

# RealPll Insight

개인정보 로그 분석,  
오/과탐 로그 Out!

AI 기반 탐지 • 1~8단계 정확도 • 실시간 모니터링

## CONTENTS

# 차례

---

**01**   필요성

---

**03**   기대 효과

---

**02**   제품 개요

---

**04**   제품 기능

# 탐지는 되지만, 오탐과 과탐에 묻혀 감사를 하지 못한다

고유식별번호를 포함한 계좌번호, 카드번호 등 개인정보 문서를 사용하는 환경에서, 이를 모니터링하고 유출을 탐지·차단하는 제품들은 **구조적으로 많은 오탐과 과탐을 발생시킬 수밖에 없습니다.**

개인정보보호 담당자는 유출을 모니터링·차단하고 정상 사용에 대한 소명을 기록해야 하지만, 부족한 인원으로는 이 양을 처리할 수 없습니다.

## 현장에서 벌어지는 일

- 01 오탐과 과탐이 너무 많아 실제 개인정보 유출에 대한 감사를 하지 못함
- 02 대부분의 회사가 오탐·과탐 로그까지 포함해 탐지 로그를 보관
- 03 유출 사고가 발생한 뒤에 추적하는 사후 대응 형태로 운영
- 04 실시간 개인정보 유출에 대한 신속한 대응이 불가능

# 탐지 로그 중 실제 개인정보 로그만 식별해 단계별 신뢰도로 제공합 니다

개인정보 탐지·차단 제품은 구조적으로 오탐과 과탐이 발생합니다. RealPII Insight는 AI 기반 학습과 자체 고유 패턴을 통해 개인정보 탐지 로그 중 실제 개인정보 로그만 식별하고, 이를 단계별로 구분하여 신뢰성을 확보해 실시간 모니터링이 가능하도록 한 제품입니다.

## INPUT

개인정보  
탐지 로그

오탐·과탐 혼재

## ANALYZE

AI 학습 +  
자체 고유 패턴

이중 분류 체계

## FILTER

실제 개인정보  
로그 식별

1~8단계 정확도

## OUTPUT

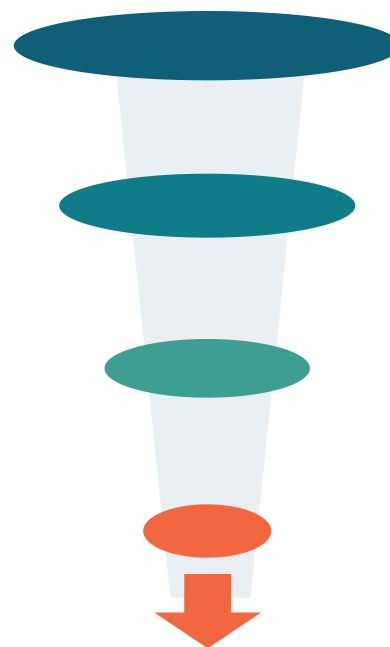
실시간 모니터링  
및 소명

신속한 대응

## 검토할 로그는 줄고, 대응 속도는 빨라집니다

- 불필요한 개인정보 탐지로 인한 리소스 낭비 방지
- 실시간 탐지를 통해 유출 사고에 대한 신속한 대응 가능
- AI 기반 기술을 활용한 정교한 탐지 및 분석 제공
- 단계별 탐지 정확도 설정으로 유연한 운영 가능
- 철저한 원시 로그 관리 및 소명 기능으로 데이터 신뢰성 확보

탐지 로그가 걸러지는 흐름



### 로그 분석

전체 개인정보 탐지 로그 수집 **100**

### 실제 개인정보 추출

오탐·과탐 로그 자동 제거 **32**

### 정확도 표기

1~8단계 신뢰도 부여 **24**

### 세부정보 보기

실시간 감사 및 소명 처리 **18**

담당자가 실제로 검토하는 로그는 **약 18%**만 남습니다.

※ 단계별 로그 감소 흐름을 나타낸 개념도입니다.

