



Free software, Open source For Security



오픈소스 DB보안 소프트웨어



***F**ast Implementation*

***E**asy Operation*

***L**ow Cost for Your Security*

CONTENTS

A decorative graphic on the left side of the slide. It features a large, light gray circle containing several concentric arcs in shades of blue and gray. At the bottom of the slide, there are silhouettes of five people in business attire, appearing to be in a meeting or presentation. One person is holding a laptop, and another is gesturing with their hand.

1. 개요

2. 특징점

3. 시연

4. 발전 방향

1. 개요

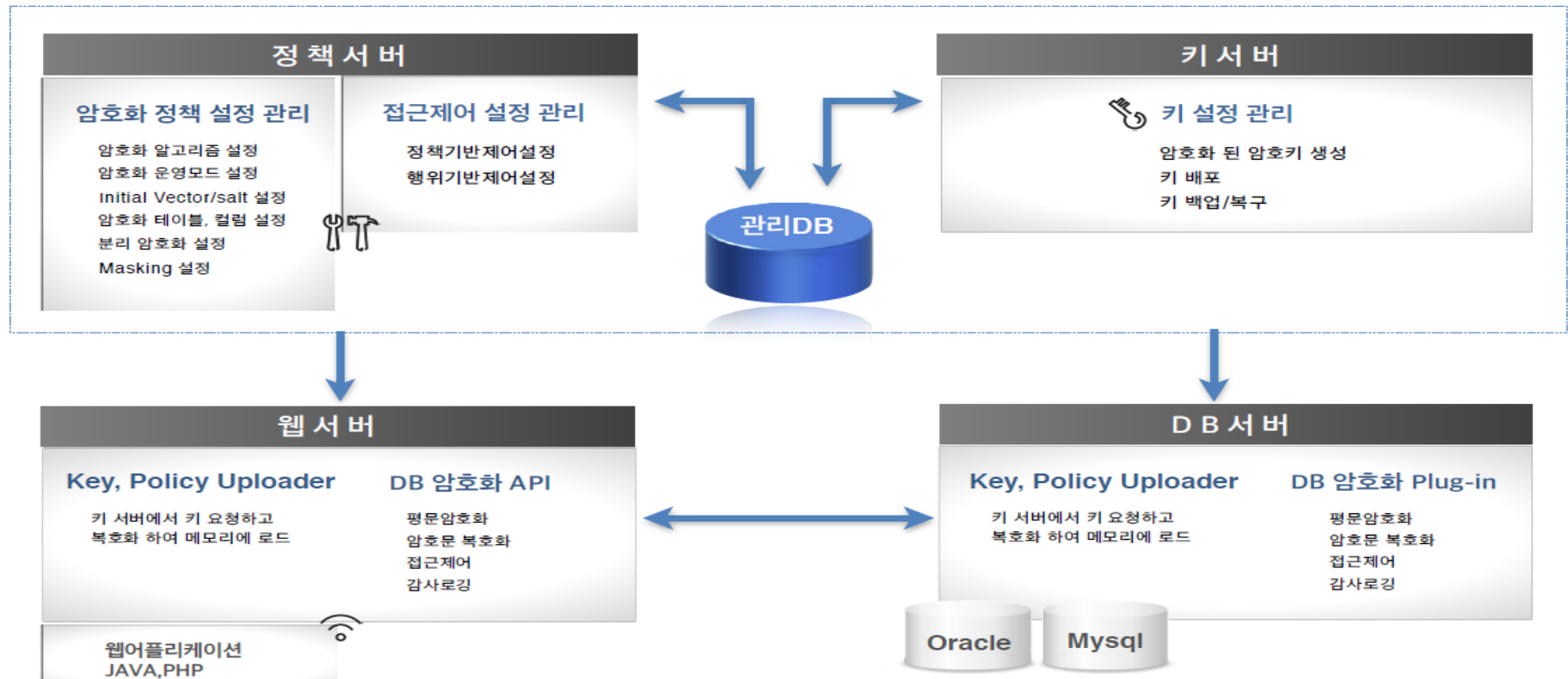
DB의 컬럼 단위 선택적 암호화 및 접근제어 소프트웨어로써 가장 많이 사용되는 Oracle, Mysql DB Plug-in과 JAVA, PHP 웹 어플리케이션에 대한 API를 지원

