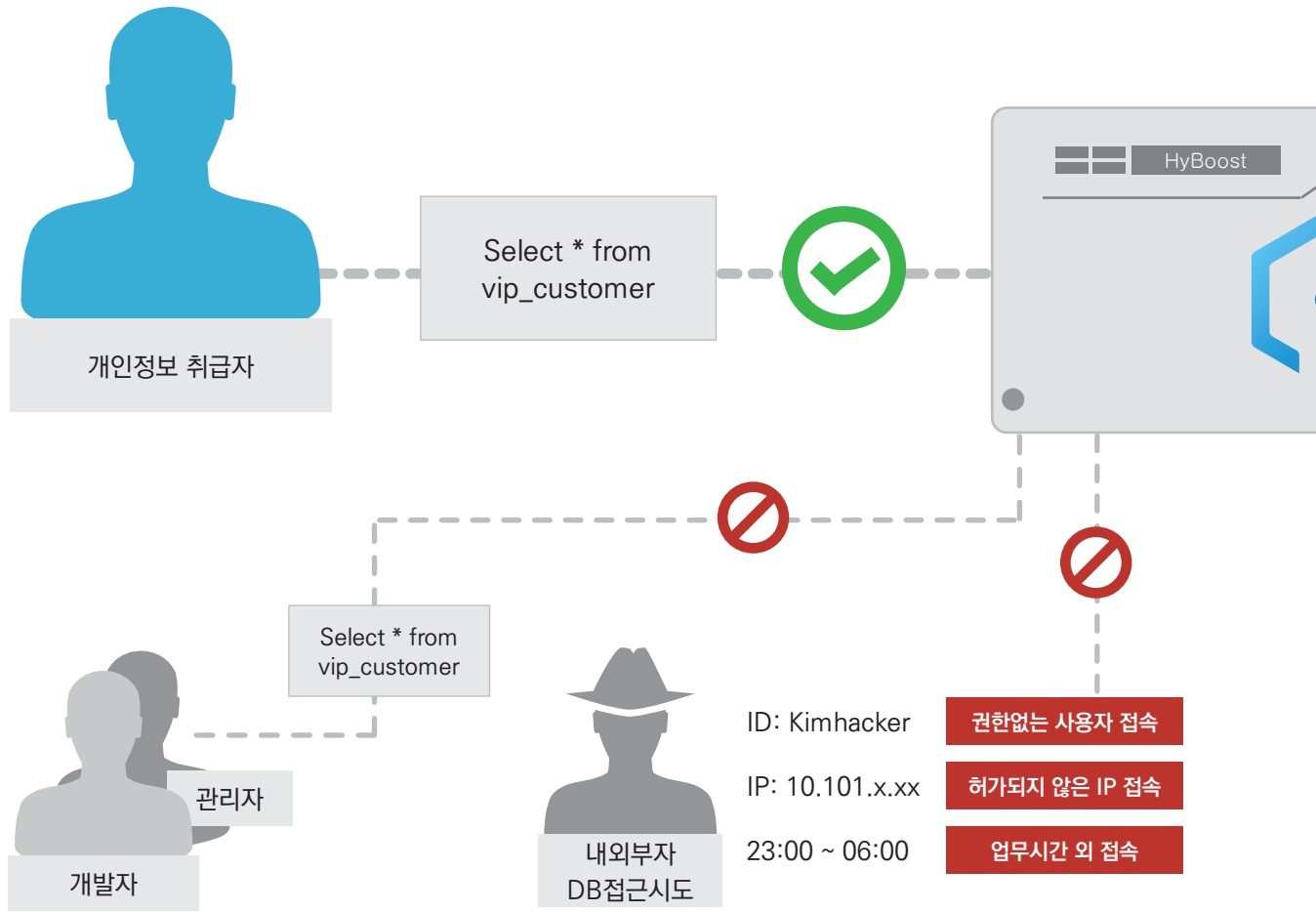




국내 엔터프라이즈
시장 점유율 1위
DB 방화벽 솔루션

SOMANSA

I . DB접근제어 : 사용자, 부서, 권한, 시간대별 접근통제



01 권한, 업무시간 이외 접근 세부 통제

사용자 IP 및 IP 대역 차단/허용	DBMS 계정별 접속 차단/허용	시간대별 접근 설정
----------------------	-------------------	------------

