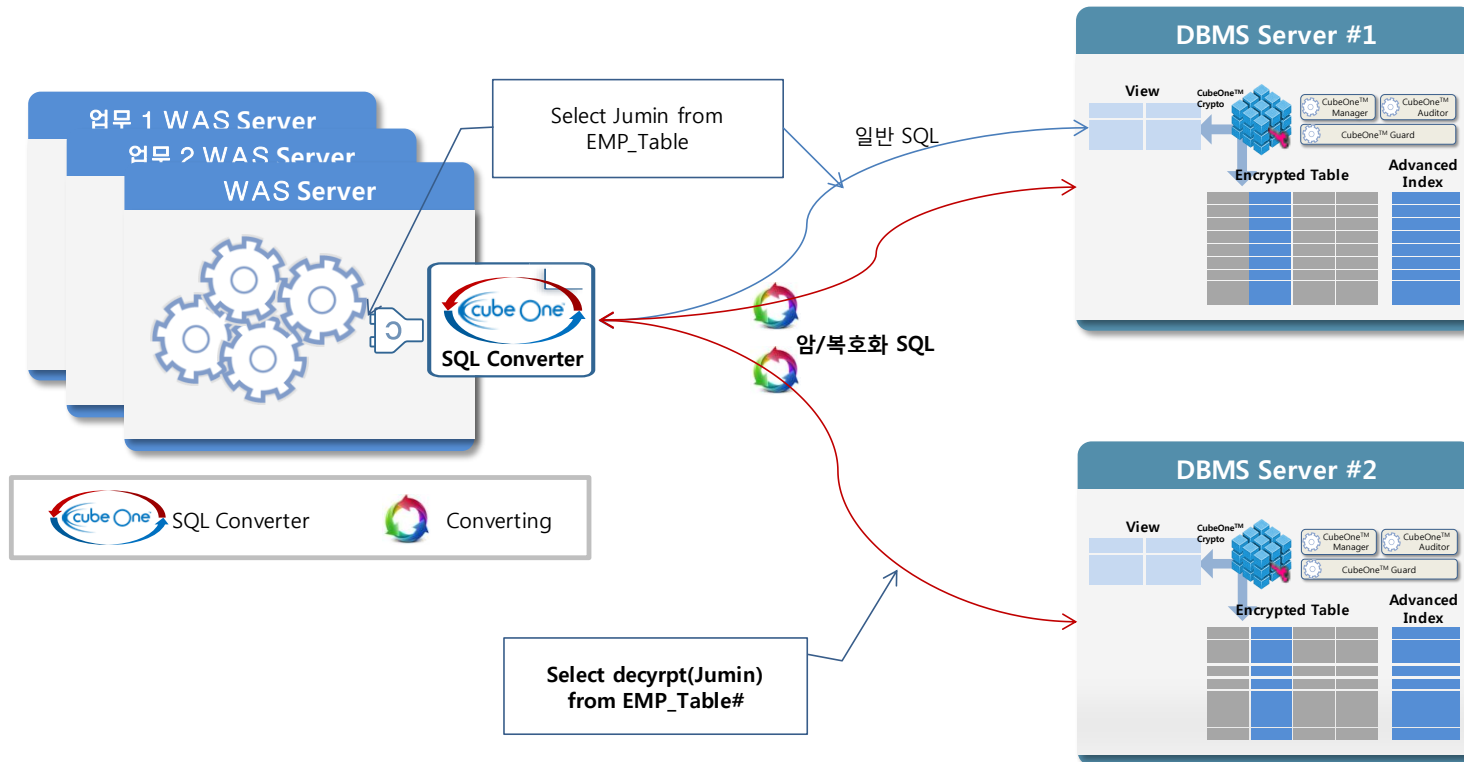


※ CubeOne Beacon은 Option 입니다.




## Application 소스코드 변경 최소화

❖ CubeOne™ SQL Converter는 JAVA(WAS) 환경에서 작성된 Application의 암호호화 관련 SQL을 CubeOne™ 환경의 최적화된 SQL로 자동 변환을 지원함으로써 사용자의 Application 변경 요구를 최소한으로 유지 합니다.