## 주요 기능 요약

8가지 기능

### 01 AI 기반 탐지 기술 적용

인공지능 기술로 탐지 정확도를 극대화하고 학습을 통해 탐지 성능 향상

### 03 오탐·과탐 로그 분석 및 처리

오탐과 과탐을 자동 분석·필터링하여 실제 탐지 결과만 제공

### 05 실시간 유출 로그 탐지

실시간 로그의 빠른 분석으로 개인정보 유출 로그 신속 탐지

### 07 '-' 없는 번호 수동 확인

주민등록번호·신용카드·여권번호를 인식해 탐지하고 수동 확인 지원

### 02 실제 개인정보 탐지 시 알람

중요한 개인정보가 탐지될 경우 즉시 관리자에게 알람 전송

### 04 단계별 정확도 구분 (1~8단계)

탐지 결과를 1~8단계로 구분하여 높은 신뢰도 제공

### 06 원시 로그 저장 및 조회

원시 로그 저장·조회 기능으로 비교 및 수동 확인 제공

### 08 소명 기능 지원

탐지된 로그에 대한 사용자 소명 기능으로 보호조치 극대화

## 기능 상세 01

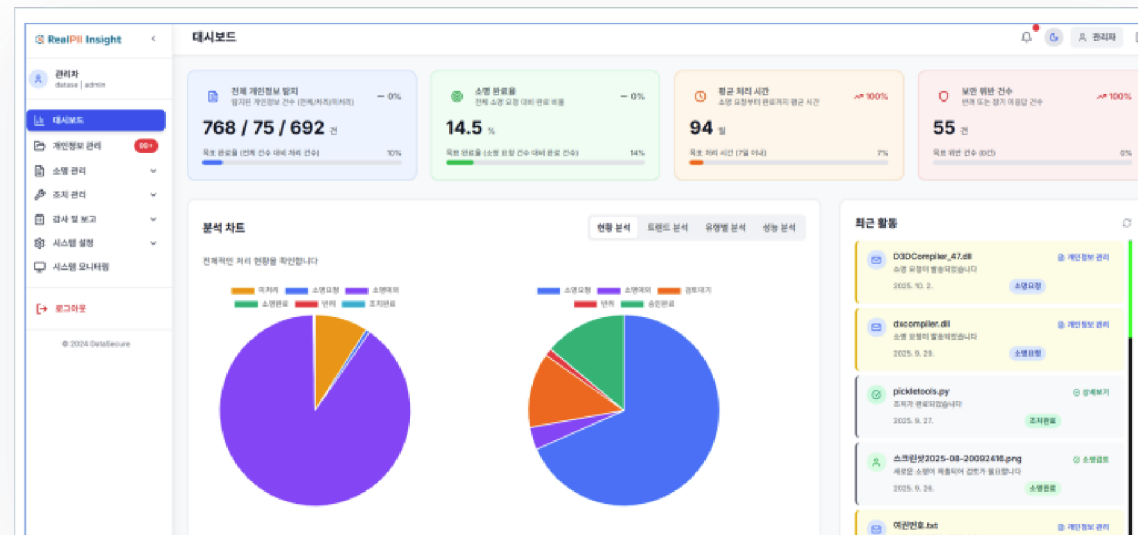
# AI 기반 탐지 기술 적용

인공지능(AI) 기술을 통한 탐지 정확도 극대화 및 학습을 통해 탐지 성능 향상

**STEP 1 데이터 학습**  
지속적인 데이터 학습으로 정확도 향상

**STEP 2 AI 알고리즘**  
최적화된 알고리즘 적용

**STEP 3 탐지 성능 향상**  
오탐 감소 및 탐지율 증가



탐지 현황 대시보드 · 분석 차트

# 개인정보 오탐·과탐 로그 분석 및 처리

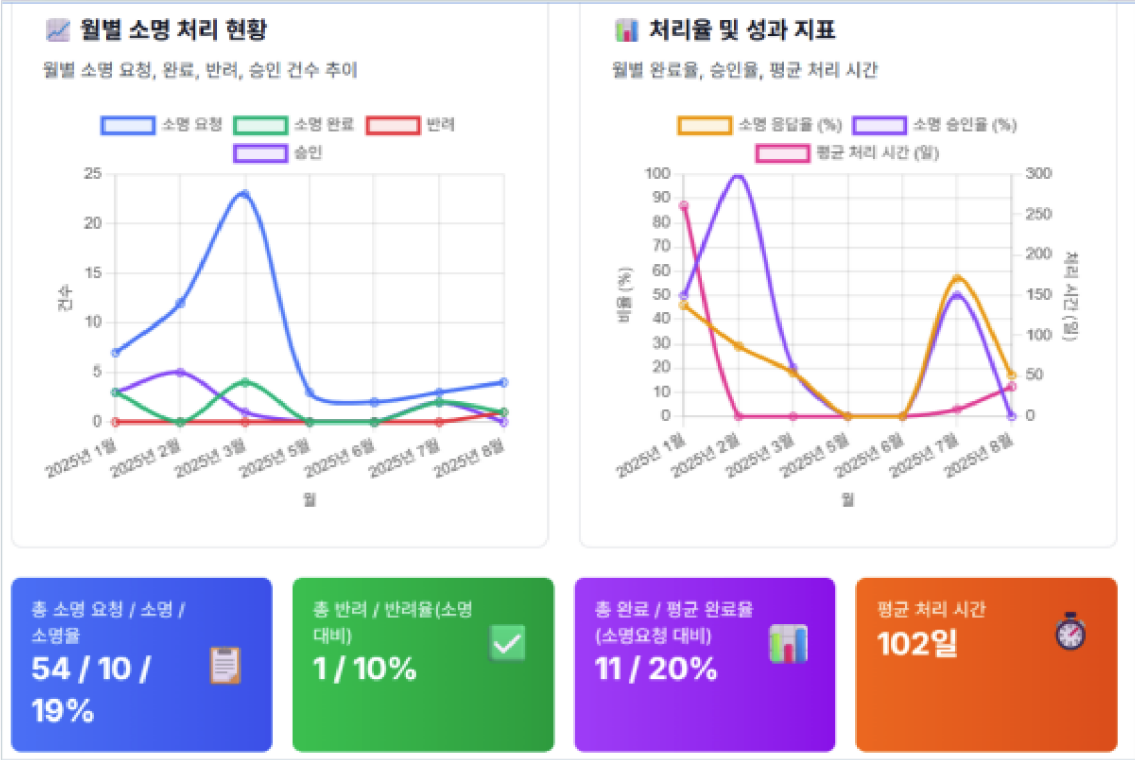
오탐과 과탐을 자동으로 분석하여 필터링하고, 실제 개인정보 탐지  
결과만 제공합니다.

01 로그 분석

02 실제 개인정보 추출

03 정확도 표기

04 세부 정보 보기



월별 소명 처리 현황 · 처리율 및 성과 지표

# 실시간 실제 개인정보 유출 로그 탐지

실시간 로그의 빠른 분석으로 개인정보 유출 로그를 신속하게 탐지합니다.

개인정보 관리

개인정보 검출 현황 및 소명 관리

Excel 내보내기

파일 업로드

전체 7,691

미처리 692

소명요청 54

소명예외 6,923

소명완료 10

반려 1

승인완료 11

Q

파일명 또는 개인정보 내용으로 검색...

고급 필터

| <input type="checkbox"/> | 파일명                                                                                               | 개인정보 유형 | 상태   | 검출 정확도    | AI 예측값 | 검출일          | 작업 |
