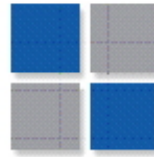
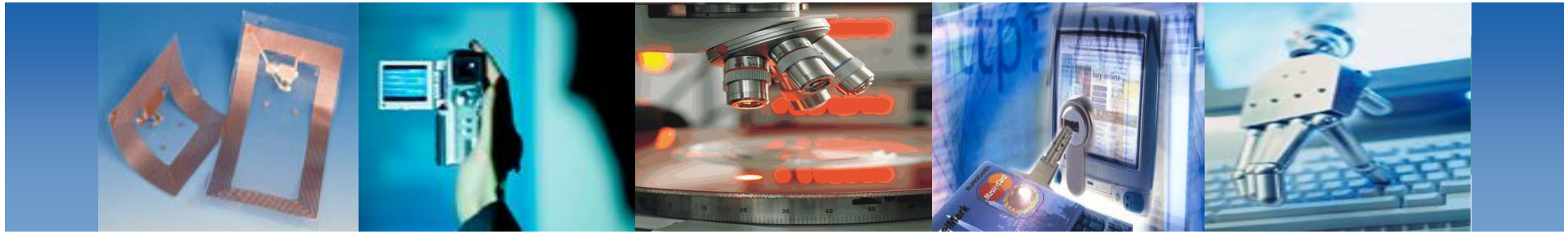


INNOLIME



내부 정보유출 방지를 위한 DB 보안 전략

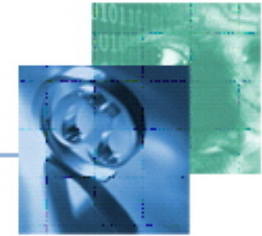
2006. 5
이 노 라 임



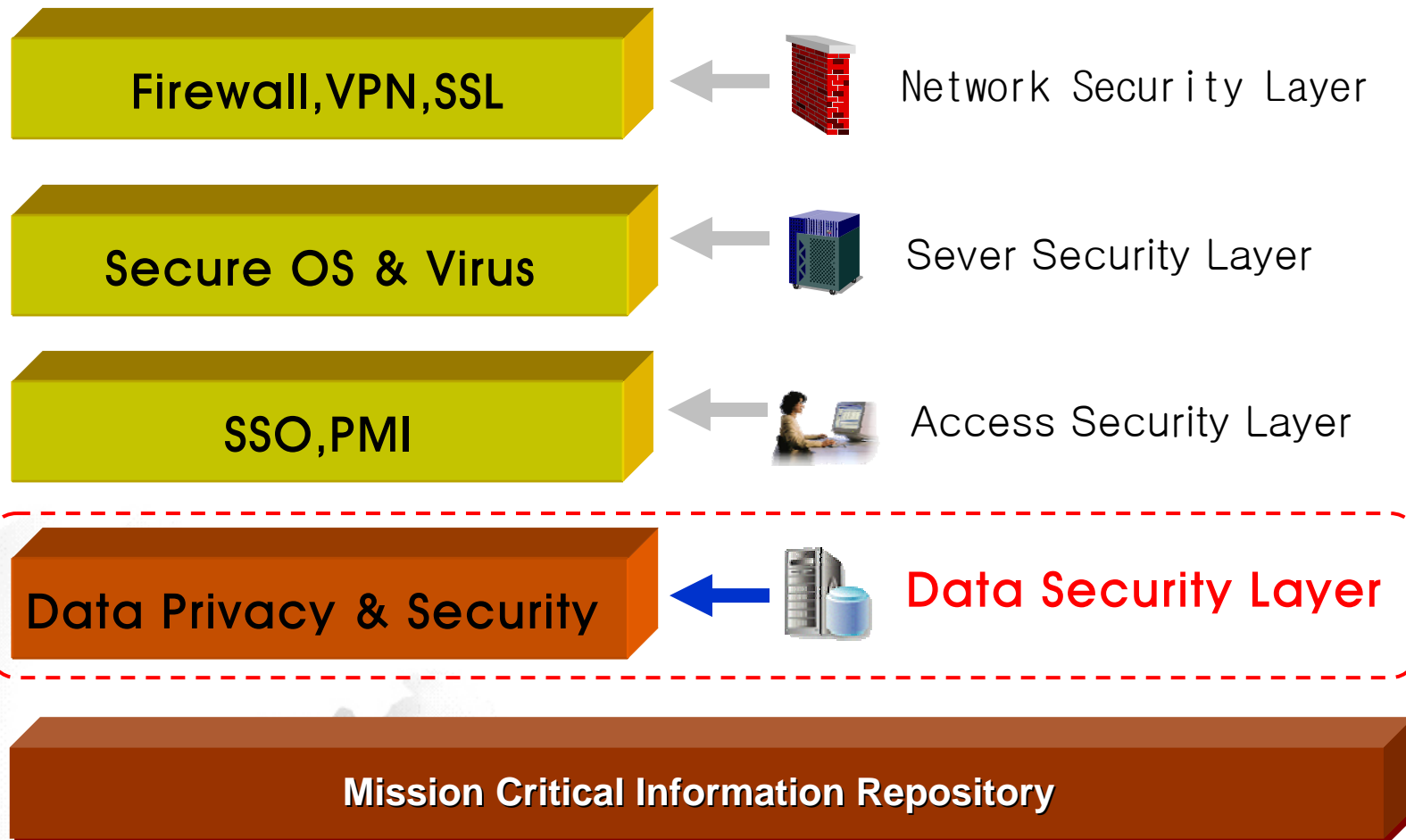
정보보호 분야의 이해

- 1 정보보호 현황
- 2 단계별 정보보호 대책
- 3 정보유출 사고 사례
- 4 내부 정보유출에 대한 규제

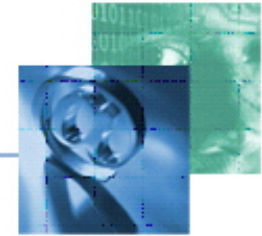
정보보호 현황



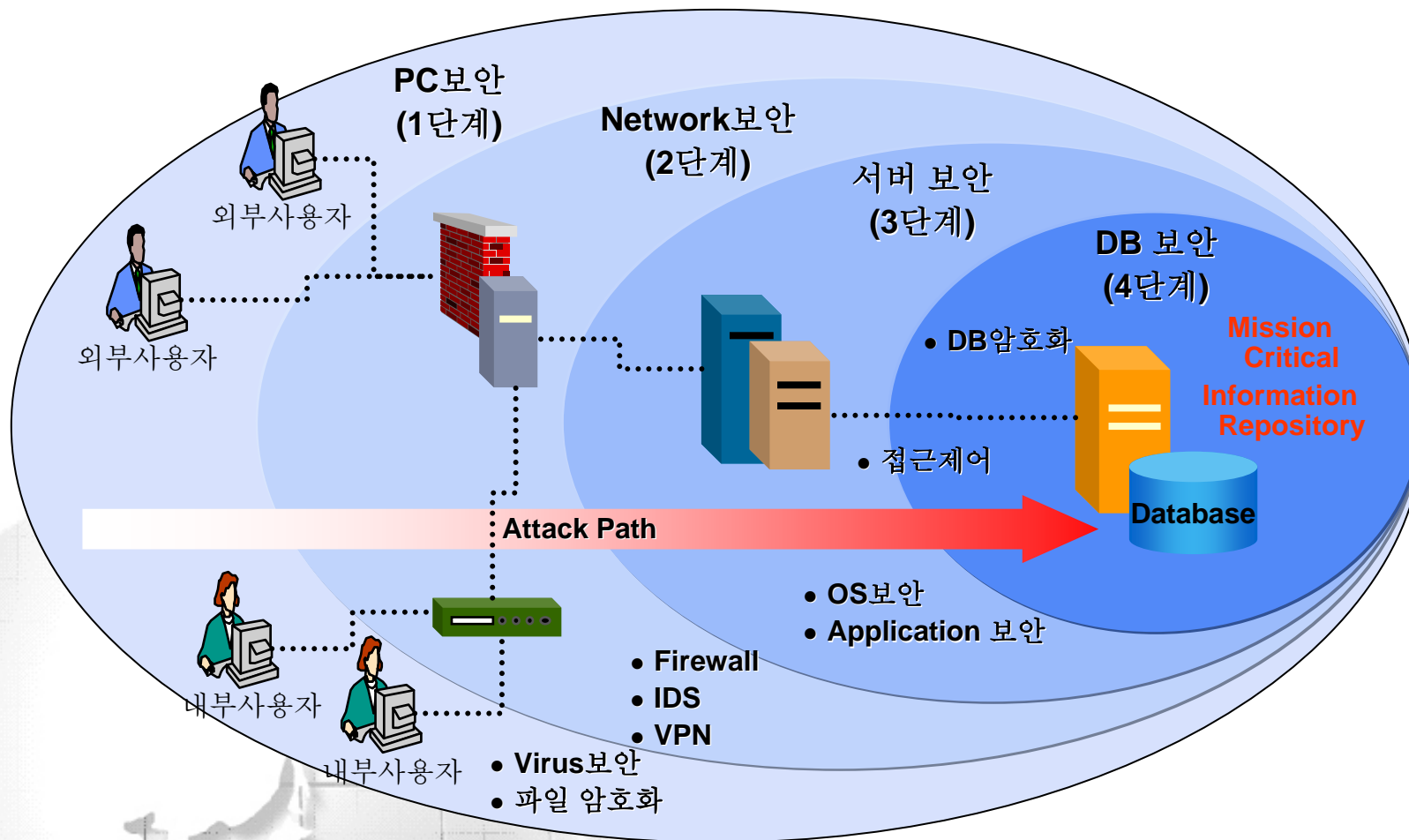
- 정보보호에 대한 관심이 네트워크, 시스템, 바이러스 대한 보안을 넘어 보안의 최종 핵심 대상인 **데이터 보안**의 인식이 확산



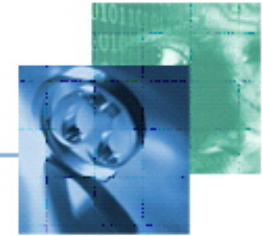
단계별 정보보호 대책



- IT의 보급 및 확산에 따라 정보보호는 PC 보안, Network 보안에서 서버보안까지 도입, 발전되었으나 **중요 데이터 정보유출**에 대한 감시 및 보안 체계는 상대적으로 취약



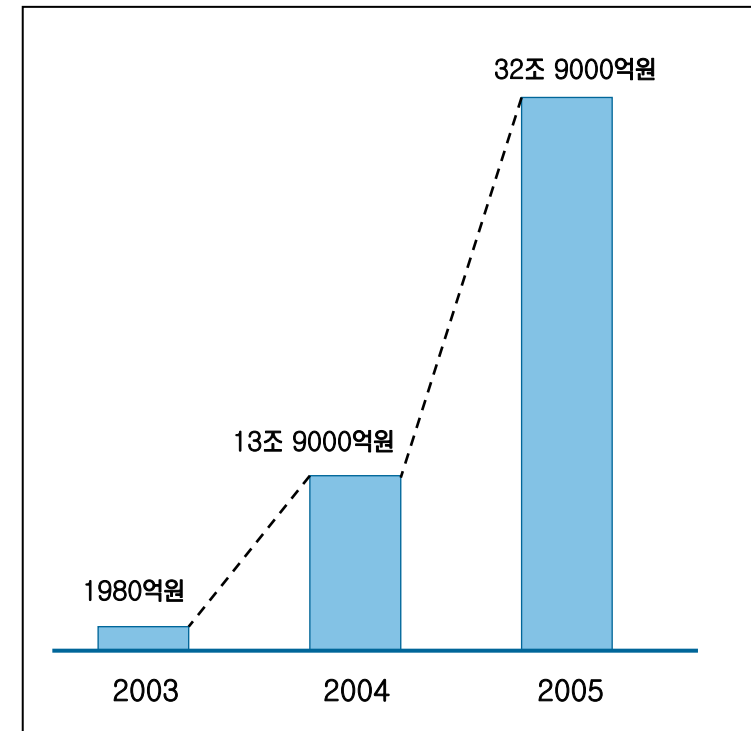
정보 유출 사고 사례



국내 내부 정보 유출 피해액 추이

Top 10 Customer Data Loss Incidents – 2005 to date		
Company/Organization	Number of Affected Customers	Date of Initial Disclosure
Card Systems	40,000,000	17-June
Citigroup	3,900,000	6-Jun
DSW Shoe Warehouse	1,400,000	8-Mar
Bank of America	1,200,000	25-Feb
Time Warner	600,000	2-May
LexisNexis	310,000	9-Mar
Ameritrade	200,000	19-Apr
Polo Ralph Lauren	180,000	14-Apr
ChoicePoint	145,000	15-Feb
Boston College	120,000	17-Mar
Total # of customers affected	48,055,000	

