개인정보보호 준수를 위한

접속기록관리 솔루션 도입시 고려사항 및 고도화 방안

개인정보접속기록 관리 No.1 /
조달판매실적 9년 연속 1위 / (조달청 누계 점유율 62%)

CC인증
ISIS-1079-2021

Good Software인증
14-0245

ISO9001:2015
2019.09

WEDS | ㈜위즈코리아

CONTENTS

WEEDS

01

WEEDS BlackBox Suite

개인정보 접속기록 개요 및 필요성

접속기록 관리 시스템 도입 의무화

WEEDS

1. 개인정보 접속기록의 환경변화

□ 2019년 개인정보의 안전성 확보조치 기준 변경

○ 접속기록 생성시 정보주체 정보를 포함하여 기록

○ 개인정보 다운로드시 사유 확인

○ 접속기록 보관 기간 최대 2년 확대

☞ 접속기록 단순 기록에서 명확(필수기록 5가지 항목을 포함)하게 기록

□ 2022년 공공부문 개인정보 유출 방지대책 (7.14)정부종합 대책

○ 개인정보 접속기록 관리 도입 의무

○ 집중관리대상(공공) 시스템 선정과 3단계 안전조치의무

☞ 권한변경 이력관리, 접속기록 관리, 소명 통지

□ 2023년 개인정보보호법 개정

○ 개인정보보호법, 시행령 강화

○ 관리적 기술적 보호조치 기준과 안전성 확보조치 기준 통폐합

☞ 공공시스템 운영기관 특례 신설

2. 개인정보의 안전성 확보조치 기준 비교 (1/4)

변경 전	변경 후 (※주요 변경사항만 표시)
제2조(정의)	제2조(정의)
이 기준에서 사용하는 용어의 뜻은 다음과 같다.	이 기준에서 사용하는 용어의 뜻은 다음과 같다.
10. "개인정보처리시스템"이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.	1. "개인정보처리시스템"이란 데이터베이스 시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
	2. “이용자”란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제1항 제4호에 따른 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
19. "접속기록"이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.	3. "접속기록"이란 개인정보처리시스템에 접속하는 자가 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.

2. 개인정보의 안전성 확보조치 기준 비교 (2/4)

변경 전	변경 후
제4조(내부 관리 계획의 수립·시행 및 점검)	제4조(내부 관리 계획의 수립·시행 및 점검)
① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다. 1. 개인정보 보호책임자의 지정에 관한 사항 2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항 3. 개인정보취급자에 대한 교육에 관한 사항 4. 접근 권한의 관리에 관한 사항 5. 접근 통제에 관한 사항 6. 개인정보의 암호화 조치에 관한 사항 7. 접속기록 보관 및 점검에 관한 사항 8. 악성프로그램 등 방지에 관한 사항 9. 물리적 안전조치에 관한 사항 10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항 11. 개인정보 유출사고 대응 계획 수립・시행에 관한 사항 12. 위험도 분석 및 대응방안 마련에 관한 사항 13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항 14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항 15. 그 밖에 개인정보 보호를 위하여 필요한 사항 ② [별표]의 유형1에 해당하는 개인정보처리자는 제1항에 따른 내부 관리계획을 수립하지 아니할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항 제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다. ③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다. ④ 개인정보보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상으로 점검・관리 하여야 한다.	① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다. 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다. 1. 개인정보 보호 조직의 구성 및 운영에 관한 사항 2. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항 3. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항 4. 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항 5. 접근 권한의 관리에 관한 사항 6. 접근 통제에 관한 사항 7. 개인정보의 암호화 조치에 관한 사항 8. 접속기록 보관 및 점검에 관한 사항 9. 악성프로그램 등 방지에 관한 사항 10. 개인정보의 유출, 도난 방지 등을 위한 취약점 점검에 관한 사항 11. 물리적 안전조치에 관한 사항 12. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항 13. 위험 분석 및 관리에 관한 사항 14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항 15. 개인정보 내부 관리계획의 수립, 변경 및 승인에 관한 사항 16. 그 밖에 개인정보 보호를 위하여 필요한 사항 ② 개인정보처리자는 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수, 업무성격 등에 따라 차등화하여 필요한 교육을 정기적으로 실시하여야 한다. 1. 교육목적 및 대상 2. 교육 내용 3. 교육 일정 및 방법 ③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다. ④ 개인정보보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상 점검·관리하여야 한다.

2. 개인정보의 안전성 확보조치 기준 비교 (3/4)

변경 전	변경 후
제8조(접속 기록의 보관 및 점검)	제8조(접속 기록의 보관 및 점검)
① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관・관리하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관・관리 하여야 한다. ② 개인정보처리자는 개인정보의 오・남용, 분실・도난・유출・위조・변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부관리 계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다. ③ 개인정보처리자는 개인정보취급자의 접속기록이 위・변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.	① 개인정보처리자는 개인정보취급자의 개인정보처리시스템에 대한 접속기록을 1년 이상 보관·관리하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관·관리하여야 한다. 1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우 2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우 3. 개인정보처리자로서 「전기통신사업법」 제 6조 제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우 ② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보의 다운로드가 확인된 경우에는 내부 관리계획 등으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다. ③ 개인정보처리자는 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하기 위한 조치를 하여야 한다.

2. 개인정보의 안전성 확보조치 기준 비교 (4/4)

WEEDS

제 3장 공공시스템 운영기관 등의 개인정보 안전성 확보조치 (변경 후)

제 14조 ~ 17조

제14조(공공시스템운영기관의 안전조치 기준 적용)
① 다음 각 호의 어느 하나에 해당하는 개인정보처리시스템 중에서 개인정보보호위원회(이하 “보호위원회”라 한다)가 지정하는 개인정보처리시스템(이하 “공공시스템”이라 한다)을 운영하는 공공기관(이하 “공공시스템운영기관”이라 한다)은 제2장의 개인정보의 안전성 확보 조치 외에 이 장의 조치를 하여야 한다.
1. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 단일 시스템을 구축하여 다른 기관이 접속하여 이용할 수 있도록 한 단일접속 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우
가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템
나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템
다. 정보주체의 사생활을 현저히 침해할 우려가 있는 민감한 개인정보를 처리하는 시스템
2. 2개 이상 기관의 공통 또는 유사한 업무를 지원하기 위하여 표준이 되는 시스템을 개발하여 다른 기관이 운영할 수 있도록 배포한 표준배포 시스템으로서 대국민 서비스를 위한 행정업무 또는 민원업무 처리용으로 사용하는 경우
3. 기관의 고유한 업무 수행을 지원하기 위하여 기관별로 운영하는 개별 시스템으로서 다음 각 목의 어느 하나에 해당하는 경우
가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템
나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템
다. 「주민등록법」에 따른 주민등록정보시스템과 연계하여 운영되는 시스템
라. 총 사업비가 100억원 이상인 시스템

② 제1항에도 불구하고 보호위원회는 다음 각 호의 어느 하나에 해당하는 개인정보처리시스템에 대하여는 공공시스템으로 지정하지 않을 수 있다.
1. 체계적인 개인정보 검색이 어려운 경우
2. 내부적 업무처리만을 위하여 사용되는 경우
3. 그 밖에 개인정보가 유출될 가능성이 상대적으로 낮은 경우로서 보호위원회가 인정하는 경우

제15조(공공시스템운영기관의 내부 관리계획의 수립・시행)
공공시스템운영기관은 공공시스템 별로 다음 각 호의 사항을 포함하여 내부 관리계획을 수립하여야 한다.
1. 영 제30조의2제4항에 따른 관리책임자(이하 “관리책임자”라 한다)의 지정에 관한 사항
2. 관리책임자의 역할 및 책임에 관한 사항
3. 제4조 제1항 제3호에 관한 사항 중 개인정보취급자의 역할 및 책임에 관한 사항
4. 제4조 제1항 제4호부터 제6호까지 및 제8호에 관한 사항
5. 제16조 및 제17조에 관한 사항

제16조(공공시스템운영기관의 접근 권한의 관리)
① 공공시스템 운영기관은 공공시스템에 대한 접근 권한을 부여, 변경 또는 말소하려는 때에는 인사정보와 연계하여야 한다.
② 공공시스템운영기관은 인사정보에 등록되지 않은 자에게 제5조 제4항에 따른 계정을 발급해서는 안된다. 다만, 긴급상황 등 불가피한 사유가 있는 경우에는 그러하지 아니하며, 그 사유를 제5조 제3항에 따른 내역에 포함하여야 한다.
③ 공공시스템운영기관은 제5조 제4항에 따른 계정을 발급할 때에는 개인정보보호 교육을 실시하고, 보안 서약을 받아야 한다.
④ 공공시스템운영기관은 정당한 권한을 가진 개인정보취급자에게만 접근권한이 부여·관리되고 있는지 확인하기 위하여 제5조 제3항에 따른 접근 권한 부여, 변경 또는 말소 내역 등을 반기 별 1회 이상 점검하여야 한다.
⑤ 공공시스템에 접속하여 개인정보를 처리하는 기관(이하 “공공시스템 이용기관”이라 한다)은 소관 개인정보취급자의 계정 발급 등 접근 권한의 부여·관리를 직접하는 경우 제2항부터 제4항까지의 조치를 하여야 한다.

제17조(공공시스템운영기관의 접속기록의 보관 및 점검)
① 공공시스템 접속기록 등을 자동화된 방식으로 분석하여 불법적인 개인정보 유출 및 오용·남용 시도를 탐지하고 그 사유를 소명하도록 하는 등 필요한 조치를 하여
야 한다.
② 공공시스템운영기관은 공공시스템 이용기관이 소관 개인정보취급자의 접속기록을 직접 점검할 수 있는 기능을 제공하여야 한다.

3. 변경 내용 요약 (1/2)

WEEDS

□ “접속기록” 이란 (제2조 3항)

○ “접속기록"이란 개인정보처리시스템에 접속하는 자가 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.