쿼리툴(Toad, Orange, Golden 등) 통제	Telnet, FTP, SFTP, SSH 등의 원격 프로토콜 통제
--------------------------------	--------------------------------------

DB접근통제 정책설정

비인가 접속차단

02 테이블, 칼럼에 대한 접근권한 설정가능

접근통제 대상 테이블명 입력

테이블: vip_customer

접근통제 정책 적용

사용	우선 순위	대응 행동	타입	정책 이름
<input checked="" type="checkbox"/>	1	차단	Prevent	Oracle_개인정보테이블

[비권한자] 대상 테이블 접근 차단

```
SQL> select * from vip_customer;
select * from vip_customer
1행에 오류:
ORA-00900: reject (DB-i Policy)
```

II. 로그분석 및 검색 : 세션 및 SQL 로그, 빅데이터 분석

DB-i

DBMS타입/ DBMS이름	ORACLE/ Marketing
로그ID	95927373_3214_1234_abcde
요청일시	2022-04-07 13:25:07
응답일시	2022-04-07 13:25:07
에이전트 ID	1234567
응답코드/행수	1403 / 6
쿼리분류	DML
수행쿼리	"select* from customer"

DB

단일 웹콘솔로
이기종 DBMS 통합관리
(Oracle, MS SQL, DB2,
SAP HANA 등 18+종류 DBMS 지원)

Microsoft **SQL Server** **ORACLE** **MySQL** **SYBASE**
IBM DB2 **ALTI**BASE **TERADATA** **Informix**

01 법에서 요구하는
세부 이력정보 모두 기록
(법, 대통령령 등 하위법령, 해설서 포함)

세션 로그	SQL 로그	Telnet/FTP 로그
사용자 정보 접속 일시 세션 정보 수행시간 DBMS정보 접속프로그램명 ...	수행내역 쿼리 종류 테이블, 칼럼 차단/허용여부 개인정보 패턴 조회 데이터 등 ...	Telnet SSH FTP SFTP

정기적(월 1회 이상) 접속기록 점검 시,
비인가 개인정보 처리, 대량의 개인정보 조회 등의
행위 탐지 및 대응조치 가능

02 빅데이터 검색엔진

항목	DB-i	타사 솔루션
대량로그 검색속도	고속검색 (1~3분)	저속검색 (#시간 소요)
복수조건 검색시 성능영향	성능저하 없음	성능 저하
동시 다수자 검색시 성능영향	성능저하 없음	성능 저하
로그저장소 안정성 가용성	· 이중화 구성가능 (고가용성) · 샘플링 저장 없이도 CPU 부하 없음	· 이중화 불가 (낮은 가용성) · 샘플링 저장 (쿼리 선택적 저장) 불가 시 CPU 부하로 인한 속도 저하 발생