|--------------------------|---------------------------------------------------------------------------------------------------|---------|------|-----------|--------|--------------|----|
| <input type="checkbox"/> | C:/Users/datasecure/Pictures/Screenshots/스...<br>EPP IP - 192.168.100.136 - Content Aware Prot... | 카드번호    | 소명완료 | 3/8 (38%) | 50.0%  | 2025. 8. 20. |    |
| <input type="checkbox"/> | D:/DataSecure/PrivacyInfo/sample/여권번호.txt<br>EPP IP - epp.datasecure.kr:4422 - Content Aw...      | 여권번호    | 반려   | 1/8 (13%) | 50.0%  | 2025. 8. 12. |    |
| <input type="checkbox"/> | D:/DataSecure/PrivacyInfo/sample/여권번호.txt<br>EPP IP - epp.datasecure.kr:4422 - Content Aw...      | 여권번호    | 소명요청 | 2/8 (25%) | 50.0%  | 2025. 8. 12. |    |
| <input type="checkbox"/> | D:/DataSecure/PrivacyInfo/sample/여권번호.txt<br>EPP IP - epp.datasecure.kr:4422 - Content Aw...      | 여권번호    | 소명요청 | 1/8 (13%) | 50.0%  | 2025. 8. 12. |    |
| <input type="checkbox"/> | C:/Users/ajs04/.cache/puppeteer/chrome/wi...<br>EPP IP - epp.datasecure.kr:4422 - Content Aw...   | 카드번호    | 소명예외 | 3/8 (38%) | 50.0%  | 2025. 8. 8.  |    |
| <input type="checkbox"/> | C:/Users/ajs04/.cache/puppeteer/chrome/wi...<br>EPP IP - epp.datasecure.kr:4422 - Content Aw...   | 카드번호    | 소명예외 | 3/8 (38%) | 50.0%  | 2025. 8. 8.  |    |