○ 개인정보 취급자 => 개인정보처리시스템에 접속하는 자

□ 접속기록 2년 이상 보관기준 강화 (제8조 1항)

○ 5만명 이상 정보주체에 관한 개인정보를 처리 하는 경우

○ 고유식별정보 또는 민감정보를 처리 하는 경우

○ 개인정보처리자로서 전기통신사업법 제6조 1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우

3. 변경 내용 요약 (1/2)

□ 공공기관의 개인정보보호 강화 (제3장:제14조~제17조)

○ 공공시스템운영기관 등에 대한 특례 신설

○ 집중 관리대상이 되는 공공시스템의 지정 기준 규정

*(예시) 100만명 이상 개인정보 처리 또는 개인정보취급자 수 200명 이상인 단일접속 시스템,
대국민 행정 민원업무 처리에 사용되는 표준배포시스템 등

○ 공공시스템별로 내부 관리 계획에 관리책임자 지정 및 안전조치 등에 관한 사항을 수립.시행

○ 접근권한 부여 변경 말소 시 인사정보와 연동, 원칙적으로 인사정보에 등록되지 않은 자에게 계정 발급 금지

○ 접속기록을 자동화된 방식으로 분석하여 불법적인 개인정보 유출 및 오용/남용 시도를 탐지 (예, 접속기록관리시스템 등)

- 공공시스템 이용기관이 소관 개인정보취급자의 접속기록을 직접 점검할 수 있는 기능을 제공

4. 접속기록 필수항목

WEEDS

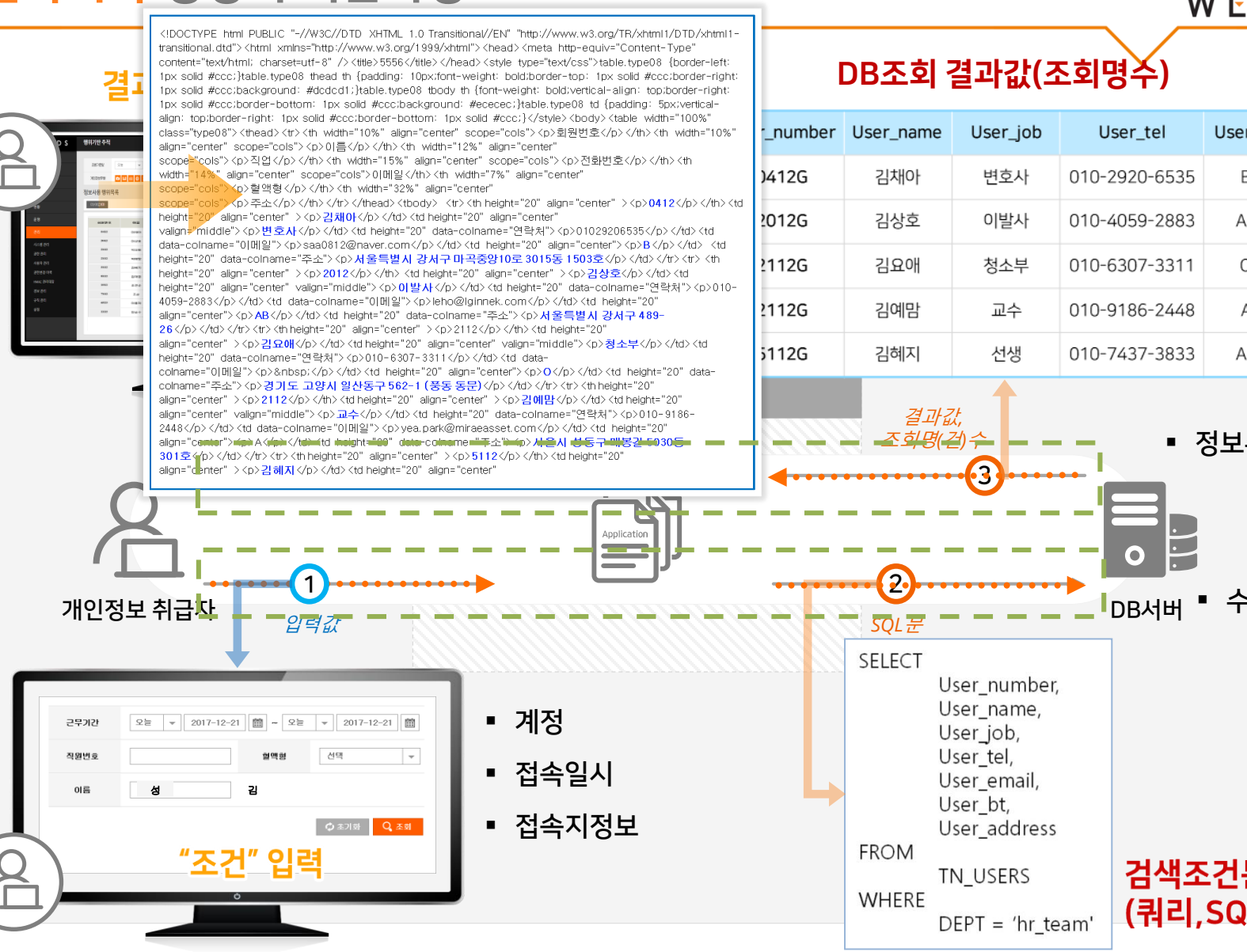
핵심 사항

☐ 법규 준수를 위한 **필수 포함항목(5종) 기록**

식별자	처리한 정보주체 정보	접속일시	접속지 정보	수행업무	조회명(건)수
gd.hong (사용자 ID)	홍길동 (ID, 학번, 사번, 검색조건문 등)	2024년 5월 1일 15시 12분 11초	172.68.11.2 (접속지 IP주소)	조회, 갱신, 다운로드 등	230명
누가	누구의	언제	어디서	업무내역	조회된 사람의 명수

5. 접속기록 생성의 기본사항

WEEDS



6. 잘못된 접속기록 생성은?

WEEDS

✓ 관련 법규 미 준수에 의한 과태료 처분 사례 및 시스템 재구축 사례 증가

WEEDS

02

WEEDS BlackBox Suite

개인정보 접속기록 생성 기술

접속기록 생성 방식별 특징

WEEDS

1. 개인정보 접속기록 생성 방식

✓ SW방식 (로깅모듈 플러그인)

- BCI 방식
- JAVA필터 방식
- JDBC 드라이버 교체

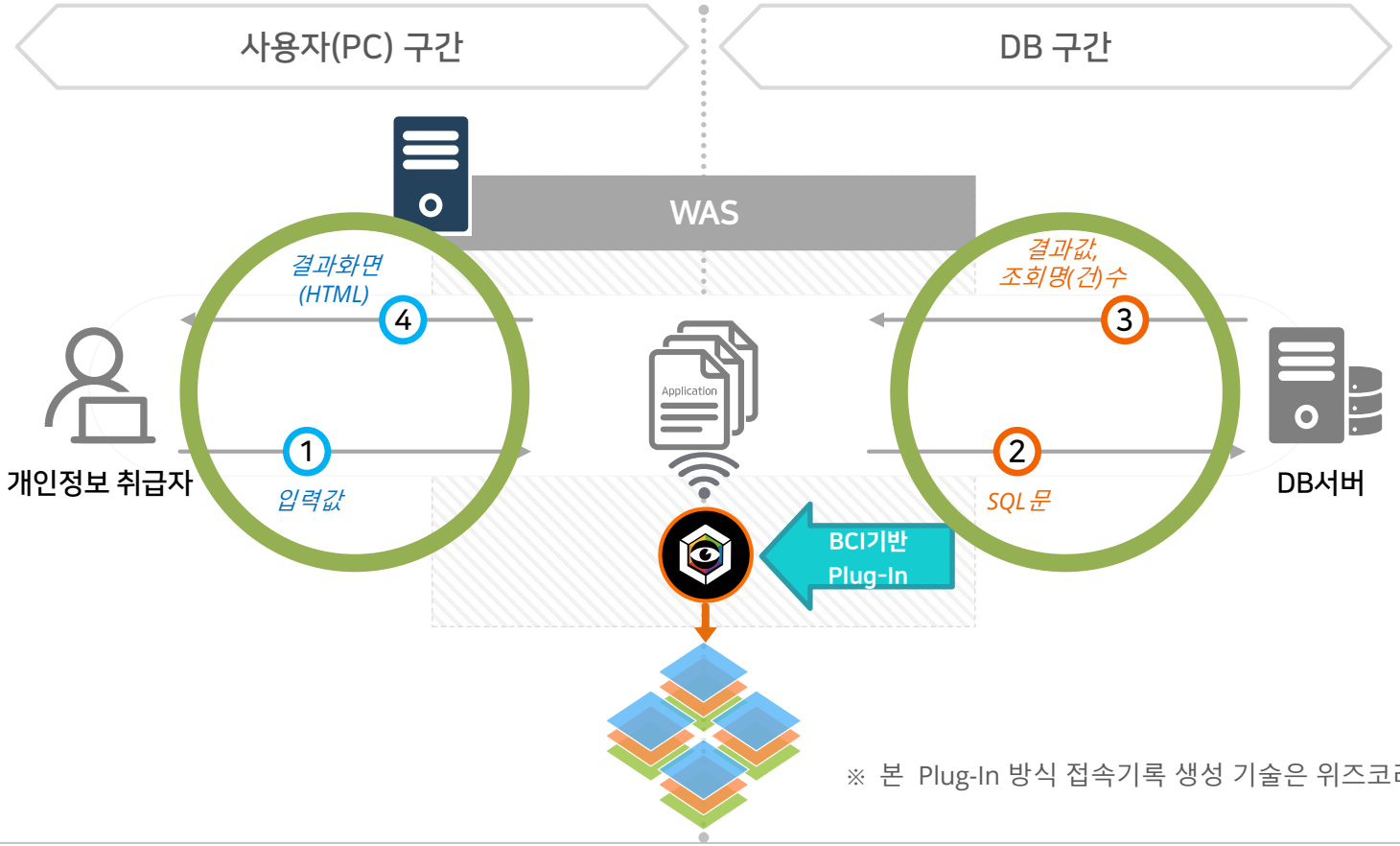
✓ NW방식 (네트워크 패킷 처리)

"㈜위즈코리아는 모든 방식의 로깅 솔루션 및 원천 기술 특허를 모두 보유한 국내 유일의 기업입니다."

