Server-i 가 필요한 3대 이유

이유 1 2016년의 가장 중요한 개인정보 보호조치는 〈점검→파기〉

유효기간 지난 개인정보가 파기되지않고 쌓여있는 것이 **적폐**

어떤 개인정보가 어디에 얼마나 있는지 모르는 것이 **비정상**

2015년 〈점검→파기〉를 주내용으로 법정부(종합대책) 발표

- 법정부연합 [금융회사 개인정보유출 재발방지 종합대책] 발표
- 국무총리실 법정부 TF [국가적 개인정보대청소] 선포

법령근거없는 주민번호 〈점검→파기〉

〈점검→파기〉로 **적폐해소 비정상의 정상화**

유출되지 않아도 〈점검→파기〉하지 않으면 형사처벌

개인정보 미파기 적발시 2년 징역 2천만원 벌금 정보통신망법 73조1의 2호

이유 2 〈점검→파기〉 최우선 대상은 서버

[서버에서 발생한 천만명 유출사고 ①②③]

천만명 유출사고 ①	천만명 유출사고 ②	천만명 유출사고 ③
2014년 카드사	2011년 정보통신사	2011년 금융권

[천만명유출사고의 원인 ①②]

유출사고의 원인 ①	유출사고의 원인 ②
DB서버와 웹서버 내 개인정보를 〈미점검 → 미파기〉	DB서버와 웹서버에 〈파일대량 유출수단〉연동

서버에 연동해서는 안되는 〈파일대량유출수단〉은 무엇인가?

USB	FTP	공유 디렉토리	해킹툴
2014년 카드사	2011년 정보통신사 실제 재판에서 유죄판결	법이 명시한 유출수단 형사처벌 영업정지	2011년 금융권

유죄냐? 무죄냐? 선택에 달려있습니다

이유 3 서버 〈점검→파기〉 솔루션은 시장1위를 선택하십시오

- 감사기관: 감사원
- 제1금융(은행): KB국민은행, 하나은행, 신한은행
- 금융: 삼성생명, 삼성카드, Cigna 라이나생명, 비씨카드, LIG 손해보험, AIG, KB 생명, Hyundai Card
- 공공: 대한민국역사박물관, 삼정회계법인, 한국도로공사, 헌법재판소
- 기업: SK telecom, SK planet, 삼성SDS

Server-i 가 있어야만 준수할 수 있는 법규정

모든 공공기관, 기업, 단체에 적용 〈개인정보보호법〉

조항	법규정	귀사의 체크리스트	Server-i 법규준수기능
2조 (정의)	〈개인정보처리의 개념〉 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 연계, 연동	사내 서버의 개인정보현황을 분석하고 있는가?	사내서버의 개인정보현황 분석
28조 (취급자감독)	〈개인정보취급자〉에게 적절한 관리/감독 시행	사내 서버의 개인정보 현황분석 후 위험순위를 매겨서 서버에 접근할수 있는 개인정보취급자를 위험순위에 따라 관리하고 있는가?	서버 내 개인정보 위험순위에 따라 서버 책임부서 및 취급자 관리
21조 (파기)	① 개인정보가 불필요하게 되었을 때에는 복구/재생되지 않도록 지체없이 파기	서버 내 저장된 개인정보가 유효기간이 만료되면 지체없이 파기하는가?	서버 내 유효기간이 만료된 개인정보 검출 및 파기
24조 (고유식별정보처리제한)	고유식별정보(주민, 여권, 운전면허, 외국인등록번호) 암호화	서버 내 고유식별정보저장현황을 주기적으로 점검하고 암호화저장하고 있는가?	서버 내 고유식별정보 저장현황분석 및 국정원 암호화모듈로 암호화저장
32조 (개인정보파일등록)	공공기관은 개인정보파일명칭, 운영근거/목적, 항목, 처리방법, 보유기간, 제공받는 자를 행자부에 등록	서버 내 개인정보현황 파악 후 불필요한 개인정보를 파기한 후 행자부에 등록하는가?	서버 내 개인정보현황분석 및 파기

