IBM i Solution Seminar Agenda

# DB 접근제어 Chakra MAX Power i 소개

BA Solutions

http://www.basolutions.co.kr

# → 목 차

# 웨어밸리 – 연혁

| | |
|---|---|
| 회사명 | ㈜웨어밸리 |
| 설립연도 | 2001년 2월 1일 |
| 대표자 | 손 삼 수 |
| 사업분야 | 시스템 통합, 컨설팅, 소프트웨어 개발 |
| 소재지 | 서울시 마포구 상암동 1605<br>누리꿈스퀘어 연구개발타워 6층 |
| 자본금 | 15억 |
| 직원 수 | 70명 |
| 조직 | 영업본부, 제품기획실, 기술본부, 기술연구소,<br>전략사업본부, 품질경영실, 경영지원실 |
| 전화번호 | (02)743-4910 (대표전화)<br>(02)743-4912 (FAX) |
| 주요 제품 | Chakra, Trusted Orange, Cyclone, Orange |
| 특기사항 | - **특허취득 (제 0481130호)**<br>- **GS 품질 인증 (04-0038)**<br>- 조달청 우수제품 인증 (제2005047호)<br>- 신제품 인증 (NEP-1605(KT))<br>- 신소프트웨어상품대상 (제184호)<br>- 제14회 다산기술상 수상<br>- **국내 최초 CC인증 (EAL-4 등급)**<br>- **신기술혁신 국무총리상 수상**<br>- **장영실상 수상** |

| | |
|---|---|
| 2010 | ▪ **세계일류상품(차세대) 선정 – DB보안 소프트웨어**<br>▪ **2010 대한민국 IT INNOVATION 대상 – 국무총리 표창 수상**<br>▪ 신기술실용화 유공기업 정부포상 (지식경제부 장관 표창)<br>▪ 제10회 매경우수벤처기업대상 기업부문/ 경영자부문 수상<br>▪ 2010 KOTRA 보증브랜드 기업 선정 : 2010.05<br>▪ KOTRA SW 글로벌 스타 육성기업 선정 : 2010.04<br>▪ **IR52 장영실 상 교육과학기술부 장관상 수상 : 2010.03**<br>▪ **Chakra CC 인증 형상관리(EAL4, CISS-0216-2010) : 2010.01** |
| 2009 | ▪ **하이테크어워드 수출 1천만 달러 달성 대상 : 2009.12**<br>▪ Chakra 미국 특허 등록 결정(미국 특허청)<br>▪ **중소기업기술혁신대전 신기술혁신 국무총리상(금상)수상 : 2009.09**<br>▪ Hi Seoul 브랜드 기업 200만불 수출석탑 수상<br>▪ 기술혁신형 중소기업(Inn-Biz) 인증 : 2009.02.06 |
| 2008 | ▪ Chakra CC인증(국내 최초 : EAL4, CISS-0109-2008) : 2008.07.29<br>▪ DB 취약점 분석 솔루션 Cyclone GS 인증 : 2008.04 |
| 2007 | ▪ 남미 브라질 Chakra V3.1 수출 : 2007.11.23<br>▪ CC인증 평가계약 : EAL-4 등급 : 2007.03.28<br>▪ SUN Microsystems와 Security 솔루션 분야 파트너 체결 |
| 2006 | ▪ 독일 Adversio AG사와 Chakra, Orange 솔루션 공급계약 체결<br>▪ 조달청 샤크라 제3자 단가계약 체결 (No:00068013100)<br>▪ 일본 Inter Link와 Orange 총판 계약 체결 |
| 2005 | ▪ 샤크라 특허 취득 (등록번호:제0481130호)<br>▪ 샤크라 조달청 우수제품 인정 (등록번호:제2005047호)<br>▪ 제 14회 다산 기술상 수상 (2005.09.12)<br>▪ **Chakra V3.0 발표** |
| 2004 | ▪ Orange V3.0 , Trusted Orange V2.0 발표<br>▪ **일본 AIS 그룹 NST-Japan과 Chakra 공급 계약 체결**<br>▪ 샤크라 2.x TTA SW GS마크, 신기술인정 (KT마크) |
| 2003 | ▪ Orange for Oracle GS 인증, Veritest 국제인증 획득<br>▪ **Trusted Orange Version 1.0 제품발표** |
| 2002 | ▪ **Chakra 1.0 제품발표** |
| 2001 | ▪ Orange for Oracle Version 1.0 제품발표<br>▪ ㈜웨어밸리 법인설립 및 등기 |

# 웨어밸리 – 고객현황

## 국내 최초 DB보안 솔루션 개발, 시장 개척. 국내/외 700여 기관, 1,000여 개 라이선스 공급.

| 구분 | 고객 구분 | 주요 납품 고객 |
|---|---|---|
| 국내 | 공공 기관 | 대검찰청, **금융감독원(1~2차)**, 금융결제원, 금융 연수원, 농업진흥청, 문화정보센터, 관세청, 교육인적자원부, **정부통합전산센터(1차~3차), 정통부 통합전산2센터**, 국세청, 한국석유공사, 한국교육개발원, 대통령기록관, 서울시재난본부, 한국산업기술진흥협회, 서울지하철공사(1~5차), 공무원연금관리공단, **지역정보개발원**, SH 공사, KOTRA, 인천광역시, 경주시, 송파구, 장흥군, 진도군, 노원구, 충청남도, 화성동탄문화센터, 행정자치부, 한국청소년진흥센터, 공군본부, 공군군수보급소, 작전사령부, 국방품질관리소, 계룡대 체력단련장,서울지방경찰청, 한국도로공사(1차~2차), 중앙공무원교육원, 한국가스안전공사, 광주광역시동구, KISTI, 근로복지공단, 서울시소방재난본부, 질병관리본부, 결핵연구원, 국회사무처, 국토해양부(판교U-City), 병무청, 예천군, 통계청, 경북 농업기술원 , 부산도시공사,한국건설기술연구원, 인천공항세관, 국민체육진흥공단,지식경제부,중소기업청 , 방위사업청,국방과학연구소,인천광역시도시개발공사, 한국과학기술기획평가원, 한국산업단지공단, 우정사업정보센터, 한국교육학술정보원(전국시도교육청) , 도로교통공단, 중소기업진흥공단, 한국토지주택공사, 한국무역협회, 해양경찰청 , 한국과학기술원(KAIST), 전자부품연구원, 창업진흥원, 부산시설관리공단, 울산원자력교육원 , 중앙입양정보원, 한국정보화진흥원(NIA), 울산남구도시관리공단 , 한국특허정보원, 군포시설관리공단, 대한상공회의소, 에너지기술평가원 , 독립기념관, 경남농업기술원, 음성군청, 논산시, 인천상수도사업본부, 국가과학기술위원회 외.. |
| | 금융 기관 | **국민은행, 외환은행, 신한은행**, **삼성카드**, 현대카드, KB카드, 롯데카드, 마이비카드, 이비카드, 효성캐피탈, 대한투자증권, 대우증권, 메리츠증권, 키움닷컴증권, 푸르덴셜투자증권, 신영증권, KB신용정보, 대우캐피탈, 아주캐피탈, 고려상호저축은행, 스위스상호II저축은행, **삼성화재,** 대한생명, 신한생명, 현대하이카, 미래에셋생명, PCA생명, SK증권, 상호저축중앙회, 교원나라상호저축은행, 프라임상호저축은행 , 스마트로, KIS 정보통신, 서울보증보험, KB투자증권, 유화증권, 하나HSBC, KOCES, 한국정보통신,현대해상화재보험, 부산하나로카드, JTNET, KB금융지주,원캐싱, 현대커머셜, 서울신용평가정보 , 국민연금관리공단, 메리츠금융정보, 메리츠화재, 외환선물, 하나캐피탈, 금융투자협회, 리딩투자증권, ING생명보험 외.. |
| | 서비스/ 제조/ 통신 | **POSCO,** LG필립스, **KT**, 한화석유화학, 효성FMS, **삼성코닝정밀유리**, 금호타이어, 서초케이블, 현대홈쇼핑, 삼성테스코(1~3차), **인터파크,** 팍스넷, 그라비티, 세정, 서울아산병원, 서울의료원, 보라매병원, 중대의료원, 충주건국대 병원, 분당서울대병원, 마산삼성병원, 동국대경주병원, 충남대병원, 경상대학교병원, 제주대학교병원, 택시조합공제회, 대상정보기술, 대림산업, 한미약품, 현대모비스, 현대중공업, 현대미포조선, SBS골프채널, 한국무역정보통신, C&M커뮤니케이션, 스카이72, 현대백화점, 동아백화점, 마산대우백화점, 스타리온, 한국타이어, S-Oil, 아시아나IDT, 성남문화재단, KT&G, 농수산홈쇼핑, SK브로드밴드, 한국원자력의학원, 노틸러스효성, S-oil, 다음커뮤니케이션, Ncsoft, 스포츠토토 , 한국전력공사전력연구원, 그랜드코리아레저 , SK커뮤니케이션즈, 한국NSK, **삼성전자**, 안철수연구소, SK커머스 플래닛(11번가), 책임테크툴, 사이버로지텍,SBS콘텐츠허브, 아모레퍼시픽, 롯데리아 , 창명해운, 전자랜드, 후지필름, 하이마트,SK브로드밴드미디어, 위메이드엔터테인먼트, 바른손게임즈, 넥슨, 한화리조트&호텔, 태영건설, 태영CC, 롯데건설, 한빛소프트, 한국도시가스, 소프트웨어공제조합, 썬앳푸드 , 한국사이버결제, 삼호중공업, 쿠쿠전자 외.. |
| | 교육 기관 | 건국대, 경원대, 대불대, 선문대, 대진대, 청운대, 대구대, 한국항공대, 전북대, 제주대, 경인교육대, 진주교대, 혜전대, 배화여대, 청주교대, 구미1대학, 성신여대, 부산디지털대학교, 단국대, 부천대, 창원전문대, 국민대, 국제디지털대학, 삼육어학원, 영남대학교, 원광디지털대학교, 한국해양대학교, 강원교육정보원, 한국기술교육대학교,충청남도교육청, 충청북도교육청, 경상남도교육청, 경남교육연구정보원,, 대구가톨릭대학교, 공주대학교, 경상대학교, 광주광역시정보원, 연세대학교, 경북전문대학, 원광대학교, 울산과학대학,경성대학교, 한국과학영재학교, 동아대학교, 영산대학교, 전라북도교육청, 대구 한의대 ,대구교육대학교, 계명문화대학, 동명대학교 , 강원외국어교육원, 대학교육협의회, 남서울대학교, 한양대학교, 우송대학교, 충주대학교, 유한대학, 과학기술연합대학원대학교 외 |
| 일본 | 금융, 제조, 서비스, | **150여 고객 사** |
| 중국/대만 | 통신, 교육, | 청화 텔레콤 , 크리스챤 University, NTNU |
| 브라질 | 금융 | Prudential Insurance (브라질 최대 국영보안기관) |
| 캄보디아 | 공공 | NIDA |
| 말레이시아 | 교육 기관 | Universiti Teknologi Malaysia, UMMC(병원) |
| 독일 | 통신/금융 | German Telecom, FITS(금융 DataCenter) |

# 개인정보 보호법 개요

## 사고 사례

### <침해사고 사례>SK컴즈


11년 7월 해킹으로
싸이월드, 네이트의
3,500만명 개인정보 유출

- 개인정보에 대한 관리적, 기술적 보호조치 준수의 중요성 확인
  - ☞ 사상최대 분량의 개인정보가 유출되었으나 정보가 암호화되어 유출 개인정보 해독 불가능
- 대형 해킹 사고라도 사소한 원인인 경우가 많으므로 보안관리와 투자가 중요

### <침해사고 사례> 현대캐피탈


11년 2월 해킹 공격으로
175만명 개인정보 유출

- 퇴직자 ID, 비밀번호 미삭제 등 관리 미흡
- 홈페이지 보안 관리미흡
- 유출시 해독 방지를 위한 암호화 조치 미흡

**개인정보 보호 관심 증대** → **개인정보보호법 시행**

[개인정보보호 의무 대상자] - 350만으로 확대
공공기관, 정보통신서비스제공자, 준용사업자, 신용정보 제공 서비스 이용자, 비영리 단체, 법원 등 헌법기관, 비영리 단체 등

# 개인정보 보호법 개요

## 개인정보 보호법이란 ?

### 개인정보?

일반적으로 **"특정 개인을 식별하거나 식별할 수 있는 정보"**

즉, 개인과 관련된 일체의 정보는 모두 개인정보에 해당될 수 있다(예: 성명, 주소, 연락처, 직업 등)

직접 관련이 있는 정보 뿐만 아니라 **그 개인에 대한 타인의 의견, 평가, 견해 등 제3자에 의해 생성된 간접적인 정보**(예: 신용평가 정보 등)도 해당될 수 있다.