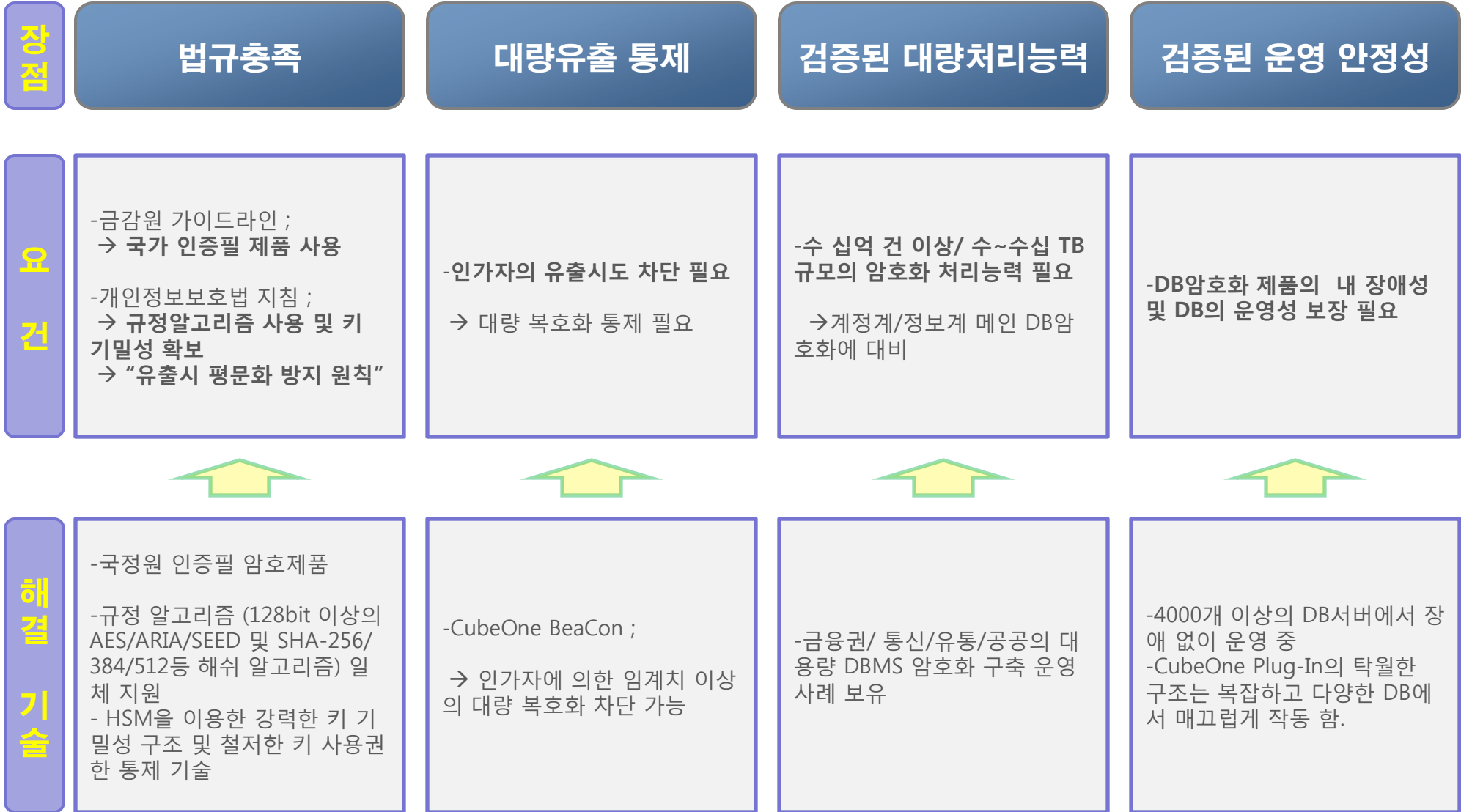
※ CubeOne SQL Converter는 Option 입니다.

## CubeOne™ 기능 요약

| 구분     |  | 특성 및 적용 기술   |
|--------|--|--|
| 암호화 기능 | 암호화 단위                                 | <ul style="list-style-type: none"> <li>컬럼 단위로 선택하여 암호화.</li> </ul>   |
|        | 지원 알고리즘<br>(KLIB V2.x,<br>Plug-In/API) | <ul style="list-style-type: none"> <li>국제적으로 널리 통용되는 표준 암호화 알고리즘 지원.<br/>대칭키 알고리즘: ARIA, SEED, AES, DES, 3DES(TDES) – CBC모드<br/>일방향 알고리즘: SHA-1/256/384/512 with SALT 지원</li> <li>국내 표준 알고리즘을 지원합니다. 국정원 검증필 암호모듈(KLIB V2.0) 탑재</li> <li>보안 정책 배포 시 공개키 방식의 알고리즘 채택.</li> </ul>  |
|        | Index 암호화 및 색인 검색<br>(Plug-In)         | <ul style="list-style-type: none"> <li><b>PK 컬럼 혹은 Unique Key 컬럼을 IV를 적용하여 암호화 (FK는 IV를 사용하지 않는것이 바람직함)</b></li> <li><b>일반 색인 컬럼에 대한 암호화 (IV적용) : 암호화 컬럼의 Index도 안전하게 암호화 되어 생성됨</b></li> <li>암호화된 컬럼에 대한 일치 검색 및 범위검색에 대한 색인 검색 (Index Search) 지원</li> <li>전방 일치 (LIKE, BETWEEN, &gt;, &lt;, &gt;=, &lt;= 등 모든 전방 일치 검색) 검색 시 Index Range Scan을 지원</li> <li>색인 검색이 지원됨에도 불구하고 암호화 데이터의 일부, 혹은 전부에 대한 복호화된 정보를 보관하지 않음. (보안성 확보)</li> <li>색인 검색을 위해 기존의 SQL문을 변경할 필요가 없음. (DBMS 제약사항 및 Non-Oracle DB는 제외)</li> </ul> |
| 접근 제어  | 권한 분리<br>(Separate of Duty)            | <ul style="list-style-type: none"> <li>암호화한 데이터에 대한 권한 통제는 강력한 알고리즘과 더불어 매우 중요한 필수 요소 임.</li> <li>기본적으로 <b>DB 관리자와 보안관리자의 권한을 분리하여 운영</b>이 가능하도록 제품이 설계되어있음.</li> <li>DB관리자는 DB 관리업무만 수행하며, 암호화된 데이터를 직접 조회 하거나 이 데이터에 접근통제 권한을 가질 수 없도록 함.</li> <li>보안관리자는 암호화된 중요 개인정보에 대한 접근통제 권한을 가짐. 또한 암호화 작업 권한도 가짐.</li> </ul>   |
|        | 접근통제 방법                                | <ul style="list-style-type: none"> <li>암호화되어 있는 데이터에 대한 접근은 사용자별 (WorkGroup별), IP /MAC Address별, 애플리케이션별, 시스템명 별로 1차 통제하며, 여기에 기간, 시간대, 요일 별로 2차 통제됩니다.</li> <li>또한 <b>패스워드 임의 변경 후의 접근 및 애플리케이션 명 변경 후 접근 시에도 복호화 차단.</b> </li> </ul>  |
| 감사     | 보안정책 이력 기록                             | <ul style="list-style-type: none"> <li>암호화된 데이터에 관한 접근통제 정책의 변경 내역은 데이터에 대한 접근기록과는 별도로, CubeOne™ Manager (GUI) 가 설치된 PC에 저장. (변경되는 모든 기록이 저장 되므로 이 기록을 통해 추적 가능)</li> </ul>  |
|        | 데이터 접근 이력 기록                           | <ul style="list-style-type: none"> <li>암호화 적용 데이터에 대한 접근 이력은 CubeOne™ Auditor와 CubeOne™ Log Manager에서 관리.</li> <li>SIUD 각각에 대한 접근 이력과 성공, 실패에 대한 이력은 컬럼 별로 선별적으로 관리할 수 있음.</li> <li>Data에 대한 접근 이력은 매우 상세하게 기록되어 유사시 내용을 추적하는데 편리.</li> </ul>  |