Source : InformationWeek, public disclosures by companies



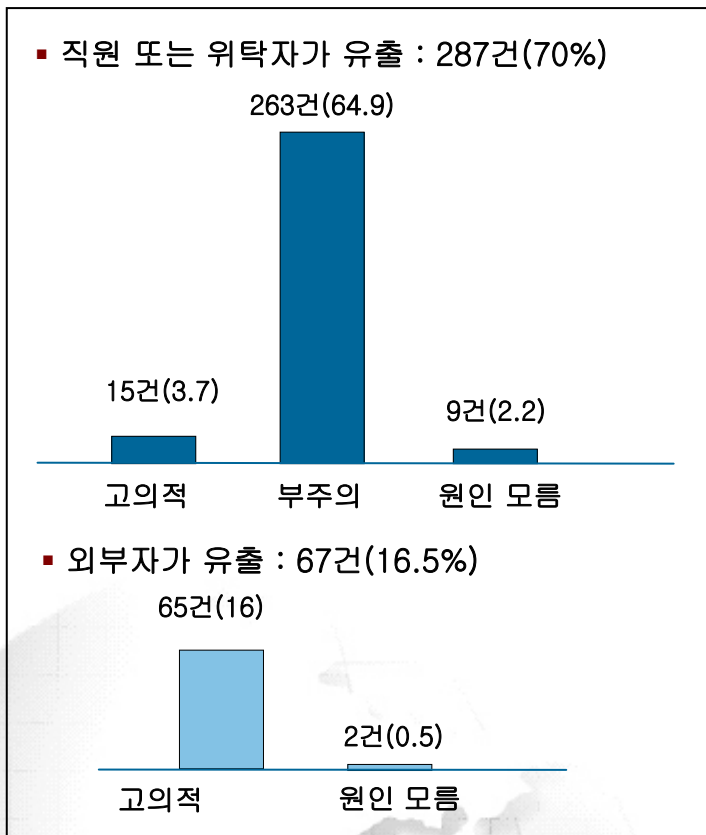
자료출처 : 한국 산업보안연구소 조사 결과

“전체 정보유출 행위 중 80%가 내부자에 의한 소행”
미국 FBI/CSI 통계 보고

정보유출 사고 사례

□ 일본 고객 정보유출 사고 유형

※ 2004년 4월부터 1년간 405건 차지하는 비중

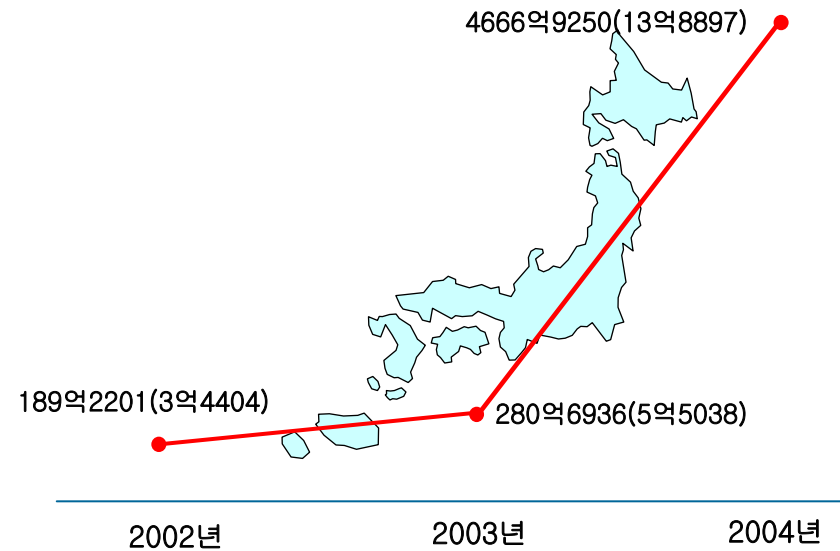


자료출처 : 일본 내각부 2005년 7월 공개 자료

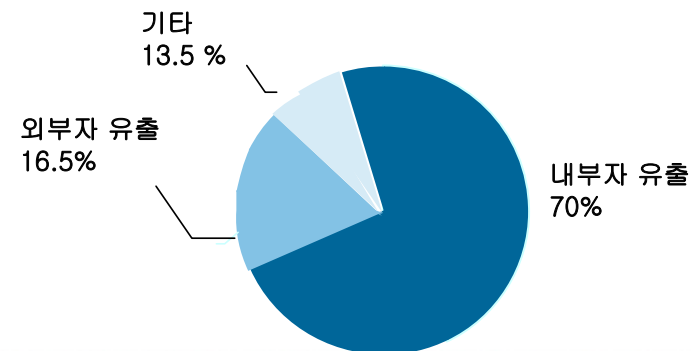
□ 고객 정보유출에 따른 일본 기업 손해 배상 총액

※ ()안은 사고 1건당 평균 손해 배상액

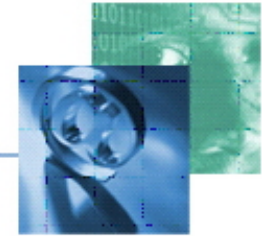
(단위: 만엔)



자료출처 : 일본 네트워크 시큐리티 협회 추산



내부 정보유출에 대한 규제



국제

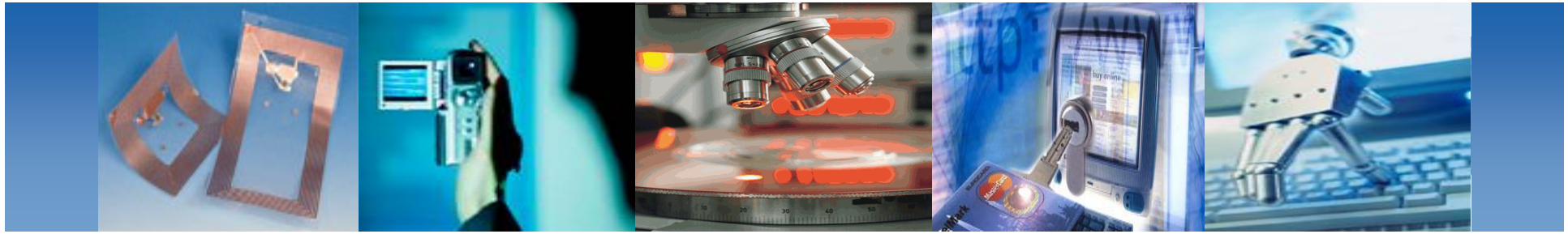
- SOX(샤베인즈-옥슬리 법안) – 비즈니스 거래의 투명성 확보
- HIPAA(의료정보보호법)
- Basel II(자기자본규제법) – 금융 거래상의 규제
- BS 7799 – 정보보안 관리체계 국제 표준

일본

- 개인정보보호법 시행(2005.05)
 - 개인정보 취급 업체 대상 기업
 - 개인 정보 이용 목적 명확화(기업의 무과실 책임)
 - 고객 정보 유출에 대해 천문학적 보상

국내

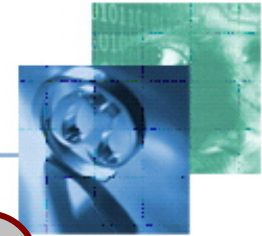
- 개인정보보호에 관한 법규정(정보통신부)
- 정보통신망 및 정보 시스템 보호에 관한 법규정
- 사이버 침해 및 전자 정보 침해에 관한 처벌 법 규정
- 금융기관 전자금융 업무 감독 규정(금융감독원)



DB 보안의 필요성과 방안

- 1 DB 보안의 필요성
- 2 DB 보안의 요구 사항
- 3 DB 보안 Best Practices
- 4 DB 보안의 이해
- 5 DB 보안 방안

DB 보안의 필요성



개인 정보에 대한 위협 증가

- 정보 유출 및 해킹의 범죄 건수가 매년 2배씩 증가
- 보안 침해 사고의 70~80%가 내부자 소행에 의해 발생

데이터베이스 보안의 취약성

- 엄격한 보안등급에 의해 계정 관리가 현실적으로 어려움
- 슈퍼 관리자(DBA)의 권한 집중화

전문적인 DB 보안 관리 필요

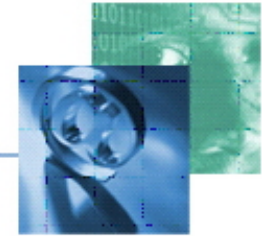
개인정보보호 법률 강화

- 개인정보보호 의무 위반한 업체에 배상 명령 - 개인정보분쟁위원회
- 개인 신상 정보는 암호화하여 저장 - 공공기관 정보보호 법률

전사적 보안 관리 체계 구축

- 방화벽에서 **Contents**까지 동일한 수준 보안 요구
- 단계별 구체화하고 핵심 자산 중점 관리가 필요

DB 보안 요구 사항



DB 보안을 위한 구비 조건

- ✓ DB 내 중요 데이터 대한 기밀성 및 신뢰성 확보 가능
- ✓ Backup Data에 대한 안전한 관리
- ✓ 비정형적 사용자 접근에 대한 사전 통제
- ✓ 특정 데이터에 접근한 사용자 및 작업 내역 추적
- ✓ 엄격한 사용자 계정 관리
- ✓ 시스템에 접근 내역을 다양한 방법으로 확인

데이터 암호화

접근 제어

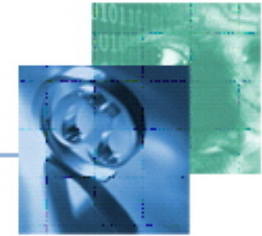
감사 기능

보안 관리

통계 및 리포팅



DB 보안 Best Practices



□ 주도 면밀한 보안 실행 계획은 최상의 DB 보안 유지하는 척도

1 Baseline
수립

2 Vulnerability
이해

3 Monitor &
Maintain

4 최신 Patch
유지

5 주기적 Audit

6 Vulnerability
평가
& 보안 감사

7 실시간 침입
탐지

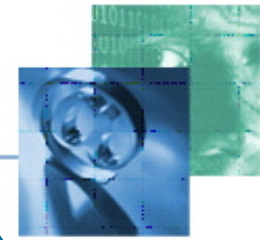
8 Encryption

9 경계 보안
유지

10 위협 요소로
부터 DB 분리

기밀성,
신뢰성,
완전성
확보한 안전한
DB 보안 시스템 구축

DB 보안의 이해



1 Identity Management

Authenticate

Finance



HR



2

Encryption

역할 기반
접근 제어

Authorize

전송 중
데이터 보호
(Data in-motion)

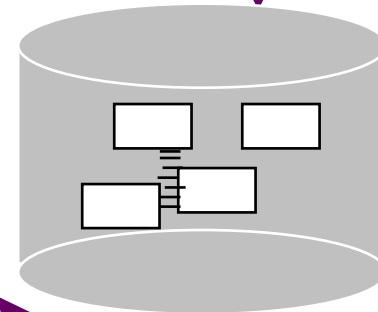


ID	Name	SSN	Dept	Label

저장된
데이터 보호
(Data at-rest)