모든 공공기관, 기업, 단체에 적용 개인정보보호법고시 〈개인정보의 안전성 확보조치 기준〉

조항	법규정	귀사의 체크리스트	Server-i 법규준수기능
5조 (접근통제)	④ 개인정보가 홈페이지, P2P, 공유설정, 공개된 무선망 등을 통해 공개 유출되지 않도록 〈개인정보처리시스템〉, 컴퓨터, 모바일에 조치	DB와 연계연동된 서버는 법적으로 개인정보처리시스템이다. DB와 연계연동된 서버에 홈페이지, P2P, 공유설정, 공개무선망 연결을 차단하고 있는가?	국내유일 형사처벌 · 영업정지 방지기능 (DB와 연계연동된) 서버에 공유설정(공유디렉토리)을 하지 않음
6조 (암호화)	① 고유식별정보, 비밀번호, 바이오정보 암호화	서버 내 고유식별정보, 비밀번호, 바이오정보 저장현황을 주기적으로 점검하고 암호화저장하고 있는가?	(DB암호화 후 생성되는) DB서버 임시Table 내 평문저장된 개인정보 검출, 경보, 암호화
	④ 인터넷구간 및 인터넷과 내부망의 중간지점 (DMZ : Demilitarized Zone)에 고유식별정보저장시 암호화	DMZ구간에 위치한 웹서버, 웹애플리케이션서버 내 고유식별정보 저장현황을 주기적으로 점검하고 암호화저장하고 있는가?	DMZ구간 내 웹서버, 웹애플리케이션서버 내 고유식별정보 검출, 경보, 암호화
	⑤ 내부망에 고유식별정보저장시 암호화 적용여부 및 범위는 다음 기준에 따른다. 1. (법33조에 따른) 영향평가결과 (영향평가대상 공공기관 경우) 2. 위험도분석결과	영향평가와 위험도분석 최우선사항인 전사적 개인정보 현황분석시 사내 서버 내 개인정보 현황분석을 포함하고 있는가?	서버 내 개인정보 보유현황 분석
	⑥ 안전한 암호알고리즘으로 암호화	서버 내 고유식별정보, 비밀번호, 바이오정보를 국정원에서 인정한 안전한 암호화알고리즘으로 암호화하고 있는가?	국정원인증 암호화알고리즘으로 암호화

정보통신서비스제공자에 적용 〈정보통신망 이용촉진 및 정보보호 등에 관한 법률〉

조항	법규정	귀사의 체크리스트	Server-i 법규준수기능
23조의2 (주민번호제한)	① (법령근거가 없는) 주민번호를 수집, 이용할 수 없다	서버에 최근 신규저장된 주민번호가 있는지 주기적으로 점검하고 있는가?	서버 내 전사적 주민번호 검출, 경보, 파기
29조의2 (파기)	② 1년 이상 휴면사용자 개인정보 파기	서버에 휴면기간 1년이 지난 개인정보가 있는지 주기적으로 점검하고 있는가?	사내서버의 개인정보 현황분석
69조의2 (고발)	개인정보 전송 및 저장시 암호화를 하지않아 유출될 경우 방통위는 기업을 검찰고발할 수 있음	서버 내 개인정보가 암호화저장되어 있는가	서버 내 개인정보 암호화
73조 1의 2호 (형사처벌)	(유효기간만료, 목적달성한) 개인정보 미파기시 2년 이하 징역 2천만원 이하 벌금	서버 내 저장된 개인정보 유효기간이 만료되면 지체없이 파기하는가?	서버 내 유효기간이 만료된 개인정보검출 및 파기