- 국내외 표준 대칭키 및 일방향 암호화 알고리즘 지원
 - SEED, AES 대칭키 알고리즘, SHA2 일방향 알고리즘 구현.
 - ECB, CBC 암호 운영 모드 지원.(예측을 통한 사전 공격에 강함)
 - Initial Vector, Salt 지원을 통해 동일 평문에 대해 고객사별 다른 암호문 산출, 보안성 강화.
- 접근제어
 - IP, USER, 시간에 대한 정책 기반 접근 제어
 - 짧은 시간, 긴 시간 기준에 따른 암호, 복호화 접근 횟수에 대한 행위 기반 접근 제어.
- Flexible SW deployment
 - DB Plug-in 방식, API 방식(PHP/JAVA용 어플리케이션 제공), Hybrid 방식 지원.
- 로그 기록
 - 접속 세션을 기반으로 컬럼별 암호, 복호화 내역 기록
- 카드번호, 계좌번호 등 암호화 라이브러리 레벨에서 Masking 제공.
- 키 생성 관리, 암호, 접근제어 정책 설정 등을 위한 사용자 콘솔 UI 제공.

2. 특징점

- ▣ 행위 기반 접근제어를 통한 소량의 잦은 정보 유출에 대한 차단.
- ▣ 암호정책, 접근제어 정책, 키 등 사용자 정의 메타 정보를 메모리에 로딩하며, 로그도 메모리에 기록하여 DISK에는 지연 쓰기 방식을 사용함으로써 고속 처리.
- ▣ Key 제로화, Key 다중, Key라이프사이클 지원을 통한 강력한 키 보호.
- ▣ 모듈화를 통해 소프트웨어에 대한 하드웨어 배치가 융통성 있게 구성 가능

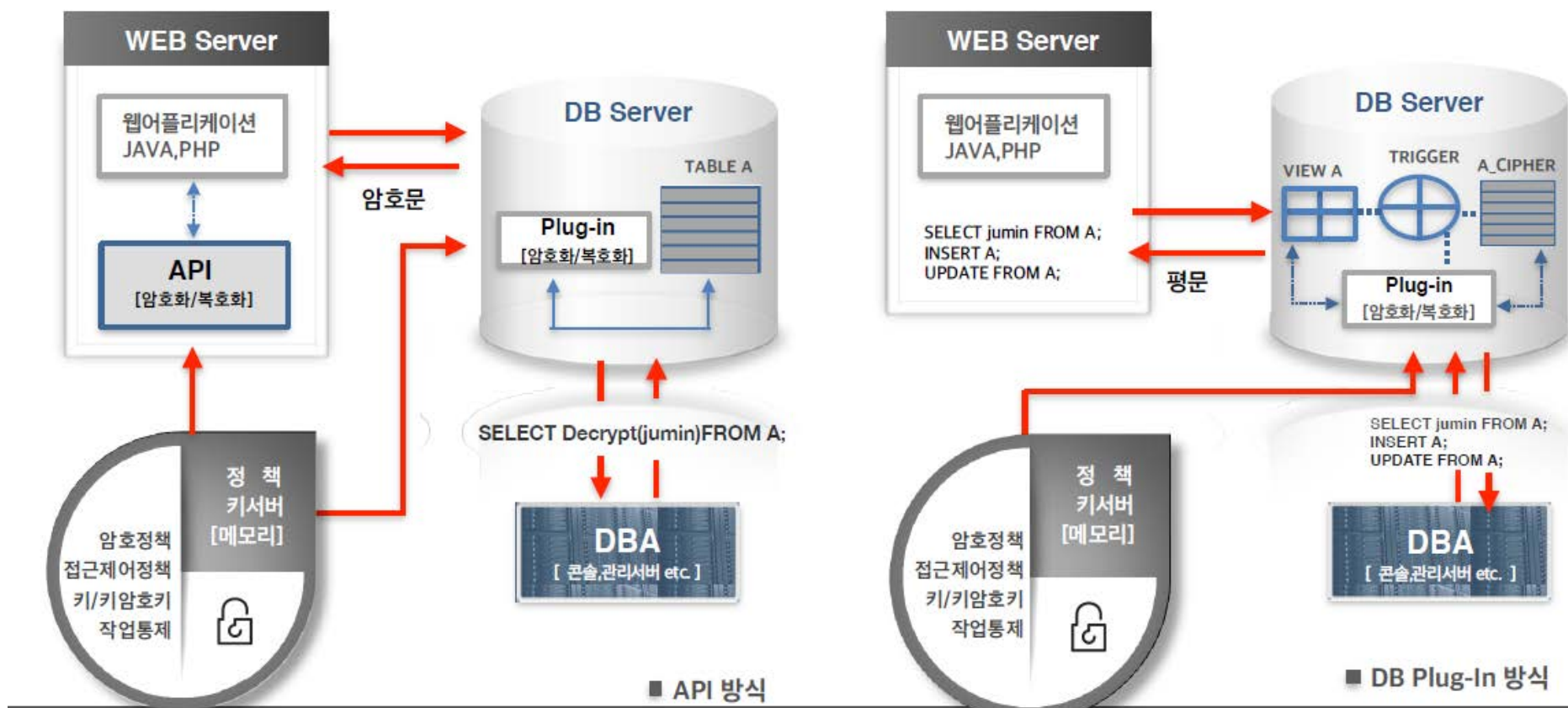
[소프트웨어 구성도]



