LG CNS

SecuXper

ChatGPT와 AI시대의 보안전문가 생존전략 웨비나

AI를 활용한 개인정보 컴플라이언스 대응사례

LG CNS 보안서비스 Innovation팀
박수현 선임

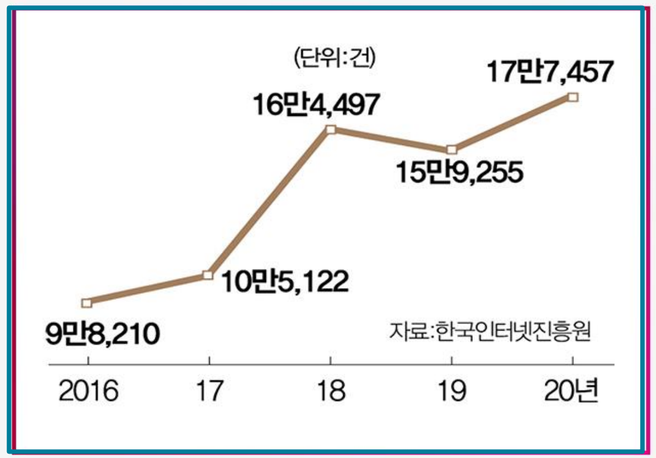
LG CNS

목 차

1 개인정보 침해위협과 동향(1/3)

개인정보 침해사고의 급증

개인정보 침해 상담신고 급증



개인정보 침해 신고·상담건수 (출처 : 한국인터넷진흥원)

주요 보안 위협 사례

- '14년 | 1억 4천만 건의 개인정보 유출
- '20년 | N번방 피의자 주민 정보 불법 조회

개인정보 침해사고 유형 분석

개인정보 침해사고 경험 유형	비율 (%) 복수응답 가능
개인정보 무단 수집하여 마케팅 목적으로 이용	46.4
내부의 보안 관리 소홀로 개인정보 유출된 경우	46.4
외부의 해킹으로 인해 개인정보가 유출된 경우	46.4
개인적인 사진이나 동영상 유출로 인한 사생활 침해	15.1
보유 및 이용기간 만료된 개인정보 파기하지 않은 경우	6.4
유출된 정보가 피싱/스미싱 등 사기성 범죄로 활용된 경우	1.7
기타	1.4

(출처: 과학기술정보통신부 –정보보호 실태조사 2021)

1 개인정보 침해위협과 동향(2/3)

개인정보 침해사고 제재

국내 개인정보 유출 벌금 부과 사례 5

순위	기업명	과징금	개인정보 유출 규모
1	인터파크	44.8억	2,540만 여건
2	위메프	18.6억	2년 연속 가입자 정보 유출
3	KT	7.5억	873만 여건
4	하나투어	3.4억	49만 여건
5	위드이노베이션	3.2억	17만 여건

출처: 보안뉴스(www.boannews.com)

