2015년 귀사가 지켜야 하는 WAS법규 3대 변화

1 DB + WAS
= 〈개인정보처리시스템〉
2014년 3월24일 시행 [개인정보보호법] 2조

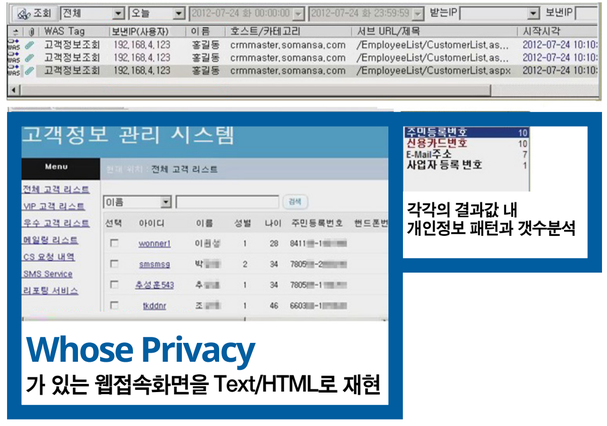
2 〈개인정보처리시스템〉
접속기록항목에
〈누구의 개인정보에
접속했는가?〉 추가
2015년 2월 개정 개인정보보호법고시
[개인정보의 안전성 확보조치 기준] 7조 2항

3 Whose Privacy가
추가된 접속기록을
최소 반기 1회 점검,
유출징후 탐지
2014년 12월 개정 개인정보보호법고시
[개인정보의 안전성 확보조치 기준] 7조 2항

오직 was-i로만 준수할 수 있습니다

Whose Privacy를 어떻게 기록하는가?

〈WAS를 연계연동한 DB접속자〉가
PC에서 보는 웹접속화면



각각의 결과값 내
개인정보 패턴과 갯수분석

was-i가 있어야만 준수할 수 있는 법규정

모든 공공기관, 기업, 단체에 적용 〈개인정보보호법〉

조항	법규정	귀사의 체크리스트	WAS-i 법규준수기능
2조 (정의)	〈개인정보처리의 개념〉 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 + 연계, 연동	〈DB와 연계, 연동된 어플리케이션〉인 WAS에 법적인 기술적 조치인 〈접근권한관리〉, 〈접근통제〉, 〈접속기록보관 및 점검〉이 이뤄지고 있는가?	● DB와 연계연동된 WAS에 〈접근권한관리〉 〈접근통제〉 〈접속기록보관및점검〉 조치
28조 (취급자감독)	개인정보취급자에게 적절한 관리, 감독 수행	〈WAS를 연계 연동한 DB접속자들〉이 누구이며 〈Whose Privacy〉에 접근하는지 관리감독하는가?	● WAS접속기록에 누가(WHO) 누구의 개인정보(Whose Privacy)에 접속하는지 기록

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

조항	법규정	귀사의 체크리스트	WAS-i 법규준수기능
4조 (접근권한관리)	① 업무에 필요한 최소한의 범위로 접근권한차등부여	〈WAS를 연계연동한 DB접속자들〉이 권한자인지 확인하고 있는가?	● WAS를 통한 권한없는 사용자의 접근을 분석하여 추후 접근권한 통제 조치
5조 (접근통제)	① 불법접근 침해방지를 위해 다음기능포함조치 1. 개인정보처리시스템 접속권한을 IP주소등으로 제한, 인가받지 않은 접근제한 2. 개인정보처리시스템접속 IP주소 등을 재분석, 불법적 유출시도탐지	WAS에서 발생하는 IP세탁에 대응하여 〈WAS를 연계연동한 DB접속자들〉 IP를 확보하고 있는가?	● WAS에서 발생하는 IP세탁에 대응하여 〈WAS를 연계연동한 DB접속자들〉IP 기록 ● WAS에 대한 개인정보 과다조회 분석, 개인정보 평문노출 분석 개인정보 접근하는 웹페이지 현황 분석
8조 (접속기록 관리 및 보관)	① 〈개인정보처리시스템〉 접속기록 최소 6개월 보관, 관리	〈WAS를 연계연동한 DB접속〉을 개인정보보호법고시 해설서를 준수하여 접속기록하고 최소 6개월 보관하는가?	〈WAS를 연계연동한 DB접속〉 접속기록을 해설서 항목대로 기록 ● WHO 기록 - 실제접속자 식별하여 기록 ● Whose Privacy 기록 - 개인정보를 조회하는 웹접속화면 기록
	② 〈개인정보처리시스템〉 접속기록 반기별로 1회 이상 점검	접속기록을 최소 반기별 1회 점검하는가?	접속기록점검시 이상징후분석을 위하여 검색기능, 웹리포트 제공
	② 〈개인정보처리시스템〉 접근로그는 위변조방지처리 보관	접속기록을 위변조방지처리 보관하는가?	(추가비용없이) 위변조방지스토리지 자체탑재 (6개월저장용량제공)