개인정보 관리 대시보드 · 실시간 탐지 현황

## 기능 상세 04

# 실제 개인정보 탐지 시 알람 기능

중요한 개인정보가 탐지될 경우, 즉시 관리자에게 알람을 전송합니다.

알림 대상 항목 선택

주민·카드·여권·계좌

항목별 정확도 기준

1~8단계 지정

전송 방식

실시간 전송 / 건수·상세

관리자 알림 설정

알림 선택

☒ 주민 번호

☒ 신용 카드

☒ 여권 번호

☐ 건강 보험

☐ 운전 면허

☒ 계좌 번호

정확도 :

7단계 이상

정확도 :

7단계 이상

정확도 :

6단계 이상

정확도 :

3단계 이상

정확도 :

4단계 이상

정확도 :

5단계 이상

전송 내용

☐ 항목별 건수만

☐ 상세 내역

전송 동작

☒ 실시간 전송

저장

취소

관리자 알림 설정 화면

# 단계별 정확도 구분 (1~8단계)

패턴 분류 + AI 학습 → 종합 정확도

전체  
7,691

미처리  
692

소명요청  
54

소명예외  
6,923

소명완료  
10

반려  
1

승인완료  
11

🔍 파일명 또는 개인정보 내용으로 검색...

🔼 고급 필터 ▾

| <input type="checkbox"/> | 파일명                                                                                          | 개인정보 유형 | 상태   | 패턴 분류<br>검출 정확도 | AI 학습<br>AI 예측값 | 검출일          | 작업 |
|--------------------------|----------------------------------------------------------------------------------------------|---------|------|-----------------|-----------------|--------------|----|
| <input type="checkbox"/> | D:/DataSecure/PrivacyInfo/sample/신용카드.txt<br>EPP IP - epp.datasecure.kr:4422 - Content Aw... | 카드번호    | 조치완료 | 8/8 (100%)      | 50.0%           | 2025. 7. 1.  |    |
| <input type="checkbox"/> | D:/DataSecure/PrivacyInfo/sample/은행계좌.txt<br>EPP IP - epp.datasecure.kr:4422 - Content Aw... | 계좌번호    | 조치완료 | 4/8 (50%)       | 50.0%           | 2025. 7. 1.  |    |
| <input type="checkbox"/> | C:/Users/USER/Desktop/개인정보검출제작용/내...<br>EPP IP - 192.168.100.136 - Content Aware Prot...     | 계좌번호    | 조치완료 | 1/8 (13%)       | 50.0%           | 2025. 3. 15. |    |
| <input type="checkbox"/> | D:/DataSecure/PrivacyInfo/sample/신용카드.txt<br>EPP IP - epp.datasecure.kr:4422 - Content Aw... | 카드번호    | 조치완료 | 8/8 (100%)      | 50.0%           | 2025. 2. 26. |    |
| <input type="checkbox"/> | D:/DataSecure/PrivacyInfo/sample/신용카드.txt<br>EPP IP - epp.datasecure.kr:4422 - Content Aw... | 카드번호    | 조치완료 | 3/8 (38%)       | 50.0%           | 2025. 2. 26. |    |

탐지 data 상세

탐지일시  
2025. 7. 1. 오후 4:56:14

소명일시  
2025. 7. 14. 오후 4:02:47

사용자 PC  
ajs04 / 121.172.109.16

원본 File  
D:/DataSecure/PrivacyInfo/sample/신용카드.txt

상태  
조치완료

탐지 항목  
카드번호

검출 정확도  
8/8 (100%)

탐지 data  
3562-\*\*\*\*-\*\*\*\*-2710...