2020년 이전 개인정보보호법

- 5년 이하 징역 등 형사처벌
- 위반 행위 관련 매출액의 3%이하 과징금

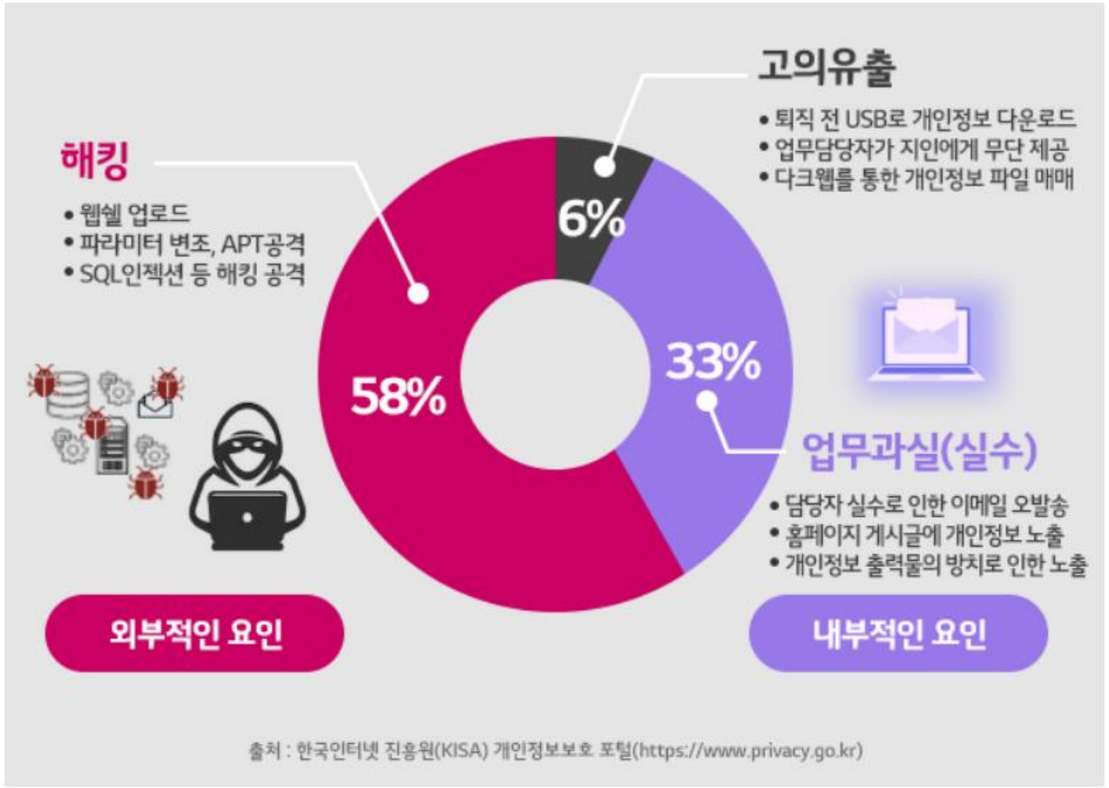
2020년 개인정보보호법 개정

- 단순 과실은 형사처벌 면제
- 연간 총 매출액의 3%이하 과징금

**개인의 형사처벌을 줄이고,
법인에 대한 경제 제재를 강화하는 방향**

출처: 2020년 개인정보보호법 개정

개인정보 유출 발생 유형



3가지 개인정보 유출 유형 발생 비율

1st
해킹 | 58%

2nd
부주의한 내부자 | 33%

3rd
고의유출 | 6%

개인정보 오남용을 막기 위한 관련 컴플라이언스

항목	내용
개인정보 처리자는 개인정보 처리시스템의 접속 기록 등을 월 1회 이상 점검하여야 한다.	접속기록 내 비정상 행위 (계정, 접속일시, 접속장소, 정보주체, 접속 빈도, 다운로드 사유)
개인정보를 다운로드한 것이 발견되었을 경우에는 그 사유를 반드시 확인하여야 한다.	다운로드 사유확인 필요 기준 (정보주체 수, 다운로드 빈도, 업무시간 외 다운로드)

대량의 개인정보에 대한 조회, 정정, 다운로드, 삭제, 출력 등의 비정상 행위 탐지와 적절한 대응조치 필요

출처: 개인정보의 안정성 확보조치 기준 해설서 (2020. 12)

3 개인정보 오남용 탐지 AI 활용방안

개인정보 오남용 탐지의 어려운 점과 AI 활용방안

개인정보 오남용 탐지 과제	어려운 점	AI를 이용한 방안
조회 대상 정보나 다운로드한 파일의 개인정보 포함 여부 판정	개인 정보에 대한 판단 기준이 없음	• AI 추론에 의한 개인정보 판단 • Query, 보유File, 웹접속로그, 시스템 메뉴 등을 분석한 AI모델 사용
업무시간 외 처리 여부 판정	업무시간 패턴이 다양함	• 업무시간 프로파일링 AI모델을 통해서 개인별 업무시간 판정 • 업무시간 기준에 따라 '업무시간 외 처리' 여부를 판정
과도한 개인정보 조회 또는 파일 다운로드 여부 판정	업무에 따른 개인정보 처리량의 정상 범위 기준이 다양함	• AI로 중요 업무 자동분류 및 이상행위 식별
개인정보 오남용 소명처리 대상 판정	소명 처리 시, 다양한 요건에 대한 종합적인 판단과 근거 제시가 필요	• AI가 판단한 정보를 바탕으로 최종 소명 처리 대상 판정

4 개인정보 오남용 탐지 AI 적용사례(1/4)