이상징후 또는 사용자 과거 로그 검색 시
드러다운 방식으로 빠르게 조회 가능

개인정보를 보유한 모든 조직에 적용

개인정보보호법 고시 <개인정보의 안전성 확보조치 기준> 준수

조	내용	기본기능	
5조 <개인정보 처리시스템 (DB)> 접근권한 관리	① 업무상 최소한으로 접근권한 차등부여	부서별, 직원별 접근권한관리	
	② 인사이동시 접근권한변경/말소	접근권한 변경/말소	
	③ 권한부여내역 최소 3년보관	접근권한 변경이력 보관	
	④ 취급자별로 한개의 계정사용, 계정공유금지	1인 1ID 제공	
	⑤ (개인정보취급자 or 정보주체대상) 비밀번호 작성규칙수립 및 적용	비밀번호규칙 강제	
	⑥ ID or PW 일정횟수 오입력시 개인정보처리시스템 접근제한	접근권한 제한	
6조 접근통제	① 불법접근, 침해방지를 위해 다음기능 포함 조치 1. 개인정보처리시스템접속권한 IP 등으로 제한 2. 접속IP 등을 재분석, 불법적유출시도 탐지	IP, ID, MAC, 시간대, 컬럼 등 다양한 조건 접근통제 - 과다조회를 통한 불법적 유출시도 탐지 - 쿼리툴, Telnet, FTP 결과값 모두 저장	
	② 외부접속시 VPN적용	DB VPN 기능으로 송수신 구간 암호화	
	③ 홈페이지, P2P, 공유설정, 공개된 무선망으로 공개/유출되지 않도록 개인정보처리시스템, 컴퓨터, 모바일기기, 관리용 단말기 조치	접근권한 제한	
	⑤ 불법접근 및 침해사고 방지를 위하여 취급자가 일정시간이상 업무처리를 하지 않을 경우 자동으로 개인정보처리시스템 접속차단	자동 로그아웃	
7조 개인정보암호화	① (고유식별정보, 비밀번호, 바이오정보를) 정보통신망으로 송수신시 암호화	DB VPN 기능으로 송수신 구간 암호화	
8조 접속기록의 보관/점검	① 개인정보처리시스템 접속기록 최소 1년이상 보관 다만 5만명 이상 정보주체 개인정보를 처리하거나 고유식별정보/민감정보를 처리할 경우 2년이상 보관	- 개인정보처리시스템 접속기록 및 조회된 정보 로깅 - 개인정보 DB 장기 누적 조회 리포팅	
	② 개인정보처리시스템 접속기록 월 1회 이상 점검 개인정보 다운로드 내역을 발견했을 경우 사유를 반드시 확인		
	③ 접속기록이 위변조, 도난, 분실되지 않도록 안전하게 보관	접속기록 로그 위변조 방지 기능	
10조 관리용 단말기 안전조치 (서버, PC, 보조매체 대상)	11조 물리적 안전조치 (서류, 보조매체 대상)	13조 파기 (전자파일, 서류대상)	<DB접근 후 개인정보 PC복제방지> DB 내 개인정보가 PC, 보조매체, 출력물로 복제되는 것을 최소화 → 조직내 암호화, 물리적접근방지, 파기대상 최소화 효과

금융기업에 적용

신용정보업 관련 규정 <기술적·물리적·관리적 보안대책 마련기준> 준수

조항		기본기능
III. 관리적 보안대책	2. 개인신용정보 조회권한 구분 가. 조회권한을 초과하여 고객정보 조회를 일정횟수이상 시도한 직원에 대한 통제장치 마련 나. 영업점 및 신용정보 관리부서의 개인신용정보 조회건수에 대해 정기적으로 점검하고 조회건수가 평소보다 급증한 부서 및 직원들을 샘플링하여 점검 실시	개인정보 DB 장기 누적 조회 리포팅



2022.04.07, DB-i V 6.1
국정원 CC인증 (EAL4등급)

- ▶ 과기정통부지정 정보보안 컨설팅전문업체 ▶ 행안부지정 개인정보 영향평가기관 ▶ 조달청 조달등록기업
- ▶ 신용평가등급 A+ 재무안정성 상위1% ▶ 창립 이래 무차입경영, 20년 연속 흑자기업
- ▶ 개인정보보호/데이터보호분야 100건이상 기술특허 보유 및 출원 (타기업대비 3배이상)

특허1

데이터베이스와 클라이언트 간 DB-VPN을 이용한 안전통신시스템 및 방법 (특허 10-1104845호)

특허2

Query에 대한 데이터베이스 응답값 분석 및 이상징후탐지를 이용한 개인정보유출방지시스템 및 유출방지방법 (특허: 10-1200907호)

특허3

개인정보 은닉화를 수행하는 DB보안방법 (특허 10-1111162호)