2. BCI 방식 (SW 방식)

WEEDS

- ✓ 일체의 누락 없는 접속기록 생성 및 데이터 무결성 100% 보장
- ✓ 사번,ID,이름 등 어떤 형태의 정보주체정보, 취급자 식별정보, SQL문 완벽 기록
- ✓ 다운로드 자동식별



※ 본 Plug-In 방식 접속기록 생성 기술은 위즈코리아만의 특허기술입니다.

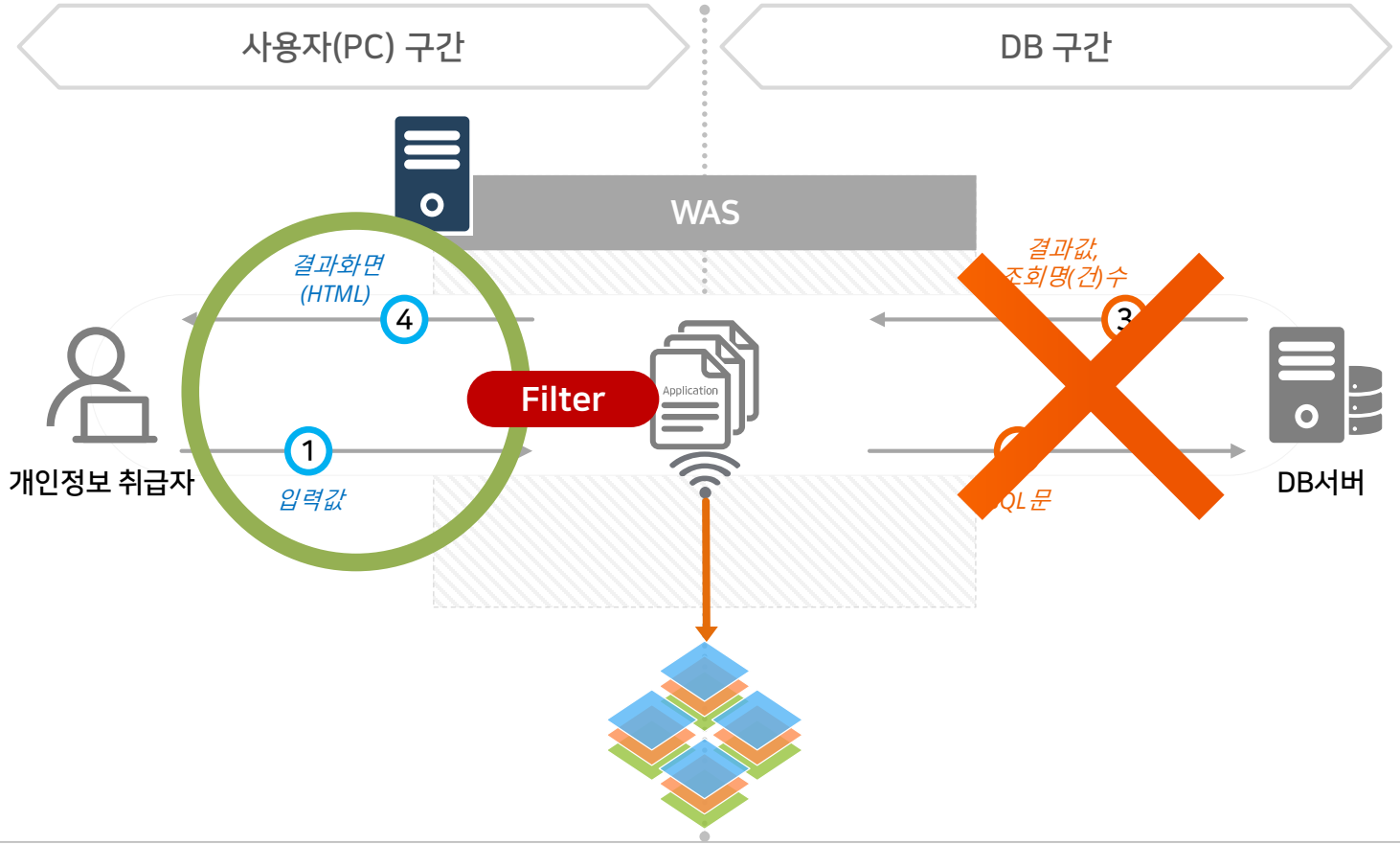
3. JAVA 필터 방식 (SW 방식)

WEEDS

✓ SQL문, SQL결과 기록 불가 ➔ 해설서에서 요구하는 SQL문 기록 불가

✓ 결과화면(HTML) 으로 정보주체정보 분석 ➔ 패턴필터링 분석 시 오류 발생

✓ 다운로드 식별 불가 (자바필터 기술력 부족 시 대상 시스템에 장애 유발)

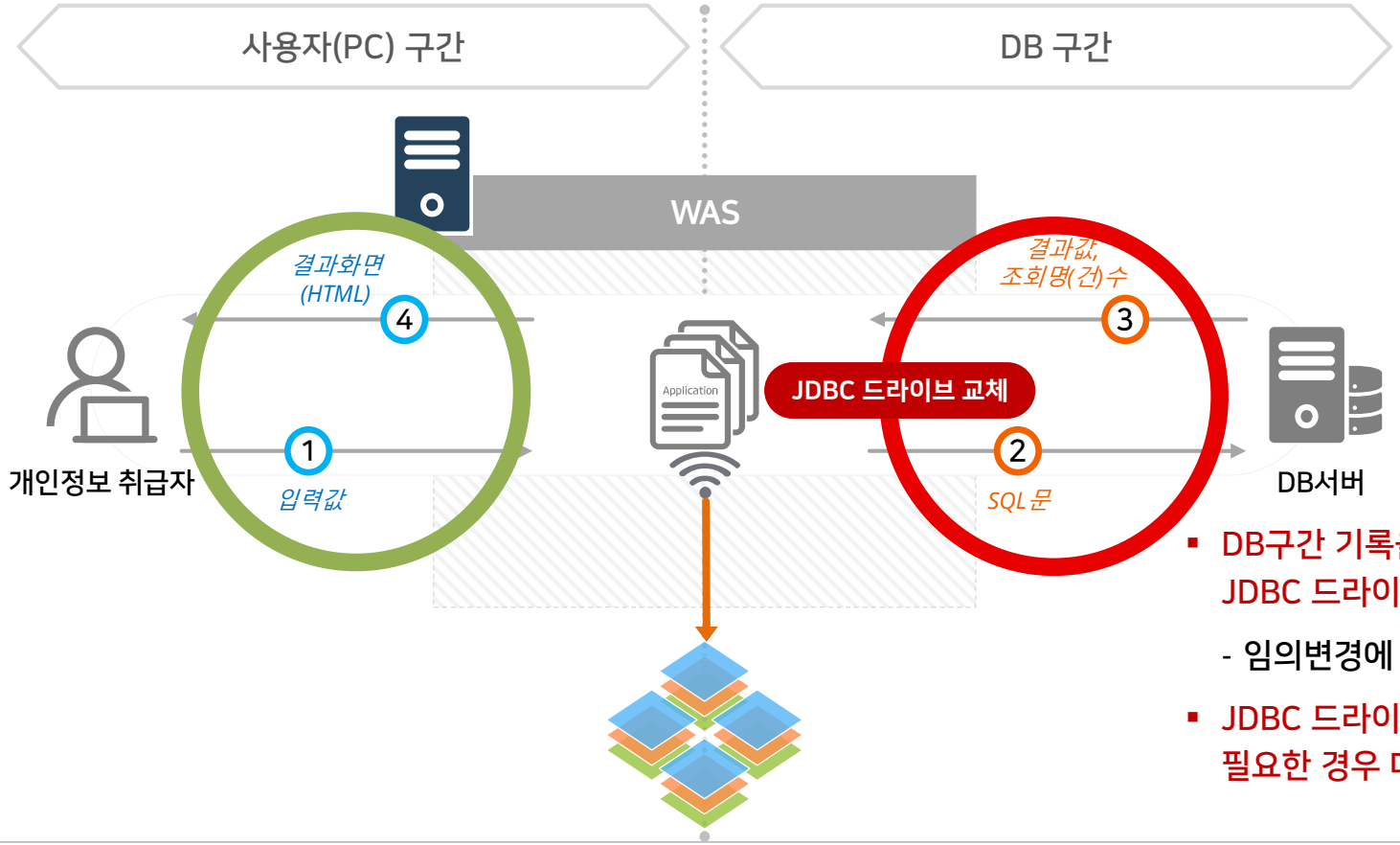


4. JDBC 드라이브 교체 방식 (SW 방식)

WEEDS

✓ DB구간 로깅을 위해 시스템내 JDBC드라이브 교체

✓ 대상 정보시스템에 과도한 영향 유발 (장애 요소 폭증)



- DB구간 기록을 위해 표준SW인 JDBC 드라이브 교체
  - 임의변경에 따른 보안문제 발생
- JDBC 드라이브 버전업, 패치가 필요한 경우 매번 재설치 발생