개인정보 오남용 취급 중요도 프로파일링

개인정보 취급 중요도 관리 기능

[AS-IS] 수동 개인정보 처리 시스템 관리

- 테이블 추가, 컬럼 추가/삭제 등이 빈번하여 현행화 어려움

[SecuXper AI] AI 추론으로 개인정보 판단

행위기반 Feature

머신러닝, 딥러닝

+

개인정보시스템 유사 컬럼명 탐지

유사어분석, 문맥이해 분류

순번	Query	추출 컬럼명
1	...TB_COM_USER	,NAME,**CLIENT_TEL**
2	...TB_CUSTOM_11	,ID,NAME,**CUSTOM_TN**

순번	웹접속 URL	추출 파라미터
1	.../user/usr=u1234	, **/usr=**
2	..../empl/empNo=11	, **/empNo=**

⋮

- 유사 컬럼명, 파라미터 등 개인정보 관련된 항목 추출
- 사용자의 행위 분석을 통해 개인정보 테이블 관리의 자동화

4 개인정보 오남용 탐지 AI 적용사례(2/4)

업무시간 외 개인정보 처리 탐지

• • • 취급자별 맞춤 업무시간 판정 기능 • • •

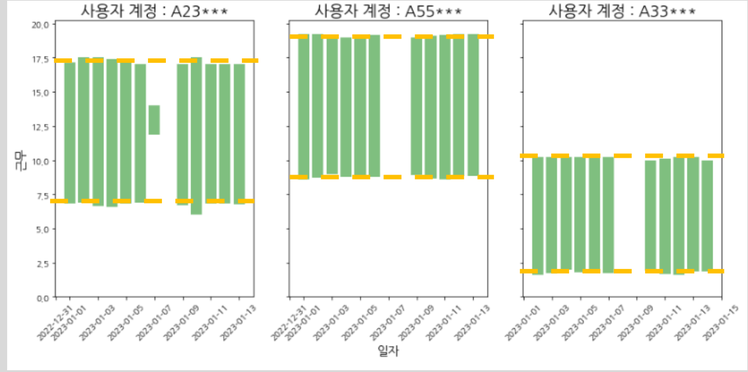
[AS-IS] 일괄적인 업무시간 기준 적용

유연근무제 등으로 인한 특정 근무 패턴 집중 탐지

- 업무 패턴을 고려하지 않은 일괄적인 업무시간 적용
- 낮은 정확도, 높은 오탐률

[SecuXper AI] 행위 기반의 업무시간 판단

취급자별 근무 이력 분석



- 사용자 행위 분석을 통해 개인정보 취급자별 업무시간 관리로 업무시간 외 개인정보 처리 탐지 정확도 향상

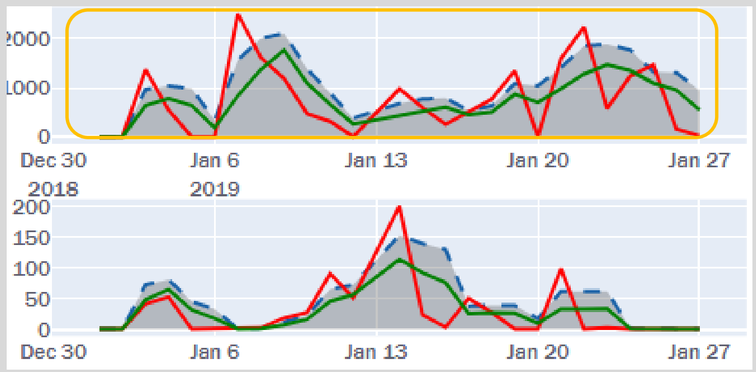
4 개인정보 오남용 탐지 AI 적용사례(3/4)