3

Auditing



Administration

4

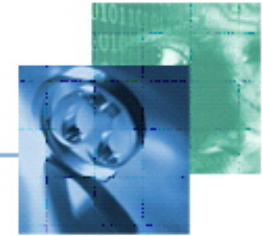
Assessment

5

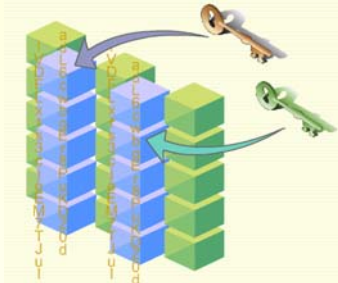
6

Intrusion detection and prevention

DB 보안 방안



데이터 암호화



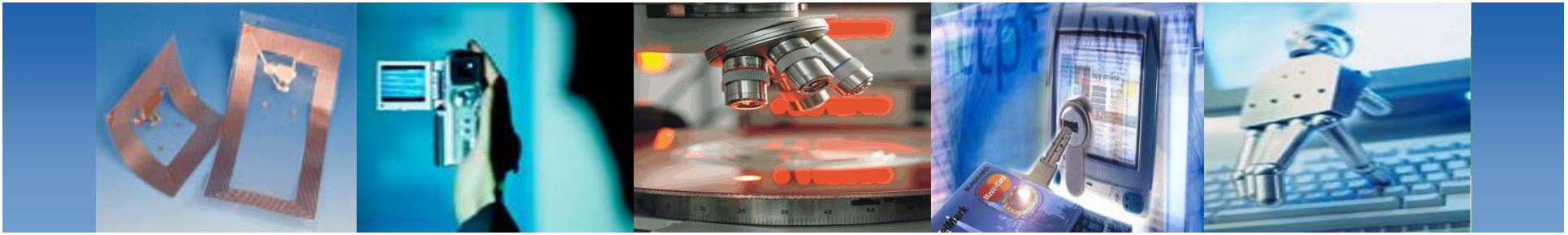
- ✓ 데이터 유출 시 해독 불가
- ✓ 내부자 정보 유출 원천 차단
- ✓ 백업 데이터 안전한 관리
- ✓ 엄격한 사용자 계정 관리

DB 보안

접근제어 & 감사



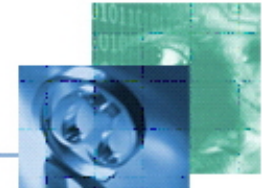
- ✓ 비정형 접근 통제
- ✓ 작업 내역 추적
- ✓ 네트워크 레벨 패킷 분석



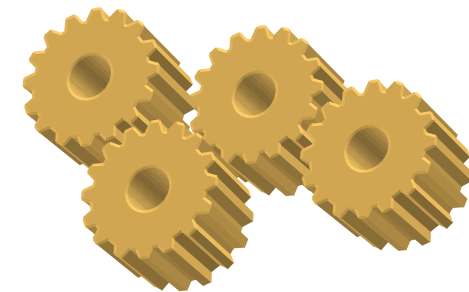
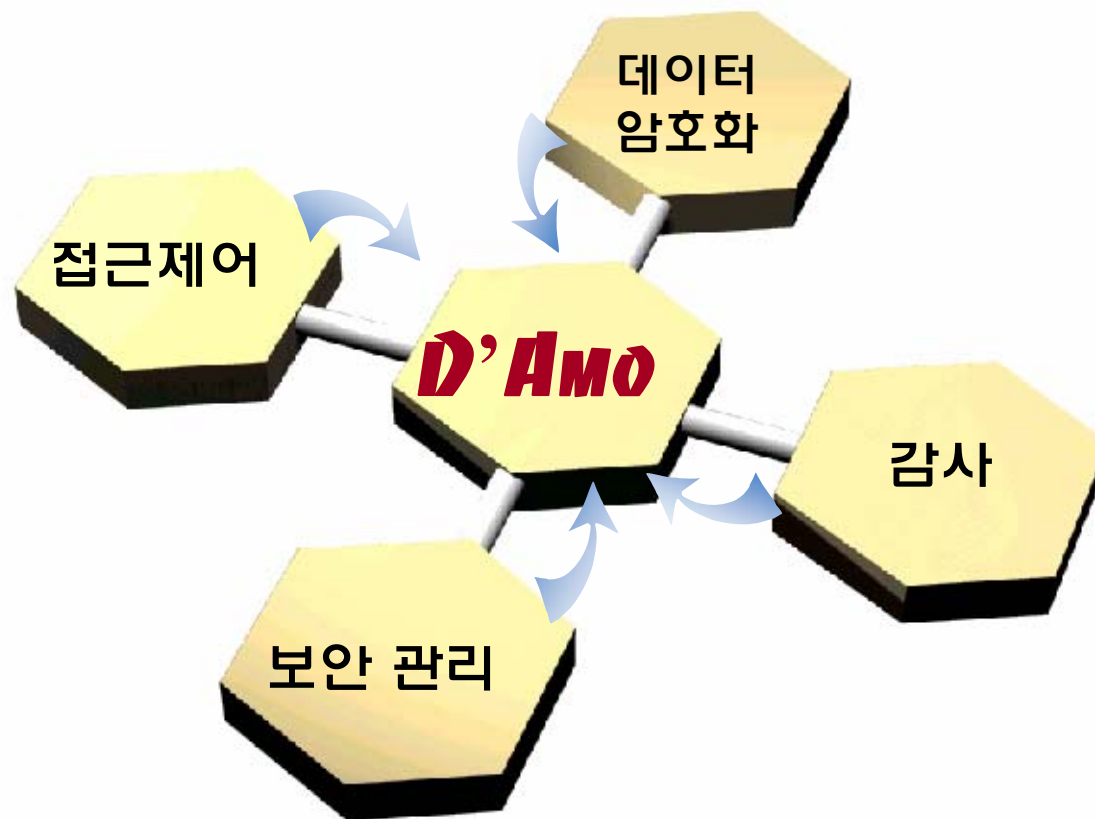
D'Amo Overview

- 1 D'Amo 란 ?
- 2 특징
- 3 적용 개념도
- 4 구성도
- 5 제품 구성 요소
- 6 키 관리 인증 체계

D'Amo란 ?

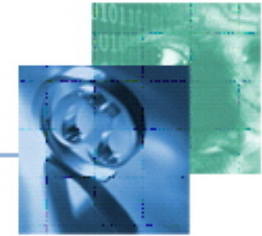


- D'Amo는 응용프로그램 수정 없이 DB 내 주요 데이터를 칼럼 단위로 암호화, 접근제어, 감사를 수행하는 통합 DB 보안 솔루션이다.

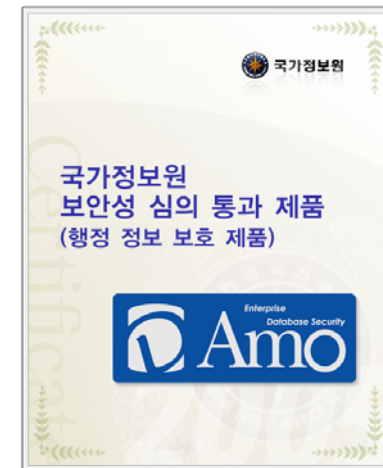


통합 DB 보안 솔루션

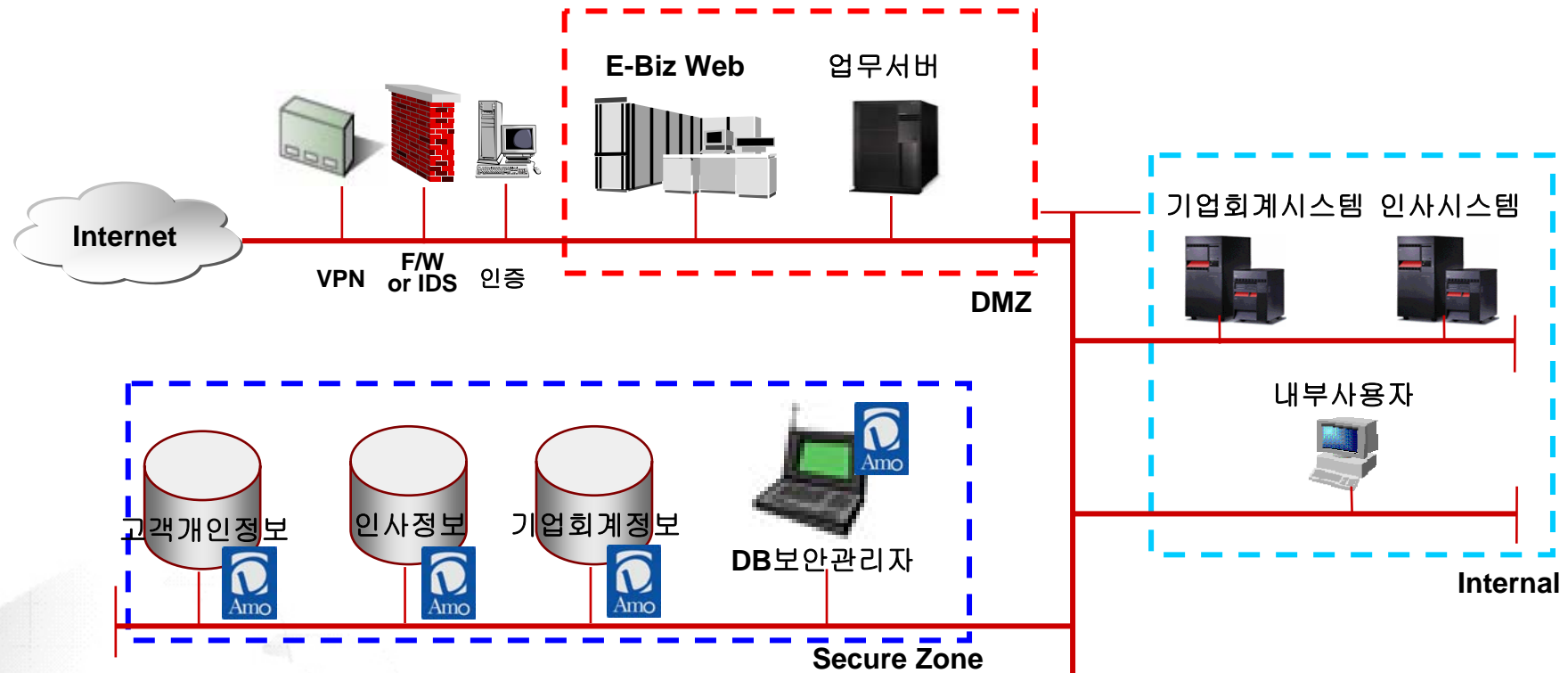
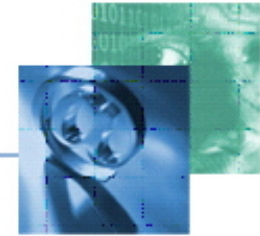
특징



- 응용프로그램에 대한 **완벽한 독립성**
- DB 내 중요 데이터를 컬럼 단위로 **선택적 암호화**
- DB 계정/IP/MAC/응용프로그램/시간대별 **DB 전체 또는 암호화 컬럼 접근제어**
- 암호화와 접근제어 기능 통합으로 **안전한 데이터 보호와 유연한 정책 적용** 가능
- (비)암호화 컬럼 단위의 작업 내역 **감사**
- 암호화된 컬럼에 대한 **보호 기능**
- **빠른 설치**를 통한 시스템 통합(1주일 이내)
- 다수의 DB 암호화를 **통합 관리**
- 국가 정보원 **보안성 심의**를 통과한 안전한 제품
- 한국정보통신기술협회(TTA) **GS 인증** 획득