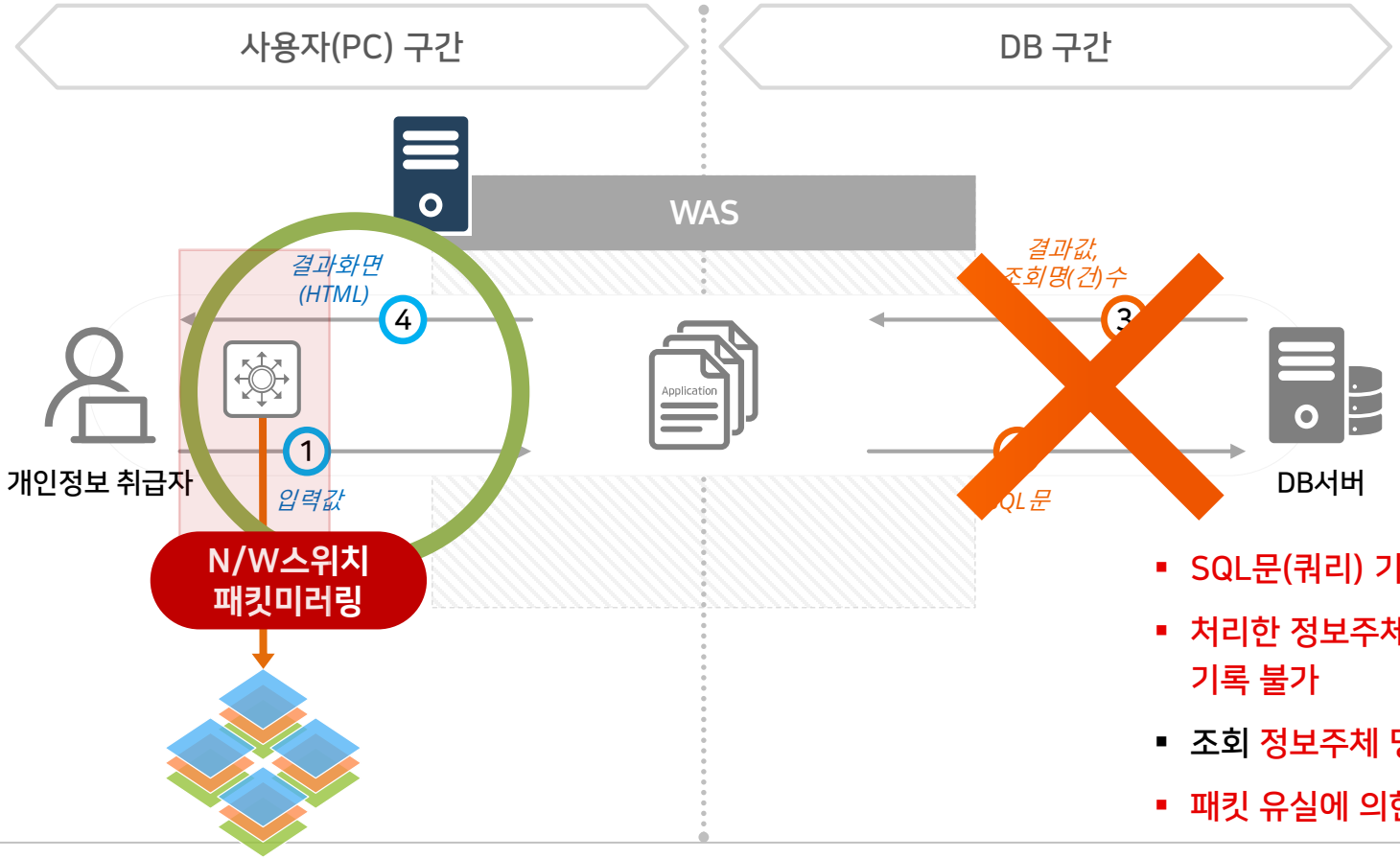
5. NW방식 (NW 컨텐츠 필터링, NW 미러링)

WEEDS

✓ 패킷 유실에 의한 접속기록 누락 발생

✓ 식별자(계정/ID) 기록 불가 상황 발생 ➔ 기준 고시 충족 불가

✓ 검색조건문(쿼리), 처리한 정보주체 정보 기록 불가



- SQL문(쿼리) 기록 불가
- 처리한 정보주체 정보(이름, ID 등) 기록 불가
- 조회 정보주체 명수 기록 불가
- 패킷 유실에 의한 누락 발생

6. 접속기록 생성 가능 항목 비교

WEEDS

구분			SW(BCI) 방식	NW방식 / 필터 방식(SW)	영향 및 비고
사용자 입력부분	1	식별자 (계정/ID)	O	X / O	NW방식 정확한 계정 기록 불가
		접속일시	O	O	
		접속지 정보 (IP정보)	O	O	
		사용자 입력값	O	O	
		접속 화면(URL 등)	O	O	
검색조건문	2	쿼리, SQL문	O	X	SQL문 미기록 시 기준 고시 충족 불가
조회결과 부분	3	정보주체 정보 (사번,ID,이름 등)	O	X	
		정보주체 처리명(건) 수	O	X	미생성시 ISMS 등 충족 불가
		조회결과값	O	X	
	4	결과화면	O	O	

WEEDS

03

WEEDS BlackBox Suite

솔루션 도입을 위한 고려사항

접속기록 생성방식별 법규 준수 여부

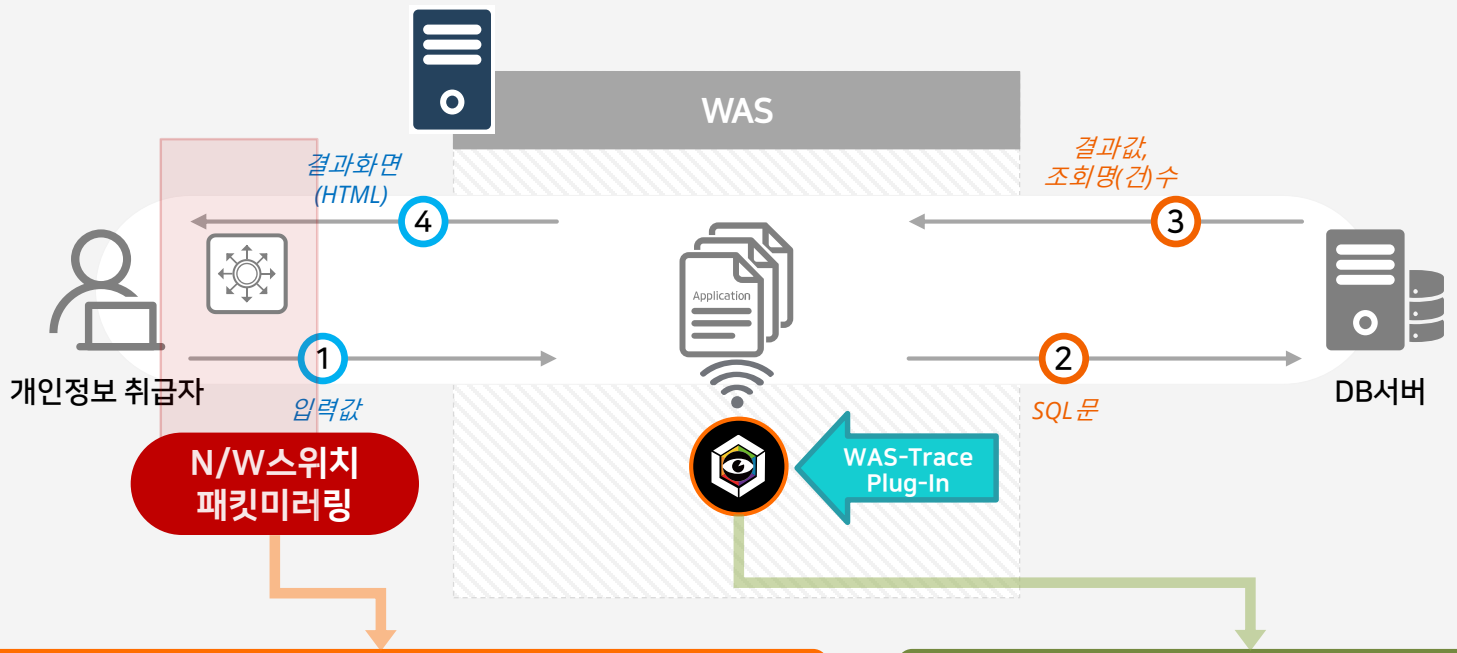
WEEDS

NW방식은 "취급자 계정(ID)"의 정확한 기록이 불가함 !

구분	식별자	처리한 정보주체 정보	접속일시	접속지 정보	수행업무	정보주체 처리명수
	kdhong (사용자 ID)	성춘향 (이름,ID / 검색조건문)	2024년 5월 1일 15시12분11초	172.68.11.2 (접속지 IP주소)	조회, 갱신 등	230명
BCI방식 (자사 SW방식)	O	O	O	O	O	O
JAVA필터 (SW방식)	O	X	O	O	△ (수동 정의)	X
NW방식	X	X	O	O	△ (수동 정의)	X

잘못된 접속기록 생성 방식의 솔루션을 선택하는 경우 기본적인 법규 준수 불가

WEB환경에서 NW방식 접속기록 생성시 정확한 정보취급자 식별 불가!



NW구간에는 "취급자 식별정보" 존재하지 않음

* 세션ID, IP주소만 존재
* 세션ID로는 취급자 식별 불가

WAS 내에는 취급자 식별정보 존재

* 세션 DATA 및 계정ID 모두 존재
* 취급자 정보 100% 정확히 식별

2. 정보주체정보

2.1 취급한 정보주체정보 기록 가능여부

WEEDS

결과화면만 기록하는 JAVA필터 및 NW방식은 이름, ID 등 "정보주체 정보" 및 검색조건문(쿼리) 기록 불가 !