2. 특징점

사용자 어플리케이션의 수정을 최소화 하기 위한 DB Plug-in 방식 , DB서버 부하 최소화를 위한 어플리케이션 API 방식, Hybrid 방식 모두 구현 가능.

[소프트웨어 사용자 구성 방식]



3. 시연 (기본 기능 시연)

정책설정

아이디 admin

비밀번호

로그인

3. 시연 (기본 기능 시연)

Mysql Plug-in을 활용한 암호,복호화

```
root@fo4sLIVE01:/usr/src/jimant/core/approachManager
[root@fo4sLIVE01 approachManager]# mysql -uroot -p test
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 76
Server version: 5.1.73 Source distribution

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

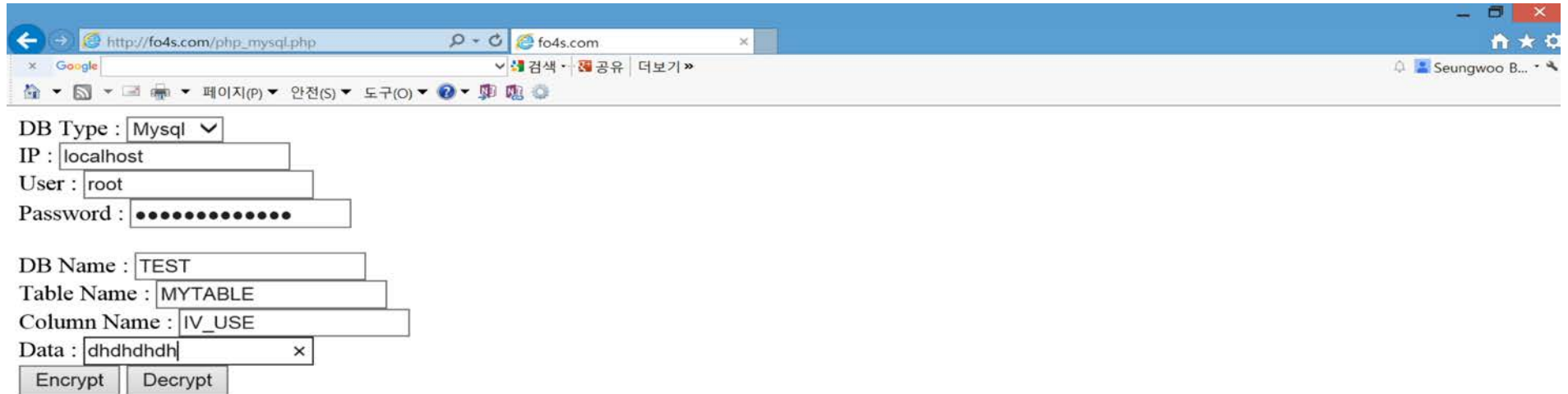
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> █
```

3. 시연 (기본 기능 시연)

Mysql API를 활용한 암호화



The screenshot shows a web browser window with the URL `http://fo4s.com/php_mysql.php`. The page contains a form for MySQL database operations. The form fields are as follows:

- DB Type :
- IP :
- User :
- Password :
- DB Name :
- Table Name :
- Column Name :
- Data :

Below the form, there are two buttons: and .