## CubeOne™ 의 기능 요약

| 구분            |                  | 특성 및 적용 기술   |
|---------------|------------------|--|
| 키기밀성          | KCMVP 기준 인증필     | <ul style="list-style-type: none"> <li>마스터키와 컬럼 암호키를 비롯한 각종 키의 생성과 키 사용정책의 설정 및 배포 메커니즘이 인증기준대로 안전하게 이용/관리됨.</li> <li>보안관리자에 의해 관리되는 Console Manager에서 최초 키와 정책을 생성하여 정책서버에 저장함.</li> </ul>  |
|               | <br>HSM 지원       | <ul style="list-style-type: none"> <li>다수의 서버에 키와 정책의 자동 배포를 위해 정책서버에 통합 저장함.</li> <li>HSM을 적용하는 경우, HSM이 장착된 전용 서버를 이용하며, HSM을 사용하지 않는 경우는 일반 서버를 사용하면 됨.</li> <li>HSM을 적용하면 CC Level 4+ 등급을 충족함.</li> </ul>  |
| 실시간 통제 (옵션)   | <br>대량 복호화 차단    | <ul style="list-style-type: none"> <li>CubeOne BeaCon Option을 이용하면 인가자가 인가조건일 지라도 정해진 건수 이상의 복호화를 차단할 수 있음.</li> <li>임계치를 정하여 3단계(Warning/Alert/Fatal)로 구분하여, SQL 기록/복호화 차단/ 세션의 강제종료 등의 후속 Action을 실행할 수 있음.</li> <li>이 기능을 이용하면 SQL Injection이나, 복호화 권한을 가진 내/외부 사용자의 과도한 복호화 시도(유출이 우려되는 상황)를 통제 할 수 있음.</li> </ul> |
|               | <br>암호복호 모듈 모니터링 | <ul style="list-style-type: none"> <li>CubeOne Crypto(암호화 모듈)를 실시간 모니터링하며, 암호/복호 상황(성공/실패/오류)을 대쉬보드 형태로 일목요연하게 모니터링 할 수 있는 화면을 제공함.</li> <li>일/주간/월간 평균 패턴 분석 화면을 제공하며 문제의 SQL을 Drill Down하여 조회할 수 있음.</li> <li>복호화 오류 등의 이벤트 발생시 관리자에게 통보 및 경고 상황을 화면에 출력 함.</li> </ul>   |
| SQL 자동변환 (옵션) | Java 소스 무수정      | <ul style="list-style-type: none"> <li>JSP로 코딩된 프로그램내에 있는 SQL문장의 수정을 하지 않고 JSP 바깥에서 문장 변환이 이루어 지도록 함.</li> <li>보안성과 적용성이 뛰어난 Plug-In 암호모듈을 DB서버에 설치하고, WAS 서버에 Agent를 설치하여 이 agent가 자동변환 시키는 구조.</li> <li>WAS 서버의 Configuration에 Agent 등록만 하면 JSP는 재 컴파일하지 않아도 됨.</li> </ul>   |

