유출사고시 법원이 **기업의 유무죄를 판단**하는 기준
〈선량한 관리자의 의무〉 3대요건 최적화 솔루션

법규를 준수하였는가?

방송통신위원회 정보통신망법 고시
〈개인정보의 기술적 관리적 보호조치 기준〉

행정안전부 개인정보보호법 고시
〈개인정보의 안전성 확보조치 기준〉

개인정보보호 1위기업에서 국내유일 법연구와 판례해석을 거쳐 개발하였습니다

[천만명 유출사고] 재발을 방지하는가?

2008년 A사
유출자는 자회사 PC 업무계정으로 주민번호 등을 PC로 전송받아 엑셀파일로 저장 후 DVD 2장, 외장하드 2곳에 복사
(출처 : 대법원 2012.12.26 선고 판결문)

2011년 B사
해커는 컴퓨터에서 DB백업명령어로 개인정보DB를 덤프포맷파일로 저장하고...FTP로 서버에 내려받고...
(출처 : 대구지법 2014.02.13 선고 판결문)

2012년 C사
〈개인정보처리시스템접속기록〉은 네트워크에서의 침입탐지시도를 위한 로그기록 전반이 아닌 〈개인정보 DB에서의 개인정보 열람·수정·삭제·출력 등 작업을 위한 접속기록〉을 의미하는 것으로...
(출처 : 서울중앙지법 2014.08.22 선고 판결문)

유죄냐? 무죄냐? 선택에 달려있습니다

〈집단소송판례에서 법원이 명시한 과실〉로 인한 유출사고가 귀사에서 재발하면 어떻게 될까요?
***DB-i*를 선택하셔야 하는 이유입니다**

기술적보호수준이 동종업계 평균 이상인가?

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
- 정부통합전산센터(DBMS 500대)

기업 / 공공 / 금융

최고의 대기업, 공공기관과 같은 보호수준임을 입증하실 수 있습니다

세계 최초 〈과다조회를 통한 불법적 유출시도탐지〉에 최적화된 개인정보패킷분석엔진 탑재

DB-i HyBoost

- SW버전보다 3~5배 성능 향상
- 패킷로스 0%, 정확성 100%
- 복잡한 설치는 NO, 꽂아서 바로쓴다
- 사내 트래픽량에 맞춰 선택 (하이부스트 100, 500, 1000, 10G)

개인정보를 보유한 모든 조직에 적용 개인정보보호법 고시 〈개인정보의 안전성 확보조치 기준〉 준수

조	내용	기본기능	4대 강점
4조 〈개인정보 처리시스템=DB〉 접근권한관리	① 업무상 최소한으로 접근권한 차등부여	부서별, 직원별 접근권한관리	〈DB접근 후 개인정보 PC복제방지〉 〈개인정보 조회권한〉 허용, 〈PC복제권한〉 차단으로 권한차등부여
	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	
5조 접근통제	① 1. 개인정보처리시스템접속권한을 IP 등으로 제한	IP, ID, MAC, 시간대, 컬럼 등 다양한 조건의 접근통제	
	2. 접속IP 등을 재분석, 불법적유출시도 탐지 〈2014 집단소송판례〉에서 가장 중요한 과실항목임		〈과다조회를 통한 불법적유출시도 탐지〉 IP 등 기본적정보 외에 쿼리툴, Telnet, FTP 결과값을 모두 저장 → 각각의 결과값 내 개인정보패턴과 갯수분석 → 검색, 리포팅으로 개인정보유출시도 탐지
	② 외부접속시 VPN적용		〈DB VPN〉
6조 암호화	② (고유식별정보, 비밀번호, 바이오정보를) 정보통신망으로 송수신시 암호화		〈DB VPN〉
7조 접속기록의 보관/점검	① 개인정보처리시스템 접속기록 최소 6개월 보관		〈과다조회를 통한 불법적유출시도 탐지〉 쿼리툴, Telnet, FTP 접속기록(명령어&결과값) 저장 → 접속기록 내 개인정보패턴과 갯수분석 → 검색, 리포팅을 활용하여 점검
	② 개인정보처리시스템 접속기록 반기별로 1회 이상 점검 2014년 신설규정		
	③ 접속기록위변조방지보관		〈로그위변조방지스토리지〉