3. 시연 (기본 기능 시연)

Mysql Plug-in 접근제어

```
root@fo4sLIVE01:/usr/src/jimant/core/approachManager
[root@fo4sLIVE01 approachManager]# mysql -uroot -p F04S
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 80
Server version: 5.1.73 Source distribution

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

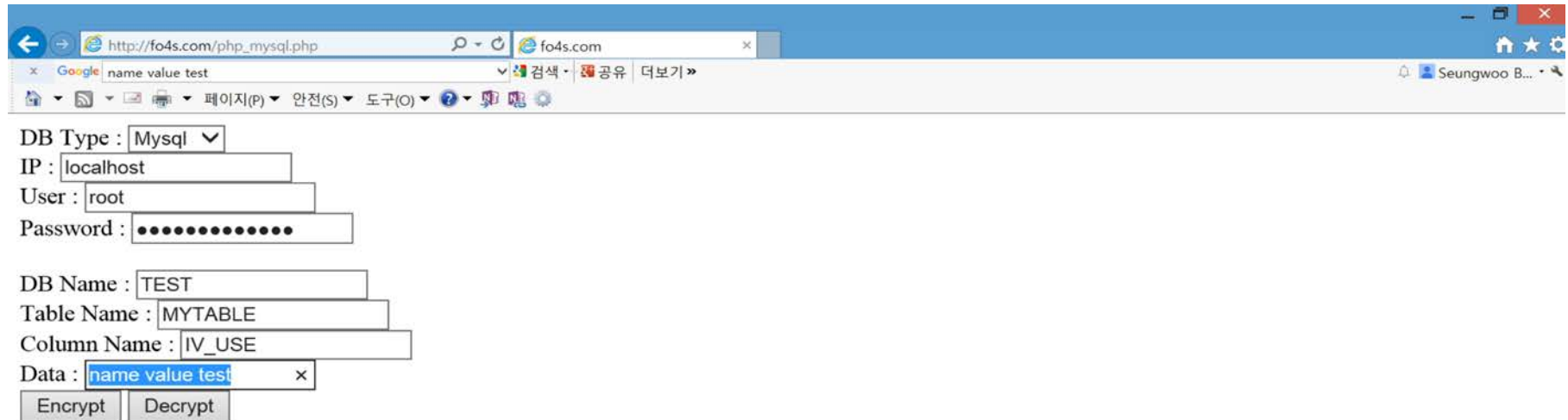
mysql>
mysql> update POLICY_ACCESS_CONTROL set CONNECT_DB_USER = 'allowance';
Query OK, 1 row affected (0.00 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql>
```

I

3. 시연 (기본 기능 시연)