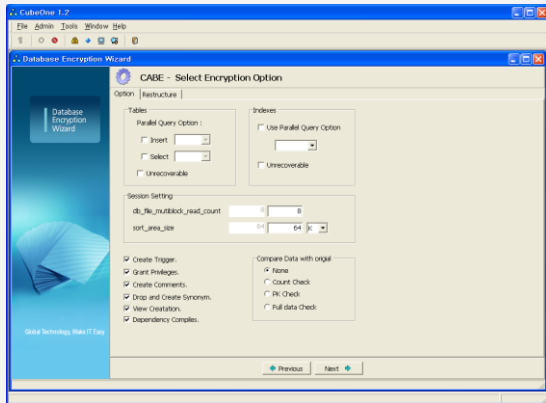


# 2. CubeOne™ 주요 특징점

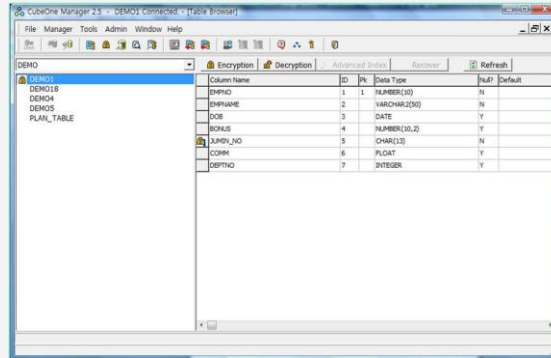


편리한 운영 관리환경 제공

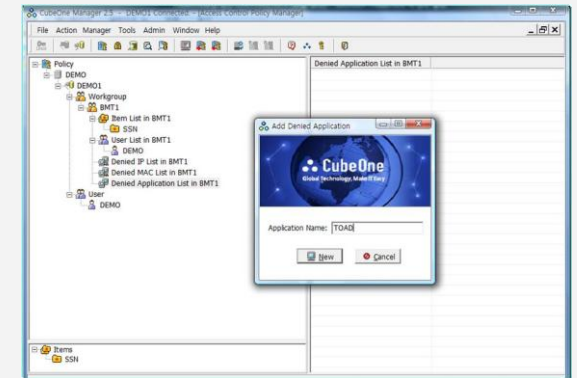
## 초기 암호화 GUI 지원



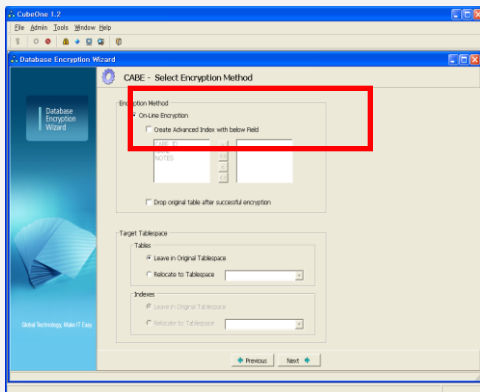
## Encryption Manager



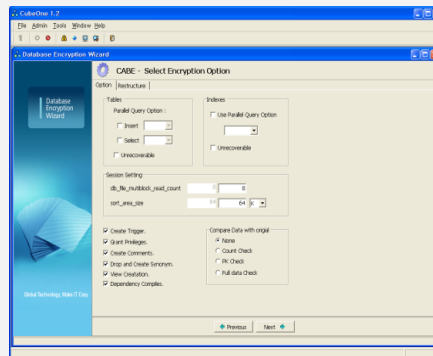
## CubeOne™ Policy Manager



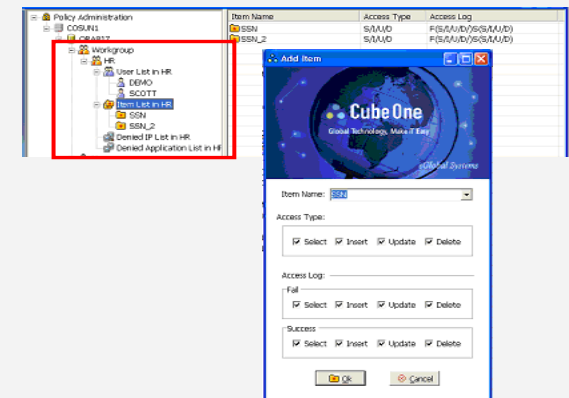
## Dual Mode 설정



## Encryption/Decryption Wizard



## 접근제어 통제



## 시스템 리소스 사용량 유지 [Plug-In]

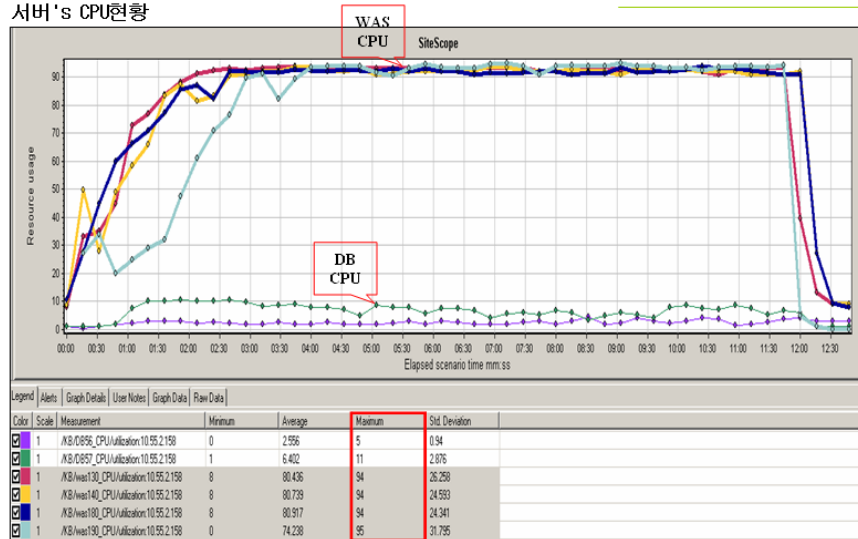