구분	식별자	처리한 정보주체 정보	접속일시	접속지 정보	수행업무	정보주체 처리명수
	kdhong (사용자 ID)	성춘향 (이름,ID / 검색조건문)	2024년 5월 1일 15시12분11초	172.68.11.2 (접속지 IP주소)	조회, 갱신 등	230명
BCI방식 (자사 SW방식)	O	O	O	O	O	O
JAVA필터 (SW방식)	O	X	O	O	△ (수동 정의)	X
NW방식	X	X	O	O	△ (수동 정의)	X

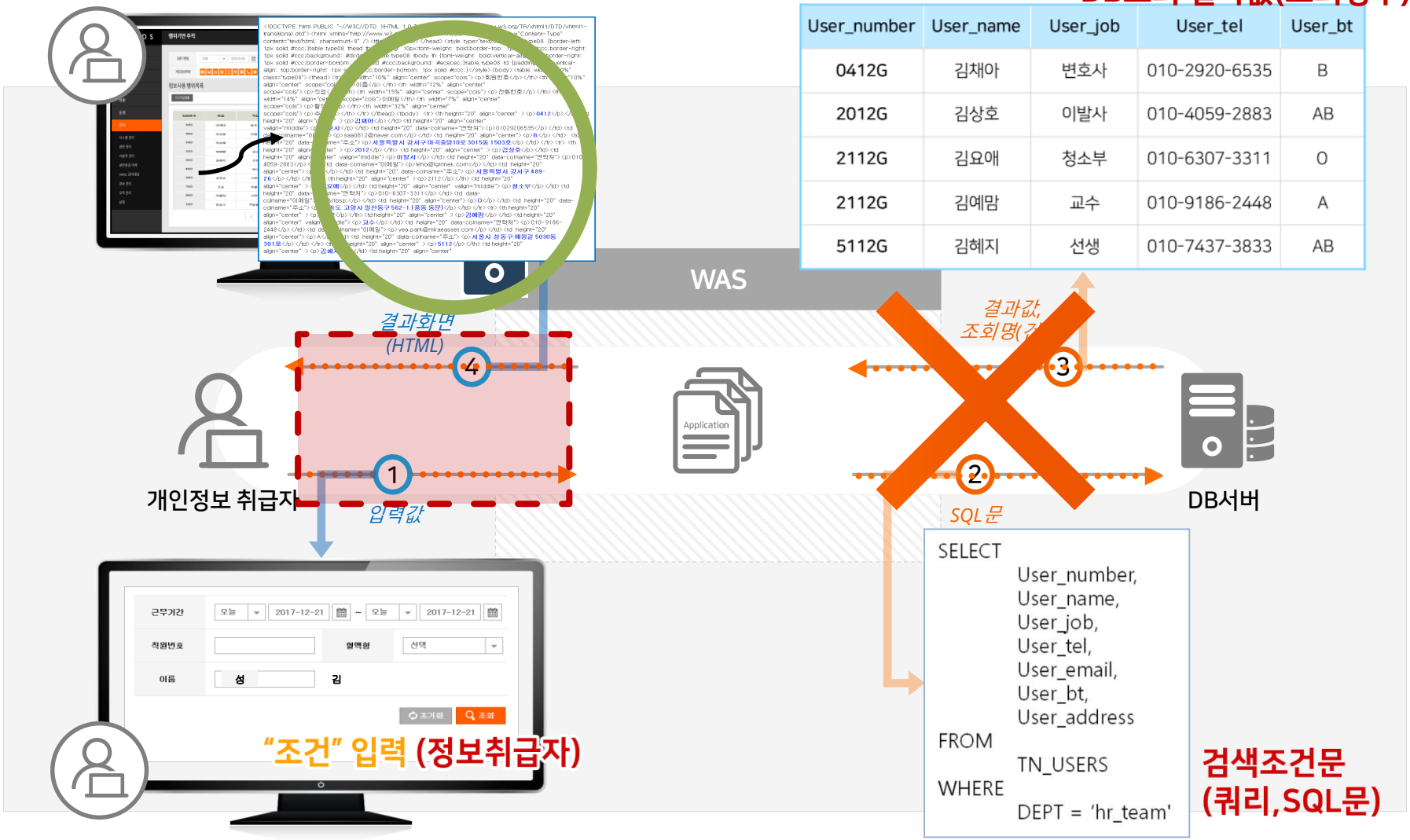
잘못된 접속기록 생성 방식의 솔루션을 선택하는 경우 기본적인 법규 준수 불가

WEEDS

필터방식 및 NW방식은 "결과화면(HTML문)"만 기록 가능

DB조회 결과값(조회명수)

User_number	User_name	User_job	User_tel	User_bt
0412G	김채아	변호사	010-2920-6535	B
2012G	김상호	이발사	010-4059-2883	AB
2112G	김요애	청소부	010-6307-3311	O
2112G	김예맘	교수	010-9186-2448	A
5112G	김혜지	선생	010-7437-3833	AB



결과화면(HTML) 패턴필터링으로는 "사번, ID, 이름" 등 다양한 형태의 정보주체 정보의 정확한 선별 불가

패턴필터링

"이제아, 변호사, 이상호, 이발사" 등 추출

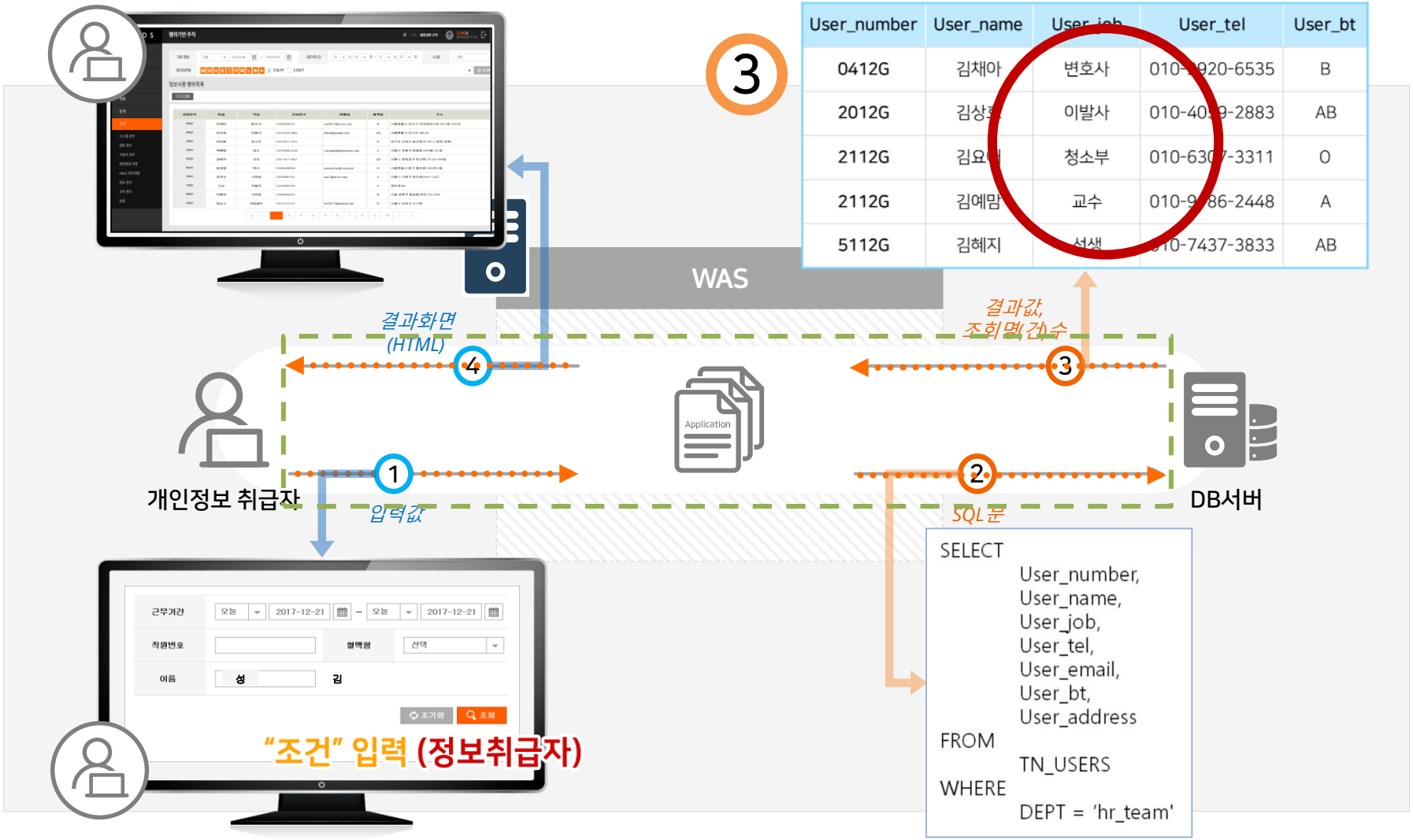
정확한 정보가 추출되었나?

오류 발생
(모든 개인정보 패턴 처리 불가)

- 사번, ID, 이름 등 정보주체정보 선별 불가
- 질병, 종교, 혈액정보 등 민감 정보 선별 불가
- 패턴필터링 오류에 의한 누락 발생

WEEDS

검색조건문(쿼리) 및 조회결과값 기록이 가능하다면?



"DB 결과값" 기록으로 "컬럼명"을 통해 이름, ID등 정보주체정보 100% 정확히 기록

2

```
SELECT
        User_number,
        User_name,
        User_job,
        User_tel,
        User_email,
        User_bt,
        User_address
FROM
        TN_USERS
WHERE
        DEPT = 'hr_team'
```

▲ 검색조건문(쿼리,SQL문)

✓ 검색조건문(쿼리)를 통해 사번, 이름, ID 등 취급된 정보주체 정보의 확인이 가능함

3

User_number	User_name	User_job	User_tel	User_bt
0412G	김채아	변호사	010-2920-6535	B
2012G	김상호	이발사	010-4059-2883	AB
2112G	김요애	청소부	010-6307-3311	O
2112G	김예맘	교수	010-9186-2448	A
5112G	김혜지	선생	010-7437-3833	AB

▲ 결과값

✓ 사번, ID, 이름 등 정보주체 정보가 포함된 컬럼명이 기록됨 (정보주체 정보 선별시 "패턴필터링"을 미사용)