- **생존하는 자연인(O), 사망(X), 법인(X).**
- **다른 정보와 결합하면 개인식별이 가능하면 모두 개인정보**

### 개인정보 보호?

정보주체(고객, 이용자)의 개인정보가 안전하게 수집·이용·취급·관리되도록 하고, 정보주체의 동의 없이 함부로 수집되거나 이용·제공되지 않도록 함으로써 정보주체의'개인정보 자기결정권'을 보장하는 것

### 개인정보처리시스템

**개인정보의 체계적인 처리를 위한 DBMS (Database Management System)**을 말한다.

공공기관, 영리목적의 민간분야 사업자, 협회·동창회 등 비영리 기관·단체를 모두 포괄
중앙행정기관, 중앙선거관리위원회·국회 등 헌법기관, 정유사, 대형마트, 비디오대여점, 렌트카업체, 부동산중개업자, 자동차매매업자, 학교, 보험회사, 은행, 통신사, 여행사, 항공사, 호텔, 학원, 협회, 동창회, 동호회 등

# 개인정보 보호법 개요

## 개인정보 보호법 주요내용

### 개인정보보호법 (법률 제10465호, 2011. 3.29, 제정 시행 2011.09.30)

| | |
|---|---|
| **제24조 고유식별정보의 처리 제한** | ③개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 **고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.** |
| **제29조 안전조치 의무** | 개인정보처리자는 **개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.** |
| **제31조 개인정보 보호책임자 지정** | ① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다.<br>② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.<br>1. 개인정보 보호 계획의 수립 및 시행<br>2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선<br>3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제<br>**4. 개인정보 유출 및 오·남용 방지를 위한 내부통제시스템의 구축**<br>5. 개인정보 보호 교육 계획의 수립 및 시행<br>**6. 개인정보파일의 보호 및 관리·감독** |
| **제70조 벌칙** | 공공기관의 개인정보 처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경하거나 말소하여 공공기관의 업무 수행의 중단·마비 등 심각한 지장을 초래한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다. |
| **제73조 벌칙** | 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.<br>1. 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·변조 또는 훼손당한 자 |
| **제75조 과태료** | ② 다음 각 호의 어느 하나에 해당하는 자에게는 **3천만 원 이하의 과태료**를 부과한다.<br>6. 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자 |

# 개인정보 보호법 개요

## 개인정보 보호법 주요내용

### 개인정보보호법 시행령 (대통령령 제23169호, 2011. 9.29, 제정시행 2011.09.30)

**제18조 민감정보의 범위**

1. 유전자검사 등의 결과로 얻어진 유전정보
2. 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보

**제19조 고유식별정보의 범위**

1. 「주민등록법」 제7조제3항에 따른 주민등록번호
2. 「여권법」 제7조제1항제1호에 따른 여권번호
3. 「도로교통법」 제80조에 따른 운전면허의 면허번호
4. 「출입국관리법」 제31조제4항에 따른 외국인등록번호

**제30조 개인정보의 안전성 확보조치**

① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
2. **개인정보에 대한 접근 통제 및 접근 권한의 제한 조치**
3. **개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치**
4. **개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치**
5. **개인정보에 대한 보안프로그램의 설치 및 갱신**
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

② 행정안전부장관은 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 행정안전부장관이 정하여 고시한다.

**제43조 개인정보 유출 통지의 방법 및 절차**

① 개인정보처리자는 개인정보 유출이 발생한 사실을 안 때에는 서면·전자우편·모사전송·전화·휴대전화 문자전송 또는 이와 유사한 방법을 통하여 지체 없이 법 제32조제1항 각 호의 사항을 정보주체에게 알려야 한다. 다만, 개인정보의 유출 확산 방지를 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 대응조치가 필요한 경우에는 해당 조치를 취한 후 지체 없이 정보주체에게 알릴 수 있다.

**제63조 과태료의 부과기준**

| 위반행위 | 근거 법 조문 | 과태료 금액 | | |
|---|---|---|---|---|
| | | 1회 위반 | 2회 위반 | 3회 이상 위반 |
| 차. 법 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우 | 법 제75조 제2항제6호 | 600 | 1200 | 2400 |

# 기술적 보호조치 기준고시

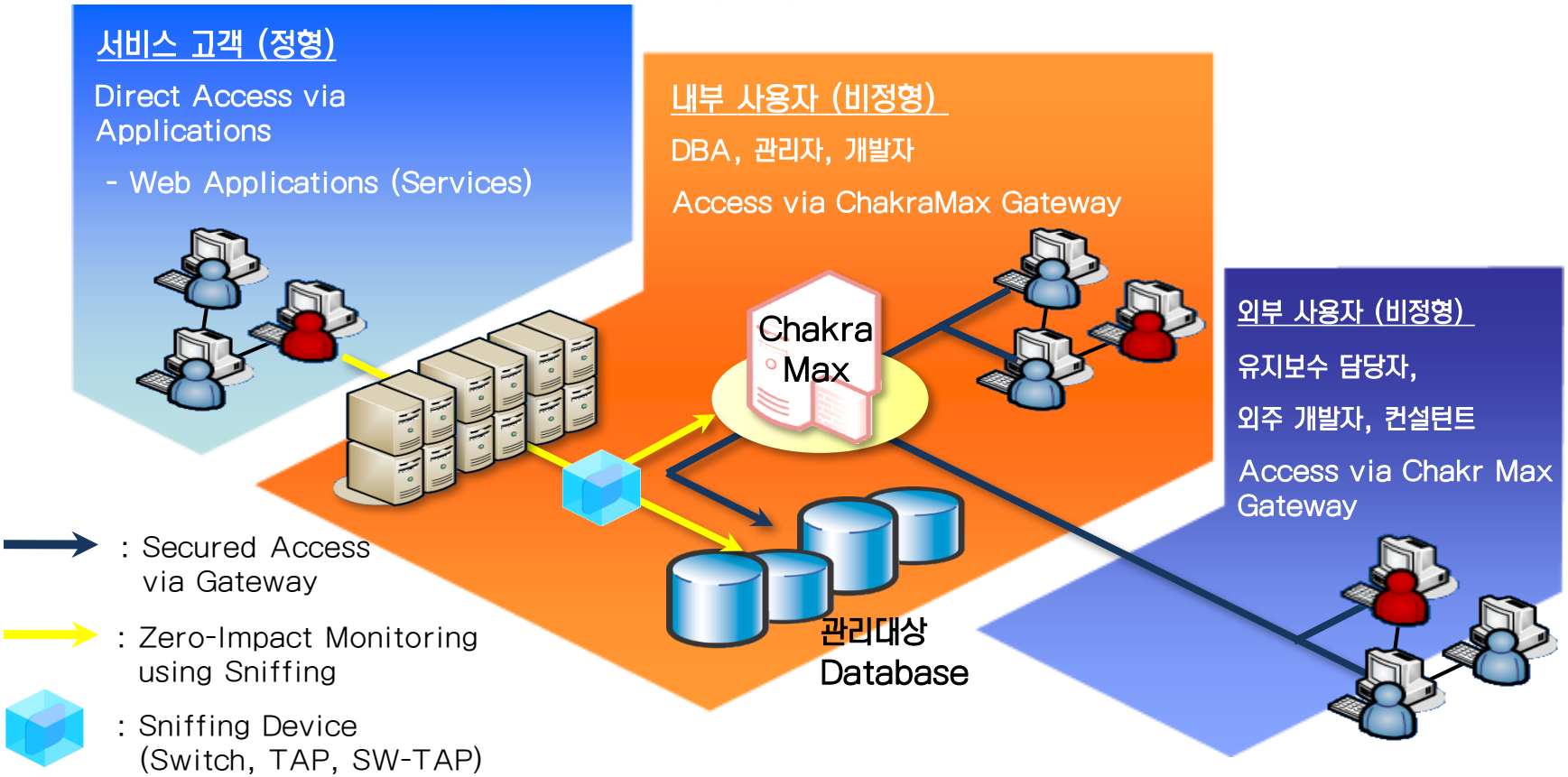
## 개인정보 보호를 위한 체크리스트

| 보안 체크리스트 | 비고 |
|---|---|
| 1. 고객 개인정보를 보호하기 위해 내부 관리 계획을 수립했는가. | |
| 2. 최소한의 정보만을 수집하고 수집 목적과 사용 범위를 사용자에게 알리고 동의를 받았는가. | |
| 3. 원래의 개인정보 수집·이용 목적이 변경되거나 추가된 경우 별도의 동의를 받았는가. | |
| 4. 개인정보 업무를 외주업체에 위탁할 때 고지하고 동의를 획득했는가. | |
| 5. 개인정보 취급자를 최소한자로 제한하고 권한을 통제했는가. | |
| √ 6. 침입차단 시스템 등 물리적인 접근통제 장치들을 설치했는가. | Chakra DB접근제어 |
| √ 7. 내부자에 의한 개인정보 유출 방지를 위해 접속기록의 보존 및 위조·변조 방지를 위해 접속기록을 관리했는가. | Chakra DB 접근 감사 |
| √ 8. 개인정보 전송 및 저장 시에는 암호화 등 보호조치를 적용했는가. | Chakra의 Data masking (중요 정보 은닉 기능) |
| 9. 조직 내 법률 부서에서 집단 분쟁 조정 및 단체소송 등 정보주체의 권리행사에 대응할 수 있는 대응체계를 구축했는가. | |
| 10. 개인정보보호 관련 각종 인증을 획득하고 감독활동을 강화했는가. | |

# DB 접근제어 제안 방식

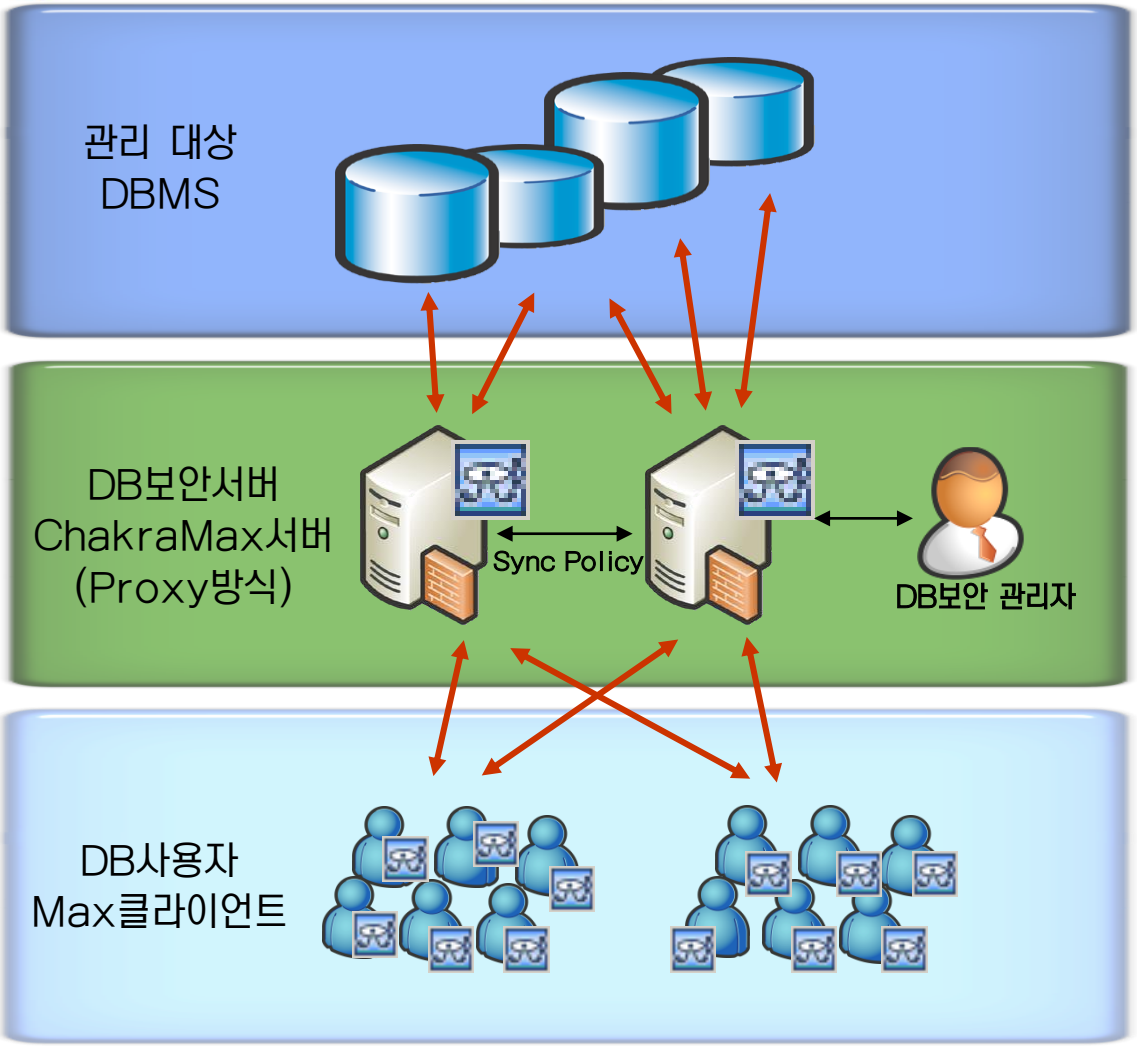
- **비정형 쿼리**를 수행하는 데이터베이스 사용자에 대해 **적극적 통제가 가능한 Gateway 적용**.
- 정형 쿼리가 수행되는 **APS혹은 WAS에 대해** 감사데이터 축적을 위해 **Sniffing 방식 적용.**