금융기관에 적용 금융회사 정보기술(IT)부문 보호업무 모범규준

조항	법규정	귀사의 체크리스트	Server-i 법규준수기능
11. 해킹 등 침해행위 방지대책	⑦ 공개용 웹서버 관리대책 (4) DMZ 구간 내에 주요정보 (이용자인적사항, 전자금융거래정보) 저장 및 관리금지(거래로그관리시 반드시 암호화 및 업무목적 종료후 파기)	DMZ구간에 위치한 웹서버 내 개인정보 저장현황을 주기적으로 점검하고 암호화대상일 경우 암호화저장하고 있는가?	웹서버 내 개인정보 검출, 암호화

금융기관에 적용 금융감독원 〈금융기관 검사 및 제재에 관한 규정〉 중 〈기술적 물리적 관리적 보안대책〉

조항	법규정	귀사의 체크리스트	Server-i 법규준수기능
1조 (접근통제)	⑥ 개인신용정보가 홈페이지, P2P, 공유설정 등을 통하여 공개되지 않도록 〈개인신용정보처리시스템〉 및 취급자 PC를 설정	DB와 연계연동된 서버는 법적으로 개인정보처리시스템이다. DB와 연계연동된 서버에 홈페이지, P2P, 공유설정 연결을 차단하고 있는가?	국내유일 형사처벌 · 영업정지 방지기능 (DB와 연계연동된) 서버에 공유설정(공유디렉토리)을 하지 않음

- ▶ 미래창조과학부지정 지식정보보안 컨설팅전문업체
- ▶ 행정자치부지정 개인정보 영향평가기관
- ▶ 조달청 조달등록기업
- ▶ 신용평가등급 A 로 재무안정성 상위1%
- ▶ 창립 이래 무차입경영, 13년 연속 흑자기업
- ▶ **국내제품 중 최초로 서버에 포함된 개인정보 파일보호 및 개인정보 보호분야 특허 20여건 등록**

SOMANSA
서울특별시 영등포구 영신로220 KnK디지털타워 9층
TEL 02)2636-8300 FAX 02)2636-8181 www.somansa.com

전면개정 2015.02, 수정 2016.01

시장1위 서버 내 개인정보보호 솔루션

Server-i

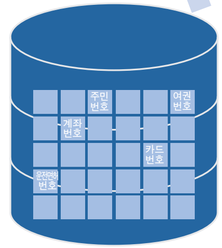
법규준수
개인정보보호법, 정보통신망법 등

국내유일
〈재판시 무죄기능〉 및 〈형사처벌 · 영업정지 방지기능〉

공용장소에 짐 쌓이듯

귀사의 서버에 어떤 개인정보가 얼마나 방치되어 있는지 아십니까?

DB암호화 후에도 DB서버에 개인정보를 평문으로 방치?

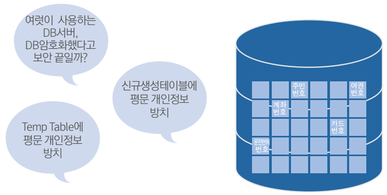


해커가 노리는 웹서버에 개인정보를 방치?

SOMANSA

〈DB암호화〉했다고 마음놓았는데 매순간마다 유효기간 만료정보, 평문정보가 늘어난다면? 〈DB Discover 기능〉

〈DB암호화〉 이후 더 위험해진 DB



유효기간이 만료된 파기대상 개인정보를 DB서버에 방치

천만명 유출사고 ①
2014년
카드사

[대구지법2014판결문 중]
'해커는 DB백업명령어(=export)로 개인정보를 파일형태로 (DB서버에) 저장하고..'

천만명 유출사고 ②
2011년
정보통신사

Benefit

DB서버 내 평문으로 방치된 개인정보현황 확인

[DB검사 대시보드]