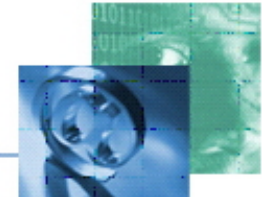


적용 개념도

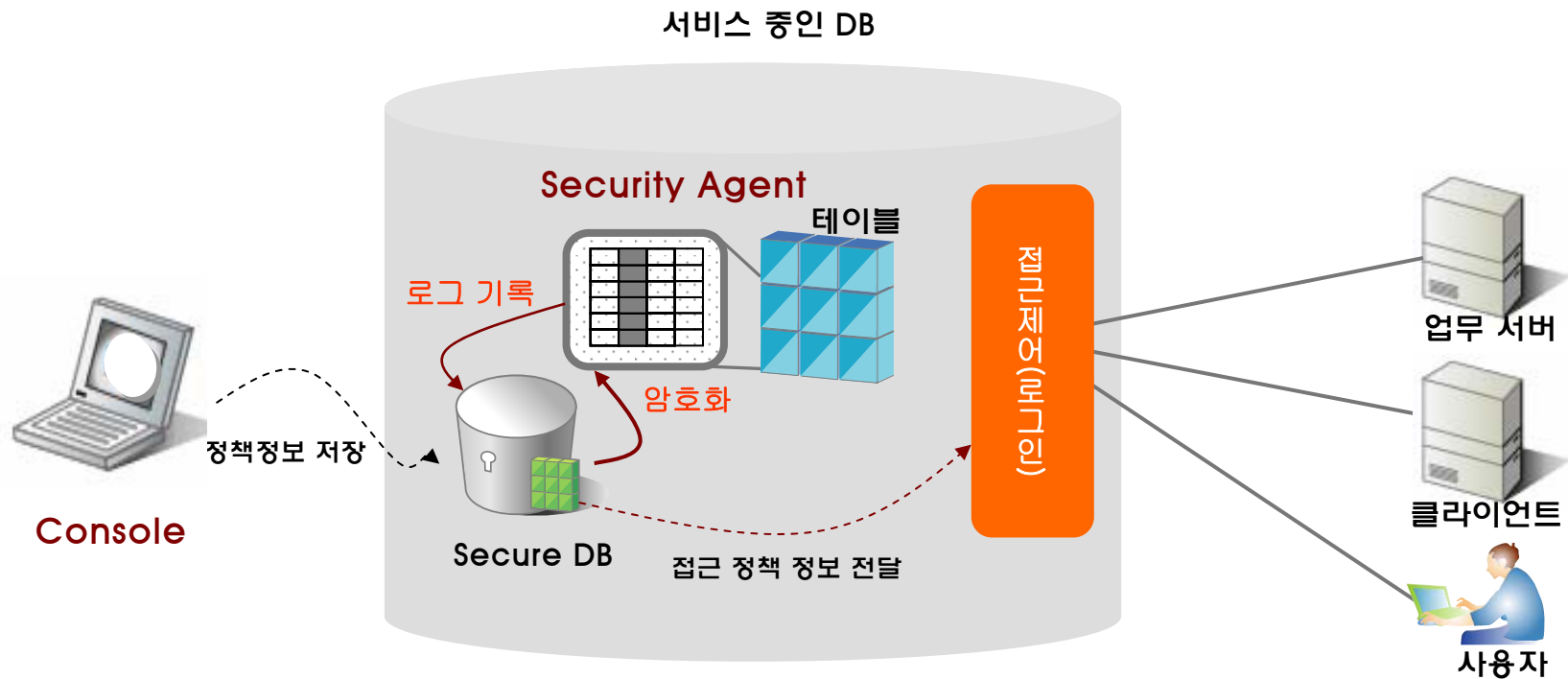


암호화 : 중요 데이터를 칼럼 단위 선택적 암호화
 접근제어 : DB 전체 또는 특정 칼럼 단위로 접근제어
 감사 : 칼럼 단위의 중요 정보 접근 내역 기록 및 추적

구성도



- D'Amo는 Console과 Security Agent로 구성된다

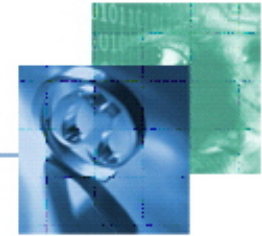


보안 관리자는 정책 설정, 접근 권한 등의 정보를 Secure DB로 전달한다

암호화 칼럼이 포함된 테이블에 대해서는 Security Agent를 통해서 조회, 추가, 수정

암호화 통신

제품 구성 요소

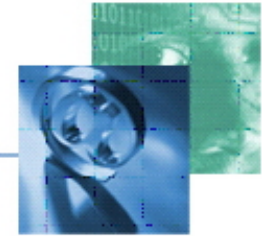


Console

- 보안 관리자는 D'Amo 인증기관에서 발급한 PKI Certificate를 이용하여 로그인
 - 편리한 One-Click 암호화 설정 및 해제
 - 접근 경로에 따른 세분화된 접근 권한 부여
 - 데이터 접근에 대한 로그 및 통계 기능
 - 암호화 컬럼에 접근 권한이 부여된 DB 계정 관리
 - 보안 정책 자동 Backup 및 Recovery 기능



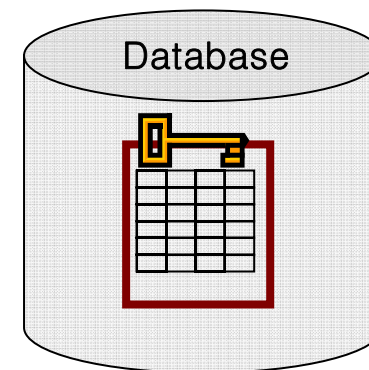
제품 구성 요소



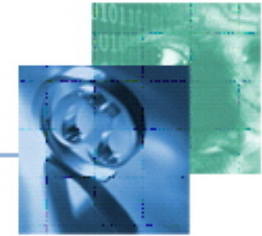
Security Agent

- 보안 관리자가 설정한 보안 정책을 DB 내에서 수행 (Plug-In 방식)

- DB 내 저장되어 있는 데이터 (at-rest)를 일괄 암호화
- 암호화가 설정된 컬럼으로 유/출입 되는 데이터의 실시간 암(복)호화
- 암호화 컬럼에 접근하는 사용자 접근 제어
- (비)암호화 컬럼에 대한 감사 기록
- 암호화된 컬럼에 대한 보호 메커니즘 생성

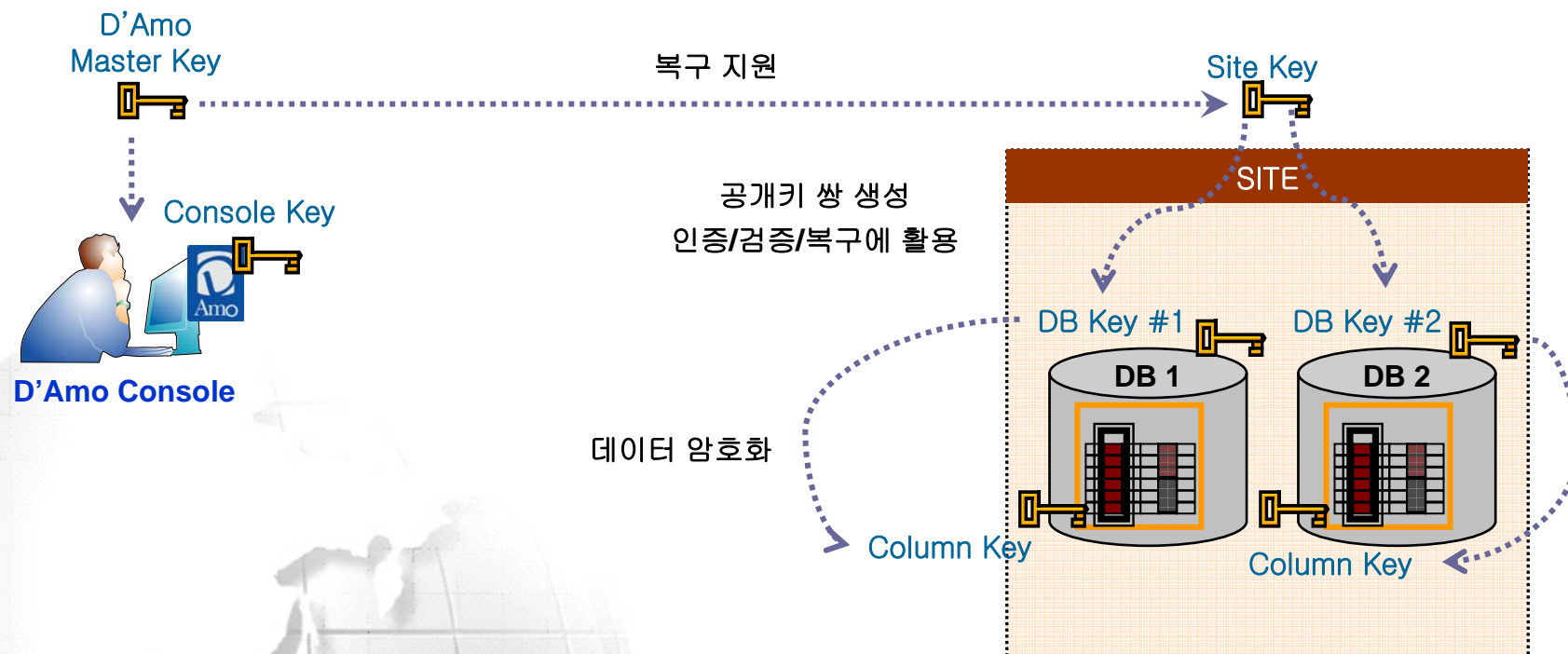


키 관리 인증 체계



Key Management

- PKI 기반의 안전한 키 관리 체계
- 5 단계 키 관리를 통해 안전한 데이터 보호와 인증 / 검증 / 장애 복구 기능 제공

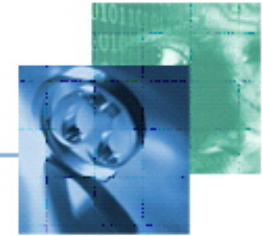




D'Amo Specifications

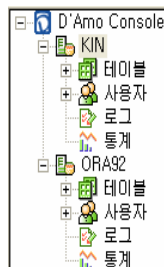
- 1 보안 정책
- 2 암호화
- 3 접근 제어
- 4 감사
- 5 보안 관리
- 6 성능 최적화

주요기능 – 보안 정책



DBMS 보안 정책

- 데이터베이스 보안관리자는 DBMS별 보안 정책을 수립
- 설정된 보안 정책으로 일괄적 적용 가능

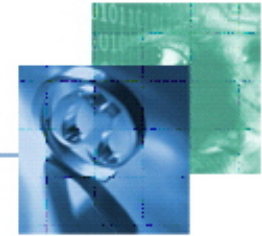


보안 정책

- 암호 알고리즘
- 운영모드
- Initial Vector
- Auto Rollback
- 로그 설정
- 감사 접근 로그 설정
- 로그 기록 모드
- 암호화 결과 반환 값
- 접근제어 허용/차단 설정