## Hybrid 방식 구성



# DB 접근제어 제안 방식

## Gateway 방식 구성




Proxy방식으로 운영되는
ChakraMax는 SQL 실행을 통제

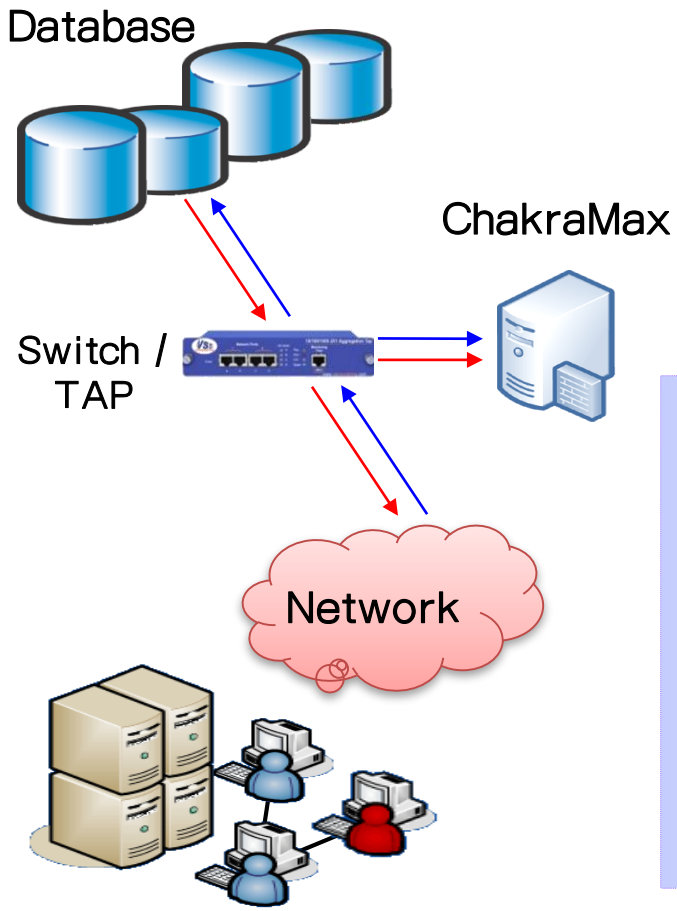
사용자는 DB직접 접속이 통제되며
보안 서버를 경유한 접속만 허가됨

보안 관리자는 ChakraMax서버에
접속하여 접근제어 정책을 설정

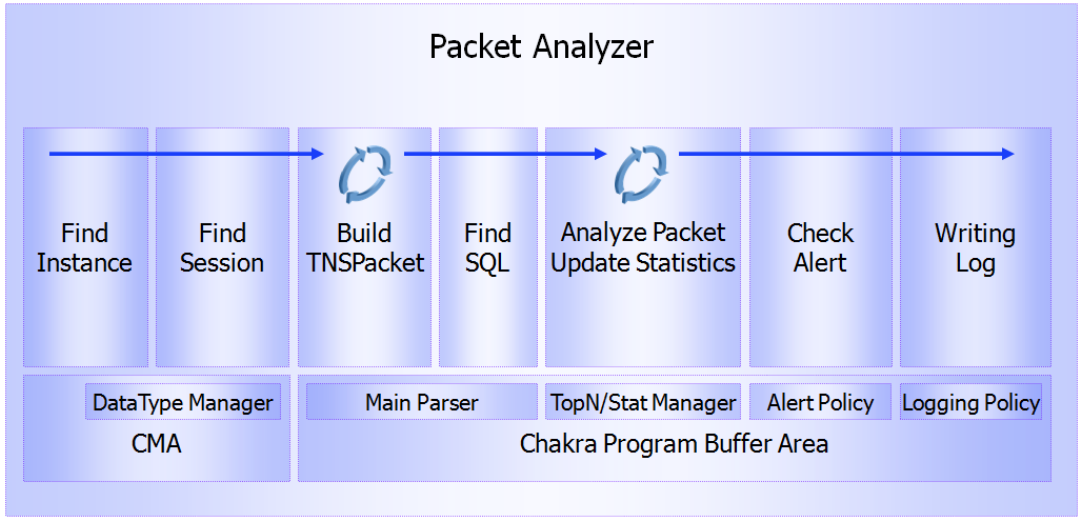
ChakraMax서버 이중화 구성을
통해 업무 연속성을 확보

# DB 접근제어 제안 방식

## Sniffing 방식 구성




- ✓ 네트워크에서 데이터베이스 패킷 수집.
- ✓ 수집된 패킷을 손실 없이 분석하고 SQL 정보 추출.
- ✓ 구문분석기를 통한 SQL 분석.
- ✓ 설정된 보안 정책을 적용하고 경고 발생 및 통제 수행.
- ✓ 수집된 SQL및 세션 정보를 저장.
- ✓ 감사 보고서 제공을 위한 다양한 통계정보 생성.



# 접근제어 적용 기능

## 제품 개요

**1. Chakra Max는 DBMS에 원격으로 접속하는 모든 Client의 작업 행위를 감시합니다.**

- Inline방식의 Gateway타입
- Proxy방식의 Gateway 타입
- Sniffing 방식의 Passive 타입
- Gateway방식과 Sniffing방식을 동시에 운영하는 Hybrid 타입

**2. Chakra Max는 DBMS 내부에서 접속하는 모든 Client의 작업행위를 감시합니다.**

- BEQ방식 접근을 감지하는 Local Agent 지원
- Local Loop 방식 접근을 감지하는 Local Agent 지원

**3. Chakra Max는 DB작업 통제를 위한 사용자 인증과 사전결재를 지원합니다.**

- **Oracle**, DB2, MSSQL, Sybase, **Teradata**, Tibero, Infomix, MySQL, PostgreSQL, Cubrid, Symfoware.
- 사용자 접근 인증
- 결재정책 (자동결재, 사전결재, 사후결재)

# 접근제어 적용 기능

## 제품 개요

**4. Chakra Max는 사용자에게 기밀 정보 노출 방지를 위해 데이터 변조 전송 (Masking)을 지원합니다.**

- Rerun Row의 Column Data 암호화 전송

**5. Chakra는 DBMS의 서비스 무 정지와 사용자의 작업안전을 위해 이중화 구성을 지원합니다.**

- Active-Standby 구성 지원
- Active-Active 구성 지원
- 비상시 Bypass 구성 지원

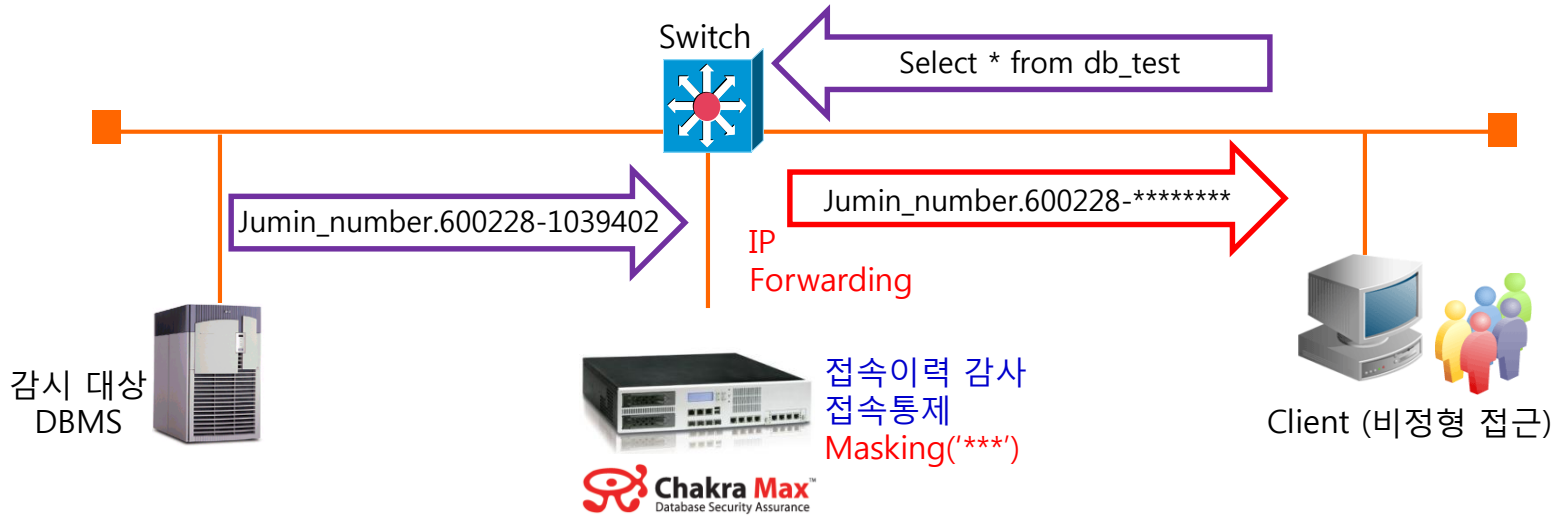
**6. Chakra는 DBMS뿐만 아니라, Server에 작업하는 모든 행위를 기록, 통제합니다.**

- SSH, Telnet, Ftp, Rlogin, R-command 모든 명령어 및 서버 반환 메시지 기록
- 통제정책에 따른 비정상 행위 경보 및 통제

# 접근제어 적용 기능

## Masking 기능

- DB서버 외부로 Network을 통한 Data 전송 시 암호화 기능




※ 전체/패턴 Masking, 포맷 문자 정의 기능이 가능합니다.

**※ 함수 파라메터로 조회되는 경우도 Masking이 가능합니다.**

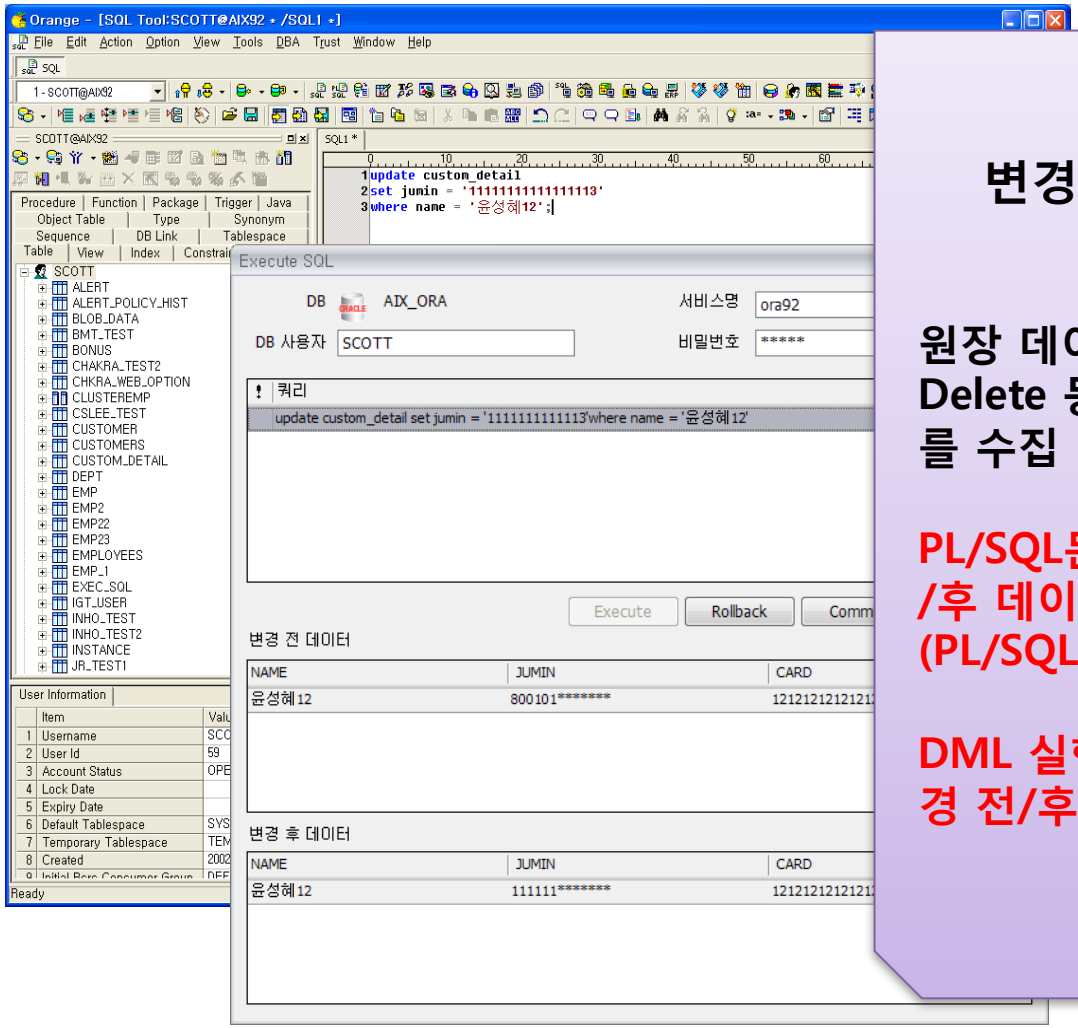
예) select concat(job, jumin_no) from cust_info;

※ 다양한 Data Type에 대해 Masking이 제공됩니다. (VARCHAR, NUBMER, DECIMAL...)