Mysql API 접근제어



DB Type : Mysql ▾

IP : localhost

User : root

Password : ●●●●●●●●

DB Name : TEST

Table Name : MYTABLE

Column Name : IV_USE

Data : name value test x

Encrypt Decrypt

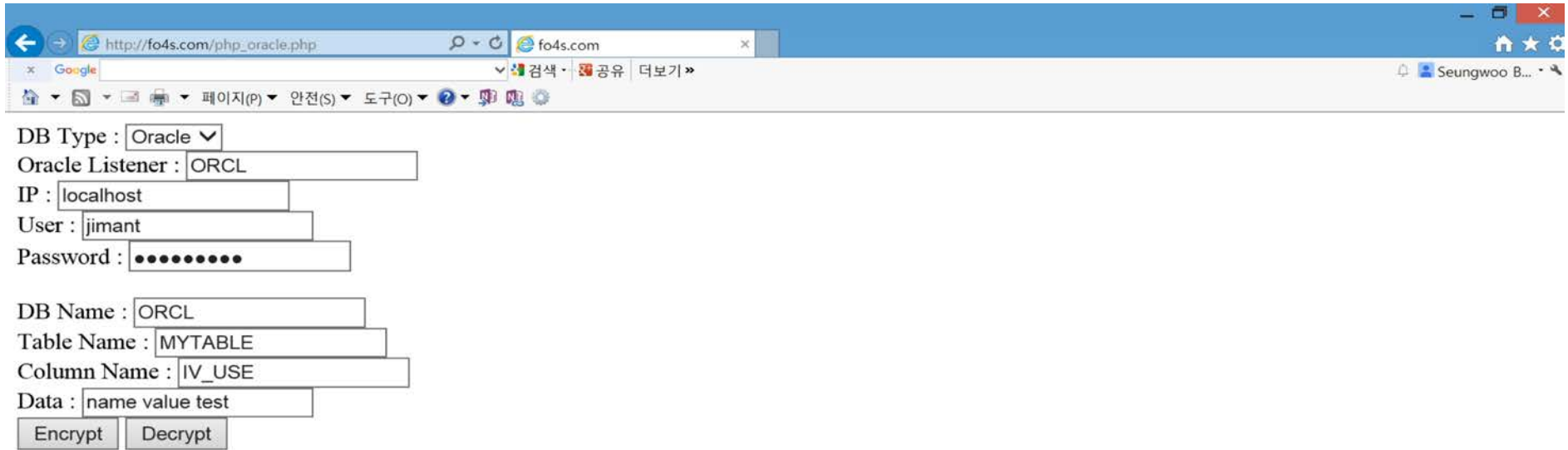
3. 시연 (기본 기능 시연)

Oracle Plug-in 암호,복호화

```
oracle@fo4sLIVE01:~  
SQL>  
SQL>  
SQL> SELECT * FROM MYTABLE;  
no rows selected  
SQL> INSERT INTO MYTABLE (IV_USE,IV_NONE,PW,PART,MASK) VALUES ('F04SIVTEST','F04SIVTEST','MYPWISTEST','PARTEST','MASKTEST');  
1 row created.  
SQL> SELECT * FROM MYTABLE;  
IV_USE      IV_NONE      PW      PART      MASK  
-----  
F04SIVTEST  F04SIVTEST  MYPWISTEST  PARTEST  MASKTEST  
SQL> █
```

3. 시연 (기본 기능 시연)

Oracle API 암,복호화



The screenshot shows a web browser window with the URL http://fo4s.com/php_oracle.php. The page contains a form for Oracle API encryption and decryption. The form fields are as follows:

- DB Type :
- Oracle Listener :
- IP :
- User :
- Password :
- DB Name :
- Table Name :
- Column Name :
- Data :

At the bottom of the form, there are two buttons: and .

3. 시연 (기본 기능 시연)

Oracle Plug-in 접근 제어

3. 시연 (기본 기능 시연)

Oracle API 접근 제어

The screenshot shows a web browser window with the URL `http://fo4s.com/php_oracle.php`. The page contains a form for Oracle API access control. The form fields are as follows:

- DB Type :
- Oracle Listener :
- IP :
- User :
- Password :
- DB Name :
- Table Name :
- Column Name :
- Data :

Below the form fields are two buttons: and .

3. 시연 (기본 기능 시연)

