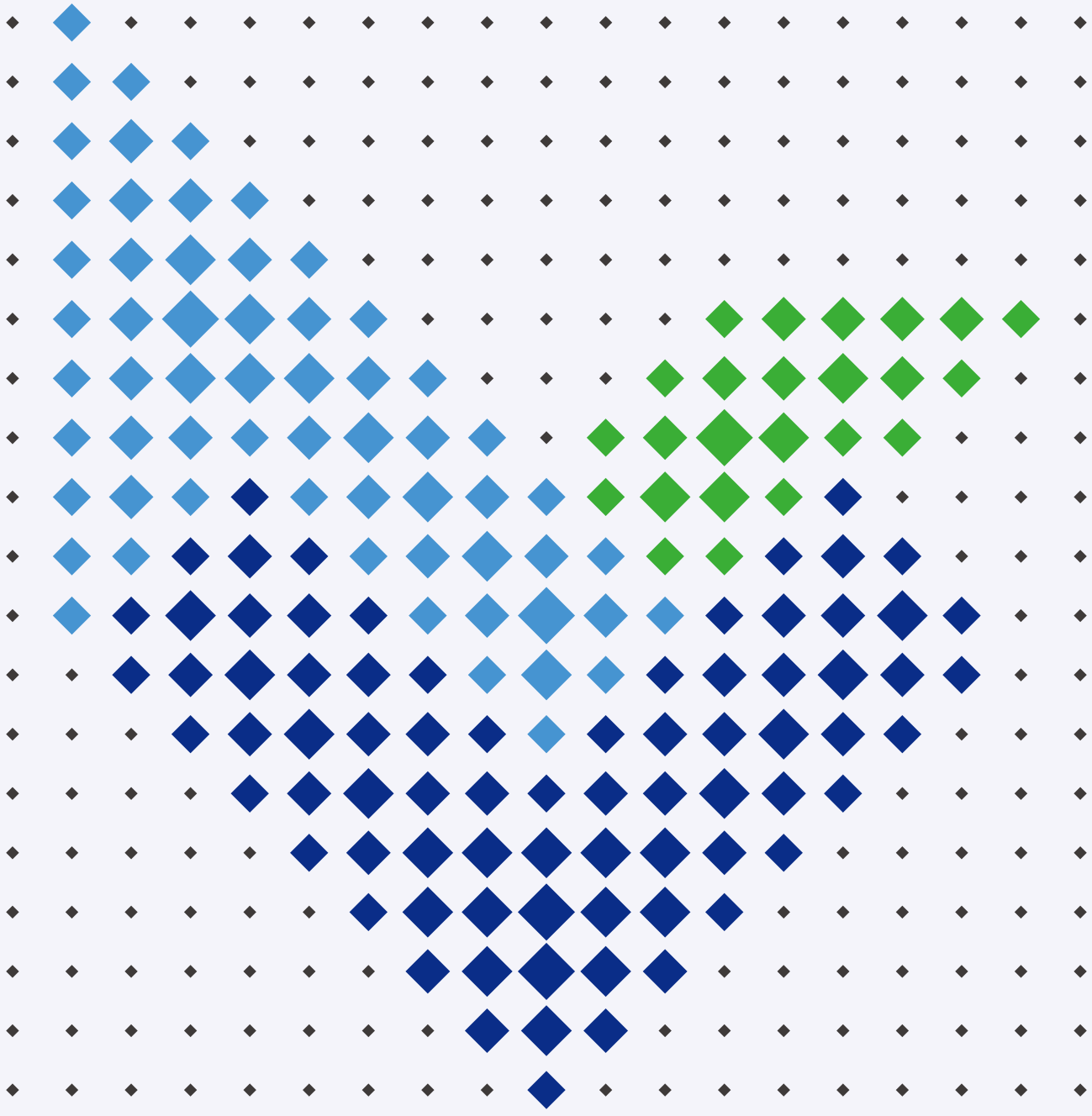
웨어밸리 로그 캐치

LOG CATCH



LOG CATCH

LOG CATCH는
개인정보보호법 준수를 위한
접근기록 관리 솔루션입니다.