Database 보안 정책 설정

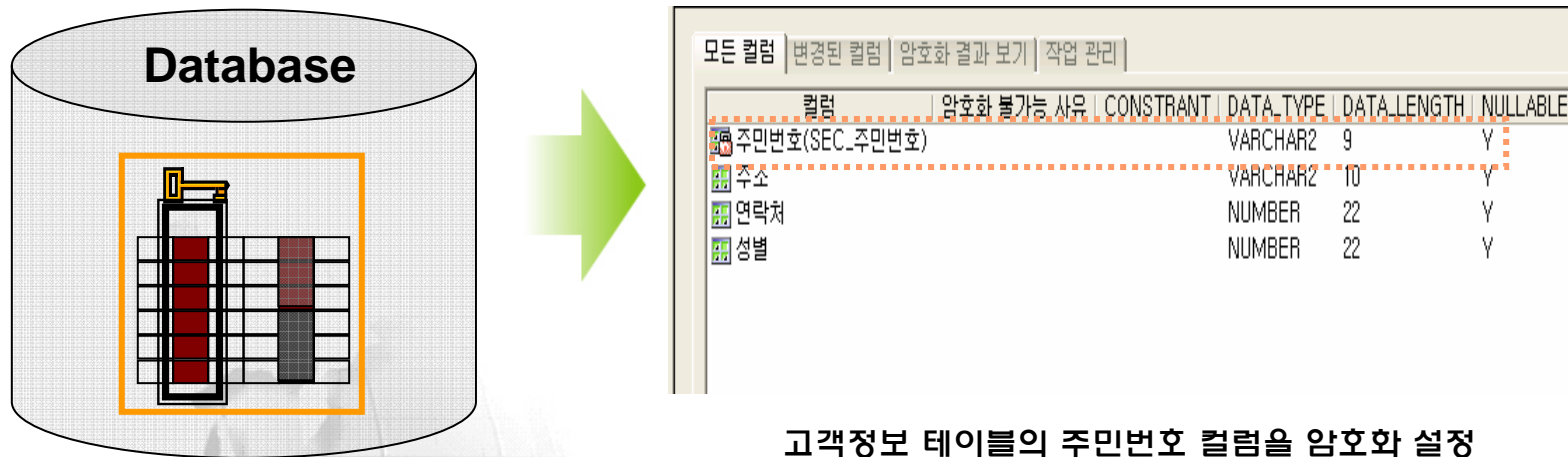
주요기능 – 암호화



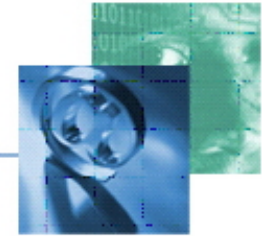
선택적 암호화

- 기업 DB 내 중요 데이터를 컬럼 단위로 선택적 암호화
- 필요한 데이터만을 암호화하여 성능 저하를 최소화하고 보안성 확보

- 아래 예는 고객정보 테이블 내에 저장되어 있는 정보 중 주민번호 컬럼 암호화한 화면임



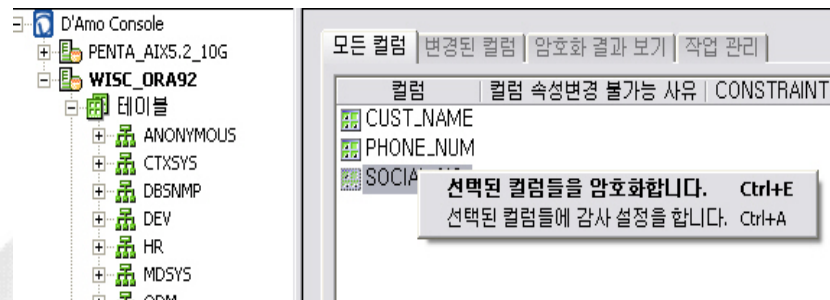
주요기능 – 암호화



컬럼 보안 정책

- 컬럼 단위 보안 정책 설정 (암호화 알고리즘, 운영모드, IV의 설정 유무 등)

- 암호화 컬럼은 다수(3개 까지)로 선택하여 일괄 처리가 가능



암호화 알고리즘
빠른 속도를 원하시면 AES, 국산 알고리즘을 원하시면 SEED를 선택하십시오.
DES의 키길이가 짧은 것을 보완하기 위해 DES를 세번 반복시키는 알고리즘.

TDES

운영 모드
하나의 Block에 대한 대칭키 알고리즘을 연속된 Block들에 대해 어떤 형태로 적용할 것인가를 선택합니다.
초기치와 평문 블록을 XOR하여 알고리즘에 입력하는 방식

CBC (Cipher Block Chainin

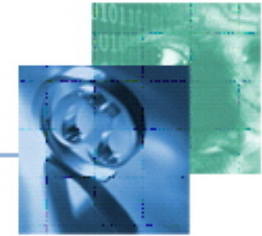
Initial Vector 사용 방안
Initial Vector는 암호화 연산의 초기값의 역할을 합니다. 동일한 값들에 대해서 다른 암호화 결과를 얻는 것이 필요하시다면 Record IV를 선택하십시오.

☐ Fixed IV ☒ Record IV

암호화 Key Import

컬럼 암호화 정책 설정

주요기능 - 암호화



암호화 Rollback

- 암(복)호화 과정 중 장애가 발생하면 원본 데이터로 자동 복구

- 암(복)호화 자동 복구는 전체 1~17 단계로 이루어지며, 암호화 적용이 완료 되면 원본데이터는 삭제됨

[정상 작업]

SCOTT.EMP 테이블의 ENAME 암호화 작업 (완료)

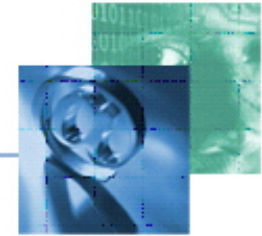
2006/03/23 17:47:50	해당 테이블의 최초 암호화 설정 준비 완료
2006/03/23 17:47:51	테이블명 변경 시작 완료
2006/03/23 17:47:51	정상 데이터 migration 준비 완료
2006/03/23 17:47:52	복호화 처리하는 object 생성 완료
2006/03/23 17:47:52	암호화 처리하는 object1 생성 완료
2006/03/23 17:47:52	암호화 처리하는 object2 생성 완료
2006/03/23 17:47:52	사용자가 사용하는 object 생성 완료
2006/03/23 17:47:53	정상 데이터 migration 완료
2006/03/23 17:47:57	테이블명 변경하는 작업 완료 완료
2006/03/23 17:47:58	Migration 데이터 검증 완료
2006/03/23 17:47:58	접근 권한 조정 1단계 작업 완료
2006/03/23 17:47:58	접근 권한 조정 2단계 작업 완료
2006/03/23 17:47:58	접근 권한 조정 3단계 작업 완료
2006/03/23 17:47:58	암호화 컬럼 속성 변경 차단 완료
2006/03/23 17:47:59	정상 데이터 컬럼에 걸린 트리거 변경 생성 완료
2006/03/23 17:48:04	정상 데이터 삭제 완료
2006/03/23 17:48:06	암호화 작업 완료

[복구 작업]

SCOTT.EMP 테이블의 ENAME 암호화 작업 (복구 완료)

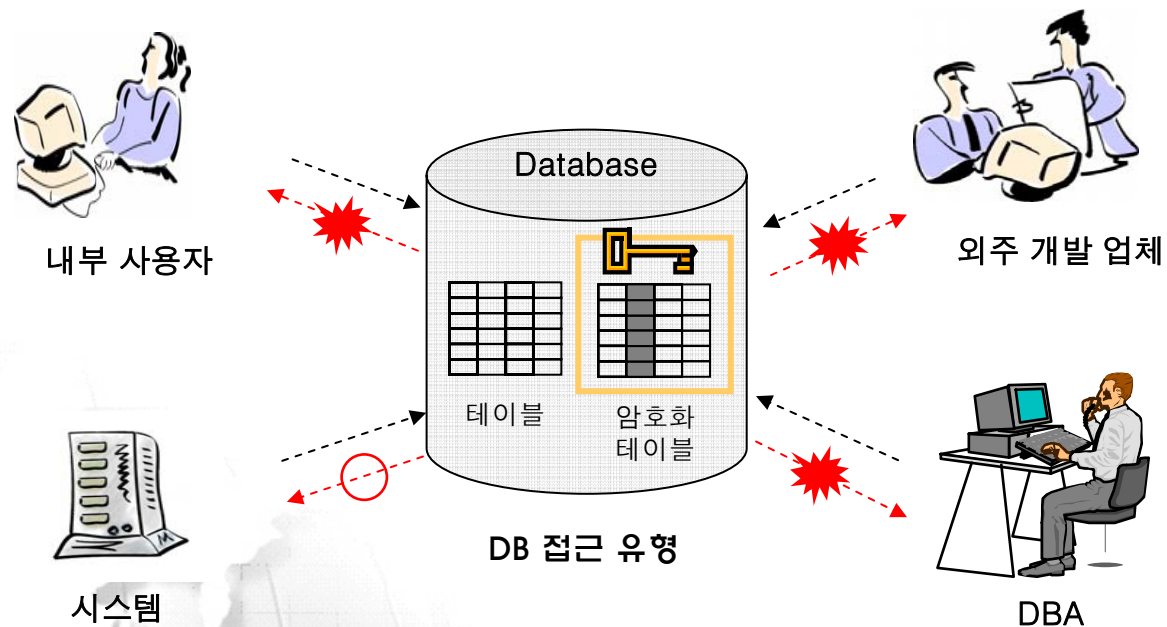
2006/02/22 10:41:26	해당 테이블의 최초 암호화 설정 준비 복구 완료
2006/02/22 10:41:26	테이블명 변경 시작 복구 완료
2006/02/22 10:41:26	정상 데이터 migration 준비 복구 완료
2006/02/22 10:41:26	복호화 처리하는 object 생성 복구 완료
2006/02/22 10:40:48	암호화 처리하는 object 생성 실패

주요기능 - 접근제어

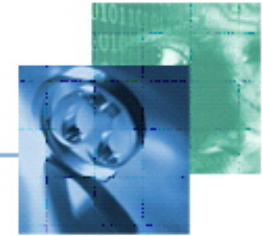


강력한 접근제어

- 내외부 인가되지 않은 사용자를 세분화하여 접근 정책 적용
- 반드시 필요한 사용자 및 시스템에게만 허용



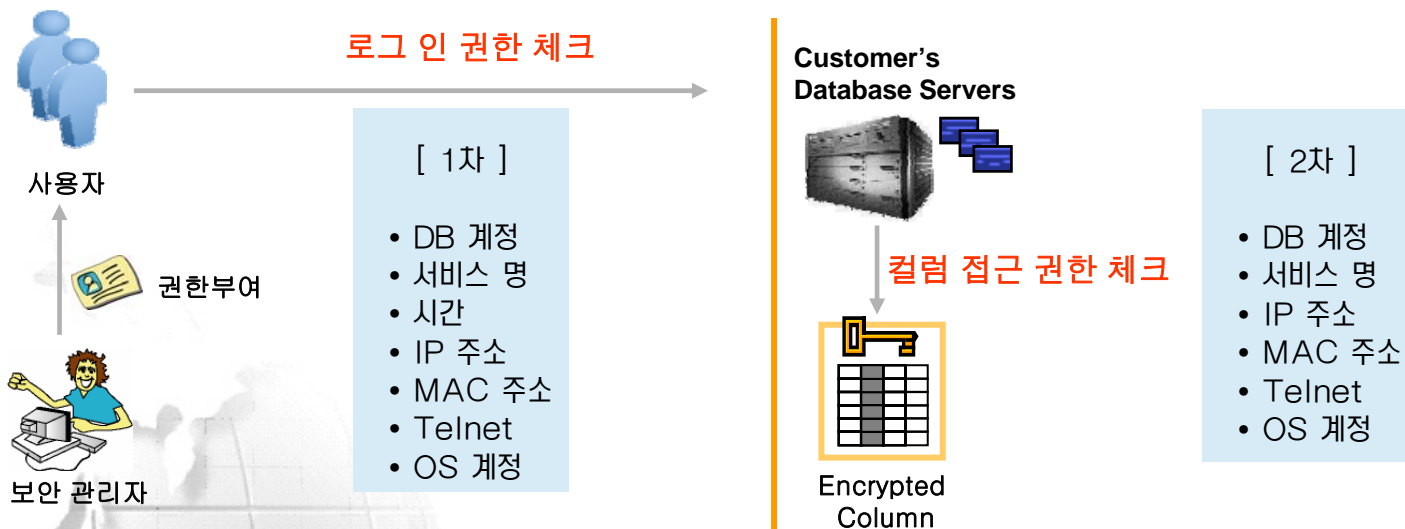
주요기능 - 접근제어



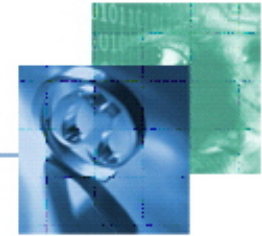
접근제어 방식

- 로그인 시와 암호화 컬럼 단위의 이중 접근제어로 완벽한 침입 차단

- 로그인 접근제어 : DB에 로그인 시 권한 체크 (1차 접근제어)
- 컬럼 접근제어 : 암호화 컬럼에 접근 권한 체크 (2차 접근제어)