**※ Masking을 위해 관리 대상 DB에 어떠한 변경도 만들지 않습니다.(경쟁사 대비 장점사항)**

# 접근제어 적용 기능

## 변경 전/후 데이터 Logging




**변경 전/후 데이터 Logging 기능 (금감원 규제 사항)**

**원장 데이터에 대한 Update/ Insert/ Delete 등 DML실행 시, 변경 전/후 데이터를 수집 하고 감사 데이터로 제공.**

**PL/SQL문장 내부에 포함된 DML도 변경 전/후 데이터 제공.**
**(PL/SQL 전용 문법 분석기 탑재)**

**DML 실행 결재 기능 사용 시, 결재자가 변경 전/후 데이터 확인 후 승인 가능.**

# 접근제어 적용 기능

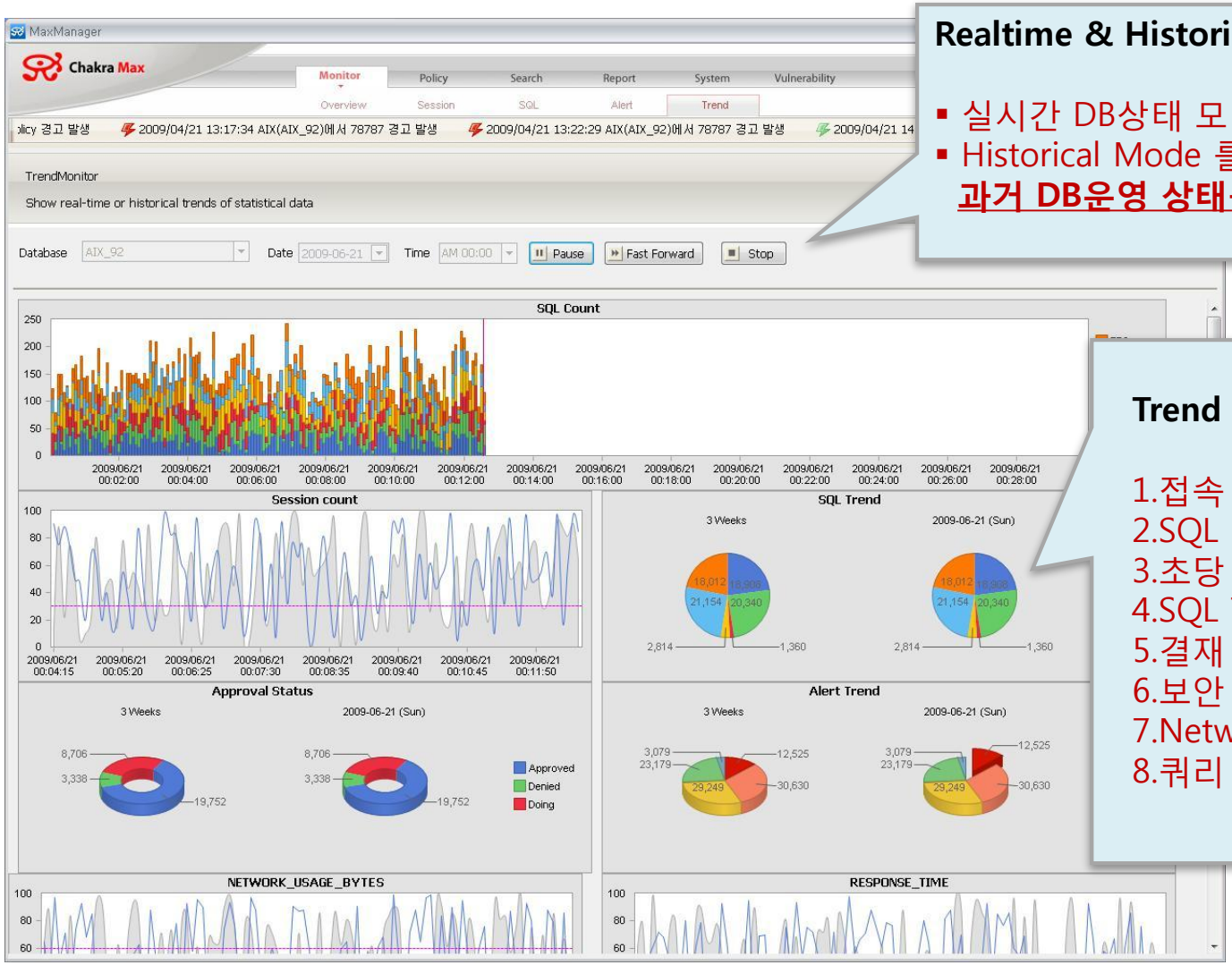
## Security Policy 통제 정책 항목

| 정책 구분 | Policy Key Word | 내 용 |
|---|---|---|
| 날자, 시간 | **Time** | 시간 범위 |
| | **Holiday** | 요일/공휴일 |
| | **Date** | 일자 범위 |
| DB 접속 관점 Session 제어항목 | **Client Ip Address** | Client IP Address |
| | **Host Name** | Client Host Name |
| | **App Name** | Application |
| | **Login User** | System Account |
| | **DbUser** | DB Account |
| | **Max User** | Max 사용자 계정 |
| | **OsUser** | Client OS Account |
| Command | **Cmd** | Telnet, FTP Command |
| Instance | **DbInstRespTime** | 평균 응답시간(최근1분) |
| | **DbInstSessCount** | Instance 세션 수 |
| Orange | **N/A** | 쿼리 결과 파일 저장 |
| | | 쿼리 결과 Copy |
| | | 쿼리 결과 Print |

| 정책 구분 | Policy Key Word | 내 용 |
|---|---|---|
| DBMS 성능 관점Session 제어 항목 | **DbSessRespTimeSum** | 세션 응답시간 합계 |
| | **DbSessRespAvg** | 세션 응답시간 평균 |
| | **DbSessRowsSum** | 세션 Return Row 합계 |
| | **DbSessRowsAvg** | 세션 Return Row 평균 |
| | **DbSessInSum** | 세션 패킷 In 합계 |
| | **DbSessInAvg** | 세션 패킷 In 평균 |
| | **DbSessOutSum** | 세션 패킷 Out 합계 |
| | **DbSessOutAvg** | 세션 패킷 Out 평균 |
| | **Idle Time** | Idle Time |
| | **DbSessSqlCount** | 세션 내 수행 SQL 건수 |
| | **DbSessFailCount** | 결과가 Fail인 SQL 건수 |
| SQL 제어 항목 | **DbSqlRespTime** | SQL 응답시간 |
| | **DbSqlRows** | SQL Return Rows |
| | **DbSqlIn** | SQL 패킷 In 건수 |
| | **DbSqlOut** | SQL 패킷 Out 건수 |
| | **DbSqlRetCode** | SQL 오류 코드 |
| | **DbSqlType** | SQL Type |
| | **DbSqlText** | Text 내 특정 Object |
| | **DbTable** | Text 내 특정 Table |
| | **DbColumn** | Text 내 특정 Column |
| | **DbSqlCommand** | Text 내 특정 Command |

# 접근제어 적용 기능

## 모니터링 – Trend Monitor




**Realtime & Historical .**

- 실시간 DB상태 모니터링 제공
- Historical Mode 를 이용하면
  **과거 DB운영 상태를 Play 할 수 있음.**

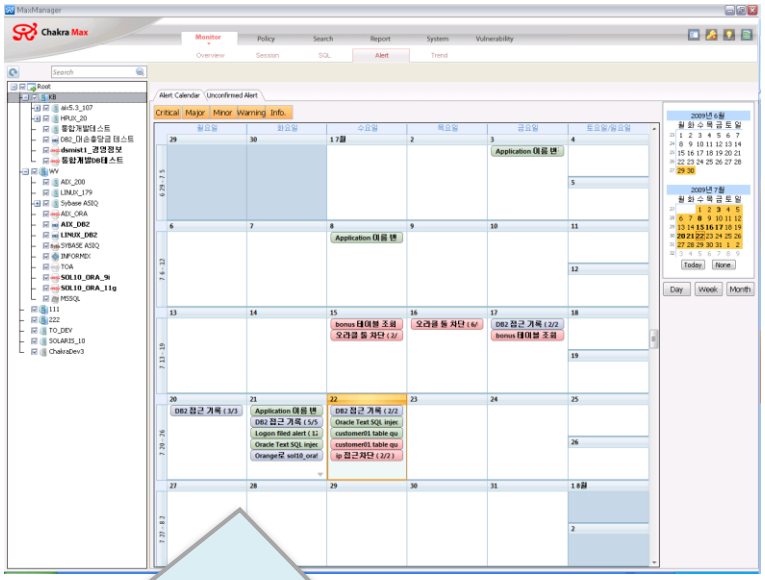
**Trend Chart List**

1.접속 세션 추이
2.SQL 평균 응답 시간 추이
3.초당 SQL 실행 횟수 추이
4.SQL Type별 실행 통계
5.결재 진행 추이
6.보안 사고 발생 추이
7.Network 사용량 추이
8.쿼리 조회 건수 추이

# 접근제어 적용 기능

## 모니터링 – Alert Monitor(1/2)

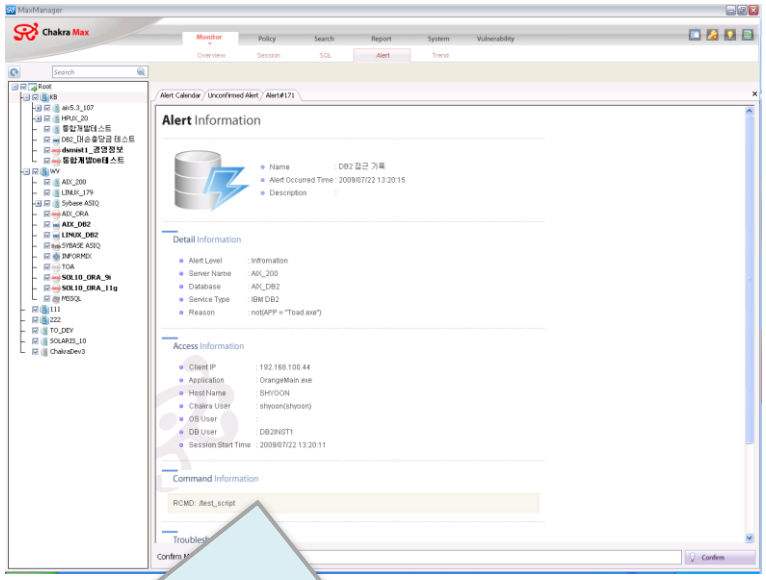
### Alert Monitor Calendar



**Alert Monitor Calendar**

- 경고가 발생된 날짜를 달력 형식을 조회.
- 주간 별, 지정된 날짜의 시간 별  조회가 가능
- 경고 등급 별로 Coloring되어 추이 파악이 용이

### Alert 상세보기



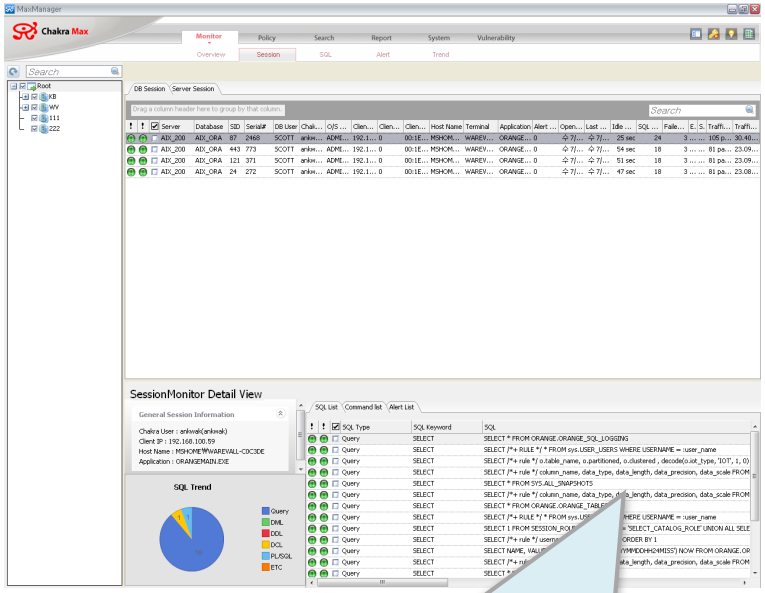
**Alert 상세 보기**

- 발생된 Alert의 내용을 HTML로 조회
- **Confirm 기능**을 통해 관리자의 **Alert 발생 내역 확인 이력을 저장**.

