HM COMPANY™

AI · ACCURACY · AUDIT · AUTHORITY

디지털 흔적을 수집하고 분석해 사실관계를 확인합니다

본부 소개서

디지털포렌식서비스본부 (ADFS)

KOLAS 국제공인 · 디지털포렌식 전문

hmcom.co.kr | hmadfs.com | 02-6237-6213

This document is confidential and was prepared by HM Company solely for the use of our client; it is not to be relied on by any 3rd party without HM Company's prior written consent.

CONTENTS

목차

I	디지털 증거를 둘러싼 환경 The Environment of Digital Evidence	03
II	ADFS 본부 소개 About ADFS	08
III	조사·진단 서비스 Investigation & Diagnostic Services	18
IV	AI 플랫폼 및 제품 AI Platform & Products	37
V	교육·컨설팅 Education & Consulting	42
VI	수행 실적 및 문의 Track Record & Contact	44

I. 디지털 증거를 둘러싼 환경

The Environment of Digital Evidence

2025년 검거된 기술유출 범죄 179건 중 82.7%가 내부 임직원에 의한 유출이었습니다. 규제는 강화되고, 디지털 증거의 요건은 정교해지고 있습니다.

⚠ 기술유출·정보유출 현황

- 2025년 검거 기술유출 범죄 중 내부 임직원에 의한 유출 **82.7%**
- 2020~2025.6 산업기술 유출 피해 추산 **23.3조원**
- 2021~2025.10 개인정보 누적 유출 **1.55억 건** 이상

규제 환경의 변화

- 고의 영업비밀 유출 시 최대 5배 배상 · 2024.08 시행
- 전자증거 보전요청 제도 · 2026.07 시행
- K-디스커버리 자료보전명령·전문가 사실조사 · 2028.02 시행 예정

기업·법률대리인의 과제

- 기업 - 수집 절차 오류, 매체 확대, 무결성 입증
- 법률대리인 - 증거능력 설명 부담, 상대방 자료 검증
- 소송 기업의 73%가 증거 확보에 어려움 · 특허청 (2025)

유출은 내부에서 발생하고 규제는 강화되고 있습니다. 이때 증거능력은 수집 단계의 절차가 좌우합니다.

기술유출·정보유출 현황

기업의 내부 비리, 기술 유출, 정보 침해 사고에서 디지털 증거는 조사와 대응의 핵심입니다. 내부자는 회사 자료에 대한 접근 권한을 보유하고 있어 주요 유출 위험 주체가 될 수 있습니다

179건

2025년 기술유출 범죄 검거 건수 (전년 대비 45.5%↑)

경찰청(2025)

82.7%

2025년 기술유출 중 내부 임직원에 의한 유출 비율

경찰청(2025)

23.3조원

2020~2025.6 산업기술 유출 피해 추산

산업통상자원부·국가정보원(2026)

개인정보 유출 규모

1.55억건 이상

2021~2025.10 국내 누적 건수

개인정보보호위원회(2025)

13배

2024년 593만 → 2025년 7,516만

개인정보보호위원회(2025)

3.0건

국민 1인당 평균 개인정보 유출 횟수

머니투데이(2025.12)

주요 기업비밀 유출 경로

외부저장매체	영업비밀·협력사 공동 개발 자료를 개인 USB 등으로 반출
이메일	이직 준비 중 회사 업무자료를 개인 이메일로 전송
클라우드	업무용 PC에서 개인 클라우드 계정에 대외비 자료 업로드
상용 메신저	전 직장 동료·외부 관계자 요청으로 고객사 연구 결과 전달
모바일 기기	업무시스템 화면 또는 기업비밀 자료를 휴대전화로 촬영

내부자 유출은 이직·퇴직 과정뿐 아니라 업무 편의, 재택·외근, 협력사 공유 등 일상적인 업무 환경에서도 발생합니다.

규제 환경의 변화

처벌은 강화되고, 증거 보전과 전문가 조사에 관한 관련 제도가 도입되었거나 시행이 예정되어 있습니다.

2024.08
부정경쟁방지법
고의 유출 시 실제 피해액의 최대 5배 배상

2025.02
전자금융감독규정
이사회 보고 의무화 · IT 내부통제 점검 표준화

2025.07
산업기술보호법
무단 삭제·훼손만으로 최대 징역 10년

2026.07
형사소송법 §215-2
전자증거 보전요청 제도 도입

2026.09
개인정보 보호법
반복·중대 위반 시 징벌적 과징금 확대

2028.02
상생협력법 K-디스커버리
자료보전명령·전문가 사실조사 신설

K-디스커버리 3대 제도

자료보전명령 - 상대방에게 증거 훼손·변경 금지 명령 신청

전문가 사실조사 - 법원 지명 전문가가 사실 조사 수행

당사자 신문 활성화 - 직접 신문 제도 강화

※ 자료보전명령을 위반하여 자료를 고의로 훼손하거나 사용할 수 없게 한 경우 7년 이하의 징역 또는 1억원 이하의 벌금

증거능력의 법적 근거

형사소송법 제313조 - 정보저장매체 기억 문자 등의 진정성립

형사소송법 제308조의2 - 위법수집증거배제 원칙

2016년 개정 후 디지털포렌식 등 객관적 방법으로도 진정성립 증명이 가능해졌습니다.

기업과 법률대리인이 마주한 과제

수집 절차와 보존 방식, 무결성 입증은 디지털 증거의 가치를 좌우합니다.

⚠ 기업이 확인해야 할 사항

- **수집 절차의 적법성**
  절차 요건을 갖추어야 확보한 자료가 증거로 인정됩니다
- **확인 대상 매체의 확대**
  클라우드·모바일 등 확인해야 할 매체가 늘고 있습니다
- **무결성의 입증**
  수집부터 보관까지의 과정을 기록으로 설명할 수 있어야 합니다
- **분석 도구와 인력**
  정밀 분석에는 전용 도구와 전문 인력이 필요합니다

⚖ 법무법인·법률사무소의 과제

- **증거능력의 설명**
  수집·보존 과정의 적법성과 무결성을 법정에서 설명해야 합니다
- **증거 유형의 다양화**
  클라우드·모바일·메신저·로그 등 형태 확대
- **상대 제출 자료의 검토**
  제출 자료의 진위와 취득 경위를 확인할 필요가 있습니다
- **소송 일정 대응**
  확보·분석·보고서 작성을 재판 일정에 맞춰 진행합니다

소송·조사 현장의 부담

73%
소송 기업이 겪는 증거 확보 어려움
특허청·벤처기업협회(2025)

40%
디지털포렌식 분석 의뢰 전년 대비 증가율
대검찰청(2023)

691만 건 이상
2024년 법원 접수 소송 사건 (전년 +3.7%)
법원행정처 사법연감(2024)

기업과 법률대리인이 마주한 과제는 다르지만 해법은 같습니다. 적법한 절차와 전문 역량을 갖춘 포렌식 파트너와 함께라면, 사고 전 위험 식별부터 사고 후 증거 확보·제출까지 일관되게 준비할 수 있습니다.

디지털 증거 주요 요건 및 판례

요건 미준수 시 증거능력이 부정되거나 조사 주체에게 법적 책임이 발생할 수 있습니다.

01 적법절차 준수

사내 규정·사전 동의 등 법적 근거로 조사 권한 확보

2007도 6243 - 취업규칙·제한 키워드 기반 분석, 정당행위·증거능력 인정

02 동일성·무결성

해시값과 취급 이력을 통해 원본과 사본의 동일성·무결성을 확인

2017도 13263 - 원본과 사본 해시값 불일치, 증거능력 전면 부정

03 참여권 등 절차적 권리 고려

수집 전 과정에 대상자·관계인의 참여 기회 제공

대구지법 2023나 320254 - 사전 고지 없는 탐지, 손해배상 책임 인정

04 선별 수집

조사 목적과 직접 관련된 정보만 한정 수집

서울고법 2019나 2032512 - 이메일 포괄 탐색, 부당징계·손해배상 인정

05 진정성립

제313조에 따른 진정성립 증명. 포렌식 등 객관적 방법 인정

2012도 16001 - 작성자 진술거부로 진정성립 미증명, 증거능력 부정

디지털포렌식이 증거가치를 결정한 최근 판례

일자 · 사건번호	쟁점	법원 판단
2024.11.14 2021다 289399	부정취득·사용의 입증 방법	시스템 로그·운영 기록 등 디지털 증거로 입증 인정
2025.02.27 2022도 1864	원본이 없는 사본의 동일성	해시값 비교로 동일성을 증명하여 증거 채택
2024.04.16 2023다 16593	무단 녹음의 증명력	원본성·편집 흔적 검증 없이는 증명력 부족

II. ADFS 본부 소개

About ADFS

2011년 설립 이후 15년, 누적 20,397건의 디지털포렌식 증거물을 처리했습니다. 민간기업 최초로 디지털포렌식 분야 KOLAS 공인시험기관 인정을 획득했습니다.

독립된 외부 전문조직

- 회계감사·소송대리를 수행하지 않는 독립 조사기관
- 사내 조직과 분리된 외부 전문조직으로 조사 수행
- 조사 대상과 이해상충이 없는 제3자 지위 유지

국제표준 기반 분석

- KS Q ISO/IEC 17025 기반 표준 절차로 시험 수행
- 인정범위 내 KOLAS 공인시험성적서 발급 · 인정번호 KT1050
- ILAC-MRA 회원국 간 시험성적서 상호 인정

15년의 수행 경험

- 2011년 설립 이후 누적 증거물 20,397건 이상 처리
- 금융·제조·유통·의료·공공 등 산업 전반 수행 경험
- 보안서약 체결 및 데이터 안전 폐기 · 보안사고 발생 이력 없음 [2026년 9월 기준]

회계감사·소송대리를 수행하지 않는 독립 전문조직으로, 국제표준(ISO/IEC 17025) 기반 분석 체계를 운영합니다.