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

조항	법규정	귀사의 체크리스트	WAS-i 법규준수기능
1조 (접근통제)	④ 〈개인신용정보처리시스템〉에 침입차단/침입탐지시스템 설치	WAS에서 발생하는 IP세탁에 대응하여 〈WAS를 연계연동한 DB접속자들〉 IP를 확보하고 있는가?	● 〈WAS를 연계연동한 DB접속자들〉IP 확보 ● WAS에 대한 개인정보 과다조회 분석 ● 개인정보 평문노출 분석 ● 개인정보 접근하는 웹페이지 현황 분석
2조 (접속기록 위변조방지)	① 〈개인신용정보〉 접속기록 저장, 월 1회 이상 확인/감독	〈WAS를 연계연동한 DB접속〉을 개인정보보호법고시 해설서를 준수하여 기록하는가?	〈WAS를 연계연동한 DB접속〉 접속기록을 해설서 항목대로 기록 ● WHO 기록 - 실제접속자 식별하여 기록 ● Whose Privacy 기록 - 개인정보를 조회하는 웹접속화면 기록
	② 〈개인신용정보처리시스템〉 접속기록위변조방지	일1회이상 점검하는가? 접속기록을 위변조방지처리보관하는가?	접속기록점검시 이상징후분석을 위하여 검색기능, 웹리포트 제공 (추가비용없이) 위변조방지스토리지 자체탑재 (6개월저장용량제공)

1위 솔루션을 선택하십시오

기업 LG전자 · NCSOFT · LG이노텍 · 롯데푸드 · AMOREPACIFIC · woongjin

공공 통계청 STATISTICS KOREA · 한국수력원자력㈜ · SH 에스에이치공사 · 대한주택보증 · GUNPO 군포시

- 미래창조과학부지정 지식정보보안 컨설팅전문업체
- 신용평가등급 A 로 재무안정성 상위1%
- 행정자치부지정 개인정보 영향평가기관
- 창립 이래 무차입경영, 12년 연속 흑자기업
- 조달청 조달등록기업

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

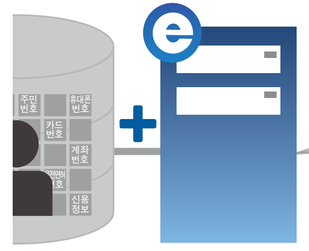
전면개정 및 2천부 인쇄일: 2015.06.05

시장1위 〈WAS를 연계연동한 DB접속〉 접속기록 및 유출징후분석

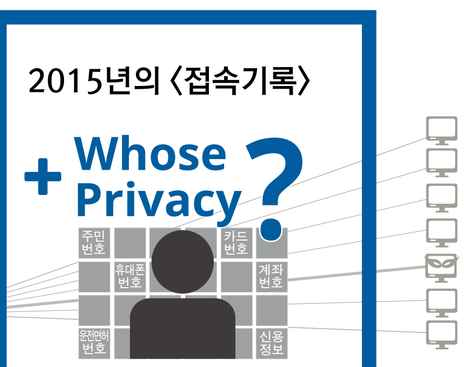
was-i

법규준수 개인정보보호법 정보통신망법

2015년의
〈개인정보처리시스템〉



2015년의 〈접속기록〉



**WAS를 통해
〈누구의 개인정보〉를
유출하는가?**를 기록해야함

SOMANSA

〈WAS〉의 보안취약점을 악용한 대형유출사고 발생

〈취약점 1〉

Whose Privacy 식별불가

〈취약점 2〉

WHO 식별불가 〈WAS를 연계연동한 DB접속자〉 IP가 WAS IP로 세탁 누구인지 알 수 없음

천만명유출사고 ① 2012년 정보통신사

천만명유출사고 ② 2008년 정유사

대리점 직원 (사고①) 자회사 직원 (사고②)

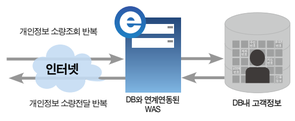
원인

WAS를 통한 소량조회 반복, 〈과다조회〉후 유출

과다조회란?