특허4

내부사용자에 의해 개인정보가 유출되는 것을 방지하기 위한 쿼리툴 통제방법 및 그 시스템 (특허 10-1153969호)

III. 내용기반 통제 : 개인정보 대량조회

(또는 업무상 최소범위 이상 조회시) 차단

세션 로그 정보

로그 ID	d669613e-b675-42cd-84f8-41f19564ceb7
사용자	관리자 (관리자 권한)
보낸 IP	192.168.1.100
받는 IP	192.168.1.100
보낸 port	49308
받는 port	49308

예) 5천건 이상의 개인정보 조회 차단 및 기록
(쿼리 종류, 개인정보 패턴 및 개수, 대응 행동 등)

쿼리 분류	쿼리 종류	테이블 이름	컬럼 이름	패턴 개수	요청 일시	처리 시간(초)	대응 행동
DML	SELECT	[CUSTOMER1]		10,024	2018-05-08 15:56:07	11.074	차단
DML	SELECT	[CUSTOMER1]		5,420	2018-05-08 15:56:07	25.295	차단
DML	SELECT	[DUAL]			2018-05-08 15:56:07	12.131	허용

조회된 데이터 확인 가능 (Whose Privacy)

실명 후 조회 데이터

NUM	NAME	SEX	JUMIN	CARD	ACCOUNTNUM
1.000000	김영환	남자	8000709-1	9441-9890	130392-79
2.000000	이연정	여자	870507-2	2436-1463	529275-98
3.000000	백수진	여자	770512-2	7653-3959	650738-67
1.000000	정남배	남자	741102-1	9441-9890	130392-79
2.000000	김영환	여자	900220-2	2436-1463	529275-98
3.000000	최아나	여자	651208-2	7653-3959	650738-67