수행 주체별 검토 관점

디지털 증거 조사는 누가 수행하는가에 따라 결과의 활용 범위가 달라집니다.

구분	회계법인	법무법인	일반 분석기관	HM ADFS
이해상충	외부 회계감사를 함께 수행할 수 있어 내부 데이터 제공 부담	해당 법인이 상대측 소송대리인이 될 가능성 고려 필요	기관별 상이	**회계감사·소송대리를 수행하지 않는 독립 조사기관**
분석 표준	회계 감사 기준 중심	법률 검토 중심	기관 자체 기준에 따른 절차	**KS Q ISO/IEC 17025 기반 표준 절차**
증거능력 입증	기관 자체 보고서. 추가 설명·검증 필요	-	일반 분석 보고서. 기관별 표현 방식 상이	**KOLAS 공인시험성적서 발급 (KT1050)**
국제 효력	별도 신뢰성 검토 필요	-	-	**ILAC-MRA 회원국 간 상호 인정**
조사 범위	재무·회계 데이터	법률 쟁점 및 제출 자료	의뢰 매체 단위 분석	**PC·서버·모바일·클라우드·이메일·메신저·외부저장매체**

※ 기관별 실제 업무 범위와 계약 관계에 따라 달라질 수 있음

독립된 외부 전문조직

회계감사와의 분리

회계감사와 독립되어 내부 데이터를 확인합니다. 외부 회계감사를 수행할 수도 있는 기관에 내부 데이터를 제공하는 부담을 지지 않습니다.

사내 조직과의 독립

내부 조직이 분석한 결과는 이해관계자로부터 객관적 신뢰를 받기 어려울 수 있습니다. 외부 전문조직의 수행으로 신뢰성을 확보합니다.

분쟁 대응 시 조사기관의 독립성

법적 대응에 대비해 독립된 기관의 전문가가 검증합니다. 조사 수행 기관이 상대측 소송대리인이 될 위험을 고려하지 않아도 됩니다.

HM Company 개요

2011년 설립 이후 디지털포렌식 전문성을 기반으로 정보유출 조사, 리스크 진단, IT 감사, 내부감사를 수행해 왔습니다.

회사 개요

설립	2011년 10월 6일 · 국내 최초 디지털포렌식 기반 전문 내부감사 기업
소재지	서울특별시 서초구 효령로70길 36-9 와이엘타워 2·3층
대표전화	02-6237-6233
사업 영역	정보유출 조사 · 리스크 진단 · IT 감사 · 내부감사

경영진

대표이사 조근호	변호사 · 前) 부산고검 검사장
부대표 이용훈	20년 이상 감사·기업진단 · 前) Protiviti Korea Director

본부 담당

박 재 현 상무
본부장 · 前 한국디지털포렌식전문가 협회 회장
jaehyun.park@hmcom.co.kr

이 정 훈 수석
디지털포렌식 조사·진단 실무총괄
jeonghoon.lee@hmcom.co.kr

조직 체계

HM Company (2011년 설립)

ADFS 본부

디지털포렌식서비스

- 디지털포렌식 서비스
- 정보유출 조사
- 정보보호 리스크·개인정보 실태진단
- IT 감사
- KOLAS 공인시험성적서 발급

RAS 본부

Risk Advisory Service

- 컴플라이언스 리스크 진단
- 경영진단·내부감사 · 직장 내 괴롭힘 조사
- 회계감사 외부전문가 조사 · PMA

AI MARU 본부

AI 연구소

- 리걸테크: 수사·증거 분석 AI
- 에듀테크: AI 학습 도구
- LLM 오케스트레이션·RAG
- 데이터 어노테이션 플랫폼 LEAP

ADFS 본부 수행 업무

증거 수집·보존	포렌식 절차 기반 이미징 · 해시 검증으로 원본성 확보
데이터 분석	아티팩트·로그·삭제 데이터 복원 및 매체 간 교차 분석
장비·SW 개발	수집·분석 전용 장비와 감사 솔루션 자체 개발·운용

연혁 및 주요 활동

2011년부터 축적해 온 조사·진단 경험이 ADFS의 기반입니다.

연혁

2011
HM Company 설립
前 행복마루컨설팅
포렌식 기반 조사 시작

2020
자체 솔루션 개발
전산자료 리뷰 플랫폼 등
자체 분석 도구 착수

2022
KOLAS 인정 획득
민간 최초 디지털포렌식
분야 인정 (KT1050)

2022
중소기업 지원사업 선정
기술유출 피해
무료 지원 전문기업

2026
AI 플랫폼 베타 운영
AI Audit Advisor
ListenTips 베타 공개

시기별 주요 활동

2011 ~ 2018
설립 · 업무확대

- 2011.10.6 국내 최초 디지털포렌식 기반 전문 내부감사 기업 설립
- 금융회사 내부감사 등 전문 서비스 제공
- 한림대학교와 포렌식연구센터 설립 · 법무법인 MOU 체결
- 감사솔루션 하이에나 · 헤이즐넛 개발

2018 ~ 2022
전문성 강화 · 서비스 확대

- 「감사 혁신, 포렌식이 답이다」 전문서적 출간
- 기업의 디지털포렌식 활용 컨퍼런스 개최 · 회계법인 MOU 체결
- 정보보안 감사 · 개인정보 실태진단 등 서비스로 확대
- 경찰청 AI 기반 범죄수사 시스템 구축 사업 수주
- 콘텐츠진흥원 클라우드 기반 증거수집 관련 과제 수주
- 2020·2021 디지털포렌식 국제대회 테크대상·챌린지 최우수상

2022 ~ 현재
공인 · AI 전환

- 2022.09 디지털포렌식 분야 KOLAS 국제공인시험기관 인정 (민간 최초)
- IITP 디지털증거 증명력 제고를 위한 인과관계 추론 과제 수주
- 중소기업 기술보호 디지털포렌식 지원단 선정
- A&C Tech 기업 선정 · eGISEC 보안엑스포 부스 운영
- 국내 최초 온라인 내부감사 경진대회 개최 (w. 한국감사협회)
- tvN 드라마 「감사합니다」 자문 · LLM 기반 컨설팅 시작

최근 주요 활동

디지털데이터 기반 조사의 필요성을 알리고 전문성을 축적하기 위한 활동을 지속해 왔습니다.

일자	내용	출처
2026.08.25	AI 익명 제보 채널 'ListenTips' 정식 출시 - 접수 이후 조사 실무까지 보조	이투뉴스
2026.06.15	AI 기반 내부감사 자문·자동화 플랫폼 'AI Audit Advisor' 베타 운영	이투뉴스
2026.06.12	AI 기반 익명 제보 채널 'ListenTips' 베타 서비스 운영	세계비즈
2025.11.24	AI·디지털 데이터 기반 감사 능력 강화 · 2025 내부감사 경진대회 성황리 종료	아주경제
2025.09.24	투명경영이 곧 경쟁력 · 기업 외부제보채널 도입 확산	뉴스로드
2024.10.10	국내 주요 대기업·로펌과 리뷰 플랫폼 'HYENA' 공급 계약 체결	서울신문

협력 · 연구 · 교육

산학협력

한림대학교 합동연구센터 · 포렌식·수사 AI 공동 연구

협회 활동

(사)한국디지털포렌식전문가협회와 기술개발·전문가 양성 주도

교육 활동

기업·공공기관·연구소 대상 수집·분석 방법론 교육

국제협력

영국 포츠머스대학·네덜란드 위트레흐트대학과 국제 공동연구

KOLAS 공인시험기관

국가 수사기관도 적용하는 ISO/IEC 17025에 따라 인정받은, 민간 최초의 공인시험기관입니다.

인정 현황

KOLAS 공인시험기관 인정

인정 기구 - KOLAS (한국인정기구, 국가기술표준원)

인정번호 - KT1050

인정 범위 - 모바일·디스크 데이터 획득 및 디지털 데이터 분석

적용 표준 - KS Q ISO/IEC 17025

인정의 의미

국제표준에 따른 시험 절차와 품질 관리 체계 운영

공인된 시험 절차와 품질관리 체계에 따른 신뢰성

분석 절차 이의 제기 시 시험 절차와 검증 기록을 근거로 설명 가능

이해관계 없는 제3자의 객관적 분석 결과 제공

국내 디지털포렌식 분야 KOLAS 인정기관

구분	기관명	인정 항목
민간	**에이치엠컴퍼니**	**모바일·디스크 획득 및 디지털 데이터 분석**
공공	사법기관	디지털·모바일 데이터 획득
공공	수사기관	저장매체·모바일 획득 및 증거 분석
민간	디지털포렌식 전문기업 A	컴퓨터·모바일 디지털포렌식
공공	국가 연구기관	저장매체 데이터 획득
민간	디지털포렌식 전문기업 B	모바일·디스크 획득·분석, 물리복구

디지털포렌식 분야 KOLAS 인정은 공공 수사·사법기관 및 전문기관을 중심으로 제한적으로 이루어지고 있습니다.
HM Company는 민간 분야 최초로 해당 인정을 획득하였습니다.

인정 범위 및 적용 규격

데이터 획득

HDD·SSD·USB 등 저장매체와
iOS·Android 모바일 기기 대상

데이터 분석

아티팩트·로그 분석 및 삭제 데이터
복구·결과 검증

데이터 검증

해시값 대조로 원본 동일성·무결성 확인

적용 규격

KS Q ISO/IEC 17025:2017 · ILAC-MRA
상호 인정

조직 및 전문 인력

수사기법을 확보한 변호사, 기업을 이해하는 회계사·경영컨설턴트, 디지털데이터 수집·분석 전문가가 협업합니다.