# 접근제어 적용 기능

## 모니터링 – Alert Monitor(2/2)

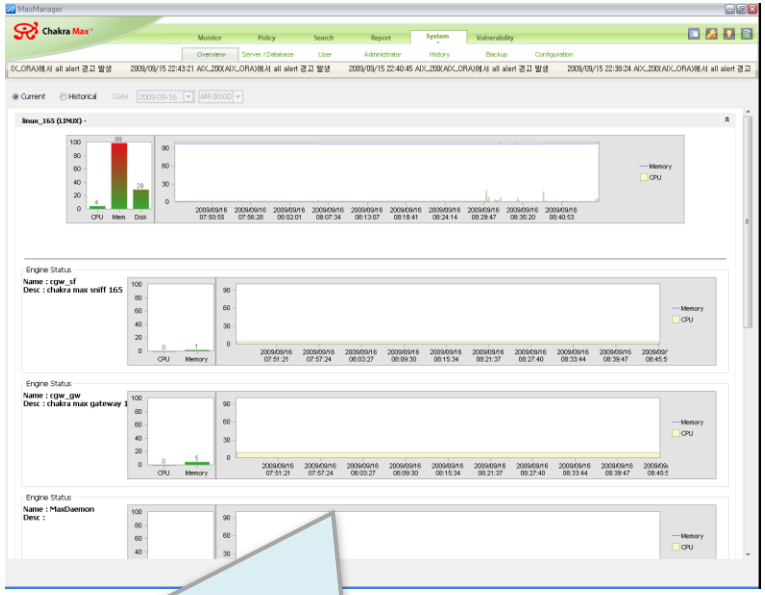
### Session Monitor




**Session Detail View**

- 선택된 세션에서 실행된 SQL혹은 Command 정보를 확인.
- 실행된 SQL의 Type별 분포 챠트

### Chakra Max Server Overview




**Chakra Max Server Overview**

- Max Server 자원 사용량 조회
  - CPU / Memory / Disk space
- Max Repository 자원 사용량 조회
  - 초당 Transaction / Network Traffic / Data space Usage / CPU, Memory

# 접근제어 적용 기능

## Database Access **Log Analysis**

**Grid View**

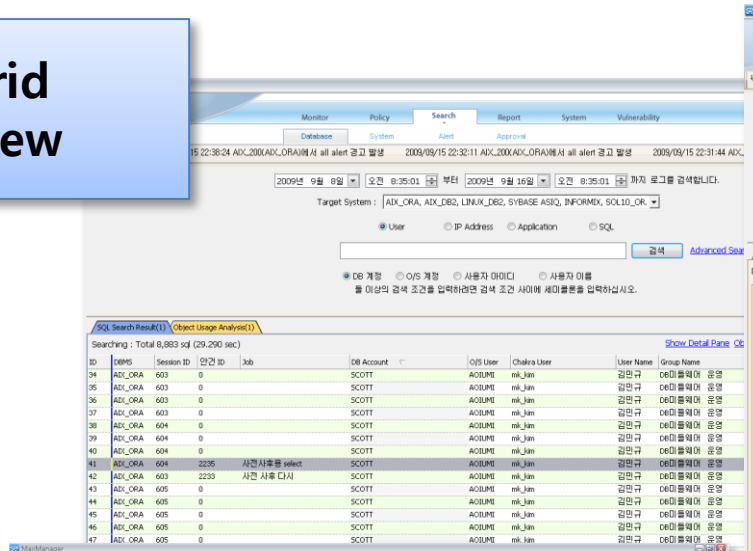
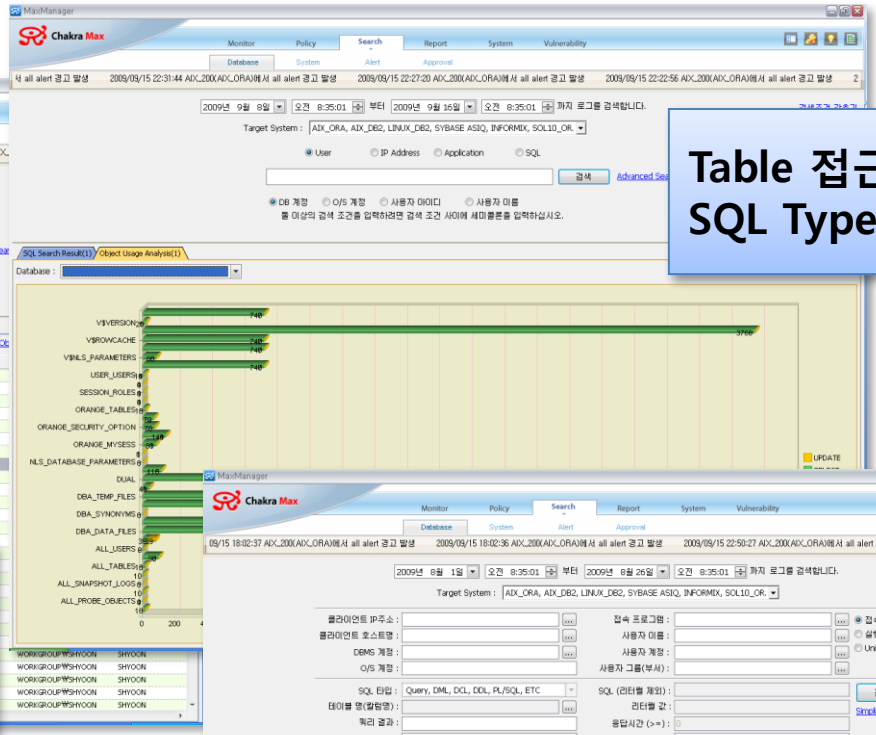
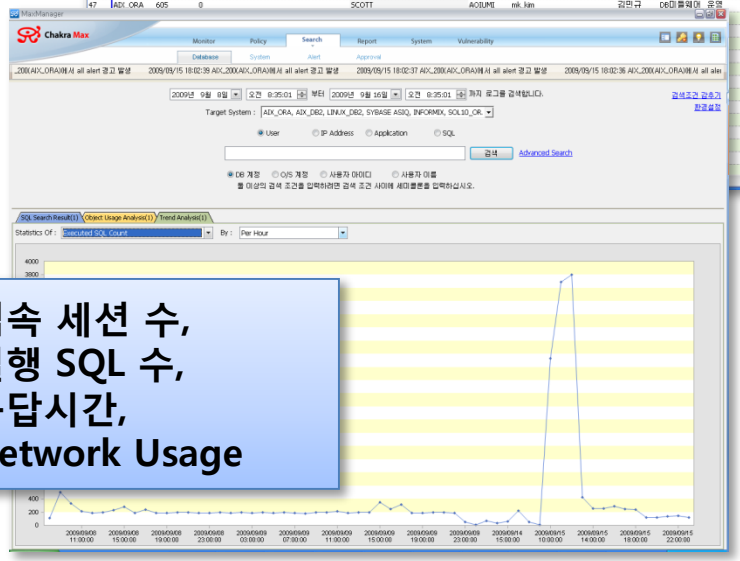
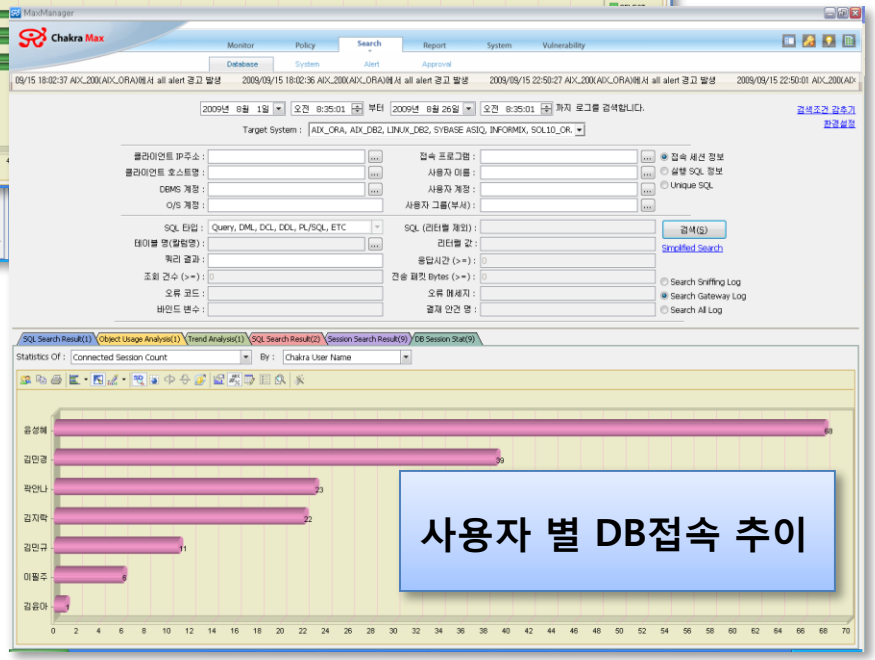


**Table 접근 통계**
**SQL Type통계**





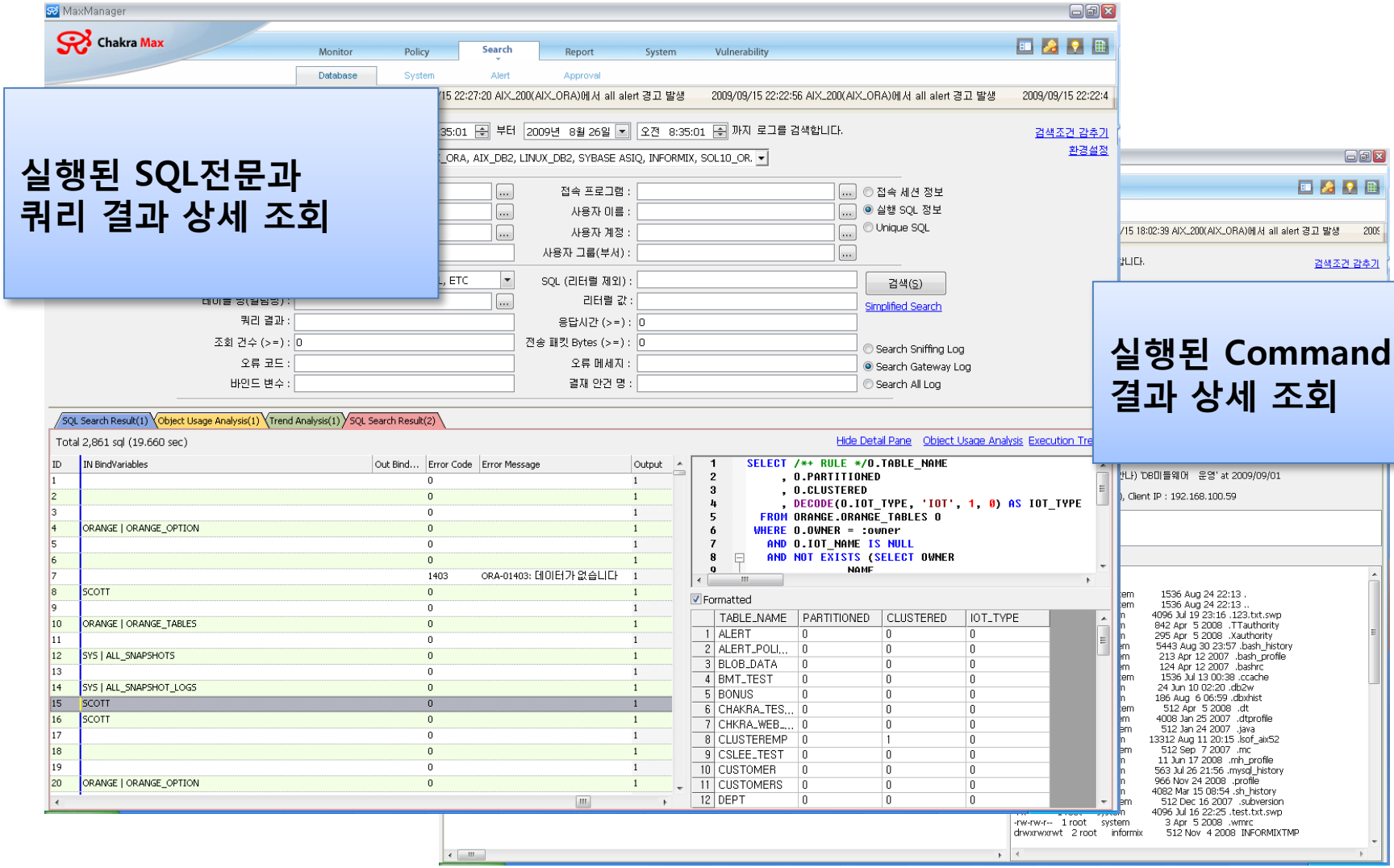
**접속 세션 수,**
**실행 SQL 수,**
**응답시간,**
**Network Usage**