기준 고시에서 요구되는 정보주체정보 및 검색조건문의 정확한 기록이 보장됨

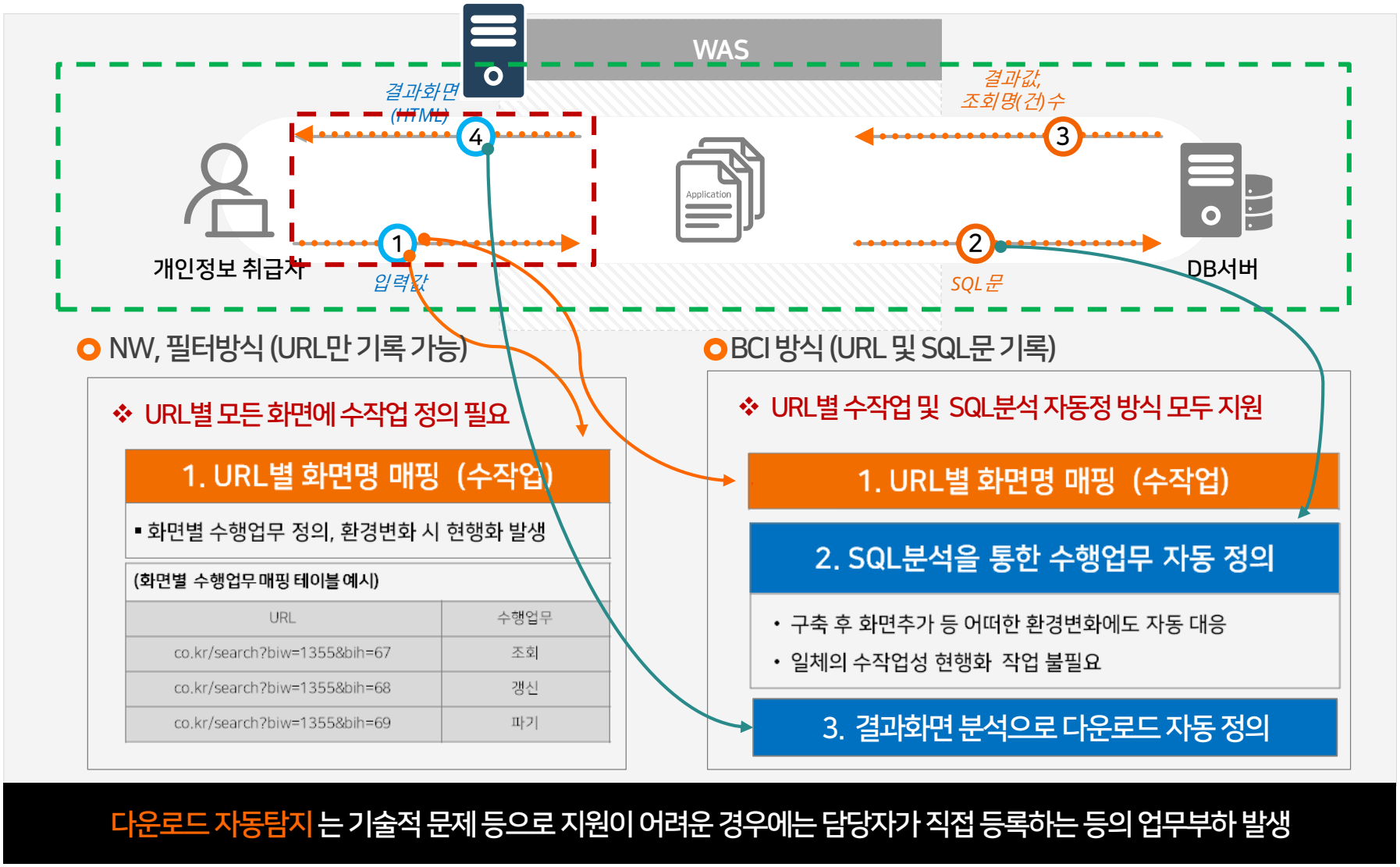
WEEDS

"수행업무 자동 정의" 구축 후 관리자 운영 편의성 확보를 위해 반드시 필요함

구분	식별자	처리한 정보주체 정보	접속일시	접속지 정보	수행업무	정보주체 처리명수
	kdhong (사용자 ID)	성춘향 (이름,ID / 검색조건문)	2024년 5월 1일 15시12분11초	172.68.11.2 (접속지 IP주소)	조회, 갱신 등 다운로드	230명
BCI방식 (자사 SW방식)	O	O	O	O	O	O
JAVA필터 (SW방식)	O	X	O	O	△ (수동 정의)	X
NW방식	X	X	O	O	△ (수동 정의)	X

잘못된 접속기록 생성 방식의 솔루션을 선택하는 경우 기본적인 법규 준수 불가

3. 수행업무
3.2 SQL문 기록시 자동정의 가능



다운로드 자동탐지 는 기술적 문제 등으로 지원이 어려운 경우에는 담당자가 직접 등록하는 등의 업무부하 발생

WEEDS

HTML(결과화면) 기록 시 개인정보 조회 명수 산정이 불가함

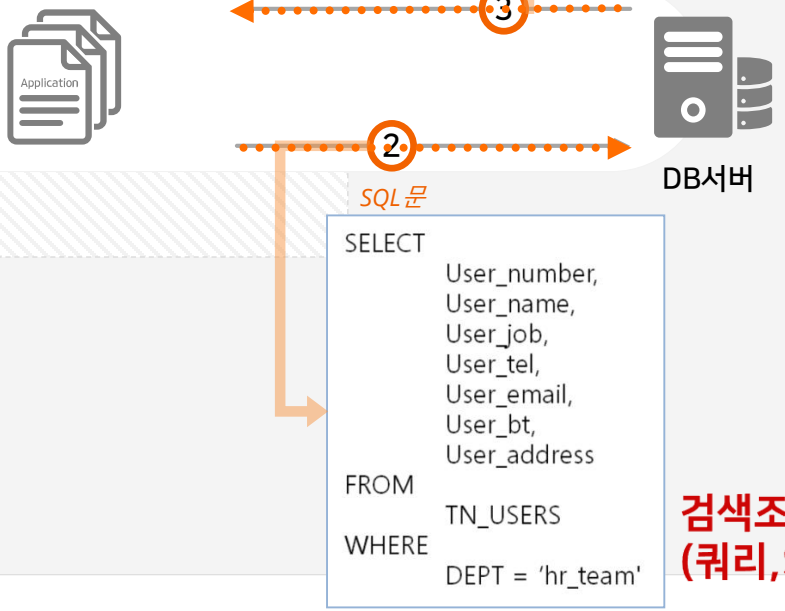
구분	식별자	처리한 정보주체 정보	접속일시	접속지 정보	수행업무	정보주체 처리명수
	kdhong (사용자 ID)	성춘향 (이름,ID / 검색조건문)	2024년 5월 1일 15시12분11초	172.68.11.2 (접속지 IP주소)	조회, 갱신 등	230명
BCI방식 (자사 SW방식)	O	O	O	O	O	O
JAVA필터 (SW방식)	O	X	O	O	△ (수동 정의)	X
NW방식	X	X	O	O	△ (수동 정의)	X

잘못된 접속기록 생성 방식의 솔루션을 선택하는 경우 기본적인 법규 준수 불가

HTML문에는 조회명(건)수 산정 불가, DB결과값을 통해서만 정확히 산정 가능

User_number	User_name	User_job	User_tel	User_bt
0412G	김채아	변호사	010-2920-6535	B
2012G	김상호	의사	010-4059-2883	AB
2112G	김요애	청소부	010-6307-3311	O
2112G	김예맘	교수	010-9186-2448	A
5112G	김혜지	선생	010-7437-3833	AB

10명



검색조건문
(쿼리,SQL문)

5. 접속기록 필수항목

식별자	처리한 정보주체 정보	접속일시	접속지 정보	수행업무	조회명(건)수
gd.hong (사용자 ID)	홍길동 (ID, 학번, 사번, 검색조건문 등)	2024년 5월 1일 15시 12분 11초	172.68.11.2 (접속지 IP주소)	조회, 갱신 등	230명
누가	누구의	언제	어디서	업무내역	조회된 사람의 명수