- 전체개인정보중 평문개인정보의 퍼센티지확인
- 평문개인정보의 패턴별 리포트 확인

Benefit

DB 에이전트 설치로 인한 업무부담 &장애가능성 ZERO

DB서버에 에이전트 ZERO

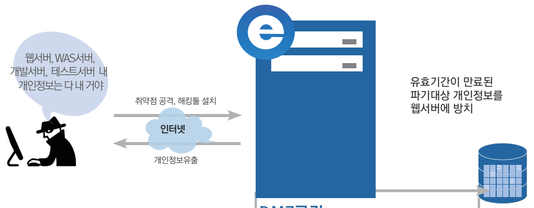
Benefit

상용화된 모든 DBMS 지원

SYBASE, DB2, ORACLE, ALTIBASE, SQL Server, PostgreSQL, Informix SOFTWARE, MySQL

웹서버, WAS서버, 파일서버 해킹만으로 대형유출사고가 발생한다면? 〈파일 Discover 기능〉

DMZ구간의 웹서버, WAS서버



유효기간이 만료된 파기대상 개인정보를 웹서버에 방치

천만명 유출사고 ③
2011년
금융권

개인정보 분석의 정교성에서 1위

개인정보 은닉파일을 다른 4개파일과 섞어서 5단계 압축파일 생성시

Server-i 개별파일 5개로 인식
압축을 순차적으로 풀어 개인정보 은닉파일 위치를 정확히 식별

타 제품 압축파일 1개로 인식
압축을 물지못하고 전체파일1개로 인식

Benefit

다중압축파일 내 개인정보파일을 정확히 식별하므로

보안담당자가 압축파일 내 모든 파일을 일일이 찾을 필요없음

개인정보파일에 암호를 걸어서 압축파일에 은폐해도 적발

Benefit

텍스트파일을 (jpg 등) 이미지파일로 확장자를 변조해도 검출

파일 커버리지에서 1위

Benefit

50개 이상 서버파일포맷 커버

Dump, TAR, gzip

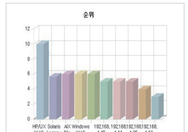
Benefit

대용량파일 커버

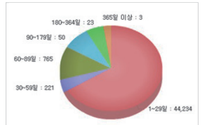
[파일검출결과화면]

대시보드로 모든 서버의 개인정보현황을 한자리에서 본다

[서버 디스커버 대시보드]
서버 내 개인정보 총개수, 부서별 보유량랭킹, 패턴별 추이 등을 직관적으로 볼 수 있음



[서버 내 개인정보 보유량 랭킹]



[서버 내 개인정보의 보유기간별 그래프]