**사용자 별 DB접속 추이**

# 접근제어 적용 기능

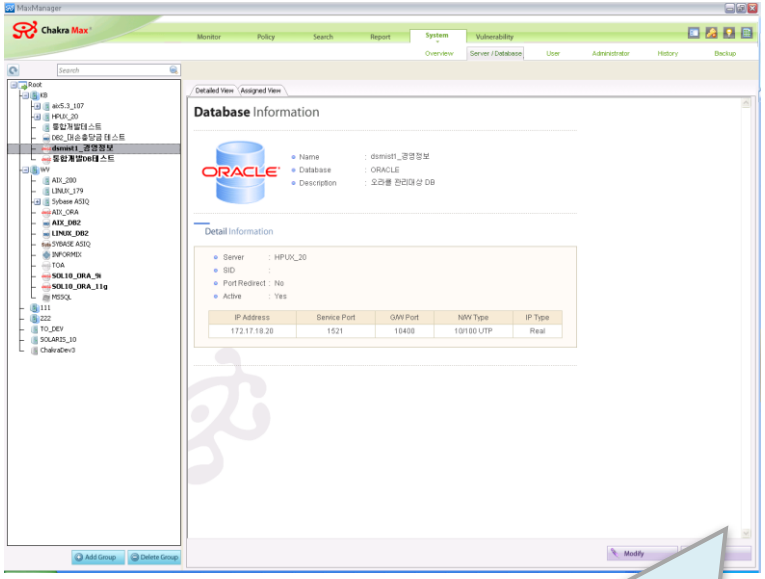
## Database Access **Log Analysis**



# 접근제어 적용 기능

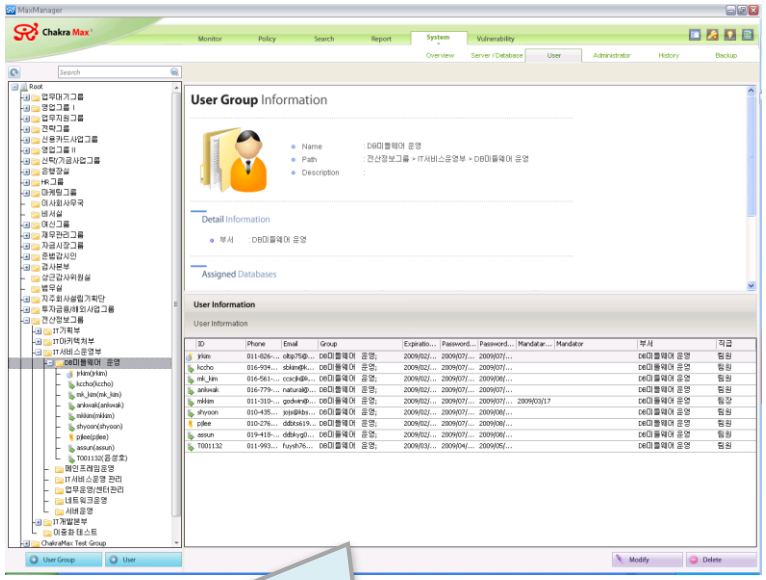
## Database,Server 관리 / 사용자/그룹 관리

### Database,Server 관리




1.관리 대상 Server와 Database는 임의의 Grouping이 가능.
**2.관리 효율성을 위해 Group별 보안 정책 관리 가능.**
3.Server와 Database에 접속 가능한 사용자 설정이 가능.
**4.Clustering Database (RAC) 환경 지원**
Node별 통합 모니터링과 리포팅 지원

### 사용자/그룹 관리

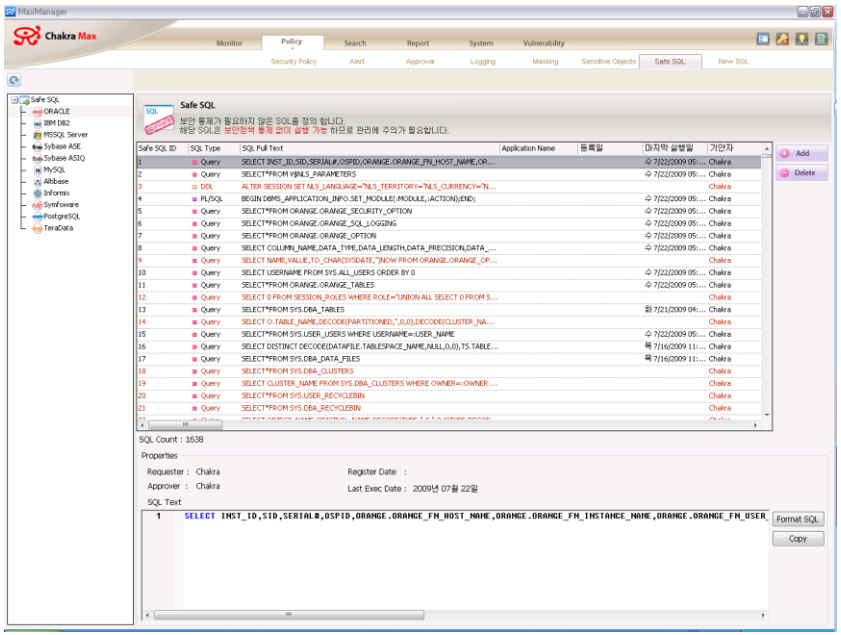



**1.Chakra Max는 사용자에게 임의의 Custom Field를 설정할 수 있고, 이를 이용한 Grouping이 가능.**
즉, 고객 요청에 따라 임의의 사용자 필드 제공 가능하며 이를 이용한 결재 경로 생성이 가능

# 접근제어 적용 기능

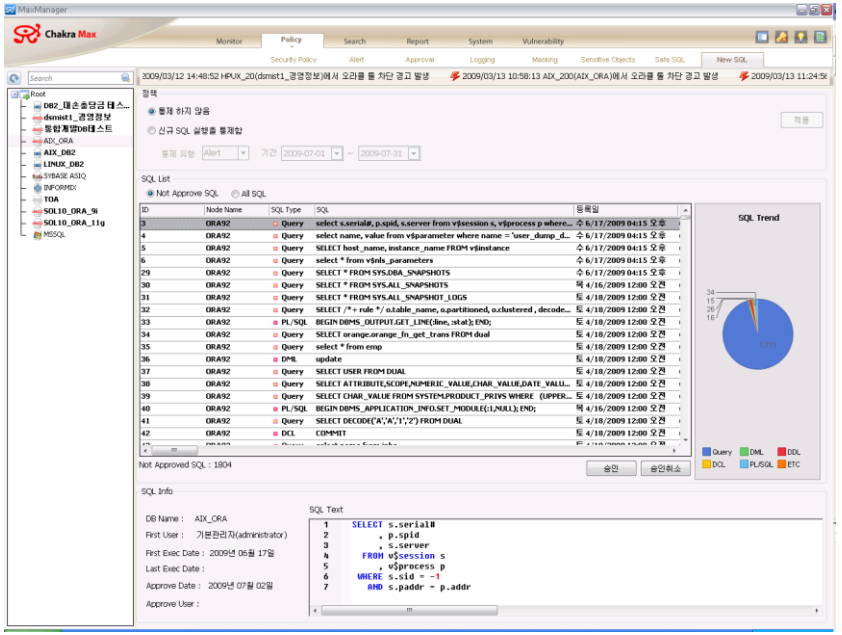
## 보안 정책

### SafeSQL




- DBMS별로 보안 상 이슈가 없는 SQL문장을 관리.
- 실무자에게 보안 시스템 사용 편의성을 제공.
- SafeSQL 등록 시기
  승인 요청자와 승인 DBA 정보 제공

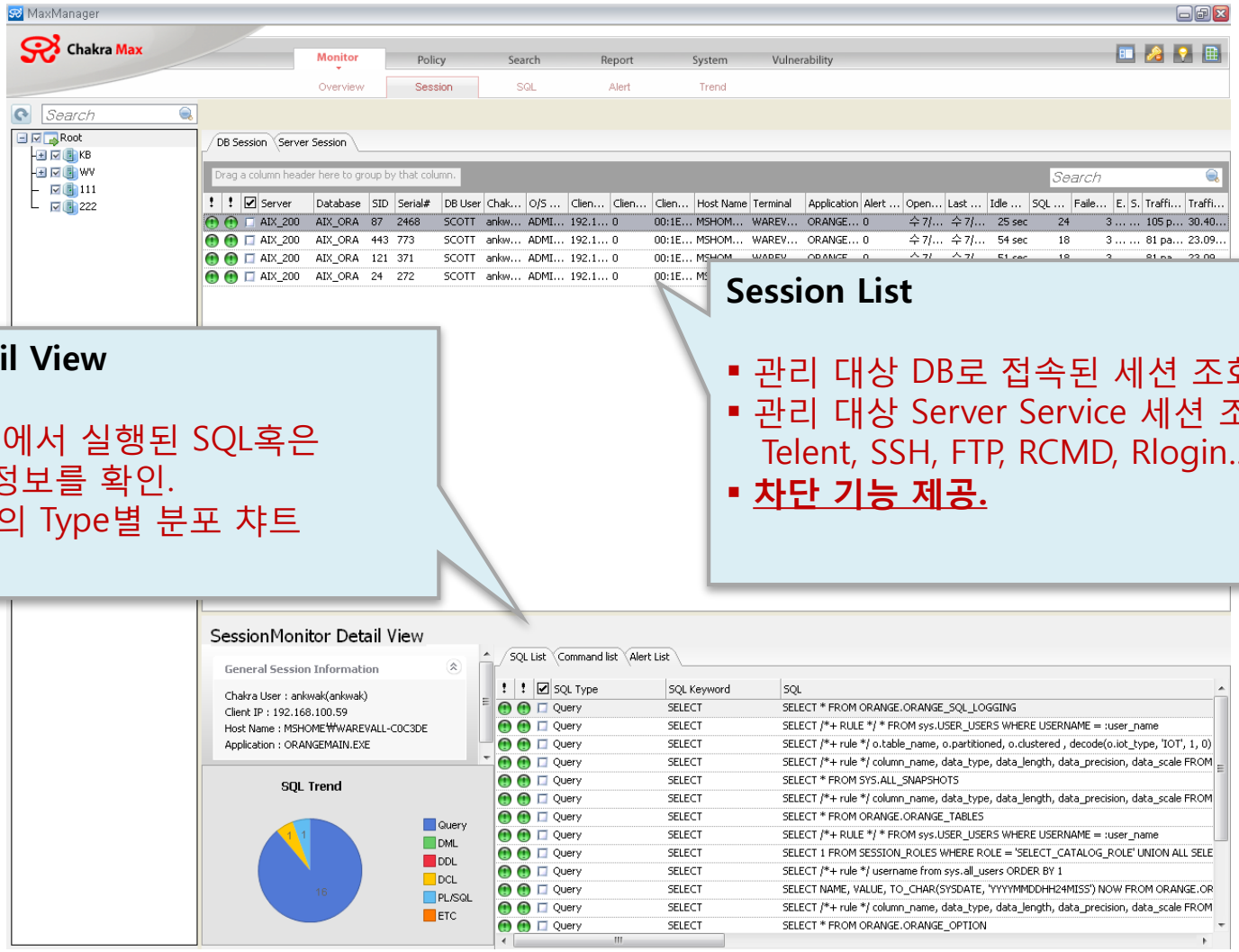
### New SQL 관리




- 관리 대상 Database에서 한 번 이상 실행된 SQL 문장을 조회
- 최초 실행 시간과 작업자 정보 제공
- Type별 SQL 통계 제공.
- 신규 SQL 실행 시 통제 혹은 경고 발생
- 신규 SQL 정책은 적용 기간 선택 가능.
- 승인/취소 기능으로 신규 SQL통제 가능.