개인정보 처리 급증이상 AI 탐지

• • • 취급자별 맞춤 급증이상 판정 기능 • • •

[AS-IS] 임계치 기반 급증 이상

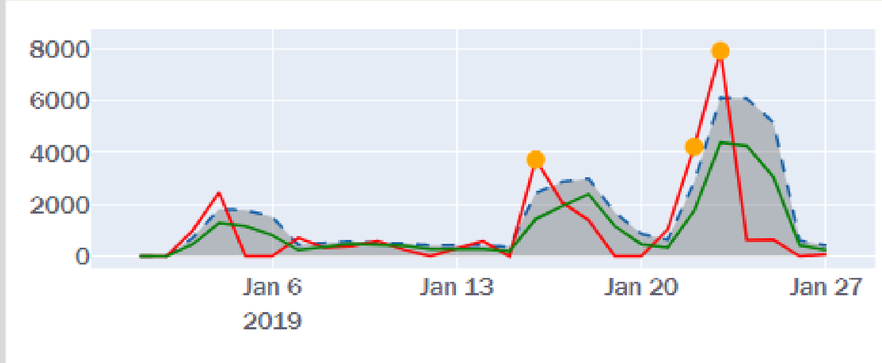
업무목적 과다 조회 취급자 집중 탐지



- 업무 패턴을 고려하지 않은 일괄적인 임계치 적용
- 낮은 정확도, 높은 오탐률

[SecuXper AI] 최신 AI모델 기반 급증이상

취급자별 과거 이력 분석



- 취급자별 과거대비 급증이상 기준을 동적으로 적용 가능
- 다양한 항목에 대한 급증이상 탐지 (휴일/야간/조회 결과 크기)

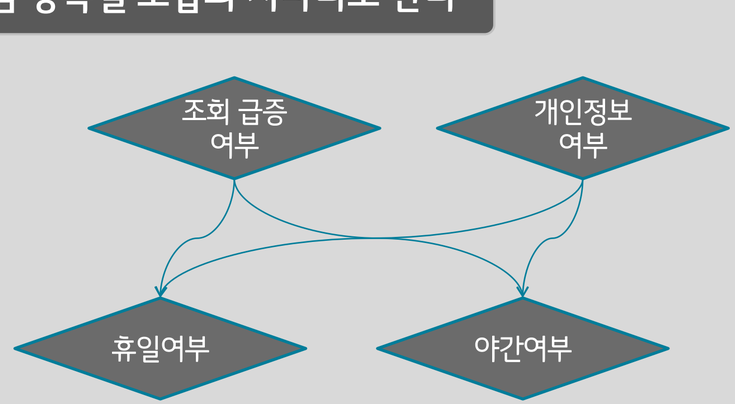
4 개인정보 오남용 탐지 AI 적용사례(4/4)