본 사례는 A사에서 CubeOne™ Plug-In을 사용하여 시스템 리소스 사용량을 확인하는 BMT를 실시한 것으로, 아래 사례와 같이 암호화 적용 시 시스템 리소스 사용량 증가가 미미한 수준임을 확인 할 수 있습니다.

**BMT 환경 : DBMS 동시 접속자 수를 50명씩 늘려서 동시 접속자 1,000명 상태를 5분간 유지**

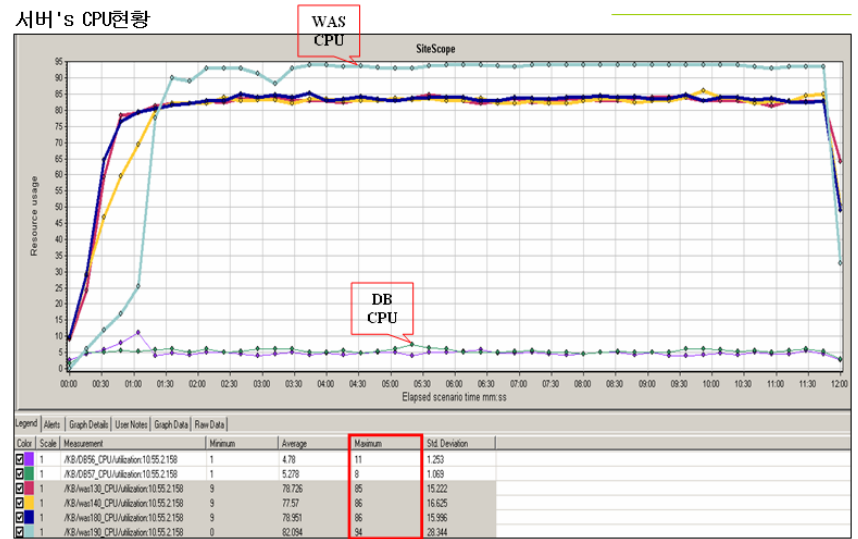
## 리소스 사용량 [A사, Plug-In BMT 사례]



서버's CPU현황



서버's CPU현황



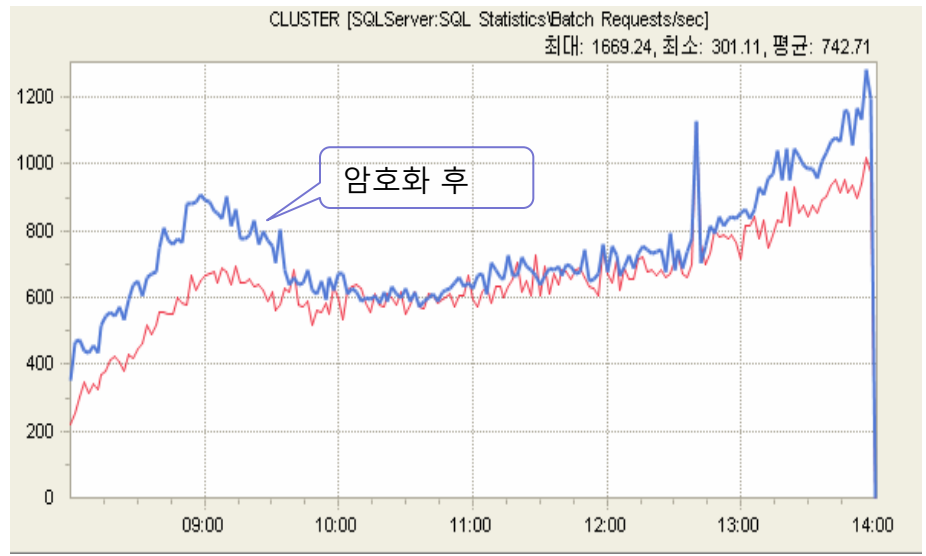
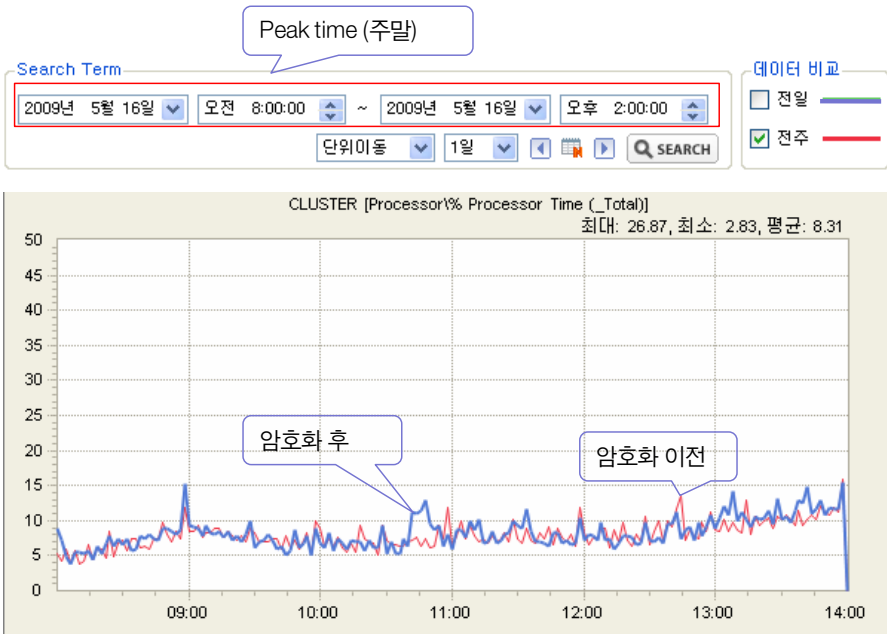
❖ 초기 일괄 적용 시 : CubeOne은 고 효율 처리 구조를 가지고 있습니다. 따라서 초기 일괄 암호화 시 유휴자원(CPU)을 효율적으로 이용 합니다.