01

LOG CATCH는 개인정보보호법 명시된 데이터베이스와 웹 서버 등의 개인정보처리시스템에서 개인정보 접속기록을 **5W1H 육하원칙으로 기준으로 생성하고 관리 및 점검 기능을 제공하는 솔루션** 입니다.

02

그동안 국내의 다양한 금융, 공공기관, 기업 고객으로부터 제품의 성능 및 품질을 검증받아 현재 **완벽한 개인정보 접속기록 관리 제품의 품질을 확보**하였습니다.

03

LOG CATCH는 현재 사용되는 다양한 Web Application Server와 Database 접근기록 관리를 개인정보보호법 기준으로 모두 지원하며, 최근 사용량이 확대되고 있는 **NoSQL DB와 클라우드 환경의 Database 및 Web Application Server의 접속기록 관리를 모두 지원**합니다.

LOG CATCH FUNCTION 로그 캐치 기능

개인정보 탐색

- 개인정보 고유식별 정보 탐색
- 개인정보 민감정보 탐색
- 사용자 정의 개인식별정보 지원
- 개인정보 자산 변동 관리

접속기록 수집

- 5W1H 접속기록 생성
- Web Application Server 접근기록 수집
- DB 접근기록 수집
- 웹 파일 다운로드 감지 및 수집

접속기록 보관

- 접속기록 안전한 보관 위한 위 변조 방지
- 접속기록 로그 이중화
- 보관 주기 및 예약 기능
- 개인정보 암호화

접속기록 점검

- 개인정보 오남용 유출 변조 위험도 분석
- 통계 기반 접속기록 점검 지표 데이터 시각화
- 개인정보 취급자, 부서단위 접속기록 추적 기능
- 다양한 감사 점검 보고서 제공
- 개인정보 접근기록 사용 소명 처리

DB 접근 통제 연계

- DB 접근 통제 접속기록 분석 기능
- 대용량 접속기록 데이터 처리
- DB 접근기록 점검 보고서

LOG CATCH

로그 캐치 기본 규격 및 사양

- 접속이력 생성
- 이상징후 상시 모니터링
- 거래관점의 접속기록 추적
- 다차원 및 패턴 분석 : IP, User ID, Transaction code 기준으로 상관관계, 업무패턴 emd 실시간 분석 기능 제공
- Keyword 검색 및 민감정보 접근조회