Finder 탐지 data  
신용카드: 3562-\*\*\*\*-\*\*\*\*-2710 신한JCB개인 Luhn checked

상세 내용  
EPP IP - epp.datasecure.kr:4422 - Content Aware Protection - Content Threat Detected: [log ID] ccd528badf8de538948f5716909a706 | [Client Computer] DESKTOP-RZ8D4HE | [IP Address] 121.172.109.16 | [MAC Address] aa-a1-59-b7-b2-ca | [Serial Number] To Be Filled by O.E.M. | [OS] Windows 10 Pro x64 19H2 (18363.1556) | [Client user] ajs04 | [Content Policy] 개인정보 관리를 제작중\_각제금지 | [Content Policy Type] 1 | [Destination Type] Web Browser | [Destination] Standard SATA AHCI Controller -> ...

패턴 분류

AI 학습

+

패턴과 AI 학습에 의한 분류를  
종합하여 정확도 도출

탐지 data 상세보기

탐지 data 상세

탐지일시

2025. 7. 1. 오후 4:56:14

소명일시

2025. 7. 14. 오후 4:02:47

사용자 PC

ajs04 / 121.172.109.16

원본 File

D:/DataSecure/PrivacyInfo/sample/신용카드.txt

상태

조치완료

탐지 항목

카드번호

검출 정확도

8/8 (100%)

탐지 data

3562-\*\*\*\*-\*\*\*\*-2710...

Finder 탐지 data

신용카드: 3562-\*\*\*\*-\*\*\*\*-2710 신한JCB개인 Luhn checked

상세 내용

EPP IP - epp.datasecure.kr:4422 - Content Aware Protection  
- Content Threat Detected: [Log ID]  
c6d528b0adfb80e538048f5716000a706 | [Client Computer]  
DESKTOP-R2B1D4E | [IP Address] 121.172.109.16 | [MAC Address] a8-a1-59-b7-62-ca | [Serial Number] To be filled by O.E.M. | [OS] Windows 10 Pro x64 19H2 (18363.1556) | [Client user] ajs04 | [Content Policy] 개인정보 관리를 제작한\_악의금지 | [Content Policy type] 1 | [Destination Type] Web Browser | [Destination] Standard SATA AHCI Controller ->

탐지 data 상세보기

패턴과 AI 학습에 의한 분류를  
종합하여 정확도 도출

탐지 목록 · 검출 정확도와 AI 예측값을 종합하여 정확도 도출

# 원시 로그 저장 및 조회 기능

원시 로그 저장과 조회 기능으로 비교 및 수동 확인을 제공합니다.