## 시스템 리소스 사용량 유지 [Plug-In]

CubeOne™의 성능은 이미 70여개의 운영 사례에서 확인된 바와 같이 OLTP성 업무에서는 성능저하가 거의 없음이 입증 되었습니다. 특히 Peak Time시 동시사용자의 증가에 따른 성능 변화는 실제 고객 사이트에서 성능 검증 자료를 참조하면 됩니다.

아래와 같은 Peak Time시의 성능 및 리소스 사용량 자료에 근거하여 암호화 후의 Application 및 DBMS 처리 성능의 저하가 최소화됨을 보장 합니다.

## Peak Time 성능[B사 운영 사례, Plug-In]



❖ 암호화 후 전주 대비 고객 접속량이 15% 많았던 상황



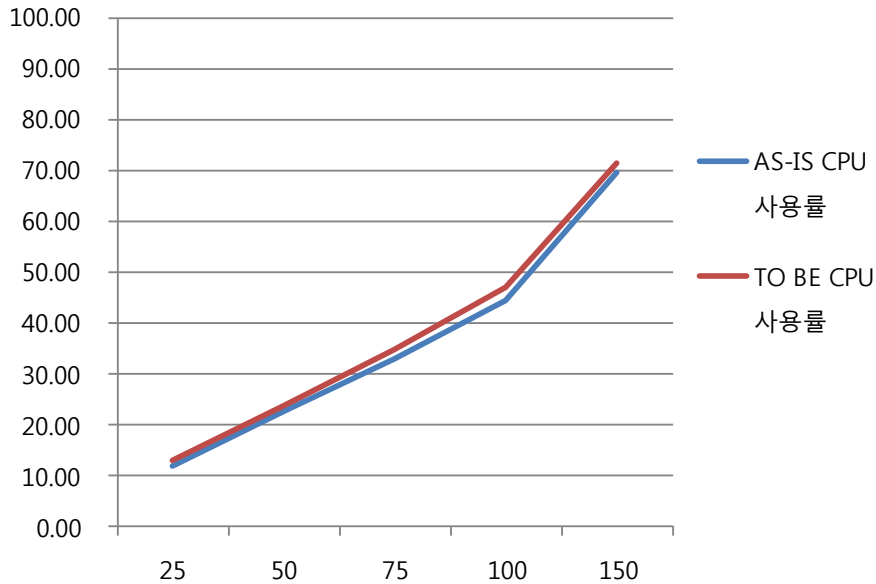
## 시스템 리소스 사용량 유지 [API]

본 사례는 고객사에서 CubeOne™ API을 사용하여 시스템 리소스 사용량을 확인하는 BMT를 실시한 것으로, 아래 사례와 같이 암호화 적용 시 시스템 리소스 사용량 증가가 미미한 수준임을 확인 할 수 있습니다.