소량조회를 과다 반복, 대량의 개인정보를 조회하는 것

= 주민번호 천만건



2014년 법원 판결 〈WAS 접속기록〉상 과실을 이유로 기업측에 손해배상 판결

서울중앙지법 2014.12 선고 판결문

〈개인정보처리시스템〉을 개인정보 DB관리시스템으로 한정하여 해석하기는 어렵고 개인정보 DB관리시스템에 접근하기 위한 〈중계서버〉와 〈어플리케이션〉도 포함하는 것으로 보아야 하기 때문이다

DB와 연계연동된 WAS를 〈개인정보처리시스템〉으로 판결

서울중앙지법 2014.08 선고 판결문

DB접근을 위한 중계서버, 어플리케이션 등도 〈개인정보처리시스템〉에 포함된다고 보고 있는바..

월 1회 이상 정기적으로 개인정보취급자가 〈개인정보처리시스템〉을 이용하여 업무수행내역을 감독하고 확인하였다면 〈개인정보처리시스템〉의 사용패턴에서 평상시와 다른 특이점을 발견하여 정보유출의 지속 및 확대를 방지할 수 있었음에도 주의의무를 다하지 못하고 ...

〈해킹프로그램〉은 〈개인정보처리시스템〉에 정상사용자처럼 접속, 조회하여 개인정보를 유출... 〈접속기록 확인감독규정〉은.... 오류 및 부정행위를 막기 위한 것으로... 비정상적인 개인정보처리패턴과 사용내역을 발견하기 위한 조치도 포함된다

〈WAS 접속기록〉 불충분, 미점검을 유출원인으로 판결

〈WAS접속기록〉에 Whose Privacy 기록의무화

2015년 개인정보보호법고시 〈개인정보의 안전성 확보조치 기준〉 해설서 개정

13. "접속기록"이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다. 해설서 7p

TIP

· 개인정보취급자가 특정 정보주체의 개인정보를 처리 한 경우, '수행업무'에는 해당 정보주체를 식별할 수 있는 정보도 포함된다. 해설서 23p

문14. 접속기록 중, 수행업무에 남겨야 하는 내용은 무엇인지?

▶ 접속기록에는 식별자, 접속일시, 접속자를 알 수 있는 정보와 수행업무가 포함됩니다.

수행업무는 정보주체의 개인정보에 대한 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄) 등의 내역을 말합니다.

특히, 개인정보취급자가 특정 정보주체의 개인정보를 처리 한 경우, '수행업무'에는 해당 정보주체에 대한 식별정보도 포함됩니다. 해설서 74p

개정 해설서 상 접속기록 항목

필수 기록항목	구분	설명
접속자 ID	WHO (누가)	개인정보취급자 식별정보
접속자 IP주소		접속지 정보
날짜 및 시간	WHEN (언제)	접속일시
수행업무	Whose Privacy (누구의 개인정보에 접속하여)	접속대상인 해당 정보주체를 식별할 수 있는 정보
	HOW (어떻게 했는가?)	열람/ 수정/ 삭제/ 인쇄/ 입력 등

was-i 법규준수 강점

〈WAS를 연계연동한 DB접속자〉가 〈PC에서 보는 웹접속화면〉

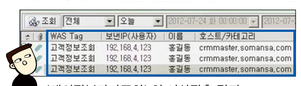
〈법규준수 강점 1〉 법규준수 접속기록

2015년 2월 개정 개인정보보호법 고시해설서 준수

Whose Privacy 기록 웹접속화면 상의 개인정보 재현

개인정보가 있을 경우에만 Text/HTML로 저장하여 용량부담 최소화

WHO 기록 〈WAS를 연계연동한 DB접속자〉 IP/ID 식별



〈개인정보과다조회〉의 이상징후 탐지 동일인물이 동일한 소량조회를 과다반복

〈법규준수 강점 2〉 (법규준수 접속기록을 기반으로 한) 이상징후분석

A기업 실제 활용에

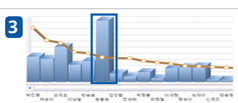
누군가 주민번호 소량조회를 반복, 〈개인정보 과다조회〉후 유출하는지 주기적으로 분석