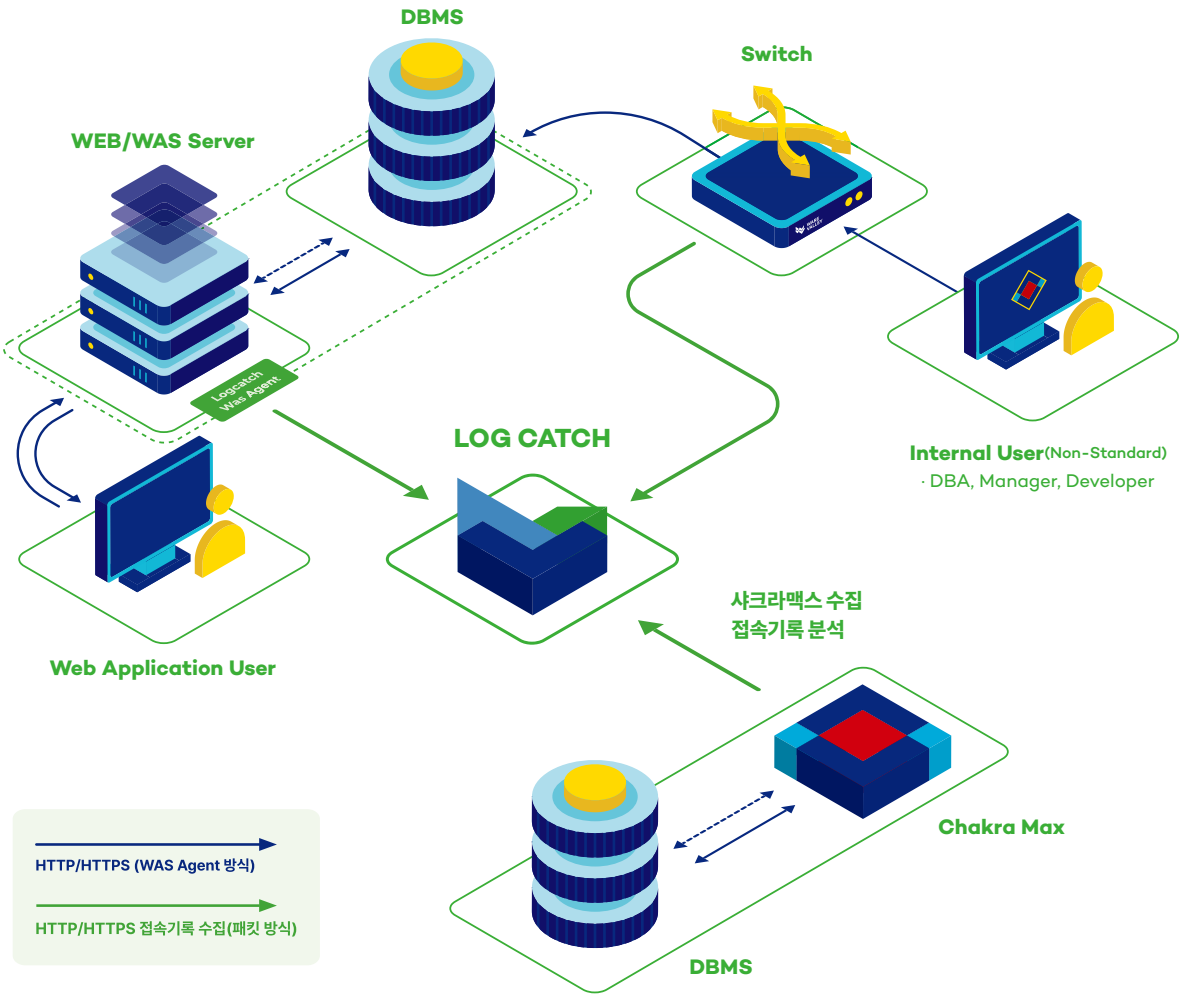
LOG CATCH

개인정보 접속 이력 통합 관리 솔루션

LOG CATCH SYSTEM 로그 캐치 시스템

LOG CATCH는 고객의 개인정보처리시스템인 웹 서버 및 데이터베이스의 접속기록 점검 및 관리를 위해 다양한 운영 환경을 지원합니다.

LOG CATCH Flow



Implementation

웹 서버 접속기록 수집(3-tier)

웹 기반 시스템인 WAS, IIS, Apache + PHP 3 Tier 환경에서
접속기록을 수집하는 방식

- Java 기반의 다양한 Web Application Server 지원
- IIS.NET 지원
- Apache + PHP 지원
- 모든 접속기록 수집

데이터베이스 접속기록 수집(2-tier)

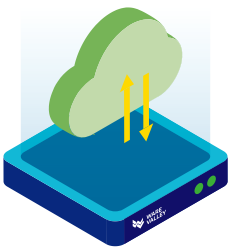
데이터베이스 직접 접속하는 정보 사용자의 접속기록을 수집하는 방식

- 데이터베이스 네트워크 패킷 분석 기술 활용
- 데이터베이스 서버에 packet agent 설치하여 특정 포트의 패킷 포워딩 기술 활용
- 기 도입된 DB 접근통제 솔루션의 접속기록 활용 방식