개인정보 취급자 점검대상 우선순위 AI 스코어링

• • • 점검대상 우선순위 종합적인 판정 기능 • • •

[AS-IS] 규칙기반 접속기록 점검

점검 항목별 조합의 시나리오 관리

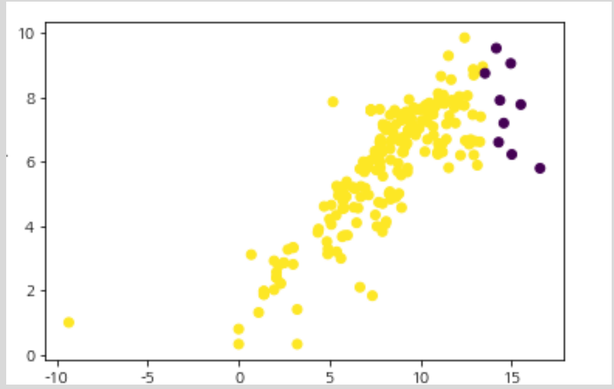


- 수 많은 조합의 시나리오 관리
- 월 평균 수십만 건 로그에 대한 임의 선별적 점검으로 인해 점검 누락 발생 가능성 높음

[SecuXper AI] 다변량 프로파일링 점검 우선순위

다양한 feature 종합

일자/ 사용자계정
조회 급증
결과 건수 급증
휴일 급증
야간 급증
AI 판정 민감정보 조회
…
중복처리
점검대상 스코어



- 다양한 feature로 비정상 취급자에 대한 종합적 지수 제공
- AI 판정 점검대상 스코어 기준 위험도 높은 취급자 집중 점검 가능

5 SecuXper AI 개인정보 오남용 탐지 솔루션 특장점

SecuXper AI 개인정보 오남용 탐지 솔루션

개인정보 오남용 탐지 솔루션 특장점

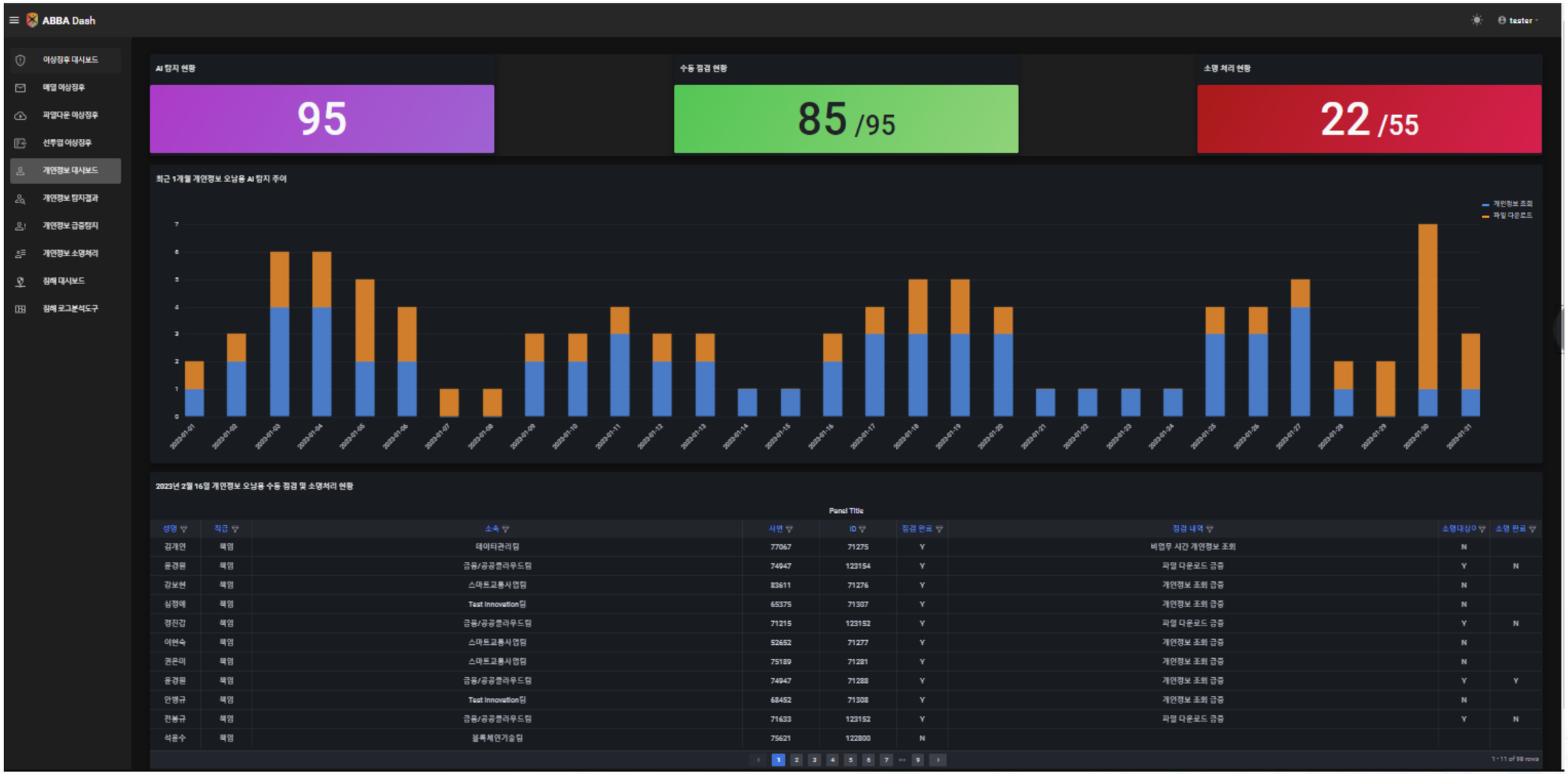
체계적인 AI운영 관리	• 라벨관리 모듈로 점검자의 점검 기준 추가 반영, 주기적인 모델 업데이트 • AI운영관리 모듈로 모델의 성능 관리
점검 업무 자동화	• 데이터 분석 / 시각화 뿐만 아니라, AI 모델이 위험도가 높은 점검 우선순위 대상 판정 • 탐지 > 점검 > 소명처리 프로세스 관리 기능 제공
개인정보관리 전문역량	• LG CNS의 전문역량으로 개인정보 오남용 컴플라이언스 완벽 준수 가이드 제공

개인정보 오남용 탐지 솔루션 주요기능

접속기록 수집 관리	• 개인정보 접속 로그 수집 및 관리 • 개인정보 로그 암호화 / 접속기록 백업 / 위변조 방지
개인정보 대상 관리	• NLP기반의 정보 대상 프로파일링 제공 • 개인정보 파일 관리 지침에 따른 자동화 관리
개인정보 취급자 관리	• 취급자의 개인정보 처리 현황 및 행위 기반 프로파일링 제공
개인정보 오남용 탐지	• AI 모델의 개인정보 오남용 탐지 결과 제공 • 점검자의 기준을 반영하는 모델 업데이트 관리
점검 / 소명 프로세스 관리	• 대상자 점검 > 소명요청 > 소명 > 검토 및 승인 프로세스 관리