주요기능 - 접근제어



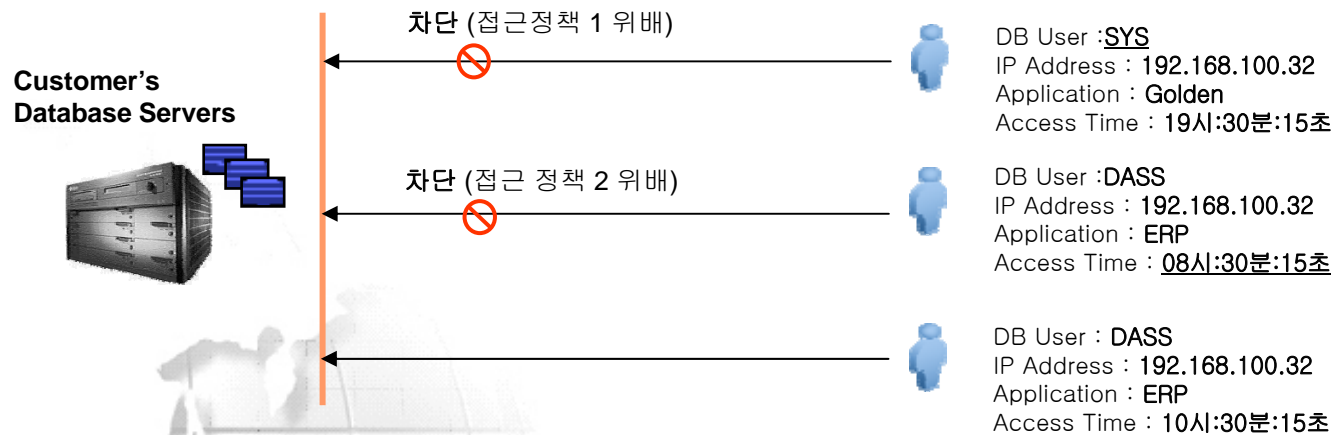
로그인 접근제어

- DB에 로그 인하는 사용자를 IP/MAC/서비스 명/시간/Telnet/OS 계정 접근제어 수행

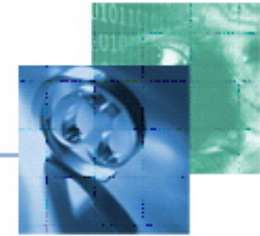
접근 정책 1 : DB User가 “DASS”이고 192.168.100.32인 경우 허용
(단, 유동 IP 환경하에서 Client 접근 제어는 MAC 주소를 이용하여 가능)

접근 정책 2 : DB 접근 가능 시간은 09:00~18:00시 까지

접근 정책 3 : 서비스 명이 ERP 인 경우만 허용



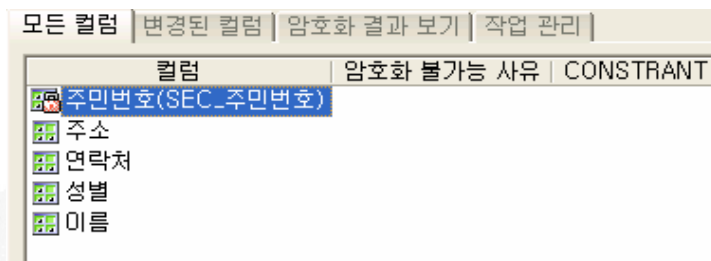
주요기능 - 접근제어



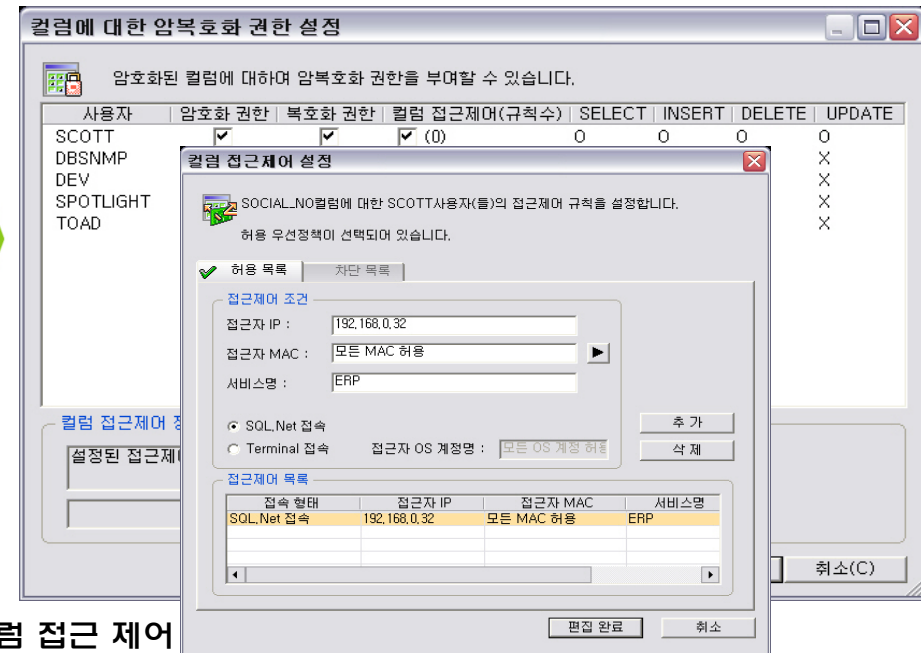
컬럼 단위 접근제어

- 컬럼에 대한 암(복)호화 권한을 분리하여 접근 제어 수행
- 암호화 컬럼 접근 제어 - IP/MAC/서비스 명/Telnet/OS 계정 접근 제어

- 주민번호 컬럼에 DB 계정 단위로 암(복)호화 권한을 분리하여 적용
- 주민번호 컬럼에 접근 제어 설정하여 적용

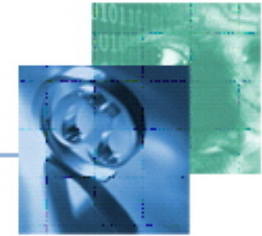


여러 계정에 접근 권한 부여 시
미리 정의한 템플릿을 이용하여
일괄적으로 적용이 가능



컬럼에 대한 암호화 권한 설정 및 컬럼 접근 제어

주요기능 – 접근제어



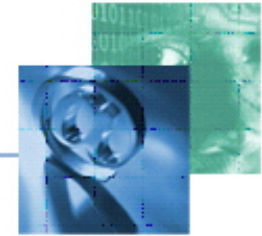
Telnet 접근제어

- Telnet으로 접속하여 접근하는 경우에 대해 SQL*Net과 동일하게 Client 사용자를 인식하여 접근제어

- Telnet 접속하여 DB 접근 시 Client IP 주소(192.168.0.100)에 대해 접근제어 설정
- Telnet 접속의 경우 시스템 O/S 계정에 대해서도 접근제어 적용 가능



주요기능 - 감사



로그 분류

- 정책 변경과 암호화된 컬럼에 대한 작업 내역을 기록 (정책로그, 이벤트 로그)

- 정책 로그 : 보안 정책 생성/변경/삭제에 대한 내용을 기록
- 이벤트 로그 : 암호화 컬럼 및 감사 지정 컬럼에 접근 내역을 기록

로그 종류

- 날짜
- 로그 구분
- 소유자
- 테이블
- 컬럼
- 작업내역
- 서비스명
- IP
- MAC
- 세션 ID
- OS 계정

정책 로그 | 이벤트 로그

검색조건

기간: 2005년 3월 8일 화요일 17 시 부터
2005년 5월 9일 월요일 18 시 까지

로그 저장

상세작업내역:

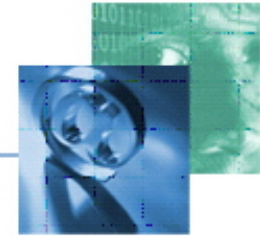
검색 시작

검색된 로그 목록

날짜	로그 구분	소유자	테이블	컬럼	작업내역	로그 발생 IP
2005/04/28 16:26:46	권한 제거	TEST	TB_TABLES	NAME	암호화 권한 제거	192.168.0.74
2005/04/28 15:44:56	암호화 컬럼 생성	TEST	TB_TABLES	NAME	암호화 컬럼 생성	192.168.0.74
2005/04/28 14:46:00	암호화 컬럼 암호화 해제	TEST	TB_TABLES.TEST_DAMO	NAME	컬럼 암호화 이전 상태로 복구	192.168.0.74
2005/04/28 14:36:13	권한 부여	TEST	TB_TABLES.TEST	NAME	암복호화 권한 부여	192.168.0.74
2005/04/26 10:34:32	권한 부여	SCOTT	TB_TABLES	NAME	암복호화 권한 부여	192.168.0.49
2005/04/26 10:34:31	권한 제거	SCOTT	TB_TABLES	NAME	암복호화 권한 제거	192.168.0.49
2005/04/26 10:34:25	권한 부여	SCOTT	TB_TABLES.LOG	NAME	암복호화 권한 부여	192.168.0.49
2005/04/26 10:34:11	암호화 컬럼 생성	SCOTT	TB_TABLES.LOG	NAME	암호화 컬럼 생성	192.168.0.49

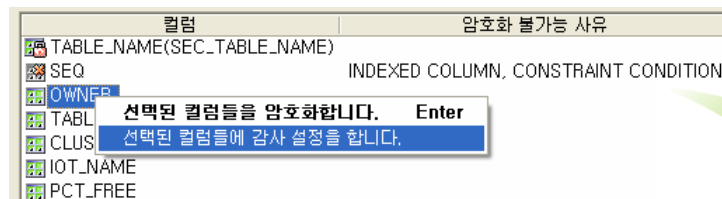
정책 로그 내용

주요기능 - 감사



감사 방식

- 암호화 컬럼을 조회하거나 수정하는 SQL 작업 100% 기록/보관
- 비암호화 컬럼에 대한 Audit Only 기능



- 컬럼 단위의 Audit Only 기능 설정

성공유무:

로그 구분:

로그 구분:

로그 저장

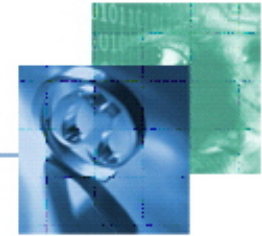
검색 시작

검색된 로그 목록

날짜	로그 구분	접근자	접근자IP	소유자	테이블	컬럼	성공유무	세션 ID
2005/05/09 17:59:04	SELECT	P5CONSOLE	192.168.0.190	SCOTT	EMP_TRG	SAL	AUDIT ACCESS	23237
2005/05/09 17:59:04	SELECT	P5CONSOLE	192.168.0.190	SCOTT	EMP_TRG	MGR	AUDIT ACCESS	23237
2005/05/09 17:59:04	SELECT	P5CONSOLE	192.168.0.190	SCOTT	EMP_TRG	JOB	AUDIT ACCESS	23237
2005/05/09 17:59:04	SELECT	P5CONSOLE	192.168.0.190	SCOTT	EMP_TRG	HIREDATE	AUDIT ACCESS	23237
2005/05/09 17:59:04	SELECT	P5CONSOLE	192.168.0.190	SCOTT	EMP_TRG	ENAME	AUDIT ACCESS	23237
2005/05/09 17:59:04	SELECT	P5CONSOLE	192.168.0.190	SCOTT	EMP_TRG	EMPNO	AUDIT ACCESS	23237
2005/05/09 17:59:55	SELECT	P5CONSOLE	192.168.0.190	SCOTT	EMP_TRG	SAL	AUDIT ACCESS	23237
2005/05/09 17:59:55	SELECT	P5CONSOLE	192.168.0.190	SCOTT	EMP_TRG	MGR	AUDIT ACCESS	23237
2005/05/09 17:59:55	SELECT	P5CONSOLE	192.168.0.190	SCOTT	EMP_TRG	JOB	AUDIT ACCESS	23237
2005/05/09 17:59:55	SELECT	P5CONSOLE	192.168.0.190	SCOTT	EMP_TRG	HIREDATE	AUDIT ACCESS	23237
2005/05/09 17:59:55	SELECT	P5CONSOLE	192.168.0.190	SCOTT	EMP_TRG	ENAME	AUDIT ACCESS	23237