3대 핵심 역량의 결합

법률 · 수사 관점

변호사

서류조사·관련자 면담 등 수사

경영·회계 분석

회계사

회계·법령 지식 기반 분석

디지털 수집·분석

포렌식 전문가

디지털데이터 수집·분석

역량 확보 3단계

01 초기 구성	변호사·회계사·경영컨설턴트·포렌식 전문가의 협업
02 노하우 확보	다양한 기업 수행을 통해 자체 방법론 발전
03 전문 인력 및 기술체계 고도화	전문 SW·장비 확보와 자체 개발로 기술 주도

경영진 · 기술고문

조 근 호	**대표이사 · 변호사**	前 부산고등검찰청 검사장 · 법무연수원장
이 용 훈	**부대표**	前 Protiviti · A.T. Kearney
Joshua I. James	**기술고문**	UNODC 컨설턴트 · INTERPOL 트레이너 · 더블린대 박사

본부 담당

박 재 현 상무

디지털포렌식서비스본부 본부장

· 前 한국디지털포렌식전문가협회 회장

· KOLAS 평가사보 · 기술전문가

jaehyun.park@hmcom.co.kr

이 정 훈 수석

디지털포렌식서비스본부 조사 총괄

· 前 한국저작권위원회 감정포렌식팀

· KOLAS 평가사보 · 기술전문가

jeonghoon.lee@hmcom.co.kr

연계 전문 조직

디지털포렌식팀	디지털포렌식 전문가 중심으로 데이터 수집·분석 수행
AI 연구팀	LLM 기반 서비스 개발 (AI 범죄수사 지원, 디지털증거 증명력 제고, EduTech 등) · 박경재 이사
내부감사팀 (RAS)	회계사 중심으로 경영 및 회계 데이터 수집·분석 · 양해원 상무 (KICPA)

분석 대상 매체

다양한 디지털 매체로부터 적법한 포렌식 절차에 따라 증거를 수집하고 분석합니다. 각 매체 특성에 맞는 수집 방법론을 적용합니다.

PC / 서버

- 파일 시스템 분석
- 레지스트리·이벤트 로그
- 파일 삭제 이력
- 프로그램 실행 이력

모바일 기기

- 통화·메신저·웹 기록
- 미디어 파일
- 앱 데이터 분석

삭제 데이터의 복구 가능성 검토

이메일

- 백업 파일 (PST·OST·EML)
- 웹메일 이용 기록
- 첨부파일 분석
- 송·수신 이력 추적

클라우드

- Google Drive·OneDrive
- 네이버 MYBOX 등
- 업로드·다운로드 이력
- 동기화 기록 분석

외부저장매체

- USB·외장HDD 연결 이력
- 파일 복사 흔적 추적
- 장치 시리얼 번호 확인
- 사용 타임라인 분석

데이터베이스

- DB 접근 로그 분석
- 쿼리 실행 이력 추적
- 데이터 변경 기록
- 권한 변경 이력 확인

매체에서 확인 가능한 흔적

연결·해제 기록

장치 시리얼 번호 · 인가 여부

삭제·은닉 데이터

복구 가능 영역 · 은닉 경로

파일 접근·실행 흔적

시간순 재구성 · 반출 정황

근접 무선 전송

AirDrop · Quick Share 사용 흔적 검토

> 단일 매체별 분석에 그치지 않고, 매체별 흔적을 교차 분석하여 자료 반출 흐름을 재구성합니다.

표준 프로세스 및 산출물

적법한 권한과 조사 범위를 확인한 뒤, 수집부터 보고까지 표준 절차로 진행합니다.

STEP 01 사전 협의	STEP 02 수집·이미징	STEP 03 검증·보존	STEP 04 정밀 분석	STEP 05 결과 보고
조사 목적·범위 협의 대상자 동의·정당한 권한 확인 비밀유지서약(NDA) 체결	쓰기방지장치로 원본 훼손 차단 비트 단위 사본(이미징) 생성 전자정보 확인서 작성	SHA-256 해시값 산출 원본·사본 동일성 확인 증거물 봉인과 이송 관리	삭제 파일 복구 사용 흔적과 이력 분석 키워드 검색·타임라인 분석	분석 결과 보고서 작성 공인시험성적서 발급 연계

Step 4. 데이터 분석 상세

연관관계·타임라인

업무시스템·문서·이메일 연관관계
타임라인 분석

은닉·삭제 추적

은닉 데이터 추적 및 분석
삭제 파일 복원

선별 탐색

핵심 키워드 검색
인터넷 접속기록 분석

수집 대상

ERP·GW 등 업무시스템, PC
USB 등 이동식 저장장치

최종 산출물

분석 보고서

법정 제출용 전문 보고서. 증거 분석 결과와 전문가 소견

해시값 검증 확인서

SHA-256 기반 원본 동일성 입증 문서

Chain of Custody 이력서

증거 인계·인수 및 이동·보관 연속 기록

KOLAS 공인시험성적서

인정범위 내 항목의 공인시험 결과 (KT1050)

적용 대상별 초점

기업

조사 목적에 필요한 범위에서 부정·비리 사실관계를 확인하고 재발 방지 근거를 확보

로펌

소송 단계에서 제출할 증거의 증거능력과 신뢰성을 확보

개인

개인정보 보호를 전제로 필요한 범위만 선별 수집·분석

장비 및 분석 환경

전문 장비와 분석도구를 활용해 데이터를 수집·분석합니다. 자체 개발 SW를 포함해 수집부터 리뷰까지 전 단계를 지원합니다.

데이터 수집 도구

업무용 PC 저장장치(HDD·SSD)를 증거수집 절차에 따라 이미징

해시값 계산 등 증거능력 확보 절차 수행 (무결성·원본성 보장)

적용 가능한 저장매체 수집 시 하드웨어 쓰기방지장치(Write-Blocker) 사용

수집 전용 장비



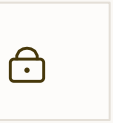
Falcon-NEO2 · 고속 이미징 장비

현장에서 원본 저장장치를 무결성이 유지된 상태로 고속 이미징. 수집 전·후 해시값 일치를 검증해 원본성을 입증합니다.



Cellebrite UFED · 모바일 포렌식 도구

iOS·Android 단말의 논리·물리 데이터를 표준 절차로 획득합니다. 통화·메신저·앱 데이터를 분석하고, 기기·OS 및 도구 지원 범위에서 삭제 데이터의 추출·분석을 수행합니다.



Write-Blocker · 하드웨어 쓰기방지장치

수집 과정에서 원본 매체에 대한 쓰기를 물리적으로 차단합니다. 장비 대여·임대 등 필요한 형태로 운용할 수 있습니다.

데이터 분석 도구

이미징 파일 상태 확인, 삭제 파일 복구, 파일 추출 환경 구축

키워드 검색 및 주요 아티팩트(접속기록·레지스트리) 분석

검증된 분석도구 활용 및 복수 도구 교차 검증
- 주요 활용 프로그램: Hyena eAudit (자체 개발 SW), Axiom, EnCase 등

분석 환경 통제

전문 포렌식 분석실

격리된 분석 환경·무결성 보장 체계 운영, 내부 품질관리 병행

품질 보증 체계

분석 결과 검토·승인 및 재현성 검증으로 결과 일관성 확보

자체 개발 역량

감사솔루션 하이에나·헤이즐넛을 자체 개발하였으며, 기술연구소에서 수집·분석 SW와 장비 개발을 지속하고 있습니다.

증거물 보안 통제

반입·반출 통제	증거물은 지정 보관함에서만 관리
접근 이력 기록	취급자·시점·목적을 전 건 기록
종결 후 안전 폐기	보안서약 체결 및 데이터 완전 삭제

III. 조사·진단 서비스

Investigation & Diagnostic Services

정보유출 조사부터 KOLAS 공인시험성적서 발급까지 6개 서비스를 제공합니다. 각 서비스는 필요성 · 방법론 · 절차 세 단계로 구성했습니다.

조사 서비스

- 정보유출 조사 - 매체별 흔적 교차 분석으로 반출 흐름 재구성
- 디지털포렌식 서비스 - 수집·보존부터 법정 제출 지원까지
- 개인 대상 포렌식 - 필요한 범위만 선별 수집·분석

진단 서비스

- 정보보호 리스크 사전진단 - 사고 발생 전 위험 영역 식별
- 수탁사 개인정보 실태진단 - 취급자 단말·저장소 직접 분석
- IT 감사·내부통제 진단 - 로그·운영 데이터로 실증 검증

KOLAS 공인시험

- KOLAS 공인시험성적서 발급 · 인정번호 KT1050
- 민간기업 최초 디지털포렌식 분야 인정 획득
- 인정범위 - 디스크·모바일 데이터 획득 및 분석

조사는 사후 사실 확인, 진단은 사전 위험 확인, 공인성적서는 결과의 대외 공신력 확보를 목적으로 합니다.

서비스 목록

조사, 진단, 공인시험, 그리고 솔루션까지 4개 영역에서 기업의 사실확인을 지원합니다.

조사 서비스

사실관계 확인이 필요할 때

- 디지털포렌식 증거 수집·보존
- 정보유출 조사
- 개인 대상 포렌식

진단 서비스

사고가 드러나기 전에

- 정보보호 리스크 사전진단
- 수탁사 개인정보 실태진단
- 정보보안 감사 · IT 감사

공인시험 서비스

표준 절차에 따른 공인시험 결과가 필요할 때

- KOLAS 공인시험성적서 발급
- 민간 최초 디지털포렌식 분야
- 공인시험기관 (KT1050)

포렌식 솔루션

분석 도구가 필요할 때

- Walnut · 카카오톡 복호화
- HYENA · 전산자료 리뷰
- AAA · AI 내부감사 자동화

서비스 선택 기준

자료가 밖으로 나간 정황이 있다	→ **조사 서비스**
사고 전에 취약점을 확인하고 싶다	→ **진단 서비스**
분석 결과를 대외에 제시해야 한다	→ **공인시험 서비스**
사내에서 직접 분석하고 싶다	→ **포렌식 솔루션**

수행 절차

1. **문의·상담**
2. **범위 협의**
3. **수행**
4. **결과 보고**
5. **개선 지원**

모든 조사는 대상자·소지자의 동의 또는 기업의 정당한 권한과 절차를 전제로 수행합니다.