6조 암호화 (서버, PC, 보조매체 대상)	9조 물리적 접근방지 (서류, 보조매체 대상)	10조 파기 (전자파일, 서류대상)	〈DB접근 후 개인정보 PC복제방지〉 DB 내 개인정보가 PC, 보조매체, 출력물로 복제되는 것을 최소화 → 조직내 암호화, 물리적접근방지, 파기대상 최소화효과


DB-i V3.1
국정원 CC인증(EAL4등급)

▶미래창조과학부지정 정보보안컨설팅전문기관 ▶안행부지정 개인정보영향평가전문기관 ▶조달청 조달등록기업
▶신용평가등급 A- 로 재무안정성 상위1% ▶창립 이래 무차입경영, 9년 연속 흑자기업

▶개인정보보호/데이터보호분야 20건이상 기술특허 보유 및 출원 (타기업대비 3배이상)

특허 1 데이터베이스와 클라이언트 간 DB-VPN을 이용한 안전통신시스템 및 방법 (특허 10-1104945호)
특허 2 Query에 대한 데이터베이스 응답값 분석 및 이상징후탐지를 이용한 개인정보유출방지시스템 및 유출방지방법 (특허 : 10-1200907호)
특허 3 개인정보 은닉화를 수행하는 DB보안방법 (특허 10-1111162호)
특허 4 내부사용자에 의해 개인정보가 유출되는 것을 방지하기 위한 쿼리툴 통제방법 및 그 시스템 (특허 10-1153069호)
특허 5 질의어 데이터량별 기반의 개인정보보호시스템 및 이를 이용한 개인정보보호방법 (특허 : 10-1211054호)

SOMANSA

서울특별시 영등포구 영등포동8가 92번지 KnK디지털타워 9층
TEL 02)2636-8300 FAX 02)2636-8181 www.somansa.com

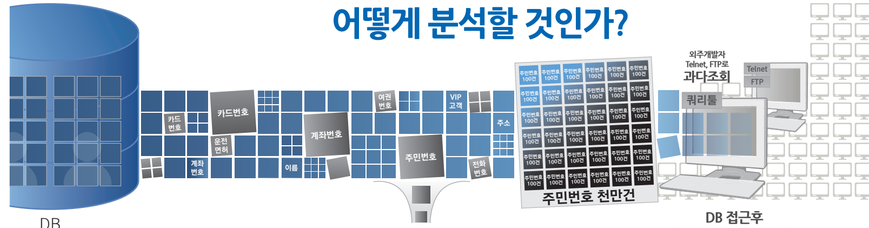
국내 엔터프라이즈 시장 점유율 1위
국내유일 컴플라이언스 DB방화벽

DB-i

법규준수 개인정보보호법 고시 '개인정보의 안전성 확보조치 기준' 만족

법규준수 정보통신망법 고시 '개인정보의 기술적 관리적 보호조치' 만족

개인정보과다조회의 이상징후 어떻게 분석할 것인가?



DB방화벽 DB-i
개인정보보호법 준수 4대 강점

강점 01 〈과다조회이용 불법적유출시도탐지〉

천만명유출사고 재발방지기능 〈2011년 유출사고〉의 원인 : 쿼리툴과 FTP를 통한 개인정보과다조회

해커가 권한자의 ID와 비밀번호를 도용하여 DB접근

유출원인 ① 쿼리툴로 개인정보과다조회 export명령어로 파일출력

FTP **유출원인 ②** FTP로 개인정보과다조회(=다운로드)

DB-i 가 있었다면? 〈과다조회 이용 불법적유출시도탐지〉기능으로 유출방지

〈2014 집단소송판례〉 〈과다조회이용불법유출시도〉 미탐지를 과실로 명시

(정보통신망법고시 4조5항 해석)
통상적업무와 다른 업무 수행, 비정상트래픽 발생시 탐지, 보안관리자가 조치할 수 있도록 감시활동을 수행할 의무가 포함된다