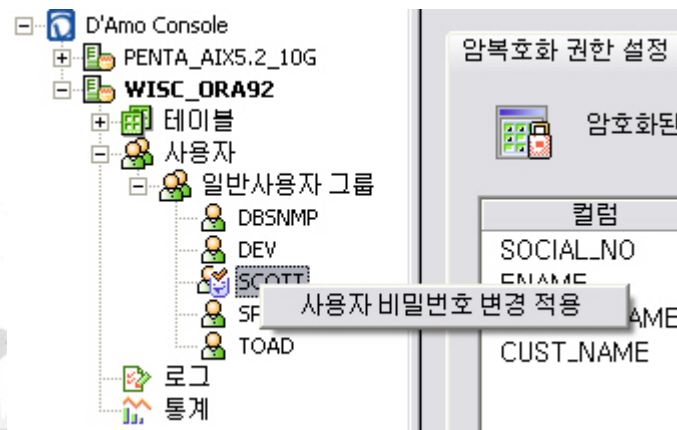
로그 검색 내용

주요기능 – 보안관리



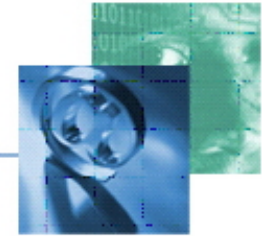
사용자 계정 관리

- 암호화 칼럼에 권한이 부여된 사용자 계정 관리
 - DBA 권한을 획득한 불법 사용자로부터 중요 데이터 보호
 - 해당 업무 담당자에 의해서만 중요 데이터 확인 가능
 - 권한 부여된 사용자의 정상적인 비밀번호 변경 시 보안 관리자에 의한 승인



사용자 비밀번호 변경 적용

주요기능 - 보안관리



로그 스케줄링

- 일정 주기마다 감사 로그 내용을 백업

로그 자동 백업 설정

☒ 로그 자동 백업 설정
☒ 지정된 시간마다 로그를 백업합니다.

마지막 로그 백업 시간 : 2006/04/28 12:00:00
다음 작업 시간 : 2006/04/30 12:00:00

일 마다 시에 로그 파일 백업

로그 보관 분량 : 일 분량을 유지함

다음 경로에 백업

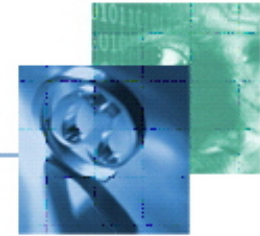
※ 로그 백업 경로는 *utl_file_dir parameter에 설정된 경로를
중의 한 값이어야 합니다.

설정 항목

- 지정일, 시간 설정
- 테이블에 보관 분량 유지
- 백업 파일 경로 지정
(utl_file_dir 경로)

감사 로그 자동 백업 설정

주요기능 - 보안관리



다양한 Reporting

- 다양한 통계 보고서 및 Graph 기능

검색 조건

- 그래프 선택
- 기간별
- 소유자
- 테이블
- 컬럼명
- 접근 IP
- 서비스명
- 접근자명



통계

보고 방법 선택
보고서: [보고서]

조건 설정
기간 조건: 2006-05-02 ~ 2006-05-02
시간: 오전 9:00:00 ~ 오후 11:59:59

기타 조건
접근자명: [접근자명]
서비스명: [서비스명]
접근자명: [접근자명]

그래프 설정
축종 대상(X-축): [축종 대상(X-축)]
접속시각 - 시간별
축종 결과(Y-축): [축종 결과(Y-축)]
☒ 공격호출 성공
☒ 공격호출 실패
☒ 암호화된 파일에 접근 차단

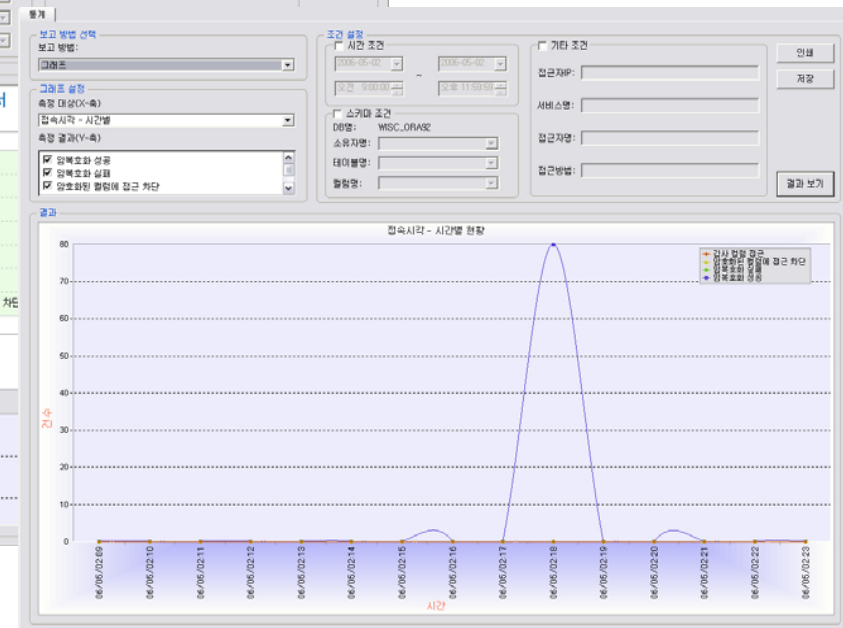
결과

D'Amo 통계 보고서

Database 명	WISC_ORA02
Server IP/Host	192.168.0.49/WISC
DB 버전	Oracle9i Enterprise Edition Release 9.2.0.7.0.32bit
DB SID	ORA02
통계 생성 날짜	2006/05/02 19:19:36
축종 대상(X-축)	접속시각 - 시간별
축종 결과(Y-축)	공격호출 성공, 공격호출 실패, 암호화된 파일에 접근 차단

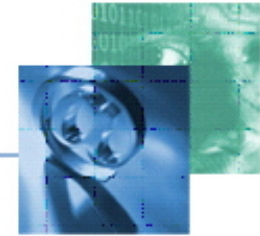
결과 그래프:

접속시각 - 시간별 현황



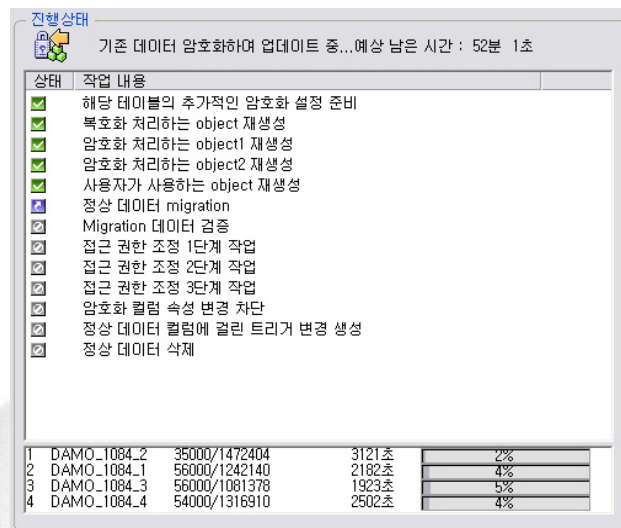
통계 보고서 및 그래프 화면

주요 기능 - 성능 최적화



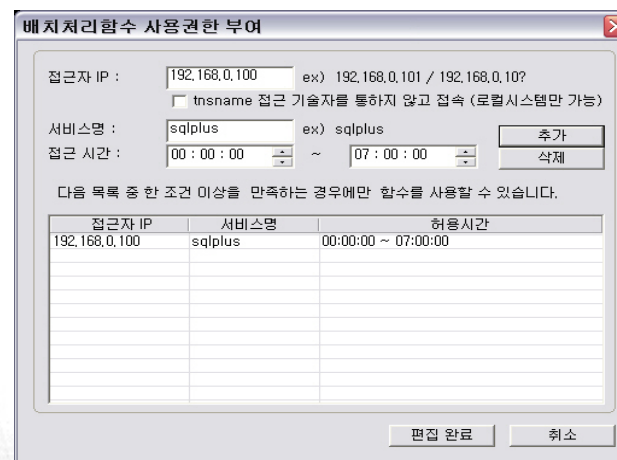
성능 최적화

- 대용량 테이블 일괄 암호화 시 다중 세션을 통한 작업으로 성능 보장
- 배치 업무에 적용 가능한 API 함수 제공하여 성능 개선



4개 세션에서 동시에 일괄 암호화 적용

- 시스템 가용성 고려하여 적절한 세션 수를 이용하여 일괄 암호화 적용
- Array Fetch를 이용한 업데이트



배치처리함수 사용권한 부여

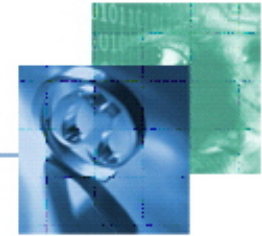
- 부여된 권한 철저한 관리
- 제공된 API를 이용하여 데이터 처리
- 배치함수 이용 매뉴얼 참조



D'Amo Implementation

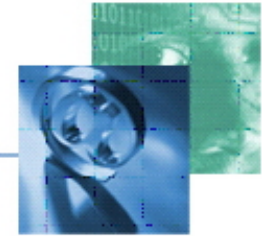
- ① 타 제품과 비교
- ② 구축 시나리오
- ③ System Requirement
- ④ Reference Sites
- ⑤ 구축 사례
- ⑤ 데모 시연

타 제품과 비교



제품 (판매사)	D'Amo (이노라임·펜타시큐리티)	암호화 툴킷 (기존 API 방식)	Obfuscation Toolkit (오라클 암호화 툴킷)
보안 대상	통합 DB 보안	데이터 암호화	데이터 암호화
구동 방식	필터 방식 (소스 수정 불필요)	응용프로그램 수정 필요	제공된 패키지 함수를 통한 개발 방식
암호화	컬럼 단위	컬럼 단위	컬럼 단위 (추가적인 개발 모듈 필요)
구성 요소	2 – Tier 기반 (장애 요소가 없음)	2 – Tier 기반 (DB – Application)	DB 서버
구축 기간	1주일 이내 통합 가능	최소 3개월 이상 (수정 범위에 따라 큰 차이)	3개월 이상
지원 알고리즘	SEED, AES, TDES, DES 등	SEED, AES, TDES, DES 등	AES, DES, TDES
접근제어	<ul style="list-style-type: none"> DB 전체 암호화 칼럼 Application, Time, DB 계정, IP, MAC, Telnet SQL*Net 등 	추가 개발 필요	추가 개발 필요
감 사	<ul style="list-style-type: none"> 암호화 컬럼 비암호화 칼럼 (Audit Only) 	추가 개발 필요	추가 개발 필요
지원 Constraints	<ul style="list-style-type: none"> Index, PK, FK, Default, Trigger 	추가 개발 필요	추가 개발 필요
유지 보수	유연한 적용	어려움	비교적 어려움