# 접근제어 적용 기능

## Session Monitor




### Session Detail View

- 선택된 세션에서 실행된 SQL혹은 Command 정보를 확인.
- 실행된 SQL의 Type별 분포 챠트

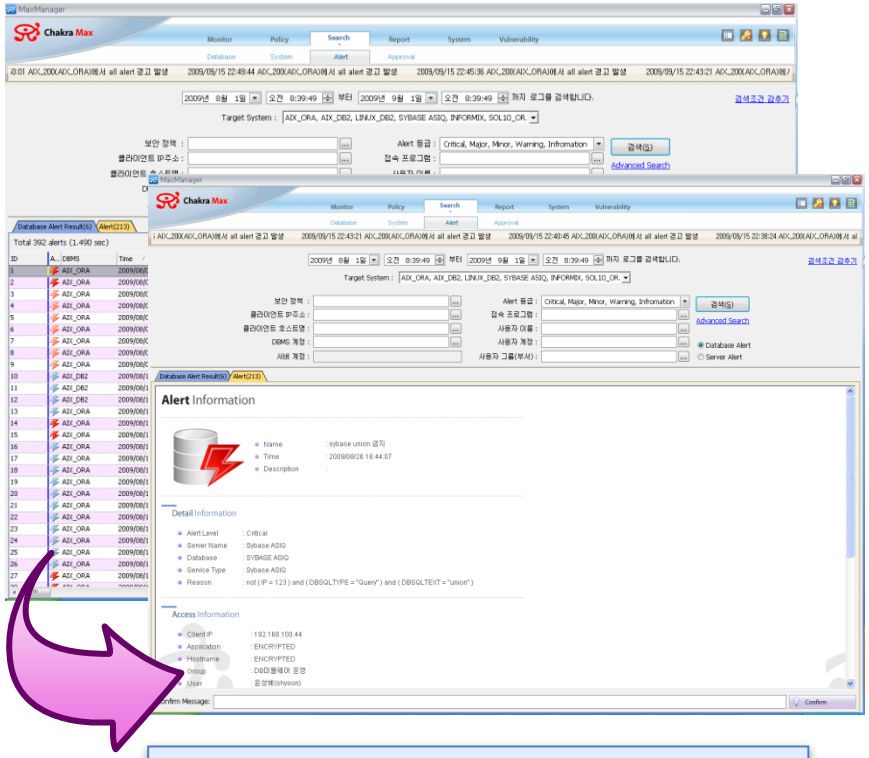
### Session List

- 관리 대상 DB로 접속된 세션 조회
- 관리 대상 Server Service 세션 조회
  Telent, SSH, FTP, RCMD, Rlogin...
- **차단 기능 제공.**

# 접근제어 적용 기능

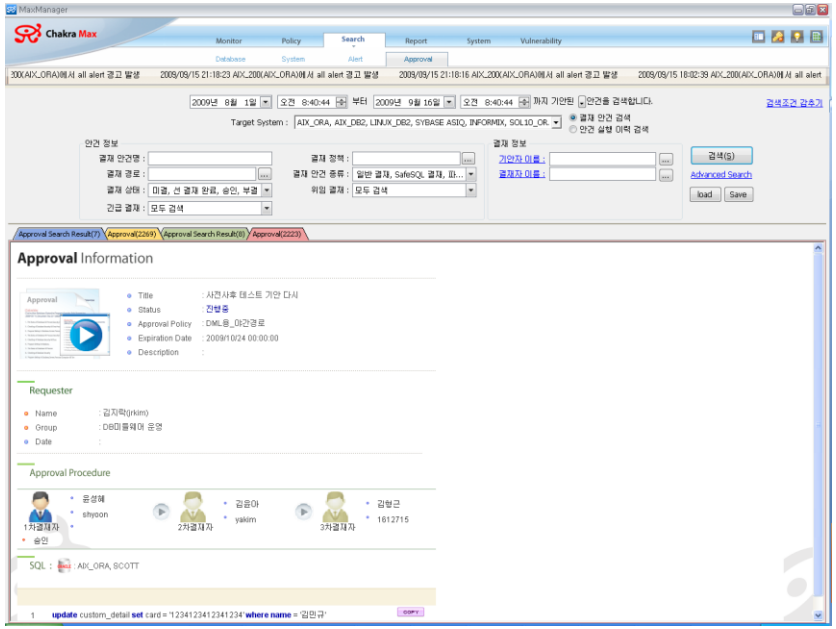
## Log Analyzer

### Alert 정보 상세 검색




다양한 검색 조건으로
Alert 발생 내역 검색이 가능하며,
발생된 Alert의 상세정보가 HTML로 제공.

### 결재 정보 상세 검색



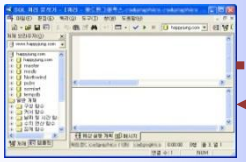

다양한 검색 조건으로
결재 안건 검색이 가능하며,
결재 안건의 상세정보가 HTML로 제공.

# 접근제어 적용 기능

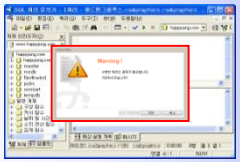
## Approval Process

### DB 작업자

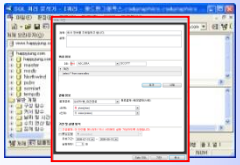
1) 쿼리 툴을 이용 SQL 작업 실행



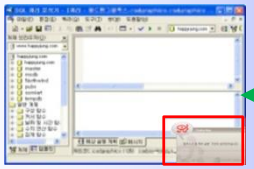
4) 보안정책에 따라 차단됨을 통지 받음



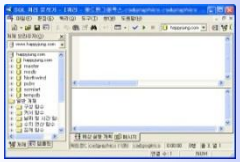
5) 지정된 결재경로에 따라 SQL 실행 기안



10) 기안된 안건이 승인 완료됨을 통보 받음



11) 승인된 SQL을 쿼리 툴로 실행



### Chakra Max

2) 보안 정책 위배. 요청된 SQL 차단

3) 사전 승인이 필요한 SQL임을 작업자에게 통보

6) 기안된 정보로 결재 경로 추출

7) 결재 경로에 따라 지정된 결재자에게 결재 요청 통보.

9) 지정된 결재자(들)의 결재 결과를 기안자에게 통보.

12) 승인된 SQL확인 후 실행을 허가

**DB Session**
Query Tool ⇔DB Gateway

**Chakra Max Session**
Max Client ⇔ Max Server

### 결재자

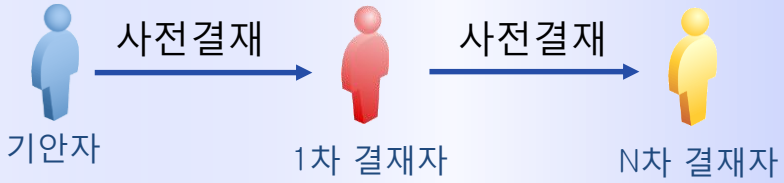
8) 결재 경로에 따라 지정된 결재자 혹은 위임 결재자가 결재 수행. 사전/사후 결재 지원

관리 대상 데이터베이스

# 접근제어 적용 기능

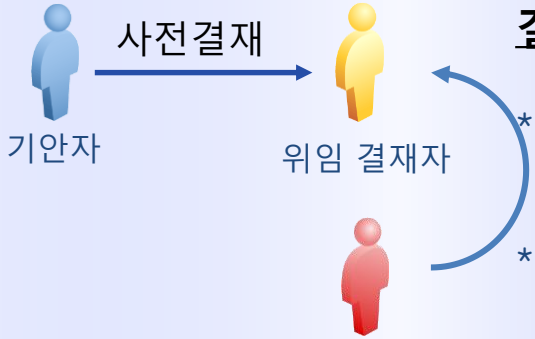
## 다양한 결재 경로

### 다 단계 결재 지원




5차 결재자 까지 지정 가능

### 위임 결재 지원

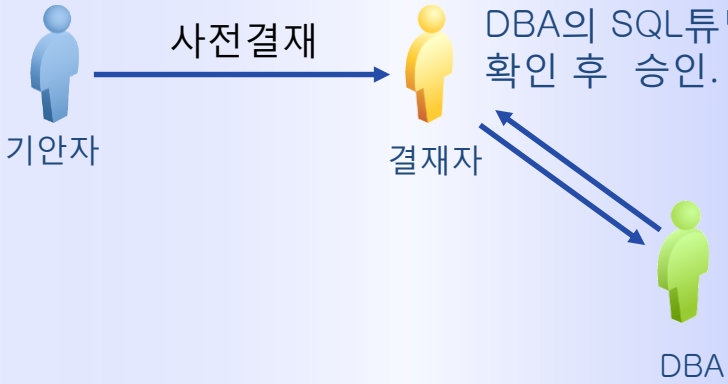



**결재권. 위임**

* 지정된 시간/기간 동안 위임 가능

* 기간이 지나면 결재권 자동 회수.

### SQL 튜닝 의뢰 결재 지원

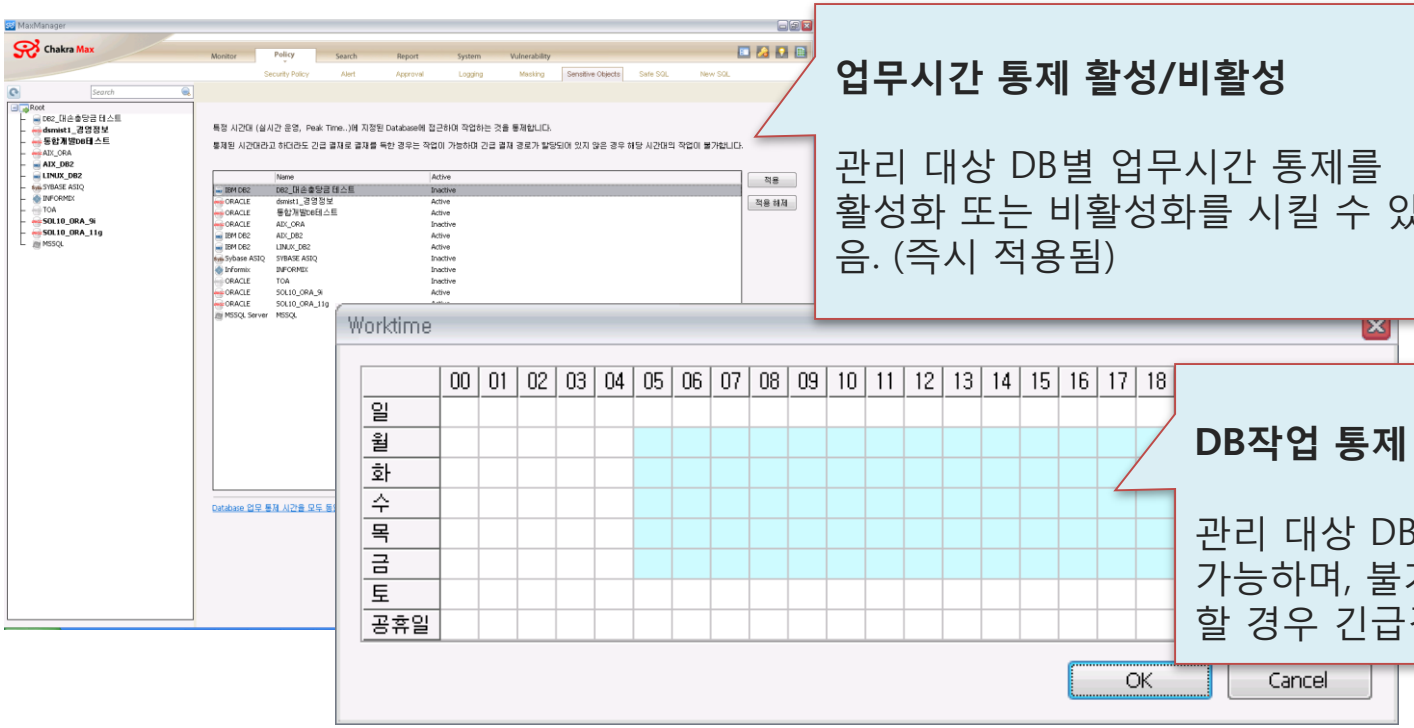



### 사후(참조) 결재 지원


사전 결재가 완료되면 기안자는 SQL실행 가능.
사후결재로 부결되면, 잔여 SQL실행 권한 취소됨.