대용량의 개인정보 파일을…FTP방식으로… 컴퓨터를 거쳐 외부망으로 전송하는 동안…FTP는 파일 전송을 위한 프로토콜로 대량의 파일을 쉽게 송수신하므로 보안상 취약

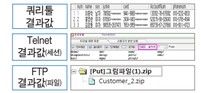
일정규모 이상 개인정보출력시 이상징후로 감지, 실제 접속권한자가 업무목적으로 작업하는지 확인하는 보안조치를 취했어야…

(대구지법 02.13 판결문 중)

월1회이상 개인정보 처리시스템 접속기록을 감독, 확인했다면 사용패턴에서 평상시와 다른 특이점을 발견, 유출을 방지할 수 있었음에도 주의의무를 다 하지 못하고..

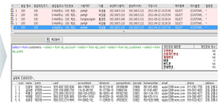
(서울중앙지법 08.22 판결문 중)

1 조회명령어뿐 아니라 결과값(=개인정보)을 함께 저장



2 각각의 결과값에 포함된 개인정보패턴과 갯수분석

3 주기적으로 개인정보과다조회자 검색



4 개인정보조회총량 리포팅

5 과다조회, 파일출력 등 이상징후발생시 〈DB블랙박스〉활영, 보안담당자에게 경고

판례해석을 거쳐 개발한 〈법원이 명시한 과실〉방지기능으로 선량한 관리자의 의무준수

Benefit 정상 이면의 비정상, 과다조회, 유출시도의 이상징후를 정확하게 탐지

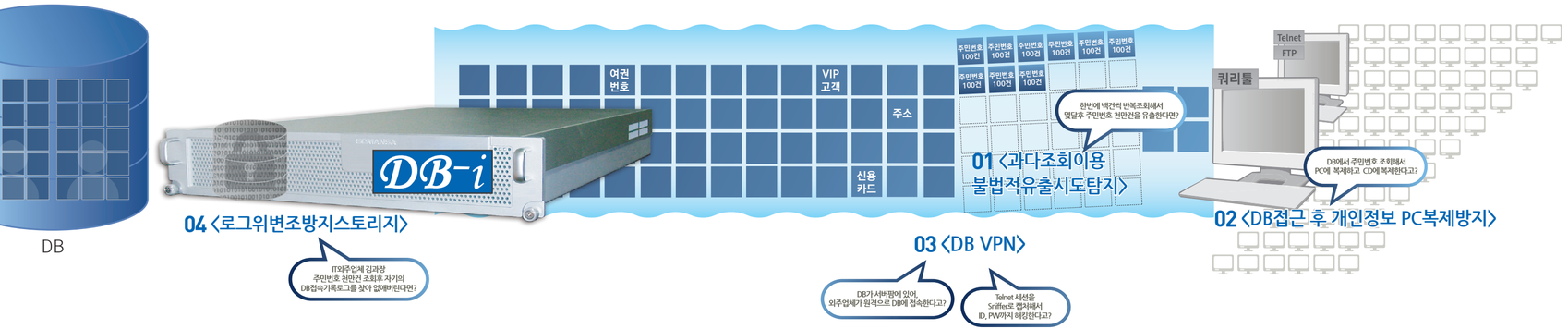
Benefit Telnet, FTP 분석 및 통제능력 국내최강

Benefit 외주개발자 or 권한자를 가장한 해커 통제 (외주개발자와 해커의 주접근통로는 Telnet, FTP)

개인정보과다조회란 무엇인가?
권한자(or 권한탈취해커, 프로그램)가 업무상최소범위를 넘어 대량으로 조회하는 것. 주로 소량조회를 장기간 반복하여 과다조회 후 유출함

법규준수 개인정보보호법 고시 〈개인정보의 안전성 확보조치기준〉
6조(접근통제시스템 설치 및 운영) 1항 2호
개인정보처리시스템에 접속한 IP 주소 등을 분석, 불법적 개인정보유출시도를 탐지
7조(접속기록의 보관 및 점검) 2항
개인정보처리시스템 접속기록을 반기별로 1회 이상 점검