정보유출 조사

서버·PC·외부저장매체·모바일·이메일·메신저·클라우드 등 주요 유출경로를 통합 분석하여 반출 경로와 관련 정황을 확인

조사 방법론 5종

01 외부저장매체

연결/해제 기록, 시리얼 확인, 관리대장 대조, 반출 타임라인 재구성

02 이메일

송수신 이력, 삭제 메일 복구, 자동 전달 규칙·위임 권한 식별

03 웹·클라우드

접속·계정 이력, 동기화 폴더·캐시, 공유 링크 생성 흔적

04 상용 메신저

대화 복원, 전송 파일 추출, 계정·기기·로그인 이력 식별

05 모바일 기기

통화·녹음 STT·메신저 로컬 DB, OCR·EXIF 분석, AirDrop 등 근접 전송 이력

조사 절차

Step 1. 기초 데이터 분석

1 사전 조사·범위 정의 › 2 분석 데이터 수집 › 3 데이터 분석

Step 2. 대상자 심층 조사

4 심층 조사 대상자 선정 › 5 인터뷰 및 포렌식 추가 분석

도입 효과

유출 피해 최소화

서버·PC 무단 반출 정황 확인 및 대응

신속한 원인 파악

메일·메신저·클라우드 경로 신속 확인

유출 경로 식별

실제·잠재 경로 식별 → 보안정책 개선

법적 대응 근거

법규·증거 절차 준수, 분쟁 대응 근거

조사 수행의 전제

매체 교차 분석

단일 매체 분석에 그치지 않고 매체 간 흔적을 대조해 반출 흐름을 재구성

중소기업 지원사업 수행

중소기업 기술유출 피해 무료 지원사업 전문기업 선정 (2022년~)

법규·증거 절차 준수

적법한 권한과 절차를 전제로 수집하여 증거능력을 확보

조사 방법론 5종

매체별 흔적을 교차 분석하여 자료 반출 흐름을 재구성합니다. 모든 방법론은 수집·보존 → 복원·파싱 → 통합 교차분석 → 상관분석 및 결과 보고의 4단계를 공통 적용합니다.

01 외부저장매체 분석

외부저장매체는 연결되는 순간부터 시스템에 사용 흔적을 남깁니다.

- **장치 식별**
  USB·외장 SSD·SD·MTP 연결/해제 기록, 장치명·시리얼 번호 확인, 사내 관리대장 대조로 인가 여부 확인
- **사용 흔적**
  외부저장매체에서 생성·접근한 폴더 이력, 생성·실행된 파일 목록 확인
- **유출 흔적**
  연결 시점 전후 행위를 타임라인으로 재구성해 반출 정황 분석

02 이메일 분석

발송· 메일, 자동 전달·외부 계정 전송 메일도 흔적을 남길 수 있습니다.

- **송수신 이력**
  발신자·수신자·일시·제목·본문·첨부파일 확인. 메일 시스템·웹메일·로컬 백업에서 기록 추출
- **삭제 메일 복구**
  이메일·첨부파일의 복구 가능성을 검토하고 가능한 범위에서 복원, 휴지통 비우기·완전삭제 등 은폐 시도 흔적 확인
- **외부 전송**
  자동 전달 규칙·위임 권한 등 지속적 유출 채널 식별, 첨부파일 해시값·메타데이터 대조

03 웹·클라우드 분석

개인 클라우드 업로드도 브라우저 기록·동기화 폴더·캐시·계정 로그에 남습니다.

- **접속·계정 이력**
  브라우저 방문 기록·검색어·다운로드 목록, 외부 서비스 로그인 계정·접속 IP·일시 확인
- **업로드·동기화**
  OneDrive·Google Drive·Dropbox 등 동기화 폴더 및 캐시 분석, 업로드·수정·삭제 이력
- **유출 흔적**
  공유 링크 생성·접근 권한 부여 등 외부 채널 식별, 사내 원본 문서와 대조하여 동일성 확인

04 상용 메신저 분석

카카오톡·텔레그램 등은 대화 한 번으로 자료가 외부로 전달되는 대표적 유출 경로입니다.

대화 내역

· PC·모바일 송수신 대화 복원

· 삭제 메시지·대화방 복원 · 키워드 분석

전송 파일

· 문서·이미지·압축파일 추출

· 사내 원본 대조로 기업비밀 선별

계정·기기

· 메신저 계정·기기·로그인 이력

· PC·모바일 동기화 · 외부 대화 상관 분석

05 모바일 기기 분석

개인 모바일 단말은 기업 보안 솔루션(MDM·DLP)의 통제 범위 밖에서 활용되는 경우가 많습니다.

통화·메신저

· 통화 이력·주소록 분석

· 녹음 파일 STT 변환 · 키워드 분석

· 메신저 로컬 DB 추출·복호화

웹·미디어

· 웹 탐색·다운로드 기록 분석

· OCR로 촬영 문서 텍스트 추출

· EXIF 메타데이터로 사내 촬영 판단

기타 채널

· AirDrop·Quick Share 근접 전송

· 생성형 AI 앱 사용·프롬프트 기록

· MDM 우회 · 탈옥·루팅 정황

정보유출 사례

세 사례 모두 정당한 접근 권한을 가진 내부자가 주체였고, 단순 열람만으로는 유출 위험을 식별하기 어려운 구조였습니다.

화장품 레시피 이직 유출

재직 중 접근 › 레시피 반출 › 경쟁사 이직

경쟁사 매출 **460억원**

유출 레시피 기반 신제품 출시 후 경쟁사 B사의 1년 내 매출

화장품 A사 R&D 연구원 2명이 경쟁사 B사로 이직하며, 재직 중 정당한 권한으로 접근한 레시피 등 영업비밀을 반출. 대법원 2024년 1월 유죄 확정.

산업	화장품
유형	영업비밀 침해(부정경쟁방지법)
기간	2018 이직 ~ 2024.1 판결
결과	대법원 유죄 확정 · 징역 6~10개월

미탐지 원인. 정상 권한에 가려진 이상 행위 / 이직 전후 점검 부재 / 반출 경로 미확인 (EBN)

차량 성능시험 자료 유출

기술자료 확보 › 개인 클라우드 › 본인 메일 전송

미탐지 기간 **4년 이상**

유출 시점부터 적발까지. 외부 클라우드·메일에 장기 보관되었으나 미탐지

C사 남양연구소 전 연구원이 2020년 12월 퇴직 직전 차량 성능시험 자료와 엔진 개발 노하우를 개인 네이버 클라우드·본인 메일로 반출.

산업	자동차 (제조)
유형	영업비밀 침해 및 업무상 배임
기간	2020.12 유출 ~ 2025.5 판결
결과	징역 1년 6개월 · 법정구속

미탐지 원인. 개인 클라우드·메일 통제 한계 / 정상 권한에 가려진 정황 / 퇴직 시점 분석 부재 (경기신문)

디스플레이 양산기술 촬영 유출

양산 설계도면 › 스마트폰 촬영 › 해외 이직

유출 대상 공정 투자 규모 **5조원**

광저우 OLED 양산공정 투자 규모. 핵심기술이 촬영으로 해외 유출

E사 광저우 공장에서 20년 이상 OLED를 담당한 팀장급 인재가 2020년 중국 업체로 이직하며 양산 설계도면 등 핵심기술을 촬영해 유출.

산업	디스플레이 · 국가핵심기술
유형	산업기술 유출 및 영업비밀 침해
기간	2020 이직 ~ 2024.8 기소
결과	2명 구속기소 · 1명 불구속기소

미탐지 원인. 물리 촬영 통제 한계 / 핵심인재 정상 권한 접근 / 이직·공모 분석 부재 (머니투데이)

공개 사례에 HM ADFS 조사방법론을 적용할 경우의 공통 검토 항목

접근·복사·반출 이력 재구성

자료 접근·복사·반출을 시간순으로 재구성

외부 전송 흔적 분석

메신저·메일·클라우드·USB·인쇄 흔적 종합 검증

비정상 행위 및 삭제 데이터

야간·주말 접근, 대량 열람 식별 · 삭제 파일 복원

정보보호 리스크 사전진단

사고가 발생한 뒤가 아니라, 발생 전에 위험 영역을 식별하고 보완합니다.

01 문서·데이터 관리실태

· 외부저장매체 - 연결·사용 흔적, 관리대장 대조

· 이메일·메신저 - 개인 계정 전송·자동 전달 규칙

· 인쇄·출력 - 로그·스풀 흔적, 이상 패턴 평가

· 웹·클라우드 - 접속·동기화 흔적, 업로드 이력

02 보안 솔루션 실효성

· 인가자 우회 - 인가 매체 반출, 예외 경로 활용

· 외부자 우회 - 자격증명 탈취, API Key·토큰 유출

· 신종 채널 - AirDrop·P2P·공유 링크 등 비정형 전송 경로

· 솔루션 회피 - 확장자 변경·암호화·압축 탐지 회피

03 정보보안 리스크 분석

· 핵심 데이터 - 식별·보유 위치 매핑, 등급별 권한

· 임직원 행위 - 접근·다운로드·전송 이상 패턴

· 협력사·외주 - 접근·반출 흐름, NDA 범위 대조

· 사각지대 - 개인 단말·원격 접속, 물리 반출

진단 절차

1 범위 정의 › 2 데이터 수집 › 3 위험 정황 식별 › 4 심층 진단 대상 선정 › 5 심층 진단·개선안 도출

도입 효과

유출 위험 사전 차단
무단 반출 위험 식별

잠재 위험 영역 식별
유출 경로 사전 점검

법적·규제 리스크 대응
법규 준수 수준 점검

부정행위 리스크 식별
이상 행위 사전 인지

진단 방법론 3종

각 방법론은 대상 식별 → 위험·우회 가능성 검증 → 결과 정리 → 개선방안 제시의 4단계를 공통으로 적용합니다.