핵심사항

☐ 개인정보처리시스템에 접속하여 수행한 모든 업무내역들의

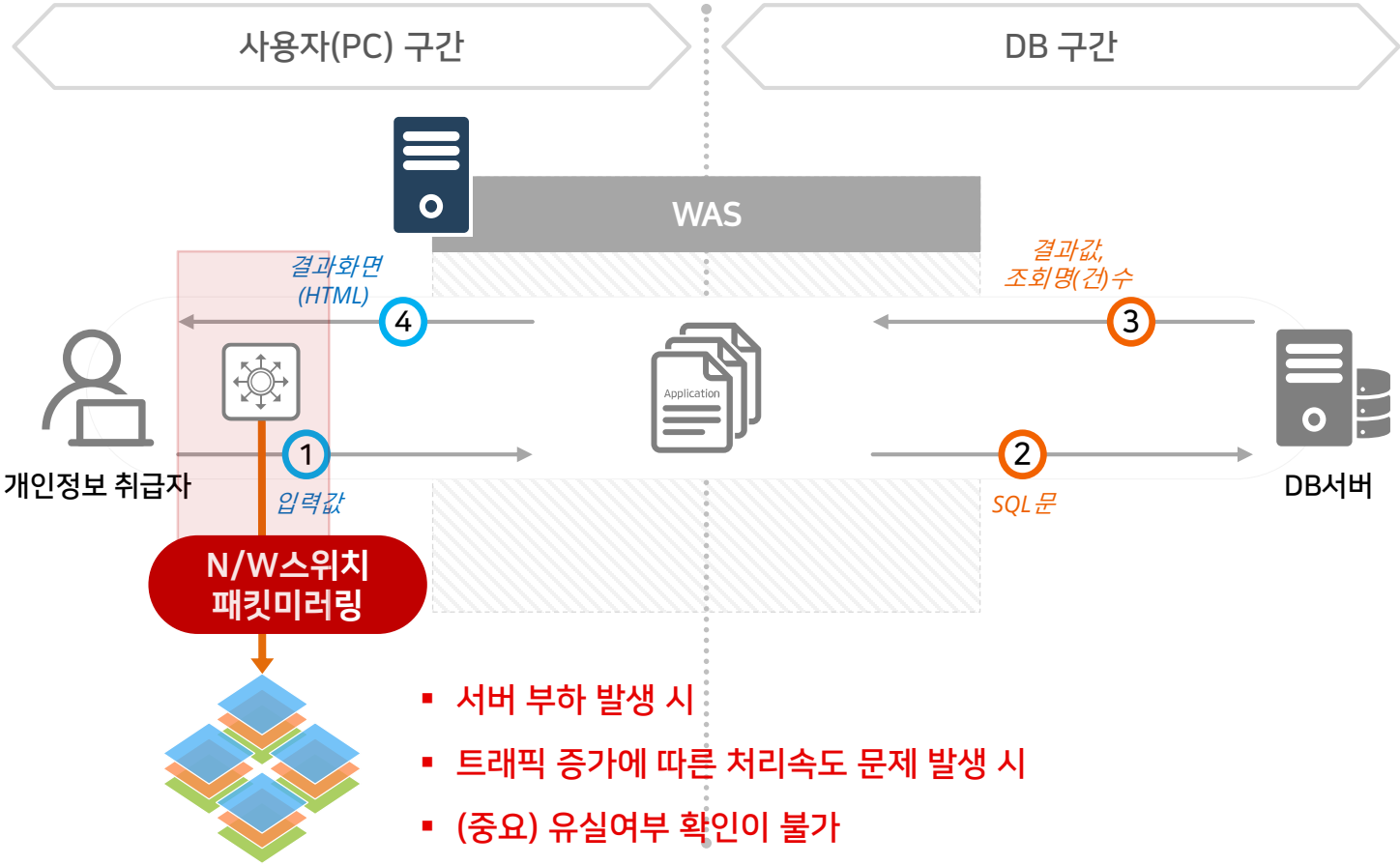
유실, 누락없는 기록

6. NW방식은 접속기록 유실에 안전한가?

WEEDS

✓ 패킷 유실에 의한 접속기록 누락 발생

➔ 기준고시 충족 불가



- 서버 부하 발생 시
- 트래픽 증가에 따른 처리속도 문제 발생 시
- (중요) 유실여부 확인이 불가

7. 잘못된 접속기록 생성 방식의 선택은?

WEEDS

구분	계정	처리한 정보주체 정보	접속일시	접속지	수행업무	정보주체 처리명수
	kdhong (사용자 ID)	성춘향 (이름,ID / 검색조건문)	2024년 5월 1일 15시12분11초	172.68.11.2 (접속지 IP주소)	조회, 갱신 등	230명

잘못된 접속기록 생성 방식의 솔루션 선택은
기본적인 법규 준수가 불가하며 운영 시 여러 관리상 문제가 초래됨

JAVA필터 (SW방식)	○	X	○	○	△ (수동 정의)	X
NW방식	X	X	○	○	△ (수동 정의)	X

잘못된 접속기록 생성 방식의 솔루션을 선택하는 경우 기본적인 법규 준수 불가

WEEDS

04

WEEDS BlackBox Suite

법규준수를 위한 고도화 방안

이상행위 탐지 및 소명 관리

WEEDS

1. 이상행위, 비정상행위 탐지

□ 이상행위, 비정상행위 기준

○ 운영 주체 별로 기준은 다를 수 있음

○ 내부관리계획에 따라 개인정보 오남용에 대한 기준 적용

□ 점검 항목 예시

접속기록 내 비정상 행위 여부 점검결과				
번호	점검항목	점검결과 (여,부)	비정상행위 조치사항 (소명 여,부)	조치결과
1	개인정보를 업무목적 외 생성 및 과다 생성 여부			
2	개인정보를 업무목적 외 조회 및 과다 조회 여부			
3	개인정보를 업무목적 외 수정 및 과다 수정 여부			
4	개인정보를 업무목적 외 과다 삭제 여부			
5	개인정보를 업무목적 외 출력 및 과다 출력 여부			
6	개인정보를 다운로드할 경우 그 사유 확인 여부			
7	평일 업무시간 이외의 시간에 개인정보 과다 처리 여부			
8	심야시간대에 개인정보 과다 처리 여부			
9	공휴일, 휴일 등에 개인정보 처리 여부			
10	동 시간대 동일 ID, 다른 IP대역으로 접속 여부			
11	취급자의 인가된 업무범위 외 과도한 접속시도 여부			
12	주민등록번호 검색 등이 가능한 조회 화면을 이용하여 업무목적 외 처리 및 과다 처리 여부			

1. 이상행위, 비정상행위 탐지

WEEDS

□ 탐지 항목 예시(1)

행위 명		행위 상세	행위 형태	탐지 예시
개인정보 조회	개인정보 과다 조회	개인정보 과다 량 조회 (설정 기간 동안 조회한 개인정보 총 건수)	1. #건 이상 or 최다 량 TOP #건	* 일간 사용자별 개인정보 조회 합계 1000건 이상 탐지 * 월간 사용자별 개인정보 조회 합계가 1000건 이상이며 TOP 3에 포함된 경우 탐지
	개인정보 과다 빈도 조회	개인정보 과다 빈도 조회 (설정 기간 동안 개인정보 조회한 빈도)	1. 일정 빈도 이상 or 최다 빈도 TOP #건	* 일간 사용자별 개인정보 조회 행위(행위건수)가 1000건 이상 탐지
	개인정보 조회 급증	O월 평균과 비교하여 개인정보 조회 수가 O배 증가 시	1. #배 이상 2. 최소 건수 #건 이상 3. 비교 대상 월 (#월~#월 or 직전 #개월 간 평균)	* 월간 개인정보 조회 건수가 직전 2개월 평균보다 3배 이상 되는 경우 탐지 - 최소 1000건 이상인 경우에만 탐지
개인정보 저장	개인정보 과다 저장	개인정보 과다 량 저장 (설정 기간 동안 조회한 개인정보 총 건수)	1. #건 이상 or 최다 량 TOP #건	* 일간 개인정보 다운로드 수가 1000건 이상인 경우 탐지 * 일간 주민등록번호 다운로드 수가 1000건 이상인 경우 탐지
	개인정보 과다 빈도 저장	개인정보 과다 빈도 저장 (설정 기간 동안 개인정보 저장한 빈도)	1. 일정 빈도 이상 or 최다 빈도 TOP #건	* 일간 사용자별 개인정보 다운로드 행위(행위건수)가 1000건 이상 탐지
개인정보 출력	개인정보 과다 출력	개인정보 과다 량 출력 (설정 기간 동안 조회한 개인정보 총 건수)	1. #건 이상 or 최다 량 TOP #건	* 일간 개인정보 출력 수가 1000건 이상인 경우 탐지 * 일간 주민등록번호 출력 수가 1000건 이상인 경우 탐지
	개인정보 과다 빈도 출력	개인정보 과다 빈도 출력 (설정 기간 동안 개인정보 출력한 빈도)	1. 일정 빈도 이상 or 최다 빈도 TOP #건	* 일간 사용자별 개인정보 출력 행위(행위건수)가 1000건 이상 탐지

1. 이상행위, 비정상행위 탐지

WEEDS

□ 탐지 항목 예시(2)

행위 명		행위 상세	행위 형태	탐지 예시
비정상 행위	특정인 개인정보 조회	수동 설정한 특정 정보주체의 개인정보를 조회시	1. #건 이상 2. 특정인 (개인정보 유형 멀티 설정)	* 특정 사람의 개인정보 조회 시 탐지 * 특정 취급자가 1건 이상의 개인정보 조회 시 탐지 (비 개인정보 취급자 모니터링)
	과도한 개인정보 저장	설정 기간내 과도한 개인정보 저장	1. #시간 이내 2. #건 이상	* 개인정보 다운로드가 연속 3회 이상 발생 시 1시간 이내에 개인정보 1000건 이상 다운로드 시 탐지
	본인 정보 조회	수행자 본인의 개인정보 조회	1. #건 이상	* 본인 정보를 조회한 경우 탐지 * 본인 정보를 1일간 2회 이상 조회한 경우 탐지
	재직자 정보 조회	재직자 개인정보 조회	1. #건 이상	* "홍길동" 이라는 이름을 조회한 경우 탐지 * 주민등록번호 검출 건 중 재직자 정보인 경우 탐지
	임직원 가족 조회	임직원 본인 / 가족 / 임직원 조회	1. #건 이상 2. 임직원 가족 정보 (개인정보 유형 멀티 설정)	* 주민등록번호 검출 건 중 임직원 가족 정보인 경우 탐지
	휴직자 접속	휴직자 계정 접속	1. #건 이상 2. 휴직자 목록 (연동 인사DB에서 확인가능 여부)	* 주민등록번호 검출 건 중 휴직자 정보인 경우 탐지
	퇴직자 접속	퇴직자 계정 접속	1. #건 이상 2. 퇴직자 구분 (연동 인사DB에서 확인가능 여부)	* 주민등록번호 검출 건 중 퇴직자 정보인 경우 탐지
	부서/팀 이외의 시스템 조회 검출 (비인가자에 의한 개인정보처리 및 접속현황)	시스템별 설정한 사용자 부서 외에 다른 부서에서 접근	1. #건 이상 2. 시스템별 접근 부서 목록	* 부서가 접근 가능한 시스템 이외의 시스템에 접근한 경우 탐지
	특정수행업무 실행	설정한 특정 업무 수행 시	1. 특정수행업무	* 다운로드 수행한 경우 탐지
	장시간 SQL 사용	장시간 SQL 사용	1. 일정 시간 이상	* SQL 실행시간이 10초 이상 걸린 경우 탐지
	조회결과 없음	조회결과 없음	1. #시간 이내 2. (결과 '조회건수 없음'이)# 건 이상	* 조회하였는데 결과건수가 0인 경우 탐지
	중요화면 과다사용	중요화면 과다사용	1. #건 이상 2. 시스템별 중요화면 목록	* 특정 URL을 접속한 경우 탐지
	O시간 이내 특정화면 접속횟수가 O건 이상인 경우 (매시간별)	O시간 이내 특정화면 접속횟수가 O건 이상인 경우 (매시간별)	1. #시간 이내 2. #건 이상 3. 시스템별 특정화면 목록	* 특정 URL을 1시간동안 10번 이상 접속한 경우 탐지

1. 이상행위, 비정상행위 탐지

□ 탐지 항목 예시(3)