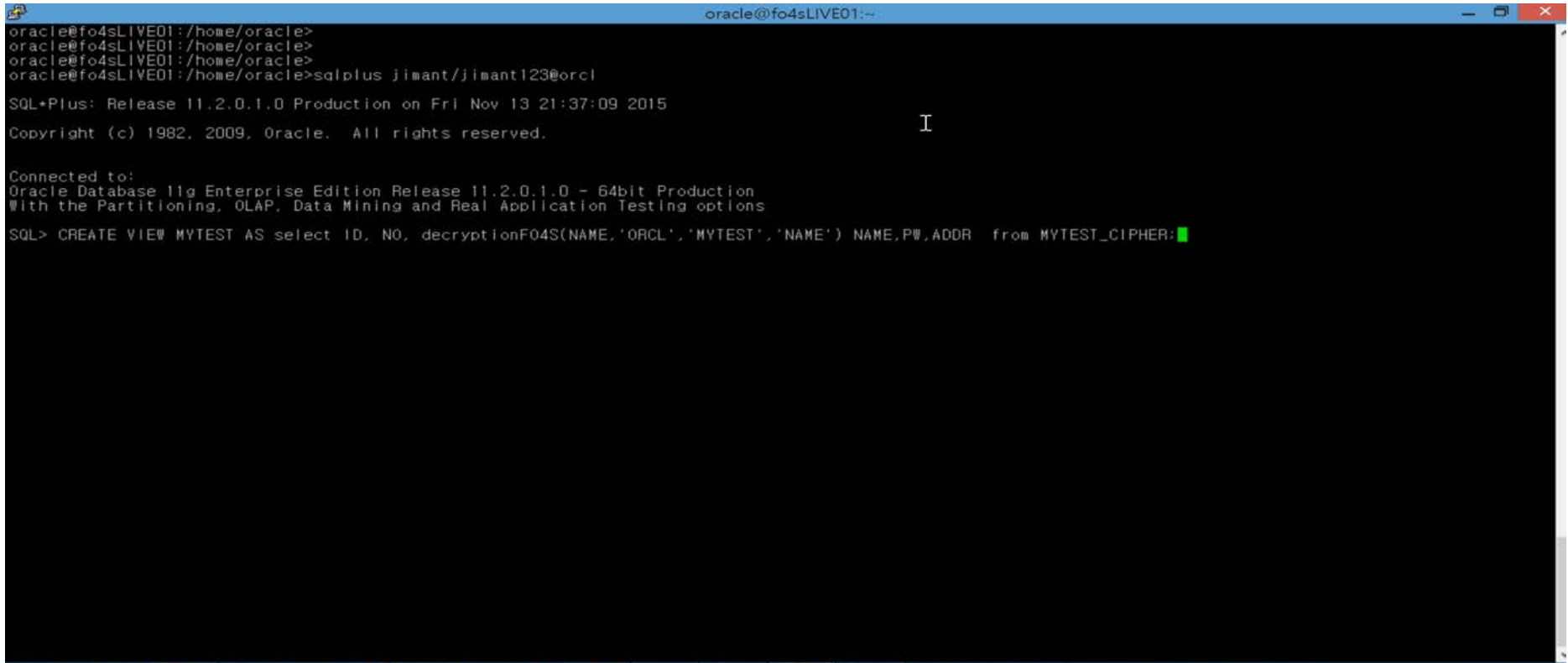
행위 기반 접근제어

```
root@fo4sLIVE01: approachManager]# mysql -uroot -p fo4s
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Your MySQL connection id is 104
Server version: 5.1.73 Source distribution
Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> update BEHAVIOR_ACCESS_CONTROL set SMALL_TIME = '0001' , SMALL_TIME_COUNT = 1 , BIG_TIME = '0002' , BIG_TIME_COUNT = 2;
```

```
oracle@fo4sLIVE01:~$
SQL>
SQL>
SQL> SELECT * FROM MYTEST WHERE ROWNUM <= 5;
```

3. 시연 (사용자 환경 구성)