01 문서·데이터 관리실태 진단

문서·이메일·저장소가 보안 정책대로 관리되는지, 정책을 우회하거나 회피한 정황까지 함께 진단합니다.

- **외부저장매체**
  USB·외장 SSD·SD카드 연결 및 사용 흔적, 사내 관리대장 대조로 인가 매체 여부 확인
- **이메일·메신저**
  개인 계정 전송 및 자동 전달 규칙, 로컬 백업파일·웹메일·사내 메신저 다채널 통합 분석
- **인쇄·출력**
  인쇄 작업 로그 및 스풀 흔적, 시간대·문서 유형·사용자별 인쇄량 기준 이상 패턴 평가
- **문서 정책 준수**
  대외비·기밀 분류, 보관기간, 접근권한 준수 여부, 분류 누락·권한 외 공유 식별
- **웹·클라우드**
  외부 클라우드 접속 기록 및 동기화 흔적, 업로드·다운로드 이력 및 이상 패턴

실제 사례. 보관기간 초과 파일 잔존 / 대외비 권한 외 보관 / 미인가 외부 전송 / 메신저 로그 평문 저장

02 보안 솔루션 실효성 진단

DLP·DRM·방화벽·MDM 등 보안 솔루션이 정책 설계 의도대로 작동하는지 실제 데이터 기반으로 검증합니다.

- **인가자 우회**
  인가 매체를 이용한 무단 반출 및 인가 클라우드 외부 동기화, 화이트리스트·예외 경로 활용
- **외부자 우회**
  사회공학을 통한 자격증명 탈취, 만료·위임 권한 악용, API Key·OAuth 토큰 외부 유출
- **신종 채널**
  생성형 AI 입력, 이미지 OCR 우회, VDI 스크린샷·재촬영 / AirDrop·P2P·공유 링크
- **솔루션 회피**
  확장자 변경, 구조 변환, 암호화·분할·압축·인코딩 탐지 회피, 예외 경로 내 영업비밀 저장

실제 사례. 캡처 후 이미지 변환 보관 / 압축·암호화로 DLP 우회 / AI 프롬프트에 대외비 입력 / 퇴직자 권한 미회수

03 정보보안 리스크 분석

영업비밀·설계자료·연구자료 등 핵심 데이터의 유출·훼손 위험을 협력사·외주 접근 흐름까지 진단합니다.

- **핵심 데이터**
  영업비밀·개인정보·설계자료 식별 및 보유 위치 매핑, 민감도 등급별 접근권한·보유기간 적정성
- **임직원 행위**
  접근·다운로드·전송 등 이상 행위 패턴 식별, 퇴사 예정자 및 권한자의 비정상 활용 정황
- **협력사·외주**
  데이터 접근 및 반출 흐름 진단, 위탁계약 및 NDA 적용 범위와 실제 사용 정황 대조
- **사각지대**
  개인 단말·원격 접속 등 관리 사각지대 위험 평가, 물리 반출·촬영·출력 등 비정형 채널

실제 사례. 위탁 계약 외 데이터 처리 / NDA 범위 밖 정보 사용 / 퇴직 예정자 대량 전송 / 기밀자료 출력 반출

디지털 통제를 벗어난 유출 사례

세 사례 모두 보안 솔루션이 작동하고 있었음에도 통제 범위 밖의 행위로 유출이 발생했습니다. 사전진단은 이러한 통제 사각지대를 점검합니다

출력물을 통한 물리적 반출

열흘간 분산 출력 › 은닉 반출 시도 › 출문 게이트 적발

반출 시도 출력량 **3,700여 장**

SOP 175건 · 국가핵심기술 2종. 반출 시도된 출력 문서량

바이오 C사 전 직원이 CDMO SOP 등 영업비밀 175건, A4 약 3,700장을 열흘간 분산 출력해 은닉 반출을 시도하다 출문 게이트에서 적발. 미수였으나 실형이 선고됐습니다.

산업·유형	바이오 / 물리적 반출 시도
기간	2022.12 행위 ~ 2025.7 판결
결과	징역 3년 실형 (미수 단계)

미탐지 원인. 일 단위 임계치만 적용돼 분산 출력 누적 미탐지 / 사전 경보 부재
HM ADFS 분석 관점. 사용자별 누적 출력량 이상치 재구성, 프린트 로그 일별·문서별 분석 (매거진한경)

아날로그 방식의 보안 통제 우회

가맹점주 조회 › 모니터 촬영·전사 › 모집인 전달

유출 개인정보 **192,088명**

3년 2개월 미탐지. 영업점 직원 12명에 의한 개인정보 장기 유출

카드 D사 영업점 직원 12명이 약 3년 2개월간 가맹점주 19만 2,088명의 개인정보를 조회해 모집인에게 전달.
파일 반출 방지 통제와 다운로드 차단이 작동하고 있었음에도, 모니터 촬영과 수기 전사 방식으로 디지털 통제를 우회했습니다.

산업·유형	금융·카드 / 개인정보 유출
기간	2022.3 ~ 2025.5 · 적발 2025.12
결과	개인정보보호위원회 조사 · 12명 징계

미탐지 원인. 아날로그 우회 채널 통제 한계 / 이상 조회 패턴 분석 미흡
HM ADFS 분석 관점. DB 조회 임계치 설정·이상 패턴 탐지, 직무군 대비 누적 조회량 비교 (경향신문)

퇴사자 인증키 미회수

재직 중 발급 › 퇴사 · 미회수 › 5개월간 접근

유출 개인정보 **3,370만 건**

약 5개월간 미인지. 역대 최대 규모 개인정보 유출

이커머스 E사 전 직원이 재직 중 발급받은 인증키로 퇴사 후에도 시스템에 접근해 약 5개월간 3,370만 건을 유출. 퇴사 시 인증키 회수·폐기 절차가 이행되지 않았습니다.

산업·유형	이커머스 / 개인정보 유출
기간	2025.06 ~ 2025.11 · 발표 2025.11
결과	개인정보보호위원회 개선권고 · 경찰 수사

미탐지 원인. 퇴사 시 권한·인증키 회수 점검 부재 / 이상 접근 패턴 분석 미흡
HM ADFS 분석 관점. 인증키·토큰 발급·회수 절차 진단, 시간대·IP·빈도 이상 접근 분석 (한경비즈니스)

수탁사 개인정보 실태진단

서면점검으로 확인하기 어려운 수탁사의 실제 개인정보 처리·보관·전송·삭제 현황을 현장에서 직접 검증합니다.

관련 법령

개인정보보호법 제26조 · 제29조

위탁자는 수탁자를 교육하고 처리현황 진단 등으로 안전한 처리 여부를 감독해야 합니다.
수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 법 위반으로 발생한
손해배상책임에 대해서는 수탁자를 개인정보처리자의 소속 직원으로 봅니다

진단 사례 · 실제 발견사항

배송 업무

카빙 복구 결과 고객정보 잔존 / DRM·암호 없이 평문 보관 / FTP 계정정보 로그 평문 저장

감정평가 업무

NAS 고객정보 암호화 없이 저장 / 취급 권한 없는 사용자 접근 가능 / 메신저 평문 로그

텔레마케팅 업무

탐지 통제 범위 밖 경로 보관 / 미취급자에게 참조 발송 / 녹취 로그 평문 저장

개인정보 유출·노출 잠재 위험요소

매체별 발견사항

보관기간 경과 파일 / DRM 미설정 / 임시 저장 경로에 개인정보 / 로그 평문 저장

보안 솔루션 우회

매체제어 우회 / 확장자 변경·암호화 / VPN 차단 우회 / 사회공학적 권한 취득

보안 정책 운영 점검

NAS 권한 미분리 / 미취급자에게 자료 전달 / 접근 IP 미설정 / 보안씰 미기재

진단 절차

1 프로세스 인터뷰 › 2 체크리스트 › 3 대상자 선정

4 현장 진단 › 5 저장매체 사본 › 6 보고서 작성

개인정보 유·노출 잠재 위험요소

일부 위험 요소는 담당자도 인지하지 못한 임시파일·로그·캐시·백업·공유폴더에 남아 있어 서면점검으로는 식별이 어렵습니다. 실제 PC·서버·클라우드 기준의 현장 정밀진단이 필요합니다.

01 매체별 주요 발견사항

- **개인정보 수집·처리**
  보관기간 경과 파일 보관 / DRM·자체 암호 미설정 / 임시 저장 경로(AppData 등)에 개인정보 존재 / 업무 프로그램 로그에 평문 저장
- **메신저·이메일**
  불필요한 개인정보 포함 메일·대화 보관 / 미취급자에게 본문·첨부 전송 / 경과 메일을 로컬 백업(PST)으로 보관
- **웹사이트·클라우드**
  상용 클라우드(MYBOX·Gmail·OneDrive)에 개인정보 보관 / 브라우저 자동 로그인·계정정보 저장 / 캐시에 개인정보
- **서버**
  퇴사자 계정 미회수로 외부 접근 가능 / URL 파라미터 변조로 로그인 없이 접근 / 운영 로그에 개인정보 자동 기재
- **기타 저장매체**
  완전삭제 미흡으로 파일 복구 / 비인가 매체 전송 이력 / 접근제어 없는 공유 폴더·NAS

02 보안 솔루션 우회 유형

설정 범위·예외 경로·사용자 권한·파일 변환 방식에 따라 우회 가능성이 남으며, 인가 사용자의 비정상 행위를 완전히 막기는 어렵습니다.