법규준수 정보통신망법 고시 〈개인정보의 기술적 관리적 보호조치〉
4조(접근통제) 5항
불법접근방지를 위해 다음 기능 포함 시스템설치운영
1. 접속권한을 IP 등으로 제한 비인가접근제한
5조(접속기록) 1항
개인정보처리시스템 접속기록을 월 1회 이상 점검



강점 02 〈DB접근 후 개인정보 PC복제방지〉

사전차단을 원한다면 〈QTC〉

DB 접근 후 개인정보 PC복제를 사전차단
Copy & Paste 차단
파일생성 차단
인쇄 차단

QTC (Query Tool Control)

사후감사를 원한다면 〈DB블랙박스〉

DB에 접근해서 개인정보를 과다조회한 후 → PC에 파일로 복제한 후 → DVD로 유출했다면? / 웹메일로 유출했다면?

유출자 PC 화면촬영, 동영상으로 재생

법규준수

정보통신망법고시 8조 준수
정보통신서비스제공자는 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며 용도에 따라 출력항목을 최소화한다

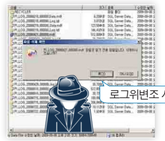
개인정보보호법 고시 5조 1항2호 준수
개인정보처리시스템에 접속한 IP 주소 등을 분석하여 불법적인 개인정보 유출시도를 탐지

개인정보보호법 표준지침 18조 1항(개인정보처리자감독)
개인정보취급자의 개인정보처리범위를 업무상 필요한도 내에서 최소한으로 제한하여야 한다

Benefit 외주인력 개인정보처리범위 업무한도내에서 최소 제한
DB접속 후 개인정보를 화면으로 조회하는 권한 / PC에 복제, 출력하는 권한 구분

Benefit 완벽한 포렌식감사자료생성
네트워크 접근로그 + DB블랙박스로그(엔드포인트단)

강점 04 〈로그위변조방지스토리지〉 자체탑재(추가비용없음)



기존문제점
WORM 스토리지 **추가구입 가격** 1 TeraByte 당 = **수천만원**
CD 및 DVD구매비용 및 교체시간, 느린 검색으로 인한 **업무효율 저하**

Benefit **추가비용없이 로그위변조방지구현 업무효율 상승으로 인건비절감!**

법규준수 개인정보보호법, 정보통신망법, 금감원 모범규준

개인정보보호법 고시 8조 2항
개인정보처리자는 개인정보취급자의 접속기록이 위변조 및 도난분실되지 않도록 해당접속기록을 안전하게 보관

정보통신망법 고시 5조 3항
정보통신서비스제공자 등은 개인정보취급자의 접속기록이 위변조되지 않도록 해야 한다

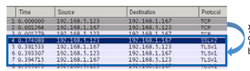
금감원 내부통제모범규준 9조
로그기록보관상태를 연1회 점검, 점검결과 5년 기록 및 관리

강점 03 〈DB VPN〉으로 송수신구간 개인정보암호화(SSH대체 효과)

Benefit SSH(Secure SHell)대체, 별도의 VPN솔루션 도입필요없음

Benefit 쿼리툴 결과값 / Telnet 세션 / FTP 파일 → 전송시 암호화

Benefit DB관리자와 서버팜이 물리적으로 떨어져 있을 때 필수기능



평문프로토콜이 암호화프로토콜로 바뀜

[송수신구간 패킷캡쳐화면]

법규준수

개인정보보호법 고시

6조 2항
개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속시 가상사설망(VPN) 또는 전용선 등 안전한 접속수단을 적용

7조 2항
개인정보처리자는 개인정보를 정보통신망을 통하여 송,수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화

천만명유출사고 재발방지기능 〈2008년 유출사고〉의 원인 : DB접근 후 개인정보PC복제

유출원인 ① 내부 권한자가 WAS를 통해 소량조회를 반복하여 〈개인정보과다조회〉

유출원인 ② DB접근후 과다조회한 개인정보를 PC에 복제

유출원인 ③ DVD에 저장, 유출

WAS-i 가 있었다면? WAS를 통한 〈개인정보과다조회 이상징후분석〉

DB-i 가 있었다면? 〈DB접근후 개인정보 PC복제방지〉로 차단/탐지