사용자 베이스 테이블 Drop, View와 Trigger를 생성하여 사용자 어플리케이션의 수정 없이 설치, 운영.



```
oracle@fo4sLIVE01:~/home/oracle>
oracle@fo4sLIVE01:~/home/oracle>
oracle@fo4sLIVE01:~/home/oracle>
oracle@fo4sLIVE01:~/home/oracle>sqlplus jimant/jimant123@orcl

SQL*Plus: Release 11.2.0.1.0 Production on Fri Nov 13 21:37:09 2015

Copyright (c) 1982, 2009, Oracle. All rights reserved.

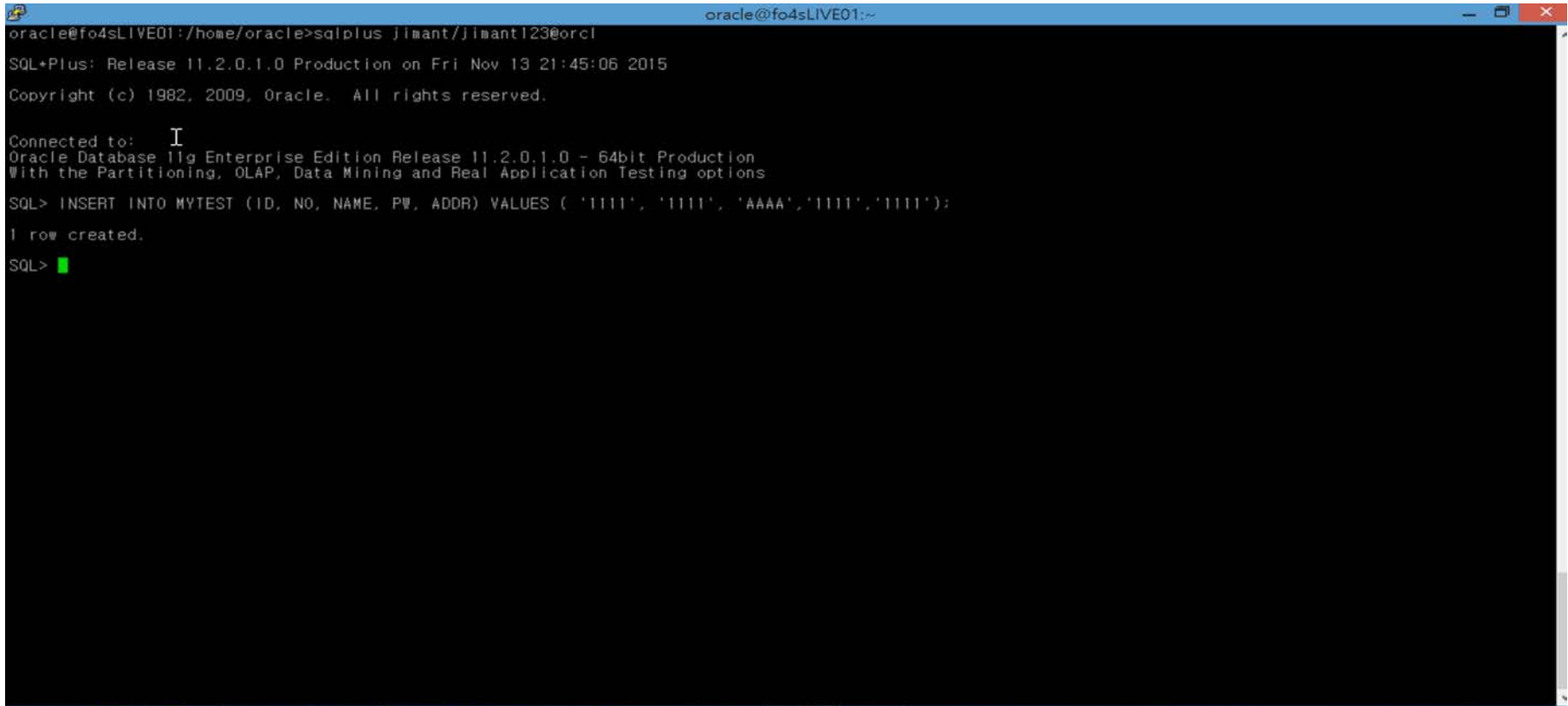
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> CREATE VIEW MYTEST AS select ID, NO, decryptionF04S(NAME,'ORCL','MYTEST','NAME') NAME,PW,ADDR from MYTEST_CIPHER;
```


3. 시연 (사용자 환경 구성)

암호화 이후에도 인덱스를 통한 검색이 가능함.