행위 명		행위 상세	행위 형태	탐지 예시
업무시간 외 개인정보 조회	업무시간 외 심야시간 조회	평일 업무 시간 외 개인정보 조회/저장/수정/삭제/출력	1. #건 이상 2. 설정 시간 내(심야시간) 3. 액션 (조회/저장/수정/삭제/출력(or조건))	* 평일 22시 이후에 개인정보 조회 시 탐지
	휴일 개인정보 조회	주말(토/일)과 공휴일에 개인정보 조회/저장/수정/삭제/출력	1. #건 이상 2. 설정 시간 내 3. 액션 (조회/저장/수정/삭제/출력(or조건))	* 휴일/공휴일에 개인정보 조회 시 탐지
로그인 이상행위	동일 IP 다수 ID 접속	동일한 IP에서 기간 내 다수 ID로 접속	1. 다수 ID 건 수 2. 설정 시간 내	* 동일한 접속지 IP에서 2개 이상의 취급자 ID 발생 시 탐지
	동일 ID 다수 IP 접속	동일한 ID를 기간 내 다수 IP에서 접속	2. 다수 IP 건 수 2. 설정 시간 내	* 동일한 취급자ID에 대해 2개 이상의 접속지IP 발생 시 탐지
	로그인 실패	O시간 이내 일정 횟수 이상 로그인 실패	1. #시간 이내 2. #건 이상	* 1시간 내에 연속 5번 이상 "로그인실패" 라는 수행업무 발생 시 탐지
	비인가 IP접속	비인가된 IP로 접속	1. 비인가 IP 목록	* 설정된 IP로 접속한 경우 탐지
미인가자 조회	개인정보취급권한 미보유자 접속	개인정보취급자가 아닌 사용자가 접속	1. 개인정보취급권한자 목록 (수동등록 or View 연동)	* 개인정보 취급권한이 없는 사용자가 접속한 경우 탐지
기타	비사번 형태 ID	비사번 형태의 ID 접속	1. 인사DB 사번값과 비교	* 취급자ID가 취급자 정보 테이블에 없는 경우 탐지

2. 소명 절차 마련

□ 행위 탐지 후속처리

○ 개인정보 담당자 및 개인정보 취급자에게 알람(이메일, SMS, 메신저 등)

○ 개인정보 취급자 해당 행위에 대한 사유 직접 소명 등록 -> 상급자에게 품의 진행(승인)

○ 개인정보 담당자의 책임과 권한을 개인정보 취급자에게 분산

□ 다운로드 사유 관리 (제2장:제8조 2항)

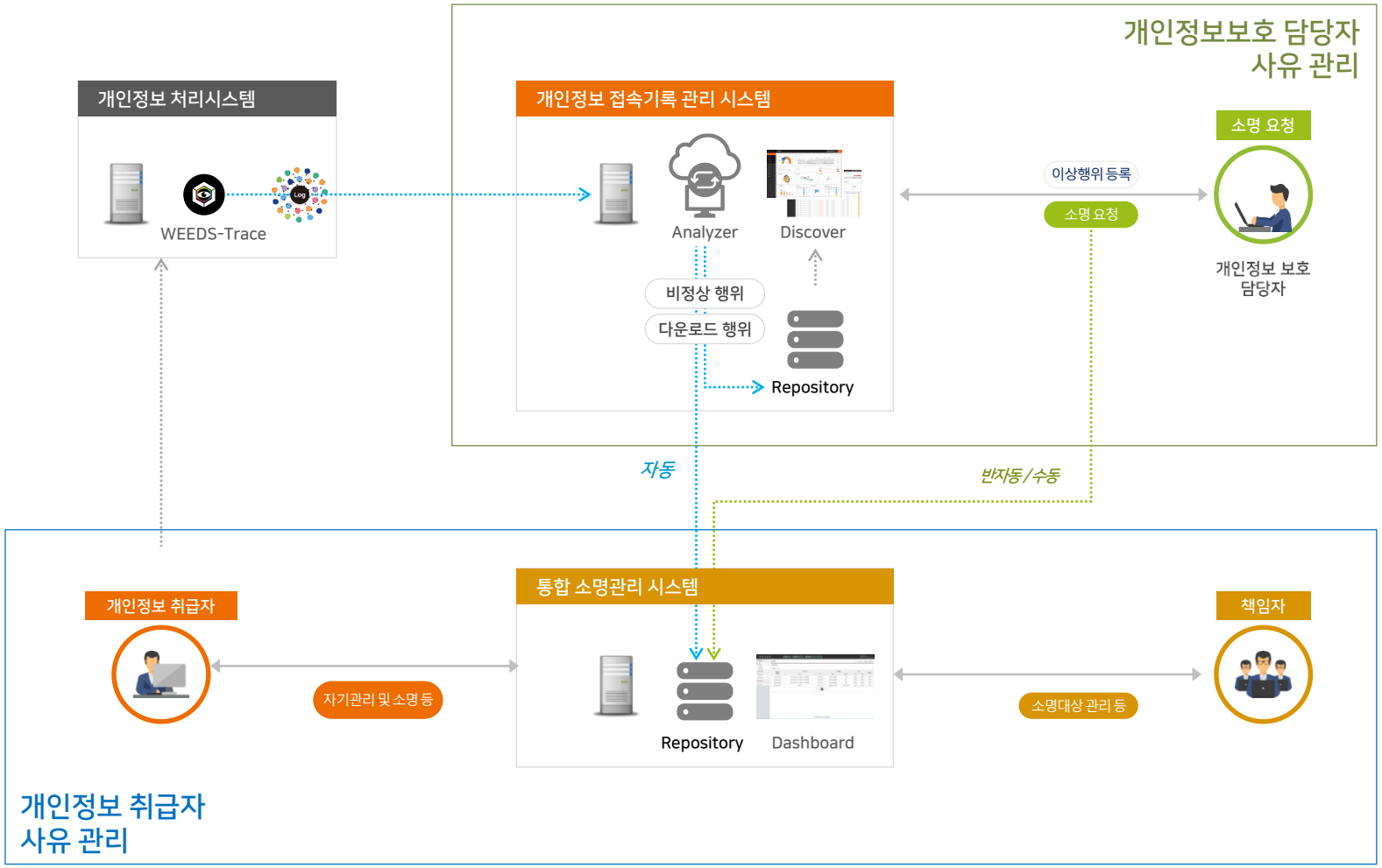
○ 개인정보의 다운로드가 확인된 경우에는 내부 관리계획 등으로 정하는 바에 따라 그 사유를 반드시 확인

□ 공공시스템에서 소명조치 (제3장:제17조 1항)

○ 공공시스템 접속기록 등을 자동화된 방식으로 분석하여 불법적인 개인정보 유출 및 오용·남용 시도

➔ 개인정보보호 자기관리 및 통합 소명관리 시스템 도입

3. 이상행위, 비정상행위 통합 소명 관리 구축



㈜위즈코리아는
대한민국 「개인정보 접속기록 관리」분야 시장 1위 기업으로 정보보호 전문 기업입니다.

대한민국 개인정보 접속기록 관리 시장 1위!

시장점유율
(누적 62%)

고객수

판매량

납품실적

일반

- 설립일 : 2003년 7월 1일
- 소재지 : 서울시 강서구 가양동 우림블루나인BD 21층
- 사업분야 : 정보보호, 개인정보보호, 업무보안 등

기술

- 업무/감사 증적 생성
- 내부위협 통합관제, 분석 및 이상행위 감시, 대응 솔루션 일괄 보유
- 원천기술 및 지적재산권 일괄 보유 (11건 취득 / 19건 출원)

역량

- 조직 : 본사(서울), 영남지사 (대구), 호남지사 (광주), 충청지사(대전)
- 역량 : 개인정보 등 정보보안 솔루션 자체 개발 및 기술 보유
  정보보호 분야 전문가로 개발 및 기술인력 구성

경험

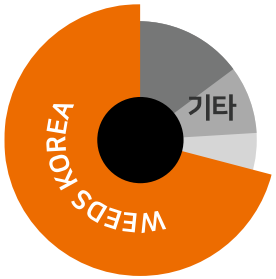
- 국내 최다 업무보안시스템 구축 실적 (국내 최고 수준의 경험 및 노하우 보유)
- KISA, 경찰청, 경기도청 등 다수 공공기관 및 한국은행, 한국증권금융, 삼성카드, 롯데이커머스, 하나생명 등 다수 민수 적용

개인정보 접속기록 생성/관리 솔루션 위즈블랙박스슈트는 700여 다양한 고객사의 정보처리시스템 25,000여대에 적용 되어 안정적으로 운영 중입니다.

중앙부처

산하소속기관(공사 ·공단 등)

광역 자치단체



기초 자치단체

※출처:조달청 '18년 이후 3개년 기준

중앙부처	검찰, 경찰청, 기상청, 외교부, 국가보훈처, 인사혁신처, 보건복지부, 기획재정부, 과학기술정보통신부, 국토교통부	外 다수
공사/공단	한국마사회, 공무원연금공단, 근로복지공단, 한국가스안전공사, 한국공항공사, 한국도로공사, K water, 한국지역난방공사, KERIS	外 다수
기업	Hanwha Hotels&Resorts, 롯데쇼핑 e커머스, 롯데렌탈, GS칼텍스, 대우건설, 에스원, AhnLab, 삼정 KPMG	外 다수
금융	삼성카드, 롯데카드, 하나생명, Heungkuk 흥국생명, 한국은행, NH농협캐피탈, 한국증권금융 Korea Securities Finance Corp., BMW GROUP Financial Services Korea, 한화손해보험	外 다수
지자체	Yangju 양주시, 광주시 GWANGJU CITY, 양평, 제천시, Global Inspiration 세계속의 경기도, 순천시, 시흥시 SIHEUNG CITY, Jeju 제주특별자치도, DAEGU 대구광역시	外 다수
대학/병원	국립 한국방송통신대학교 Korea National Open University, 가천대학교, 동국대학교 dongguk university, 가톨릭대학교 THE CATHOLIC UNIV. OF KOREA, 성결대학교 SUNGKY, 고려대학교 KOREA UNIVERSITY, 국립중앙의료원 national medical center, 국민건강보험 일산병원 National Health Insurance Service Ilsan Hospital	外 다수

WEEDS

감사합니다.

우리는
세상의 감추어진 위험을 찾아
세상이 보다 안전해짐에 공헌합니다.