개인정보 접속기록 규격 준수

5W1H 육하원칙 접속기록 생성

- WHO(사용자 ID), WHEN(접속 일시), WHERE(개인정보처리시스템),
  WHAT(개인정보), HOW(조회, 수정, 삭제, 등록 등), WHY(사유)
- 접속기록 분석 시 인사정보를 연계 처리



Cloud

다양한 클라우드 호환성 지원

- 멀티 클라우드 환경 지원(AWS, AZURE, GCP, NAVER, KT,...)
- 온프레미스와 클라우드 환경 동시 지원
- 클라우드 웹 서버 및 데이터베이스 접근기록 관리

LOG CATCH FEATURES 로그 캐치 특징

개인정보 자산 관리

데이터베이스 내의 개인 고유식별 정보 및 민감정보 자동 탐지하고 접속기록에 대한 개인정보 유출 오남용 등 위험도 분석 용도로 사용

- 네트워크 대역폭 내에서 대상 데이터베이스 및 웹 서버 자동 식별 기능
- 데이터베이스 내의 개인 고유식별 정보 및 민감정보 자동 탐색
- 개인 고유식별 정보를 인식하기 위한 다양한 패턴 정규식 지원

개인정보 접속기록 수집

웹 서버, 데이터베이스의 접속기록 수집하고 개인정보보호법에 명시된 5W1H 육하원칙 기준으로 생성하는 기능 제공

- 다양한 웹 서버의 개인정보 접속기록 수집 및 생성 기능 제공
- 다양한 데이터베이스의 접속기록 수집 및 생성 기능
- HTTP 비정형 데이터 개인정보 접속기록 수집 및 생성 기능
- 웹 서버 파일 다운로드 자동 감지 및 수집 기능

개인정보취급자 계정 관리

웹 서버 및 데이터베이스에 접속하는 계정과 인사정보를 연동하여 개인정보 취급자 식별 기능 제공

- 인사정보 연동 기능 제공
- 스케줄러를 통한 인사정보 변동 사항 동기화
- DB보안 시스템 자체 리소스 모니터링 제공

위험도 분석

개인정보 접속기록 분석 통한 다양한 통계 정보를 생성하고 개인정보 유출 오남용 훼손 위변조 등과 같은 위험 행위에 대한 정보를 제공

- 데이터베이스 내의 개인정보 탐색 정보를 바탕으로 오탐 없는 개인정보 사용 현황 분석 기능
- 인사정보 연동을 통한 다양한 위험도 분석 정보 제공
- 위험도 분석 통한 개인정보 오남용에 대한 소명 기능 제공

접속기록 안전한 보관

접속기록 위변조 및 도난 분실되지 않도록 해당 접속기록을 안전하게 보관하는 기능 제공

- WORM(Write Only Read Many) 기능을 활용하여 날짜 단위 원장 접속기록 저장 및 보관
- 개인정보 접속기록 시 암호화
- 저장소 이중화 지원
- 위변조 식별을 위한 해시값 사용
- 보관 주기 및 보관 저장소 외부 연동 지원
- 보관 데이터 복원 및 조회 기능 제공

개인정보 접속기록 사유(소명) 관리

개인정보 접속기록 분석 결과 유출 및 오남용 등의 위험 행위로 감지되는 경우 소명 처리를 통한 개인정보보호법 준수 기능 제공

- 위험 정보 사용자에게 이메일로 해당 접속기록에 대한 소명 메일 발송 기능 제공
- 접속기록에 대한 소명 화면을 제공
- 감사 증적 자료 활용

개인정보 파일 다운로드 감지 및 사전 소명 처리

웹 서버를 통한 개인정보 파일 다운로드에 대한 자동 감지 및 사전 소명 처리 기능 제공

- 웹 서버의 파일 다운로드 자동 인식 기능 제공
- 파일 다운로드 시 사전 소명 페이지를 통한 사용 용도를 입력받아 감사 증적 자료 활용
- 사전 소명 시 불 이행 시 강제 접속 해제 기능 제공