- **매체제어 우회**
  USB 동시 연결 또는 빠른 탈부착 반복 / 탐지 범위 밖 매체 사용 / 인가 매체 복사 후 무단 반출
- **파일탐지 우회**
  확장자 변경 또는 암호화 / 스크린샷·구조 변경으로 타 파일 변환 / 예외 설정 경로에 영업비밀 저장
- **웹접속 탐지 우회**
  VPN 등 차단 우회 수법 / 블랙리스트 미포함 URL로 차단 대상 접속
- **사회공학적 우회**
  기망으로 접근 권한 부정 취득 / 만료된 접근 권한 계속 사용

03 보안 정책 운영 점검 유형

서면진단에서 양호한 결과를 받은 수탁사라도 현장에서는 접근권한·보관기준·로그 관리·파기 이행이 제대로 운영되지 않는 사례가 빈번합니다.

- **접근 제어**
  NAS 권한 미분리로 타 업무자가 위탁 개인정보 접근 / 문서중앙화 권한 미분리로 미취급자 접근
- **업무 프로세스**
  미취급 정산 담당자에게 개인정보 자료 전달 / 전자결재에 미취급 임원 포함 / 매뉴얼·양식에 실제 고객정보 기재
- **보안 설정·관리**
  접근 IP 미설정으로 외부 접근 가능 / DRM 범위 미흡으로 사진 등 누락 / 메신저 로그 평문 저장 / 보안씰 시리얼 미기재

HM COMPANY는 정책 설정과 실제 사용자 행위 흔적을 함께 분석해, 보관 상태뿐 아니라 우회 보관·비인가 반출 정황까지 확인합니다.

수탁사 개인정보 관리 실태 진단 사례

체크리스트 중심의 서면진단을 넘어 취급자의 PC·모바일·서버·NAS를 분석해 개인정보의 보관·전송·잔존·파기 상태를 확인한 실제 사례입니다.

배송 업무 01

배송물 전달 대행 · 이름·생년월일·주소 처리

- **완전삭제 (송·수신용 PC)**
  삭제 파일을 카빙 기법으로 복구한 결과 고객 개인정보가 포함된 문서·이미지 파일이 잔존
- **보관기준 (송·수신용 PC)**
  개인정보 포함 업무 파일이 DRM·자체 암호 설정 없이 평문 상태로 보관되고, 약정 보관기간 경과 파일이 미삭제
- **프로그램 (송·수신용 PC)**
  고객정보 송·수신에 사용되는 FTP 계정정보가 로그 파일에 평문으로 저장
- **DB (수탁사 DB)**
  마스킹 기준을 준수하지 않은 개인정보 항목이 테이블 내 존재

배송 업무 02

상품 판매·배송 대행 ·
이름·주소·휴대전화번호 처리

- **DB (택배사 DB)**
  분기별 파기확인서를 수령했음에도 약정 보관기간을 초과한 고객정보가 DB 내 잔존
- **보안솔루션 (담당자 PC)**
  고객정보가 포함된 문서를 이미지 파일로 캡처한 뒤 보안솔루션 탐지 예외 영역에 별도 보관
- **완전삭제 (담당자 PC)**
  파일을 복구한 결과 고객 개인정보가 포함된 문서·이미지 파일이 잔존
- **클라우드 (담당자 PC)**
  부서 공용 클라우드 저장 공간에 고객 개인정보가 포함된 파일이 저장

감정평가 업무

부동산 담보 평가 대행 ·
이름·생년월일·휴대전화번호 처리

- **NAS**
  고객정보가 포함된 파일이 암호화 또는 별도 암호 설정 없이 저장
- **NAS 권한**
  개인정보 취급 권한이 없는 사용자가 NAS 내 개인정보 파일에 접근 가능한 권한 구조 확인
- **메신저 (감정평가사·현장담당자 PC)**
  고객정보를 사내 메신저로 송수신한 대화 내역이 평문 로그 형태로 저장
- **보관기준 (감정평가사·현장담당자 PC)**
  개인정보가 포함된 업무 파일이 DRM 또는 암호 설정 없이 보관

텔레마케팅 업무

금융상품 가입 상담 대행 ·
이름·생년월일·계좌번호 처리

- **보안솔루션 (관리자 PC)**
  개인정보가 포함된 다수 문서가 개인정보 탐지 시스템의 통제 범위를 벗어난 경로에 보관
- **보안기준 (관리자 PC)**
  문서중앙화 솔루션의 탐지 예외 영역에 개인정보 파일이 임시파일 형태로 저장
- **이메일 (관리자 PC)**
  고객정보가 포함된 이메일을 개인정보 미취급자에게 참조 발송
- **프로그램 (상담원 PC)**
  녹취 프로그램 사용 과정에서 생성되는 로그 파일에 고객정보가 평문으로 저장

발견사항은 서면 점검으로는 확인되지 않는 항목으로, 취급자 단말과 저장소를 직접 분석해 확인한 결과입니다.

진단 절차 및 기대효과

사전 협의부터 개선 과제 제시까지 6단계로 진행하며, 위탁사와 수탁사 양측의 관리 수준을 함께 개선할 수 있도록 지원합니다

진단 절차

1 업무 프로세스 인터뷰 › 2 보안 환경 체크리스트 › 3 진단 대상자 선정

4 현장 진단 › 5 저장매체 사본 획득 › 6 분석 보고서 작성

기대효과

위탁사

- 수탁사 보안 리스크 선제적 대응
- 개인정보 관리체계 실효성 강화
- 실제 업무 절차 기준 처리 현황 확인
- 법상 관리·감독 의무 이행 근거

수탁사

- 발견사항별 개선조치로 환경 개선
- 정기 진단으로 보안 인식 제고
- 관리상 문제에 따른 법적·평판 리스크 예방

기존 서면진단과의 차이

기존 수탁사 진단 - 서면·자기진단 중심

- 내부관리계획 문서 점검 위주
- 수탁사 자가진단·체크리스트에 의존
- 실제 매체에 남은 개인정보·우회 보관 발견 어려움
- 실제 개인정보 처리 현황 파악에 한계

HM COMPANY 수탁사 진단 - 실제 매체 기반 정밀진단

- PC·모바일·서버·NAS 등 매체 직접 분석
- 서면 점검 내용 대비 실제 개인정보 현황 비교 검증
- 보안솔루션·서버 등 시스템 취약점 식별
- 유출 위험 분석 및 개선 컨설팅 도출

디지털포렌식 서비스

사건의 절차적 특성과 쟁점에 맞추어 증거 확보, 보존, 분석, 보고서 작성까지 지원합니다.

시나리오별 대응 체계

유형	시나리오	HM ADFS 프로세스
퇴직자 데이터 반출	핵심 인력 퇴사 시 기업 비밀 반출 의심	PC·모바일 이미징 → 외부저장매체·이메일 전송 이력 분석
내부 비리·횡령	회계 부정, 금품 수수 등 내부 비리 의심	이메일·메신저 분석 → 거래 내역 교차 검증 → 보고서 작성
소송 증거 확보	민·형사 소송 중 디지털 증거 제출 요구	적법한 절차에 따른 증거 수집 → CoC 관리 → 법정 증거 제출 지원
정보유출 사고	고객 개인정보·산업기밀 외부 유출 정황	현장 출동 → 유출 경로 추적·범위 파악 → 보고서 작성
K-디스커버리 대응	법원의 자료보전명령·전문가 사실조사 통보	리걸홀드 수립 → 데이터 무결성 사전 확보 → 전문가 조사 지원

소송 유형별 포렌식 지원

영업비밀 침해

USB 연결 이력 · 클라우드 동기화 · 삭제 복구

지식재산권·특허

파일 타임라인 · 실행 이력 · Git 커밋 로그

배임·횡령 형사

전자결제 승인 기록 · ERP 거래내역 분석

명예훼손·프라이버시

SNS 원본 해시 검증 · IP 접속기록 추적

소송 단계별 협업 프로세스

STEP 01 사건 검토 및 전략 수립	쟁점 상담 · 범위·일정·비용 협의 · NDA 체결
STEP 02 증거 확보 및 보존	현장 이미징 · 해시 산출·무결성 검증 · CoC
STEP 03 분석 및 사실관계 정리	KOLAS 공인 도구 · 복구 · 타임라인 재구성
STEP 04 보고서 및 소송 자료	법정 제출용 보고서 · 공인 성적서 발급
STEP 05 법정 지원 및 의견	예상 질의 검토 · 전문가 의견 정리

증거 신뢰성 확보 지원 및 기술 검토

제출 증거의 절차적 정당성과 무결성을 관리하고, 상대방 제출 자료의 기술적 타당성을 검토합니다.

증거 신뢰성 확보

상대방 주장	HM ADFS 사전 대비
"해시값이 일치하지 않는다"	전 과정 해시 로그 보관. 수집·이송·분석·보관단계별 기록 관리
"원본과 사본의 동일성 미입증"	보존 이력 및 절차 기록 관리로원본성·동일성 설명자료 정리
"수집 절차·분석 도구가 부적절"	적법절차 체크리스트 + KOLAS 인정범위의 시험절차와 검증된 도구의 수행기록
"참여권이 보장되지 않았다"	입회·서명·고지·기록 관리로 절차적 정당성 설명 (2015도 12400)
"수집 범위가 과도하다"	키워드·기간 기준 선별 수집 및 탐색 경로 로그 (2023도 12127)
"원본이 수집 중 변경되었다"	적용 가능한 저장매체 수집 시 Write-Blocker 사용 + 수집 전·후 해시값 비교·확인

상대방 제출 자료의 기술 검토

증거 진위·변조 확인

메타데이터 교차 검증으로 변조 여부를 확인하고 증거능력에 대한 기술적 의견을 제시

메신저 대화 위변조 검증

로컬 DB 분석, 삭제·편집·시간 조작 흔적 및 캡처 조작 검증

보고서·감정서 검토

상대방 포렌식 보고서의 기술적 타당성을 검토하고 의견서를 작성

캡처·문서 조작 검증

스크린샷 원본 여부 및 문서 타임스탬프·버전 이력 검증

이메일 위조·스푸핑 탐지

헤더 경로·SPF/DKIM 분석으로 발송 경로 추적 및 위조 가능성 검토

클라우드 증거·이력 검증

업로드·공유·접근 이력 분석으로 증거 취득 시점·경로 검증

포렌식 파트너십 프로그램

전담 포렌식 파트너

NDA 체결 · 전담 전문가 지정 · 사건 이력 연속 관리

우선 대응 체계

긴급 증거보전 요청 대응 · 제출 자료 신속 검토

IT 감사 및 내부통제 진단

IT 통제의 설계와 운영 실효성은 감독기관 점검과 외부감사 대응의 근거가 됩니다. 시스템 로그와 운영 데이터로 설계·운영 실효성을 점검합니다.