| 발생일시                | Facility.Priority | Host name | Program name | syslogTag    | message                                                                                              | dic |
|---------------------|-------------------|-----------|--------------|--------------|------------------------------------------------------------------------------------------------------|-----|
| 2025-03-25 11:36:03 | auth.info         | privacy   | sshd         | sshd[42287]: | Connection closed by invalid user lsi 92.118.39.101 port 49424 [preauth]                             | -   |
| 2025-03-25 11:36:01 | auth.info         | privacy   | sshd         | sshd[42287]: | Failed password for invalid user lsi from 92.118.39.101 port 49424 ssh2                              | -   |
| 2025-03-25 11:35:59 | local10.notice    |           |              |              | nix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= 92.118.39.101           | -   |
| 2025-03-25 11:35:59 | auth.info         |           |              |              | nix(sshd:auth): check pass; user unknown                                                             | -   |
| 2025-03-25 11:29:44 | auth.info         |           |              |              | user lsi from 92.118.39.101 port 49424                                                               | -   |
| 2025-03-25 11:29:43 | auth.info         |           |              |              | ction closed by invalid user nlm 162.215.216.231 port 38794 [preauth]                                | -   |
| 2025-03-25 11:29:41 | local10.notice    |           |              |              | password for invalid user nlm from 162.215.216.231 port 38794 ssh2                                   | -   |
| 2025-03-25 11:29:41 | local10.notice    |           |              |              | nix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= 162.215.216.231         | -   |
| 2025-03-25 11:29:41 | auth.info         |           |              |              | nix(sshd:auth): check pass; user unknown                                                             | -   |
| 2025-03-25 11:29:31 | auth.info         |           |              |              | user nlm from 162.215.216.231 port 38794                                                             | -   |
| 2025-03-25 11:29:31 | auth.info         | privacy   | sshd         | sshd[42280]: | ction closed by invalid user global 92.118.39.83 port 51236 [preauth]                                | -   |
| 2025-03-25 11:29:28 | local10.notice    | privacy   | sshd         | sshd[42280]: | Failed password for invalid user global from 92.118.39.83 port 51236 ssh2                            | -   |
| 2025-03-25 11:29:28 | local10.notice    | privacy   | sshd         | sshd[42280]: | pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=92.118.39.83 | -   |
| 2025-03-25 11:29:28 | auth.info         | privacy   | sshd         | sshd[42280]: | pam_unix(sshd:auth): check pass; user unknown                                                        | -   |
| 2025-03-25 11:24:58 | auth.info         | privacy   | sshd         | sshd[42277]: | Invalid user global from 92.118.39.83 port 51236                                                     | -   |
| 2025-03-25 11:24:56 | auth.info         | privacy   | sshd         | sshd[42277]: | Connection closed by invalid user sshuser 212.122.192.241 port 57698 [preauth]                       | -   |
|                     |                   |           |              |              | Failed password for invalid user sshuser from 212.122.192.241 port 57698 ssh2                        | -   |

전체

Message :

발생일 :

검색

RSYSLOG 상세

발생 일시

2025-03-25 11:35:59

facility/priority

local10.notice

hostname

privacy

program name

sshd

syslogTag

sshd[42282]:

message

pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=162.215.216.231

닫기

RSYSLOG 상세 조회 화면

# 소명 기능 지원

확인

소명 상세 정보

조치

소명 재요청

탐지된 개인정보 로그에 대한 사용자 소명 기능으로 보호조치를 극대화합니다.

### 대기 중인 소명

소명 요청 후 대기 중인 항목을 관리하고 재요청 또는 예외 처리를 진행합니다.

총 대기 건수

54

평균 대기 일수

181일

긴급 처리 (14일 초과)

52

7일 이내

0

검색

파일명, 소명코드, 이름 검색...

우선순위

모든 우선순위

요청일 시작

연도-월-일

요청일 끝

연도-월-일

필터 초기화

검색

| <input type="checkbox"/> | 파일명                                                     | 개인정보 유형 | 소명자 정보                              | 요청일           | 우선순위      | 액션                                                  |
|--------------------------|---------------------------------------------------------|---------|-------------------------------------|---------------|-----------|-----------------------------------------------------|
| <input type="checkbox"/> | D:/DataSecure/PrivacyInfo/sample/신용카드.txt<br>GD10236596 | 카드번호    | 소명자 미지정<br>소명자 이메일 없음<br>소명자 연락처 없음 | 2025. 03. 07. | 긴급 (220일) | <div> <div> <div> </div> </div> <div> </div> </div> |
| <input type="checkbox"/> | D:/DataSecure/PrivacyInfo/sample/신용카드.txt<br>PR53449407 | 카드번호    | 소명자 미지정<br>소명자 이메일 없음<br>소명자 연락처 없음 | 2025. 03. 07. | 긴급 (220일) | <div> <div> <div> </div> </div> <div> </div> </div> |

### 소명 상세 정보

기본 정보

파일명  
D:/DataSecure/PrivacyInfo/sample/신용카드.txt

소명 코드  
GD10236596

요청일  
2025. 03. 07.

대기 기간  
220일

우선순위  
긴급 (220일)

개인정보 정보

탐지된 개인정보  
3542-9746-2163-2719

개인정보 유형  
카드번호

소명자 정보

이름  
소명자 미지정

이메일

빠른 액션

재요청

예외 처리

대기 중인 소명 목록 · 소명 상세 정보 및 재요청

# Thank You!

놀라운 정확도의 개인정보 로그 분석, 오/과탐 로그 Out!