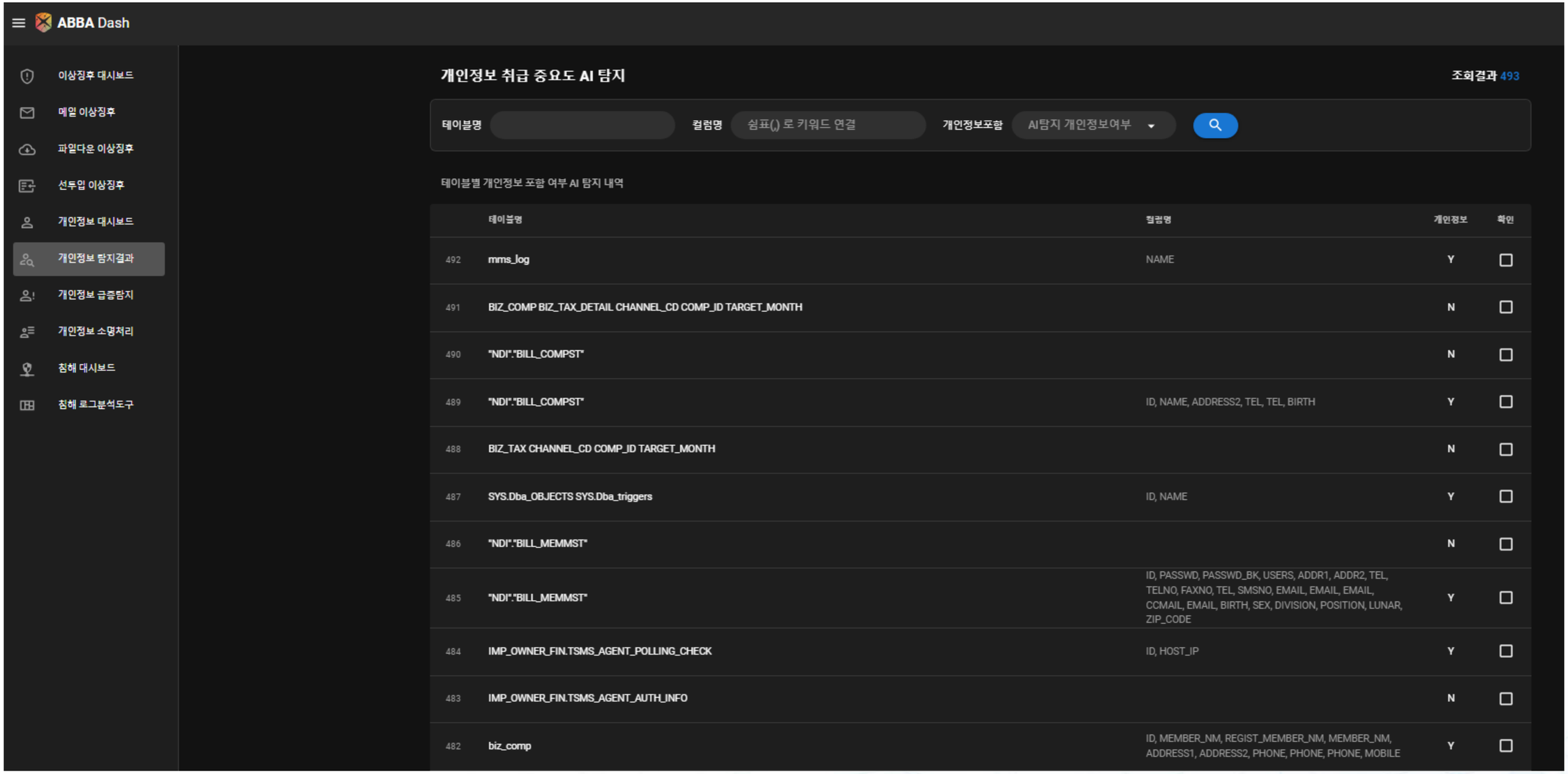
6 SecuXper AI 화면소개(1/4)