1,348억원

IT 로그·접근통제 미흡으로 인한 대규모 제재

개인정보보호위원회

27.6%

2025년 금융권 IT 실태평가 '미흡' 등급 비율

금융감독원(2025)

18.4%

자산 1,000억 미만 상장사 내부회계 '비적정'

금융감독원(2024)

IT 감사 주요 진단 범위

01 IT 내부통제 거버넌스

주요 점검 영역

· IT 내부통제 체계 · IT 리스크 평가

· 자체 IT 감사 체계 · 후속조치 관리

· 직무분리 및 업무 독립성

권한 매트릭스 교차 분석 · SoD 위반 식별

02 응용프로그램 운영 절차

주요 점검 영역

· 변경·배포·테스트 관리 절차

· 시스템 연계 · 형상 및 버전관리

· 운영상태 모니터링

변경 로그·승인 이력 · 환경 분리 검증

03 정보시스템 운영 거버넌스

주요 점검 영역

· 요청·이벤트 / 장애·문제 관리

· 구성정보 · 백업 및 복구 관리

· 접근통제 및 로그 관리

MTTR·RCA 추적 · RPO/RTO 충족 검증

IT 통제의 설계와 실제 운영 상태를 시스템 로그·운영 데이터로 실증 검증하고, 담당자 인터뷰와 현장 실사로 문서상 통제와 실제 운영의 차이를 확인합니다.

주요 발견사항 및 개선 권고

실제 IT 감사 현장에서 가장 빈번하게 식별되는 결함 유형입니다. 권한·접근통제 영역과 외부 연계·이력 관리 영역으로 나누어 정리했습니다.

01 접근권한·계정 관리

퇴직자·전환배치자 계정 미회수, 특권 계정 공유, 권한 만료기한 미설정은 비인가 접근·권한 잔존·추적 불가로 이어집니다.

주요 발견사항

- 퇴직 직원의 미회수 인증키로 대규모 개인정보 유출 (대형 이커머스)
- 계정정보 평문 저장 및 보호조치 미흡으로 침해 발생 (대형 이동통신사)
- 권한 만료기한 미설정으로 임시 권한이 장기간 유지

개선 권고 방향

- 계정 생애주기 관리 체계 구축 (인사 연계로 부여·변경·회수 자동화)
- 권한 만료기한 설정 및 정기 재검토 (최소 분기 1회)
- 계정정보 안전 저장 및 특권 계정 통제 (평문 금지·암호화·개별 계정화)

02 직무분리(SoD)·권한 매트릭스

요청·검토·승인이 동일인에게 집중되거나 개발-운영-보안 권한이 겸직되면 상호견제가 약화됩니다. ITGC 점검에서 반복적으로 지적되는 사항입니다.

주요 발견사항

- 변경 요청·검토·승인 권한이 동일인에게 집중되어 상호견제 약화
- 동일 직원이 장기간 단독으로 주요 업무를 수행하며 부정행위 발생
- 개발자가 운영 시스템 직접 접근 권한을 보유하여 사후 검증 곤란

개선 권고 방향

- 권한 매트릭스 교차 분석을 통한 SoD 위반 및 이해상충 식별
- 단독 수행 업무에 대한 독립적 감시·이중 확인 체계 구축
- 개발·운영 환경 분리 및 변경관리 워크플로우 자동화

03 외주·협력사 접근통제

외주 인력의 과도한 권한, 작업 종료 후 미회수, 외주 PC·계정 관리 미흡은 정보유출의 진입점이 됩니다.

주요 발견사항

- 외주·도급업체 인력에 과다 권한 부여 또는 종료 후 권한 잔존
- 협력 개발자의 인증키 관리 미흡으로 대규모 자산 피해 발생
- 외주 개발자 PC를 통한 고객사 접속 계정 탈취 및 개인정보 유출

개선 권고 방향

- 외주 권한 한시 부여 원칙 (작업 단위·기간 명시, 승인 기반 부여·회수)
- 협력사 인증키·자격증명 안전 관리 (별도 저장소·암호화·정기 교체)
- 외주 인력 PC 보안점검 및 접속 통제 강화 (일회성 계정·이중 인증)

04 감사추적·로그 관리

이벤트 로그 미보관, 무결성 검증 부재, 변경 전후 미기록은 사고 시 원인과 영향 범위 재구성을 어렵게 합니다.

주요 발견사항

- 관리서버 로그만 점검하거나 보관기간이 짧아 최초 침해 시점 추적 곤란
- 데이터 변경 시 변경 전·후 값이 기록되지 않아 사후 감사 추적 곤란
- 접속기록 보관기간 및 정기 점검 기준 미충족

개선 권고 방향

- 주요 시스템 로그 통합 수집·관리 및 보관기간 준수 (해시·전자서명 검증)
- 변경 전후 데이터 자동 기록 (Before/After Image)
- 접속기록 정기 점검 체계 운영 (반기 1회 이상, 임계치 기반 탐지)

수행 프로세스 · 산출물 · 기대효과

체크리스트 기반 통제 분석과 현장 실사를 병행하여, 경영진 보고에 활용할 수 있는 산출물을 제공합니다.

STEP 01 IT 환경 파악	STEP 02 관련 자료 수집	STEP 03 통제 테스트·실사	STEP 04 통제 분석 수행	STEP 05 결과 보고서 제공
IT 인프라·시스템 현황 파악 감사 범위·일정·대상 확정	정책·절차서·로그 등 필요 자료 요청	인터뷰·증적 확인 및 시스템 현장 실사	자료·테스트 결과 및 실사 결과 종합 분석	발견사항·개선 권고 경영진 보고용 산출물

주요 감사 산출물

감사 결과 보고서

- 점검 결과 요약 · 위험도 등급
- 발견사항별 원인·영향도 분석
- 경영진 요약본

IT 감사 조서

- 항목별 점검 내용·평가 근거
- 증빙자료·산출물 매핑
- 인터뷰·현장실사 결과

개선 로드맵

- 발견사항별 개선 방향
- 이행 우선순위 매트릭스
- 단계별 일정·담당 영역

IT 감사 기대효과

규제·회계 평가 대응력 확보

ITGC 결함 사전 식별·개선으로 K-SOX 및 내부회계관리제도 대응력 강화 / 적정 의견에 따른 지정감사 리스크 완화 / 금융권 IT 실태평가 미흡 등급 리스크 완화

감독·관리 의무 이행 근거 확보

감독기관 점검·조사 대응 시 IT 통제 이행의 객관적 증빙으로 활용 / 사고 발생 시 원인·영향 범위·조치 이력의 추적·재구성 가능

IT 통제 결함 사전 식별 및 개선

IT 통제 사각지대를 사전에 식별하여 시스템 운영 안정성과 신뢰성 강화

IT 통제는 더 이상 내부 운영 관리에만 머무르는 이슈가 아닙니다. 강화되는 규제 환경과 감독기관의 검증 요구 속에서 IT 통제의 설계·운영 상태는 과징금·제재·외부감사 지적·경영평가 불이익으로 이어질 수 있는 핵심 리스크입니다.

KOLAS 공인시험성적서 발급

분석 결과에 공신력이 필요할 때, 관련 법령과 국제표준에 기반한 공인시험 결과로 뒷받침합니다.

STEP 01 의뢰 접수	STEP 02 상담·목적 확인	STEP 03 표준 이미징	STEP 04 정밀 분석·작성	STEP 05 성적서 발급
온라인·이메일·전화 등을 통한 의뢰 접수	시험 목적, 대상, 범위 구체화	쓰기방지, 해시 검증 원본·사본 동일성 확인	표준 절차에 따른 분석 및 시험 결과 문서화	최종 공인시험성적서 제공

일반 분석 보고서와의 차이

일반 분석 보고서	KOLAS 공인시험성적서
기관 자체 기준에 따른 절차	ISO/IEC 17025 기반 표준 절차
기관별 표현 방식 상이	표준 절차에 따른 객관적 결과
사안에 따라 추가 검증 필요	진정성립 입증 보완 자료 제공
별도 신뢰성 검토 필요	ILAC-MRA 상호인정 체계 적용

인정범위 내 시험 항목

디스크 데이터 획득	HDD, SSD, USB 등 저장매체 대상
모바일 데이터 획득	iOS·Android 기반 모바일 기기
디지털 데이터 분석	아티팩트·로그·삭제 데이터 복구 및 검증

전 과정에 적용되는 품질관리

- 증거 이력 관리 (CoC) - 접수부터 성적서 발급까지 인계·인수 이력을 연속 기록
- 무결성 검증 - SHA-256 해시값 검증으로 데이터 변조·훼손 여부 확인
- 원본·사본 동일성 확인 - 동일성을 검증하여 진정성립 입증 보완 자료 제공

활용 단계

소송 단계

법정 제출용 보고서와 함께 발급해
객관성과 신뢰성 설명 지원

조사 단계

표준 절차 기반 시험 결과로
이해관계자에게 신뢰성 설명

KOLAS 공인 분석 절차 · 성적서 구성

의뢰 접수부터 공인시험성적서 발급까지 5단계로 진행되며, 전 과정에 품질관리가 적용됩니다.