01 개인정보보호 솔루션
23년 개발
노하우 탑재

02 법률에서 요구하는
고유식별정보 외
개인정보패턴 모두 지원

03 국내유일,
고유식별정보 체크섬
3중 보유

04 EU GDPR 준수를 위한
EU 개인정보 패턴
분석지원

IV. DB 개인정보 유출 방지

DB 접속 후 개인정보 PC무단저장 통제



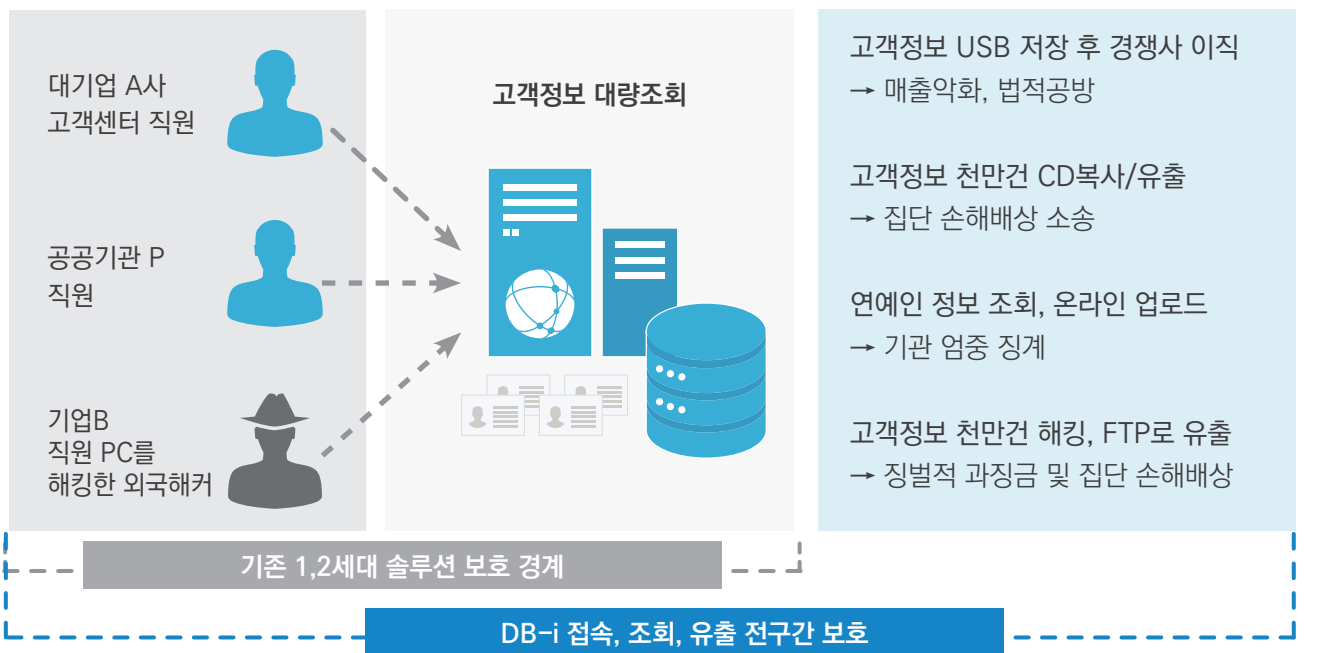
개인정보 유출차단

DB 개인정보 악용 및 실제기업 피해사례

1차: 비권한 접속시도

2차: 개인정보 대량조회

3차: 개인정보 유출 및 2차 피해



기존 DB 접근통제 솔루션은 비권한 접속 시도 및 데이터 조회에 대한 통제만 제시

- DB 접근통제를 구축하더라도 DB접속자 PC로 유출시에는 징벌적 손해배상제와 법정 손해배상제 적용 (B사, Y사 등)
- 기존 솔루션은 DB에 접근하는 관리용 단말기(DB 접속 PC)를 통한 최종 유출 시도를 막을 수 없어 법적 리스크가 큼

DB-i는 개인정보 접속, 조회, 유출 전 구간의 커버리지로 법률적·보안상의 리스크를 최소화함

- 국내 유일, DB ↔ DB 접속 PC 전 구간의 보호조치 적용
- 법률적 요구사항 100% 충족
- 최종 유출 시도 무력화

DB-i를 통해 대기업, 공공기관 수준 최적의 보호조치를 구축하실 수 있습니다

엔터프라이즈
시장 1위

서버대수&CPU
기준 시장 1위

- 삼성그룹 표준(삼성전자 포함 30개사)
- LG그룹표준(글로벌 4대 서버팜외)
- KT그룹 표준(4대 데이터센터)
- 금호아시아나그룹 표준(7개사)
- CJ그룹 표준(15개사)
- 두산그룹 표준
- 국가정보자원관리원 (DBMS 500대)

기업

삼성전자, 삼성SDI, 삼성중공업, 삼성물산, 삼성카드, 삼성생명, 삼성테크윈, 삼성섬유화학, 삼성서울병원, LG전자, LG화학, LG이노텍, 엘지하우시스, LG CNS, LG디스플레이, KT, 금호아시아나, 금호건설, 금호타이어, CK, CJ올리브네트웍스, CJ E&M, 두산, SK, SK이노베이션, SK가스, SK E&S, 롯데정보통신, 대우건설, 교보문고, 유한양행, NC소프트

공공

국가정보자원관리원, 보건복지부, 방송통신위원회, 방위사업청, 신용회복위원회, 한국교육학술정보원, 4대사회보험 연계센터, 정부청사관리본부, 국민연공관리공단, 한국생명공학연구원, 한국교직원공제회, 한국보건복지인력개발원, 한국지역정보개발원, 재료연구소, 서울교통공사, 대전도시공사, 경찰병원, 국민체육진흥공단, 원주시청, 충북도청, 익산시청, 한양대학교병원

금융

KB그룹, 씨티뱅크, 씨티증권, 농협중앙회, KDB산업은행, KDB생명, 메트라이프, 그린손해보험, 한국투자증권, KT 캐피탈, SC은행, 우리FIS, 교보라이프플래닛생명보험