상용화된 모든 서버 OS 지원

Linux, ubuntu, debian, redhat, SUSE, AIX, HP-UX, solaris, Windows Server

국정원인증받은 암호화 알고리즘으로 암호화

〈업무능률 향상기능〉 업그레이드로 검출속도 단축

〈파일대량유출수단〉을 연동하고 있다면 〈솔루션〉이 아니라 〈법적과실〉입니다

Server-i 만이 서버에 〈파일대량유출수단〉을 연동하지 않는 방식으로 개발되었습니다

〈파일대량유출수단〉 ① FTP
법원이 기업측 과실로 판결

〈파일대량유출수단〉 ② 공유디렉토리
법으로 금지

법의 의도를 읽는 소만사만이 가능합니다
〈재판시 무죄〉 및
〈보안처분 · 영업정지 방지〉 기능

DB와 연계연동되어 개인정보를 처리하는 서버도 〈개인정보처리시스템〉
2014.3.24일 시행 [개인정보보호법] 2조

확인하십시오 귀사의 서버에 무엇이 연동되어 있는지

원인① 서버 내 개인정보 〈미점검→미파기〉

천만명 유출사고 ①
2014년
카드사

천만명 유출사고 ②
2011년
정보통신사

천만명 유출사고 ③
2011년
금융권

DB서버에 유효기간 만료된 개인정보 방치

DB서버내 개인정보를 파일로 대량생성

웹서버내 유효기간 만료된 개인정보파일 방치

원인② 〈미점검→미파기〉로 개인정보가 과다저장된 서버에 〈파일대량 유출수단〉 연결

USB By 외주업체직원

FTP By 외주업체직원

해킹툴 By 해커

개인정보처리시스템에 연결되어 대량의 파일을 쉽게 송수신하는 FTP or 공유디렉토리는 법적관점에서 해킹툴과 동일

〈파일대량유출수단〉 ① FTP 법원 판결문에서 서버에 FTP연동을 과실로 명시, 손해배상 판결함

대구지법 판결문 2014.02.13	서울서부지법 판결문 2013.02.15
게이트웨이서버와 DB서버 관리자 PC에 보안상 취약한 FTP 방식의 프로토콜을 설정한 잘못	해커가 대용량 개인정보파일을 DB서버에서 게이트웨이(서버)로 내려받고 FTP방식으로 위 파일을 게이트웨이에서 *** 또는 *** 컴퓨터를 거쳐 결국 외부망으로 전송... 개인정보를 보호하기에 매우 취약한 수준이었고 그로 인하여 해킹사고를 탐지하지 못했다

FTP는 파일전송을 위한 프로토콜로 대량의 파일을 쉽게 송수신하는 역할을 수행하는 만큼 일반적으로 보안상 취약하다고 여겨지고 있는 점

〈파일대량유출수단〉의 법적인 정의에 해당

개인정보 접근권한이 있는 컴퓨터가 FTP 서버로 사용될 때 뿐 아니라 FTP 클라이언트로 사용되는 컴퓨터에서도 파일의 대량 수신뿐만 아니라 송신도 가능하기 때문에 보안상 문제가 발생할 수 있는 것은 마찬가지이다

게이트웨이(서버)의 FTP프로토콜과 DB서버관리자 PC의 FTP클라이언트기능이 ... 반드시 필요하였다 보이지 않는 점 등을 종합하면 피고는 보안상 취약한 FTP가 게이트웨이 및 개인정보접근권한이 있는 컴퓨터에서 기능하도록 함으로써 해커가 FTP방식으로 개인정보가 대량으로 외부에 유출되도록 하는 데에 기여하였다고 봄이 타당하다

〈FTP연동이 반드시 필요한가?〉의 판단기준은 다른 선택의 존재 여부임
따라서 FTP (or FTP와 맥락가치로 대용량파일을 쉽게 송수신하는 공유디렉토리)를 사용하지 않는 다른 선택이 있는데도 택하지 않았다가 유출되면 명백한 과실

〈파일대량유출수단〉 ② 공유디렉토리 공동시 과태료, 형사처벌, 영업정지

개인정보보호법 고시 〈개인정보의 안전성 확보조치기준〉 5조
④ 개인정보가 홈페이지, P2P, 공유설정, 공개된 무선망 등을 통해 공개출력되지 않도록 개인정보처리시스템, 컴퓨터, 모바일기기에 조치

행자부발간 [해설서] 31p
개인정보처리시스템 또는 업무용 컴퓨터인 경우 P2P, 공유설정을 기본적으로 사용하지 않는 것이 원칙...공유물디에 개인정보 파일이 포함되지 않도록 정기 점검하여 조치하도록 한다...

공공기관, 기업이 (개인정보처리시스템인)서버에 공유디렉토리 연결시 받는 처벌

공유디렉토리 연동시 처벌 — 과태료 최대 5천만원

공유디렉토리 연결로 개인정보 유출시 처벌 — 형사처벌 최대 2년징역 2천만원 벌금

금감원 (금융기관검사 및 제재에 관한 규정) 중 〈기술적 물리적 관리적 보안대책〉 1조
④ 개인신용정보가 홈페이지 P2P, 공유설정 등을 통하여 공개되지 않도록 개인신용정보처리시스템 및 개인신용정보취급자의 PC를 설정

금융기관이 (개인정보처리시스템인)서버에 공유디렉토리 연결시 받는 처벌

공유디렉토리 연동시 처벌	미준수 정도	원인	미준수시	공유디렉토리 연결로 개인정보 유출시 처벌	유출건수	직원처벌
		금융기관처벌	임직원처벌			
	중대	영업정지	정직이상		50건 이상	정직 이상
	보통	기관경고	감봉		5건 이상	감봉
	경미	기관주의	견책		1건 이상	견책