개인정보 오남용 탐지 현황 대시보드



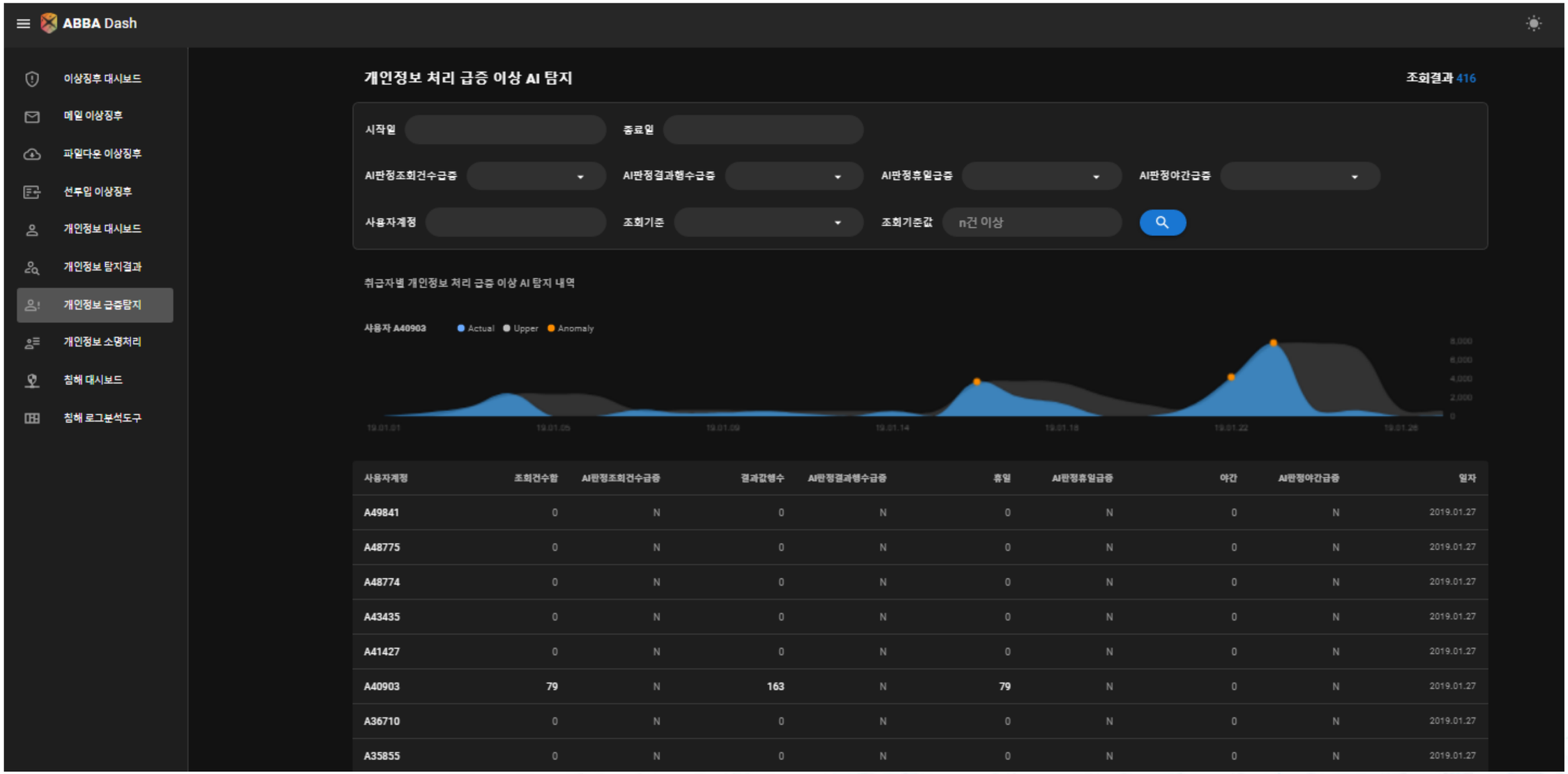
6 SecuXper AI 화면소개(2/4)