# 접근제어 적용 기능

## 다양한 결재 기능 : 긴급 결재




**업무시간 통제 활성/비활성**

관리 대상 DB별 업무시간 통제를 활성화 또는 비활성화를 시킬 수 있음. (즉시 적용됨)

**DB작업 통제 시간 설정.**

관리 대상 DB별 통제 시간 설정이 가능하며, 불가피하게 작업이 필요할 경우 긴급결재 승인 후 허가됨.

온라인에 영향을 줄 수 있는 비정형 쿼리 수행시간을 "지정된 시간대로 제한" 통제 시간 사이에도 작업이 필요할 경우를 위해, 긴급결재 지원.
설정된 작업시간 통제는 데이터베이스에 따라 설정 혹은 해제가 가능.

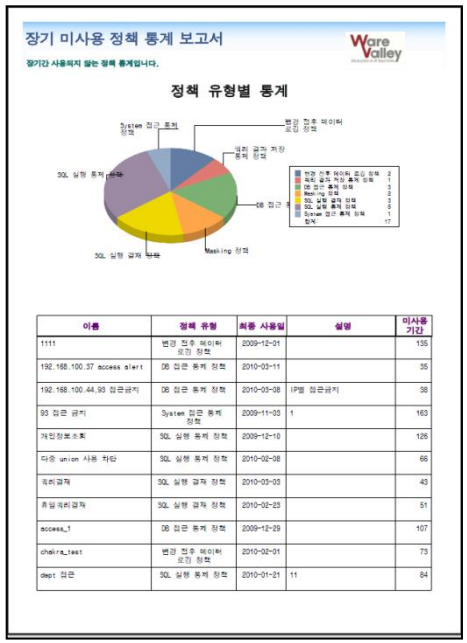
**업무 시간 통제란?**

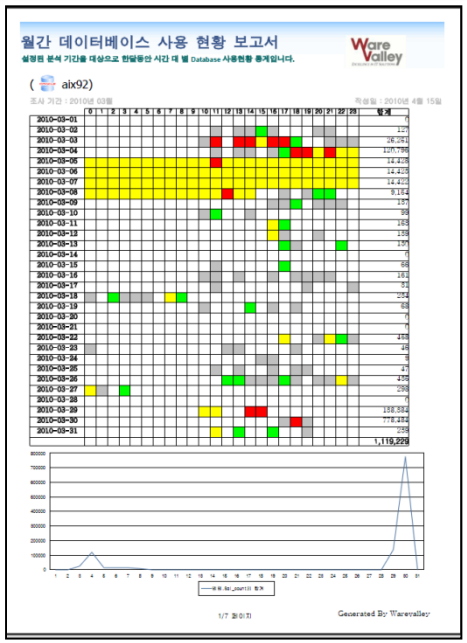
**온라인 서비스 중인 실 운영 DB에 대해 DB작업을 시간으로 통제하는 기능.**

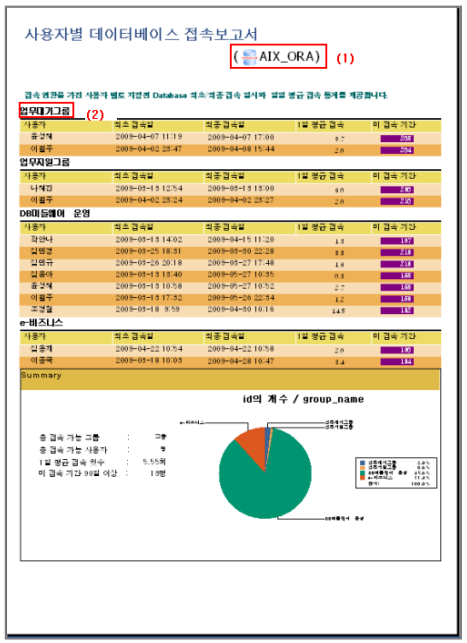
# 접근제어 적용 기능

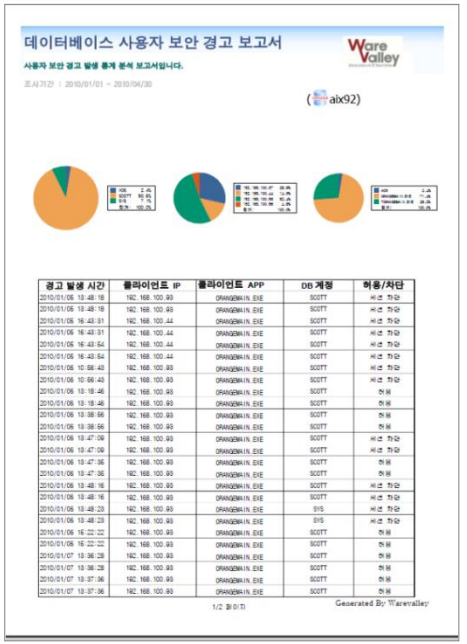
## 보안 경고 통계 보고서

| 장기 미사용 보고서 | 월간 DB사용 현황 | 사용자별 DB접속 | DB사용자 보안 경고 |
|---|---|---|---|



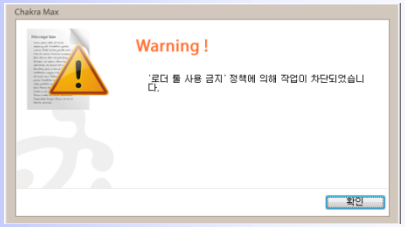



# 접근제어 적용 기능

## Integrated Features With Orange v5.0

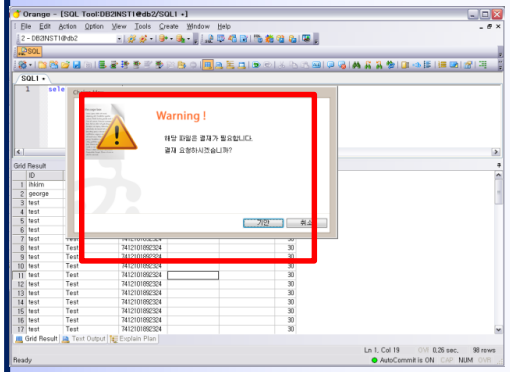
### 툴(메뉴) 사용 통제




**Load/Unload, Export,**
Space Manager, Lock Monitor, Session Monitor, Instance Monitor,
Security Manager 등…

오렌지에서 제공되는 각 Tool 메뉴 사용을 통제.

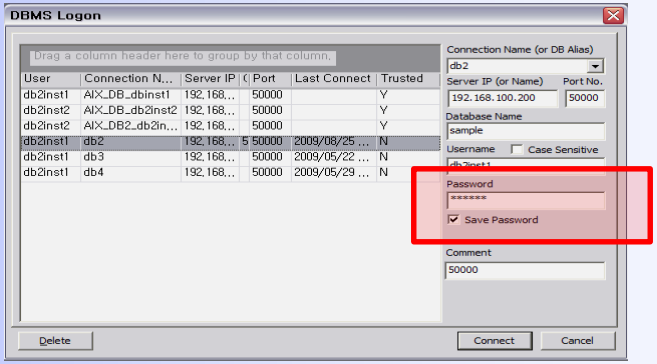
### "고객 정보" 엑셀 파일 저장 통제




고객 정보 테이블 조회 후 엑셀 파일로 저장하는 행위가 원천 통제됩니다.

1.저장 통제.
2.결재 승인 후 파일 취득.

### 가상 계정 기능




사용자에게 할당된
1인 1계정 패스워드를
샤크라 맥스로 통합 관리.

Orange를 이용한 경우만
Database접속이 허가됩니다.

# Chakra Max Power i 기능 비교

## Chakra v3.1 VS Chakra Max 기능 비교

| 구 분 | | Chakra v3.1 | ChakraMax Power-I | 비고 |
|---|---|---|---|---|
| 지원 DBMS | | Oracle, UDB, MSSQL, Sybase(IQ, ASE), Informix, Tibero, Altibase, Cubrid 등 13종 DBMS 지원 | Oracle, UDB, MSSQL, Sybase(IQ, ASE), Informix, Tibero, Altibase, Cubrid 등 13종 DBMS 지원 | |
| 지원 구성 방식 | | Sniffing, Gateway, Hybrid | Sniffing, Gateway, Hybrid | |
| 사용자 UI | 방식 | WEB 인터페이스 | C/S 방식 | |
| | Trend Monitor | | • 과거 시점 실시간 모니터 정보를 Replay 기능 제공 | |
| | Alert Monitor | | • 보안 경고를 Calendar 형태 뷰 제공 | |
| | 정책 관리 | • Wizard 기능 지원 | • 정책 생성.편집 편의성 보완<br>• DB 사용자별 적용 현황 뷰 제공 | |
| | 로그 검색 | • 로그 검색 기능 지원 | • 검색 기능 보완 | |
| | 편의성 개선 | | • 전체 뷰 구성 – 결과 상제조회 TAP 구성 | |
| 보고서 | | • 일, 시간, 주, IP/Application, DB User, DML 별 보고서 지원<br>• PDF 포맷 보고서 지원 | • 다양한 보고서 템플릿 제공<br>• pdf, html, xls, RTF, xml, txt 등 다양한 보고서 포맷 지원 | |
| 결재 | Syntax 체크 | | • SQL 구문 Syntax 체크, 하이라이트 표시 | |
| | Multi-SQL 기안 | | • Multi-SQL 기안, 여러 SQL 분리 기안 | |
| | 안건에 제약 설정 | | • 안건에 대하여 실행가능 횟수,유효기간 긴급결재 설정 기능 | |
| | 업무시간 작업통제 | | • 승인된 SQL일지라도 설정된 업무시간 실행 통제 | |
| | DBA 튜닝 결재 | | • DBA에게 SQL 안전성 검토 의뢰 기능 | |
| Orange 연계 기능 | | • 미지원(Trusted Orange 구성) | • 최신 버전의 Orange v5.0 연계<br>• SQL 실행결과 파일저장,인쇄,COPY 통제 | |

# 제품 특장점

## 경쟁사 대비 특장점 (1/2)

### 1. 일반

- ✓ 다년간 집적된 데이터베이스 프로토콜 분석 기술 적용.
  모든 프로토콜 분석 가능함. **패킷에 SQL이 포함되지 않는 Function 프로토콜도 해석 가능하며, 모든 응답 패킷 분석 분석 가능.**
- ✓ DB보안 솔루션에 특화된 전용 SQL구문 분석기를 자체 개발하여 제공.

### 2. 접근제어

- ✓ **단일 게이트웨이 서버로 750개 DB의 접근제어 적용. (정부 통합 전산센터)**

### 3. 스니핑

- ✓ 국내/외 **최대 규모 스니핑 레퍼런스** 적용. (KDDI, NTTData, Fujitsu, 국민은행, POSCO)
- ✓ 일본의 철저한 품질 점검 프로세스에서도 SQL 누락 없음. 국내 BMT에서도 항상 성능 1위.

### 4. 편의기능

- ✓ 관리자 프로그램을 통한 로그 검색 시, 메모리 부족으로 로그 검색이 중단되지 않음.
- ✓ Trend Monitor를 통해 과거 DB 접속 이력의 Re-Play 기능이 제공.

경쟁사 대비 특장점 (2/2)

## 5. 결재

- ✓ Telnet(SSH)를 경유하여 sqlplus 작업일 경우도 결재 기능이 제공됩니다.
- ✓ 작업 중인 DB세션에서 결재 상신이 이루어져도 해당 툴이 Blocking되지 않습니다.
- ✓ 승인된 안건은 지정된 실행횟수를 초과해서 실행 할 수 없습니다.
  안건 속성으로 "실행 가능 횟수", "유효기간", "긴급실행" 설정이 제공됩니다.
- ✓ 기안된 안건이 승인되어도 지정된 업무시간에는 실행되지 않게 가능합니다.
  "업무시간 작업 통제" 기간을 설정하면 승인된 안건이라도 실행 통제가 가능합니다.
- ✓ 결재 단계 중에 DBA를 추가시켜 기안된 SQL문장으로 인한 장애 가능성을 검증 할 수 있는 "Tuning 의뢰" 기능이 제공됩니다.

## 6. Orange2010 연동

- ✓ 여러 SQL문장의 동시 기안이 가능.
- ✓ 보안 정책에 따라 쿼리 결과의 "엑셀 파일 저장", "인쇄", "Copy" 명령 통제 및 결재 가능.
- ✓ 사용자 DB 계정 암호를 회수하여 접근 통제 시스템 우회 접속을 원천 봉쇄.


# 감사합니다

㈜비에이솔루션즈 BA Solutions
담당: 김 윤석상무 전화: 010-3227-0353 메일: tomasmkim@basolutions.co.kr
담당: 김 성진이사 전화: 010-6379-7943 메일: sungjin@basolutions.co.kr