구축 시나리오



보안 정책 1 : 고객 주민번호 암호화 ,
보안 정책 3 : SCOTT 계정 로그 인 차단 ,
보안 정책 5 : 접근 내역 기록,

보안 정책 2 : 고객 사용 금액 Audit
보안 정책 4 : App.exe 프로그램만 접속 허용
보안 정책 6 : 백업 데이터 암호화

주민번호 암호화
(보안정책 1)

고객 사용 금액 Audit
(보안정책 2)

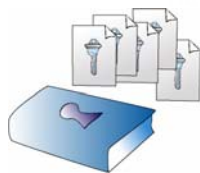
암호화 백업
(보안정책 6)

허용 (보안정책 4)



App.exe

암호화 백업
(보안정책 6)



감사기록
(보안정책 5)

로그 저장

암호화
테이블

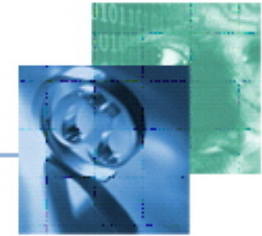
제외표준(백업의)

차단 (보안정책 3)



SCOTT

System Requirement



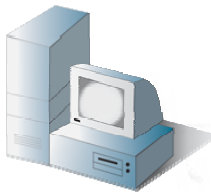
Supported Oracle Versions

- Oracle 8i, 9i, 10g (Enterprise Edition)



Supported Platforms for Security Agent

- UNIX: IBM AIX, HP HP-UX, SUN Solaris
- Linux
- Windows XP/2000/NT/98



Requirement for Console

- Pentium III or above CPU
- 256MB or more Memory
- 100MB of Disk Space or more
- Windows XP/2000/NT/98
- Oracle 8.1.7 Client (SQL*Net)

Reference Sites

공공부문

 **부패방지위원회**

 **산업자원부**
Ministry of Commerce, Industry and Energy

 **공정거래위원회**
FAIR TRADE COMMISSION

 **운전면허시험관리단**
DRIVER'S LICENSE AGENCY

 **해양수산부**
Ministry of Maritime Affairs & Fisheries


 **산림청**
KOREA FOREST SERVICE

 **기상청**
KOREA METEOROLOGICAL ADMINISTRATION

 **한국도로공사**
KOREA HIGHWAY CORPORATION

 **정보통신부**


 **정보통신부 전파연구소**


 **중소기업청**
Small and Medium Business Administration

 **재외동포재단**
OVERSEAS KOREANS FOUNDATION

 **서울특별시**

 **정읍시**
JEONGEUP-SI

 **울산광역시강북교육청**

 **울산광역시교육청**

대한민국 대표도시
변화와 경쟁의 파주

 **대한민국 육군**
Republic of Korea Army

 **대한민국공군**
Republic of Korea Air Force

 **국립수산과학원**
National Fisheries Research & Development Institute

 **innovation21**
함께하는병무청
Military Manpower Administration

 **(재)우정복지협력회**
POST WELFARE & COOPERATION FOUNDATION

금융/일반

 **서울대학교**
SEOUL NATIONAL UNIVERSITY

 **서울대학교 중앙도서관**

 **영산대학교**
YOUNGSAN UNIVERSITY

 **YNCC 여천NCC**

 **LG.PHILIPS LCD**

 **우리홈쇼핑**
WOORI.COM

No.1 재테크포털
MONETA

 **국민건강보험공단**
일산병원
NHIC Ilan Hospital

 **DACOM**
DACOM CORPORATION

 **기업은행**
Industrial Bank of Korea

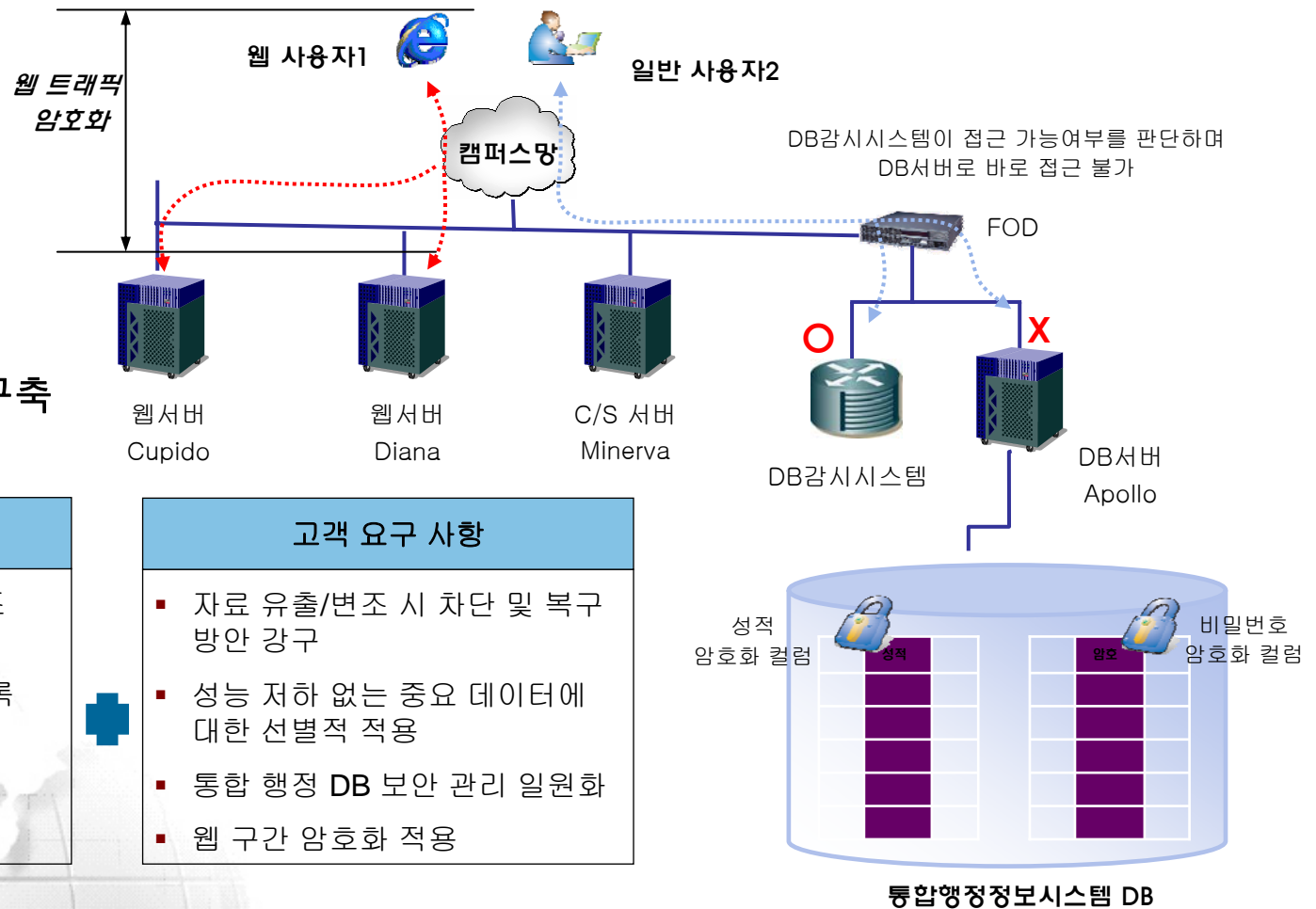
 **HSBC**

구축 사례 – S 대학교

– 성적, 교직원 비밀번호 데이터 암호화

웹 구간 암호화 제품
DB 접근제어 제품
DB 암호화 제품

통합 DB 보안 시스템 구축



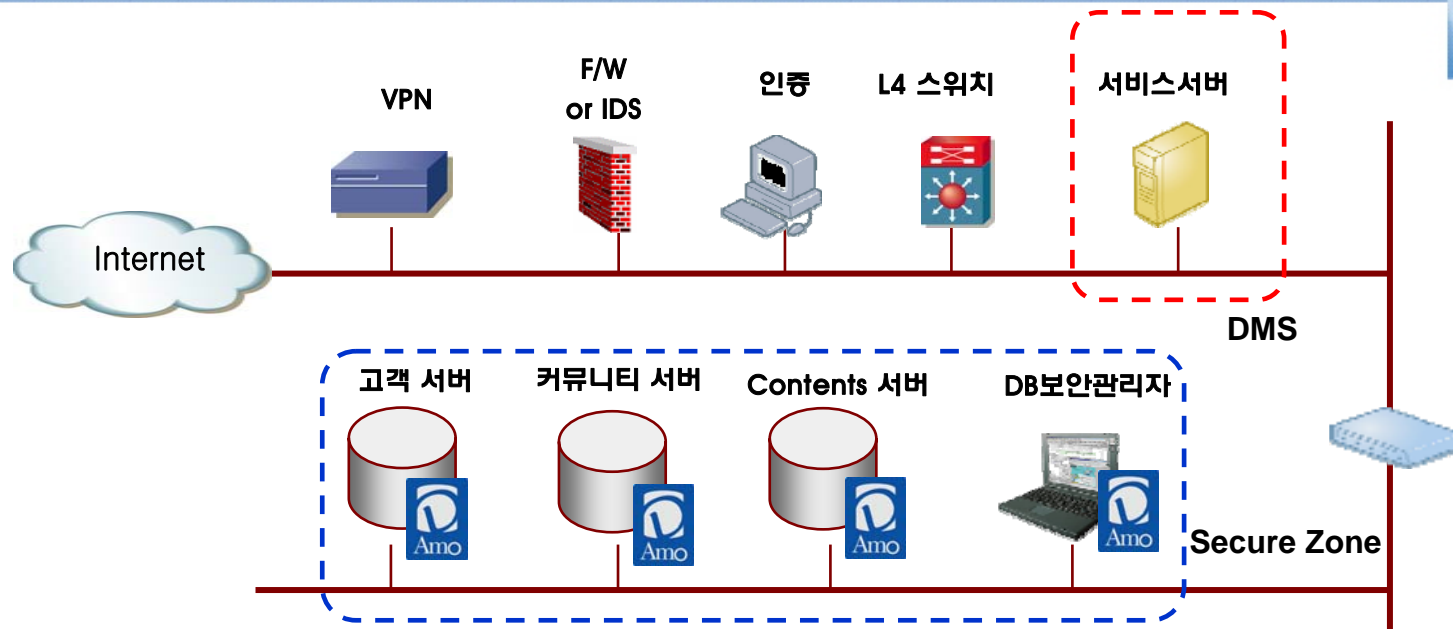
적용 사유

- 주요 데이터에 대한 유출/변조 방지 및 복구
- 접근 자료에 대한 감시 및 기록
- 통합 행정 DB 관리 일원화
- 각 업무서버의 웹 보안

고객 요구 사항

- 자료 유출/변조 시 차단 및 복구 방안 강구
- 성능 저하 없는 중요 데이터에 대한 선별적 적용
- 통합 행정 DB 보안 관리 일원화
- 웹 구간 암호화 적용

구축 사례 – S 통신사



적용 사유

- 주민번호를 암호화하여 개인정보 안전하게 보호
- 금융감독원의 지침에 따라 고객 정보 보호 필요
- 고객정보 유출 시 재정적 손실 및 이미지 실추 예방

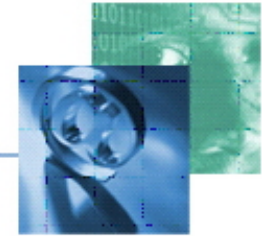
고객 요구 사항

- 가입 회원의 신상 정보를 안전하게 보호
- 개인 정보 보호 지침 준수
- 증권 거래 시 주민번호 유출 방지

기대 효과

- 간편한 적용 및 보안 관리 유연성 확보를 통해 대 고객 신뢰도 향상
- 외주 개발 업체의 고객 정보 유출 방지
- 내부자에 의한 고객 정보 도용 방지
- 서비스 이용하여 증권거래를 하는 고객 신뢰성 향상

D'Amo 데모 시연



데모 시연