개인정보 취급 중요도 AI 탐지 화면



6 SecuXper AI 화면소개(3/4)

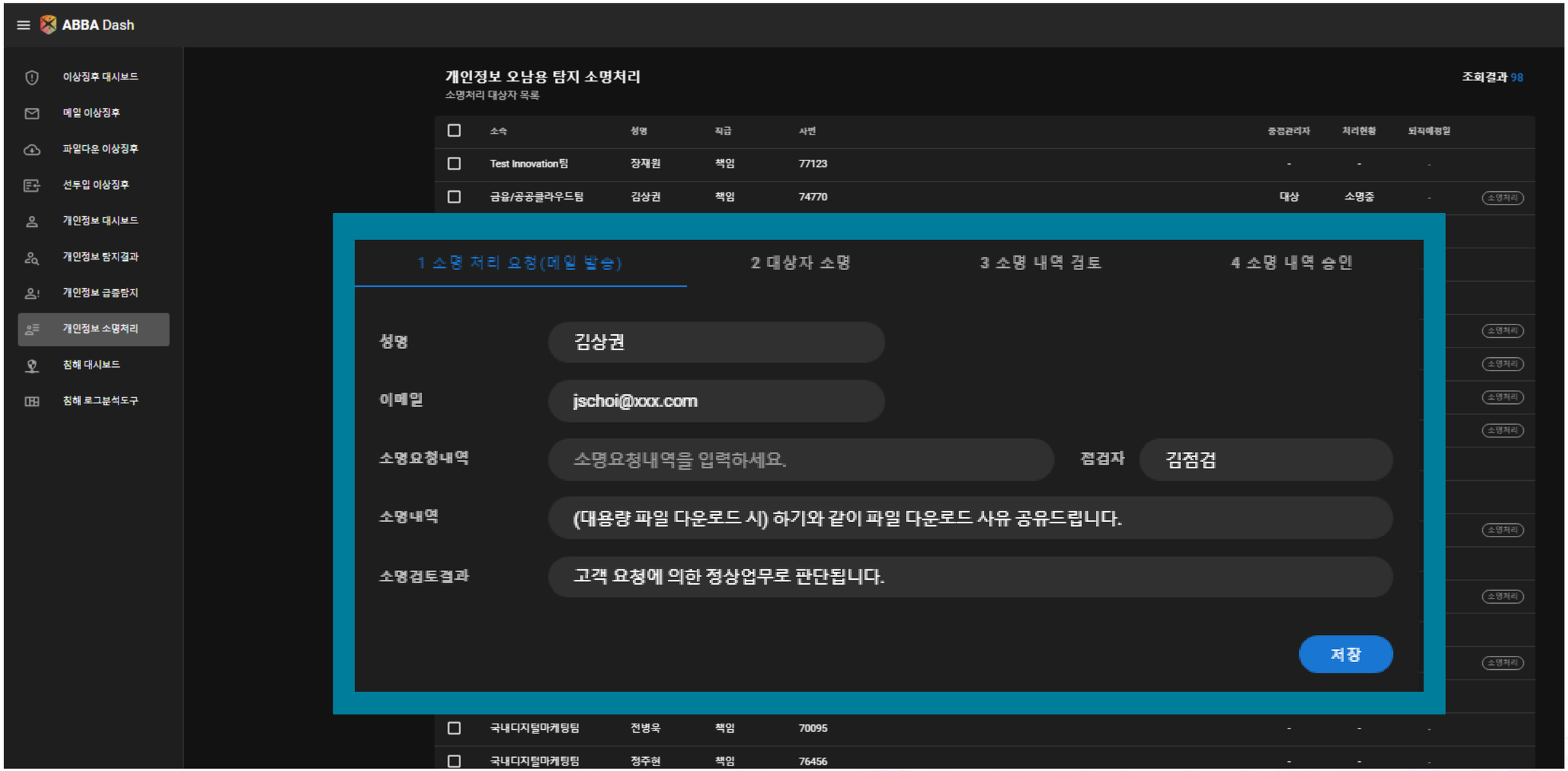
개인정보 처리 급증이상 AI 탐지 화면



사용자계정	조회건수합	AI판정조회건수급증	결과값행수	AI판정결과행수급증	휴일	AI판정휴일급증	야간	AI판정야간급증	일자
A49841	0	N	0	N	0	N	0	N	2019.01.27
A48775	0	N	0	N	0	N	0	N	2019.01.27
A48774	0	N	0	N	0	N	0	N	2019.01.27
A43435	0	N	0	N	0	N	0	N	2019.01.27
A41427	0	N	0	N	0	N	0	N	2019.01.27
A40903	79	N	163	N	79	N	0	N	2019.01.27
A36710	0	N	0	N	0	N	0	N	2019.01.27
A35855	0	N	0	N	0	N	0	N	2019.01.27

6 SecuXper AI 화면소개(4/4)

개인정보 오남용 소명처리 화면



LG CNS

AI를 활용한
개인정보 컴플라이언스 대응사례

Thank you