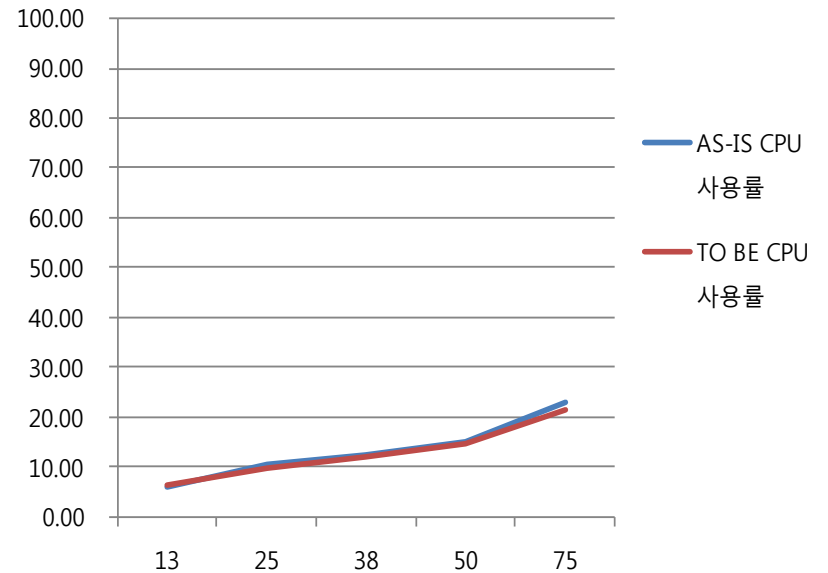
**테스트 환경 : 특정 Application 실재 서비스에 동시 접속자 수를 25명씩 늘려서 테스트 (Application 서버와 DBMS서버의 CPU 사용량 측정)**

## 리소스 사용량 [C사, API BMT 사례]

고객별 사용서비스 조회

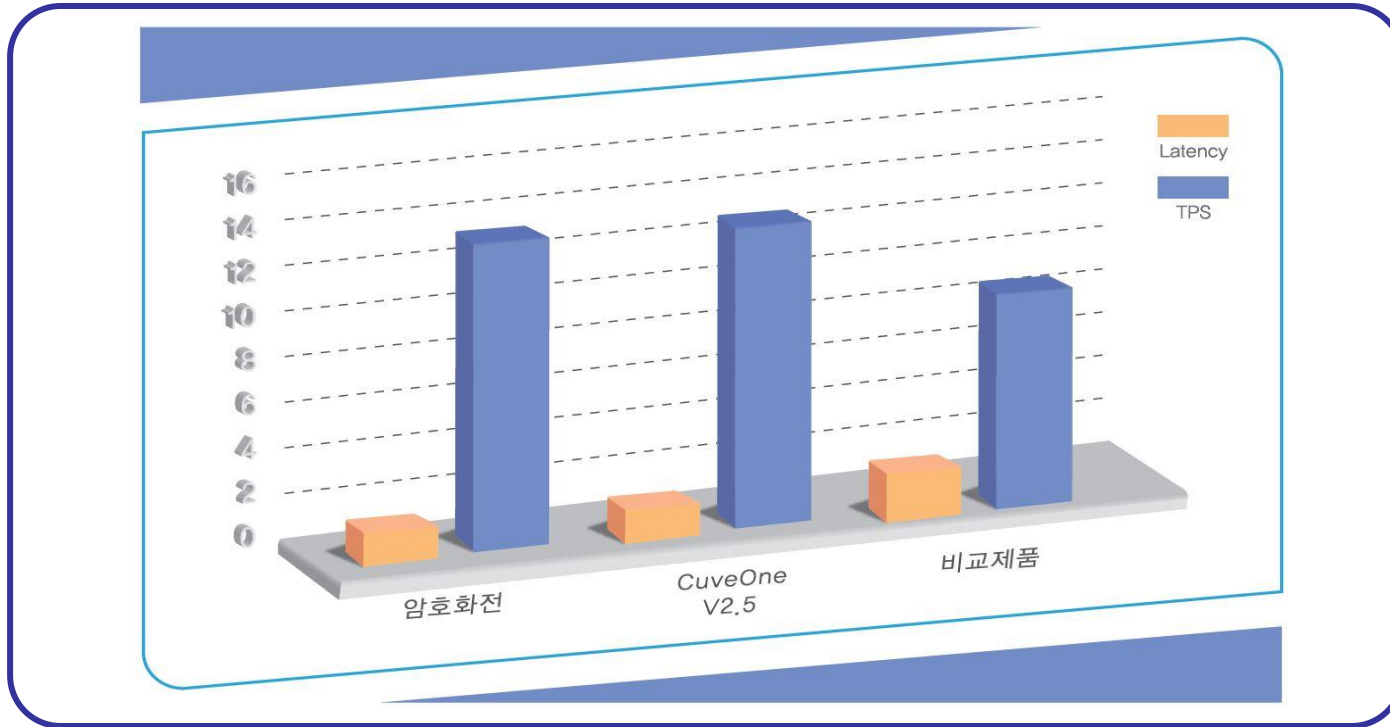


고객정보생성



시스템 리소스 사용량 증가 거의 없음 (5% 미만)

## 응답 속도 유지



### 테스트 조건 :

건수 : 50 만 건 중 OLTP 처리  
 테스트 방법 : Road-Runner (C0ncurrent 20 Session)