DB의 실행 계획을 암호화 적용 이 후에도 유지 할 수 있음.



```
oracle@fo4sLIVE01:/home/oracle>sqlplus jimant/jimant123@orcl
SQL*Plus: Release 11.2.0.1.0 Production on Fri Nov 13 21:45:06 2015
Copyright (c) 1982, 2009, Oracle. All rights reserved.

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
SQL> INSERT INTO MYTEST (ID, NO, NAME, PW, ADDR) VALUES ( '1111', '1111', 'AAAA','1111','1111');
1 row created.
SQL>
```

3. 발전 방향

□ 정보보안 산업 현황

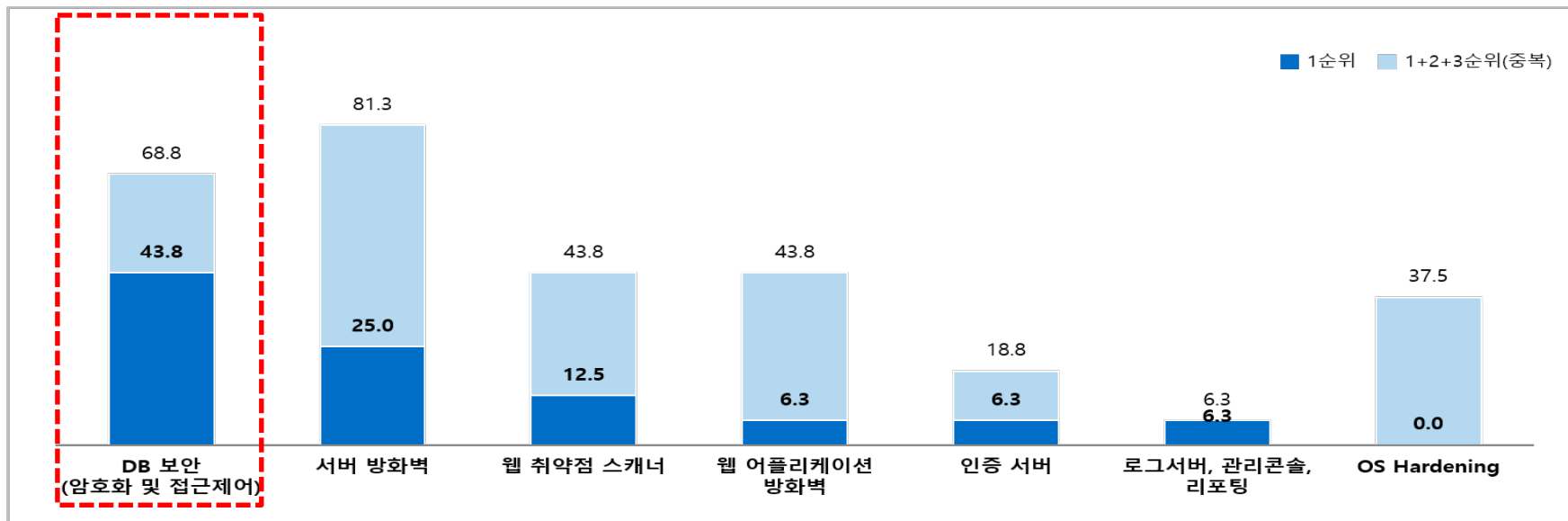
'13년 중소기업 대상 정보보안 산업 매출 비중은 대기업 대비 33%.

※출처: '13년 정보보호 실태조사, '13년 정보보호산업 실태조사 (인터넷진흥원)

하지만 표적 공격의 40%는 중소기업 대상 ※출처: 시만텍닷컴클라우드 2011년 조사

개인정보에 대한 정부, 법적 규제 강화. 2014년 개정된 정보보호법에서 개인정보의 암호화를 반드시 시행하도록 명시.

중소기업 대상 설문조사에서 DB보안에 대한 도입 필요성이 가장 높음



※출처: '15년 인사이트코리아, 오픈소스 정보보안 서비스에 대한 중소기업 설문조사

□ 발전 계획

▣ Fo4s 오픈소스 DB보안 소프트웨어 고도화

Mysql 암호화 스토리지 엔진의 개발, SQL 단위의 접근제어 및 로그 기록, 사용자 편의를 위한 콘솔의 고도화, 통합 로그 서버

▣ 커뮤니티 활성화

Github, Blog, Facebook 포럼 등 다양한 커뮤니티 채널을 통해 사용자 저변을 확대

▣ IDC, 호스팅 사업자와 오픈소스 정보보안 사업 협력 추진

▣ 정보보안 관련 정부 기관과의 오픈소스 활성화 협력 추진



THANK YOU