1 

주민번호 10개이상 접속기록 검색

2 

A의 주민번호 10개이상 접속기록이 1달간 과다함을 탐지

3 

사내 주민번호 최다접속자 랭킹확인 A가 타직원 대비 주민번호를 과다조회함을 탐지

〈WAS접속기록〉에 Whose Privacy 를 남길 수 없다면?

법이 규정한 〈접속기록〉 생성불가

개인정보보호법 보호대상인 〈정보주체의 프라이버시〉 해당정보가 없으므로

연쇄적 법규위반 1 2 3 발생

1 법이 규정한 〈접속기록점검〉불가능, 유출이상징후 탐지에 보안상 HOLE 발생

위반

개인정보보호법고시 〈개인정보의 안전성 확보조치 기준〉7조 2항

"개인정보처리시스템 접속기록을 반기별로 1회 이상 점검해야 한다"

2 유출사고시 〈개인정보보호법고시 위반으로 인한 유출〉이 명백하므로 2015년 강화된 법규에 따라 강력처벌

형사처벌 2014.11.29 시행 [정보통신망법 32조의2]

1건 유출시에도 징계 2014.6.30 시행 [금융기관 검사 및 제재에 관한 규정시행세칙]

CEO 해임가능 2014.7.31 발표 [개인정보보호 정상화 종합대책]

1인당 3백만원 손해배상 2014.11.29 시행 [정보통신망법 32조의2]

3 유출사고 이후 법이 규정한 〈유출통지〉가 불가능

접속기록에 Whose Privacy가 없다면 유출시 통지대상자를 어떻게 찾아낼 것인가?

과태료 | 소송시 불이익

개인정보보호법은 사고 후 5일 정보통신망법은 24시간내 유출통지의무화

에이전트 ZERO 방식의 강점

〈웹서버에이전트방식 대비 강점 1〉 결과적으로 더큰 비용을 초래하는 추가부담 없음

추가부담	WAS-i	웹서버 에이전트 방식
웹서버에 에이전트 설치부담	추가부담 ZERO	추가부담 발생
〈개인정보접근 웹프로그램or 페이지〉 변경시 추가개발부담		웹프로그램 변경시마다 〈웹프로그래밍개발 가이드라인〉을 준수하여 추가개발해야 하는 추가부담 발생
웹서버에서의 정보입출력(I/O)으로 인한 추가부하		웹로그 생성시 웹서버에 추가부담 발생
여러 웹서버에 흩어진 로그를 중앙집중화하는 부담		여러 웹서버의 로그를 주기적으로 중앙집중화하는 추가부담 발생
웹서버 추가시 추가작업부담		웹서버가 추가될 때마다 신규설치의 추가부담 발생

〈웹서버에이전트방식 대비 강점 2〉 개인정보유출로 이어지는 보안상 허점 없음

보안상 허점	WAS-i	웹서버 에이전트 방식
설치할 수 없는 웹서버와 프로그램언어가 있는가?	보안상 허점 ZERO	특정 웹서버와 언어에서는 설치할 수 없으므로 보안상 허점 발생
개인정보 과다조회 발생시 실시간분석/경보가 불가능한가?		로그취합으로 시간을 지체한 후에 분석 및 경보가 이뤄지므로 보안상 허점 발생
웹서버간 시간이 동기화되지 않으면 접속경로가 왜곡되는가?		웹서버간 시간동기화가 잘못되면 접속경로가 왜곡되므로 보안상 허점 발생

〈웹서버에이전트방식 대비 강점 3〉 대용량 WAS트래픽에 특화된 어플라이언스

WAS 어플리케이션로그는 데이터양이 많기 때문에 대용량처리능력이 필수

국내 유일 10G 트래픽처리

국내 유일 HTTPS암호화통신분석

로그저장 위변조방지스토리지탑재