개인정보 접속기록 모니터링

개인정보 접속기록 사용 현황 오남용 및 위험도 통계 분석 정보를 바탕으로 다양한 분석 차트 및 그래프 제공

- 개인정보 취급자 별 현황
- 개인정보 고유식별 정보 유형 현황
- 개인정보처리시스템 별 현황
- 부서 및 IP 별 개인정보 사용 현황
- 위험 행위 별 현황
- 특정 기간 또는 실시간 모니터링 지원

개인정보 접속기록 보고서

개인정보보호법 접속 관리 준수 기준으로 다양한 통계 및 상관 관계 분석 정보를 바탕으로 보고서 생성

- 개인정보 사용 현황
- 부서 및 개인정보 취급자 단위 사용 현황
- 개인정보 사용 소명 현황
- 개인정보 점검 및 보관 이행 수준 평가
- 스케줄러를 통한 보고서 자동 생성 및 발송 기능
- 다양한 관점의 보고서 지원(종합 보고서, 특정 개인, 부서 단위, 업무시스템 등)
- 개인정보 접속기록 상세 엑셀 데이터 Export 기능 지원(감사 자료 활용)

DB 접근통제 접속기록 분석 및 활용

DB 접근통제 솔루션의 접속기록 정보를 바탕으로 개인정보의 오남용, 유출, 위조, 변조 등 다차원 위험도 분석 기능 제공

- 실시간 처리 연계 기능 제공
- 배치 파일 단위 대용량 분석 처리 기능
- 스케줄러를 통한 주기 반복 실행 시간 제어
- 다양한 DB 접근통제 접속기록 데이터 포맷 지원

Cloud Compatibility
클라우드 호환성

클라우드 사용 증가에 따른 다양한 호환성 지원

- 멀티 클라우드 환경에서의 LOG CATCH 운영 지원(AWS, Azure, GCP, NAVER, KT, ...)
- 구독 형태의 LOG CATCH 라이선스 운영 지원
- 다양한 클라우드 환경 웹 서버 및 데이터베이스에 대한 접근기록 관리 기능 제공
- 전 구간 암호화 통신을 통한 사용자 전송 데이터 보호
- 클라우드 Auto Scaling에 따른 보호 대상 시스템 자동 등록 및 접속기록 관리

High Availability
고가용성

예상치 못한 시스템 장애 시에도 정상적인 개인정보 접속기록 관리 유지를 위한 이중화 기능 제공

- 각 구성요소의 Active-Standby 모드 지원

LOG CATCH
자체 보안 기능 강화

자체 보안 기능 강화

- 접속기록 로그 위변조 방지를 통한 무결성 지원
- 개인정보 접속기록 암호화
- 관리자, 사용자 운영 이력 저장

WAREVALLEY
INNOVATIVE DATA SOLUTION

웨어밸리 혁신적 데이터 솔루션

DB · System 접근제어 및 계정 통합관리 솔루션

CHAKRA MAX

DAC
DB 접근제어

SAC
System 접근제어

IAM
계정 통합관리

내부회계감사 및 ISMS-P 인증 대응

개인정보보호법 기준 데이터 처리시스템(DB · System) 보호 조치 인증 및 권한 관리를 통한 컴플라이언스 완벽 대응

DB 관리 및 개발

ORANGE

DB 성능 모니터링 및 개발 지원 도구

DB 작업 결재

Trusted ORANGE

Orange 사용자 기반의 강력한 DB 작업결재

DBMS

Petagres

빅데이터 분석/데이터웨어하우스
/데이터 마트/실시간 로그 분석

통합 로그관리

LOG CATCH

개인정보 접속이력 관리 및
이상징후 감지 및 소명 관리

LOG CATCH

개인정보 접속이력
통합관리 솔루션

WARE VALLEY

www.warevally.com

(04029) 서울시 마포구 잔다리로 81

T. 1660-1675 / **F.** 02-743-3023