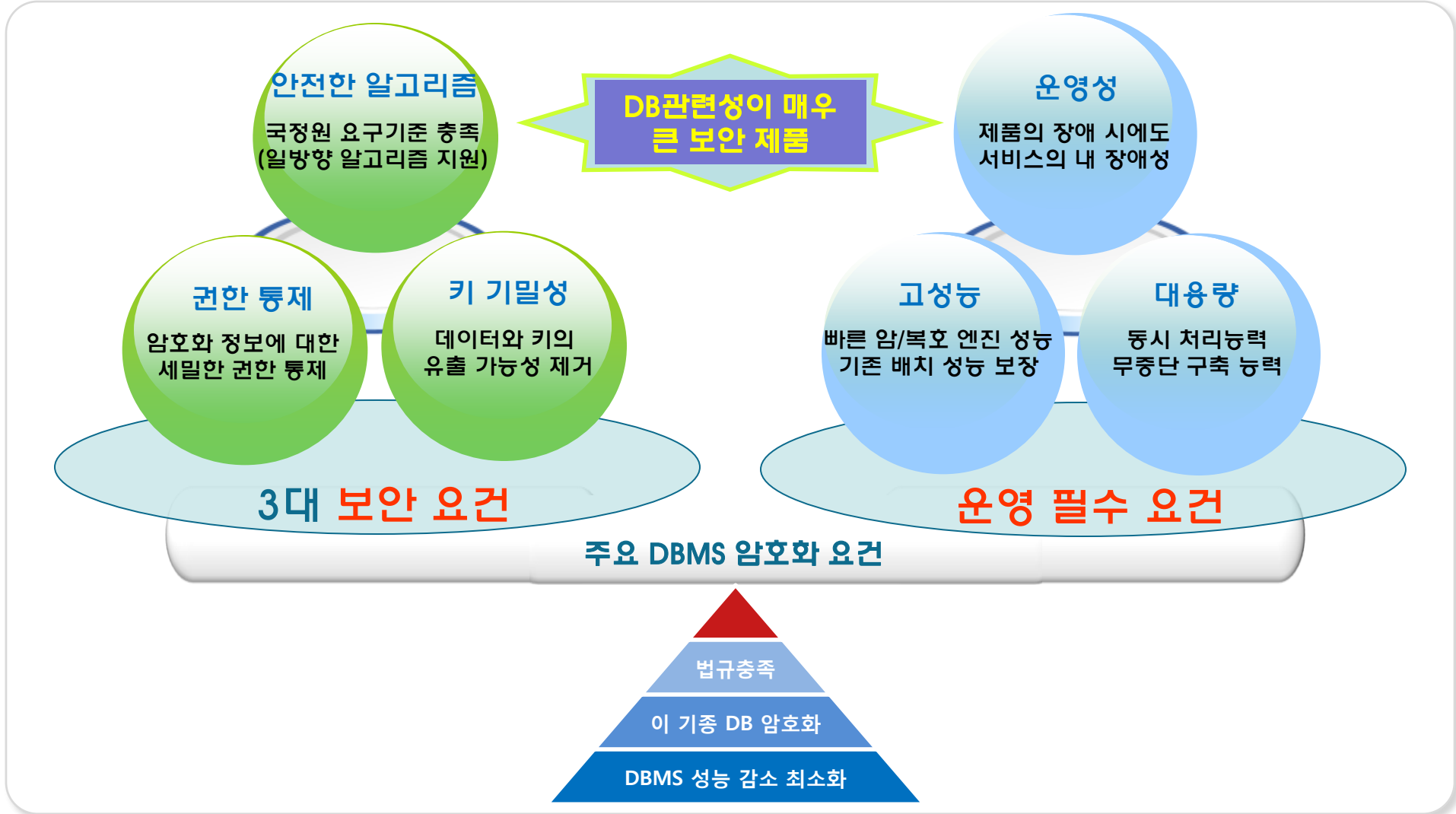
H/W : Sun 12x400MHz /12GB Mem.  
 OS : Sun Solaris 10  
 DBMS : Oracle 9.2.0.6,  
 CubeOne™ : Ver. 2.3

# 4. Reference & Success Story

## 주요 고객사

|      |  |  |  |  |  |  |  |  |  |
|------|--|--|--|--|--|--|--|--|--|
| 공공   |  |  |  |  |  |  |  |  |  |
|      |  |  |  |  |  |  |  |  |  |
|      |  |  |  |  |  |  |  |  |  |
|      |  |  |  |  |  |  |  |  |  |
|      |  |  |  |  |  |  |  |  |  |
| 교육   |  |  |  |  |  |  |  |  |  |
|      |  |  |  |  |  |  |  |  |  |
| 금융   |  |  |  |  |  |  |  |  |  |
|      |  |  |  |  |  |  |  |  |  |
| 일반기업 |  |  |  |  |  |  |  |  |  |
|      |  |  |  |  |  |  |  |  |  |
|      |  |  |  |  |  |  |  |  |  |
|      |  |  |  |  |  |  |  |  |  |
|      |  |  |  |  |  |  |  |  |  |
|      |  |  |  |  |  |  |  |  |  |

DBMS 암호화 성공 요건



# 감사합니다.



**eGlobal**  
*Global Technology, Make IT easy*

서울시 강남구 역삼동 703-5 일환빌딩 9층

㈜이글로벌시스템

Tel : 82-2-6447-6988, Fax : 82-2-6447-6989,

E-Mail : [sales@cubeone.co.kr](mailto:sales@cubeone.co.kr) ( [www.eglobalsys.co.kr](http://www.eglobalsys.co.kr) )