STEP 01 의뢰 접수	STEP 02 상담·목적 확인	STEP 03 표준 이미징	STEP 04 정밀 분석·작성	STEP 05 성적서 발급
온라인·이메일·전화 등을 통한 의뢰 접수	시험 목적, 대상, 범위 구체화	쓰기방지, 해시 검증 원본·사본 동일성 확인	표준 절차에 따른 분석 및 시험 결과 문서화	최종 공인시험성적서 제공

전 과정에 적용되는 품질관리

증거 이력 관리 (Chain of Custody)

접수부터 분석, 성적서 발급까지 증거 인계·인수 및 처리 이력을 연속적으로 기록합니다.

무결성 검증

SHA-256 해시값 검증을 통해 데이터 변조·훼손 여부를 확인합니다.

원본·사본 동일성 입증

원본과 사본의 동일성을 검증하여 진정성립 입증을 보완할 수 있는 자료를 제공합니다.

공인시험성적서 5개 구성 요소

01	시험기관 정보	공인시험기관 명칭, 주소, 인정번호(KT1050)
02	시험 방법	KS Q ISO/IEC 17025 기반 표준 절차에 따른 시험 방법
03	시험 결과	표준 절차에 따른 분석 결과, 해시값, 검증 정보
04	시험원·기술책임자 서명	시험 수행자 및 기술책임자의 확인·승인 서명
05	KOLAS 인장	공인시험성적서임을 나타내는 공인시험기관 인장

인정범위 내 시험 항목

디스크 데이터 획득	HDD, SSD, USB 등 저장매체 대상 데이터 획득
모바일 데이터 획득	iOS·Android 기반 모바일 기기 데이터 획득
디지털 데이터 분석	아티팩트, 로그, 삭제 데이터 복구 및 분석 결과 검증

※ HM Company 인정번호 KT1050 · 인정범위는 모바일·디스크 데이터 획득 및 디지털 데이터 분석입니다.

KOLAS 공인시험성적서는 소송이나 조사 단계에서 분석 결과의 객관성과 신뢰성을 설명하는 자료로 활용됩니다.

IV. AI 플랫폼 및 제품

AI Platform & Products

AI 플랫폼과 포렌식 솔루션 및 제품을 통해 조사·감사 업무를 지원합니다

AI 플랫폼

- AI 내부감사 어드바이저 - 전수 검사와 이상 징후 자동 탐지
- 모두의 제보채널 ListenTips - 익명성을 시스템 구조에 반영
- HYENA - 방대한 비정형 데이터에서 단서를 찾아내는 리뷰 플랫폼

포렌식 솔루션

- Walnut - PC 카카오톡 대화 복호화 및 열람·검색
- 암호화된 대화 데이터의 복호화와 통계 제공
- 분석 과정의 무결성 기록 관리

제품

- CRETOP - 국내 최대 기업정보 분석 솔루션
- 포렌식 이미징 장비 - 원본 무결성 보장 수집 전용
- 장비 대여·임대 등 필요한 형태로 운용 가능

수집·분류·탐지·리뷰·보고까지 반복 업무를 자동화하고, 감사인은 판단이 필요한 영역에 집중합니다.

라인업 개요

디지털포렌식과 생성형 AI를 결합해 내부감사·컴플라이언스 업무의 전 과정의 고도화를 지원합니다

AI PLATFORM

AI 어드바이저
AI Audit Advisor

AI가 먼저 발견하고, 감사인은 판단에 집중합니다.

모두의 제보채널
ListenTips

기업 내부 신고의 접수와 처리를 안전하고 투명하게 지원합니다.

비정형 데이터 리뷰
HYENA

방대한 데이터 속, 조사에 필요한 단서를 찾도록 지원합니다

PRODUCTS

Walnut

암호화된 PC 카카오톡 대화를 복호화하고 열람·검색·통계와 무결성 기록으로 정리

CRETOP · 이미징 장비

국내 최대 기업정보 분석 솔루션과 원본 무결성 보장 증거 수집 전용 장비

데이터 분석부터 보고서 자동화까지

비정형 데이터 수집·분류, 이상 징후 탐지, 리스크 스코어링, 증거 관리, 보고서 자동 생성까지 하나의 플랫폼에서 지원합니다.

경험과 직관에 의존하던 감사를, AI가 자동 수집·분석해 놓치기 쉬운 이상징후의 탐지를 지원합니다

플랫폼 적용 흐름

1 비정형 데이터 수집 › 2 자동 분류·정규화 › 3 이상 징후 탐지 › 4 리스크 스코어링 › 5 보고서 자동 생성

AI 내부감사 어드바이저

AI가 먼저 발견하고, 감사인은 판단에 집중합니다.

OVERVIEW

AI 기반 분석으로 내부감사 데이터의 위험 징후 식별과 절차 수행을 지원하는 솔루션입니다. 방대한 데이터를 분석하고 잠재 위험 요소를 식별하며, 감사 절차의 효율성과 정확성을 높입니다.

재무 데이터·운영 기록·시스템 로그를 통합 분석해 규정 준수 여부, 사기 위험, 비효율 프로세스를 자동 평가합니다. 감사팀은 반복 작업 대신 고위험 영역과 전략적 감사 계획에 집중할 수 있습니다.

선언이 아닌 데이터로 증명되는 윤리경영 - 규제는 강화되고 내부 리스크는 다양해지며 투명성 요구는 높아집니다. 강령과 함께 객관적 증거와 관리 프로세스가 뒷받침될 때 실현됩니다.

2026.06.15 AI 기반 내부감사 자문·자동화 플랫폼 'AI Audit Advisor' 베타 운영 (이투뉴스)

주요 기능

AI 기반 이상 징후·패턴 탐지
기존 방식으로 발견하기 어려운 이상징후와 패턴의 식별을 지원

자동화된 위험 평가·우선순위
리스크 수준에 따라 감사 대상 우선순위를 자동 산정

다양한 데이터 소스 통합 분석
재무 데이터, 운영 기록, 시스템 로그를 통합 분석

규정 준수 모니터링
규정 준수 여부를 상시 모니터링

감사 보고서·시각화 대시보드
분석 결과를 보고서와 대시보드 형태로 제공

사기 위험 징후 식별 및 대응
사기 위험을 사전에 식별하고 예방 조치를 지원

감사 효율성 및 정확성 향상
반복 작업을 줄이고 감사 품질을 높임

맞춤형 감사 계획 지원
조직 특성에 맞는 전략적 감사 계획 수립 지원

적용 업무 영역

구매·조달	급여·인사	경비·법인카드	재무·회계	영업·매출	재고·자산	IT·보안
분할 발주 · 단가 급등	유령 직원 · 중복 급여	분할 결제 · 의심 거래	계정 이상 · 기표 오류	매출 인식 · 리베이트	수불 불일치 · 자산 누락	권한 과다 · 접근 이상

표본이 아니라 전체 데이터를 검사하며, 해당 구성 방식에서는 AI에 표의 항목 이름만 전달되며 실제 데이터는 회사 시스템 안에 남습니다. 생성된 점검 방법은 감사인이 직접 검토·수정할 수 있고, 자체 AI 연결 옵션도 제공합니다.

모두의 제보채널 (ListenTips)

회사 외부의 익명 제보 채널. 제보자 식별 가능성을 낮추는 보호조치를 시스템에 반영했습니다.

제보자를 보호하는 익명성 설계

01 직접 식별정보 입력 최소화

이름·이메일·전화번호 등 직접 식별 정보를 입력 항목에서 수집하지 않으며, 제보 확인은 제보자가 설정한 제보번호와 비밀번호로만 이루어집니다.

02 IP 원문 미보관

접속 IP는 SHA-256으로 변환된 값만 저장하고 원본 IP는 보관하지 않으며, 필요 시에도 해시값의 일치 여부만 비교합니다.

03 외부 추적 스크립트 미사용

제보자 페이지는 외부 분석 도구나 추적 스크립트를 사용하지 않아, 접속 정보가 제3자 서비스에 수집될 가능성을 최소화합니다.

04 제보 데이터 암호화

제보 본문·첨부파일·댓글은 제보 건마다 생성되는 키로 암호화되며, 서버에는 키를 해제하는 개인키를 저장하지 않습니다.

05 무단 변경 방지를 위한 감사 로그

제보·댓글·설정 변경·로그인 등 주요 활동이 변경 전·후 값과 함께 기록되며, 관리자 권한으로도 임의 수정·삭제할 수 없습니다.

06 다층 접근 통제

2단계 인증, CAPTCHA, 역할 기반 권한 분리, 해외 IP 차단, 제보 속도 제한을 적용하고 세션은 미사용 30분 후 자동 만료됩니다.

제보 접수와 처리를 지원하는 AI

식별정보 비식별화
이름·연락처·소속 등 개인정보 비식별화 처리

핵심 요약
장문 제보를 사실관계 중심 요약

관련 규정 매핑과 검토 지원
윤리강령·내규 조항 근거 제시

조사 계획 수립
자료·인터뷰 대상 단계별 제안

문답서 초안 작성
대상자별 질문 항목 단위 구성

조사 보고서 초안
내부감사·경영진 보고용 정리

제보자 답변 초안
문의·추가 댓글 답변 초안 생성

다국어 지원
한·영·일·중 4개 언어 제공

Gemini·GPT·Claude 중 운영 환경에 맞는 모델을 선택해 연동하며, 자사 API 키 사용 시 사용량·비용을 직접 관리합니다.
· 관련 법령 - 공익신고자 보호법 제12·15조 / 근로기준법 제76조의2·3 / 개인정보 보호법 제3조 / EU 공익신고자 보호 지침

접수부터 종결까지, 하나의 시스템에서 관리

01 접수 › 02 AI 분석 › 03 조사·소통

04 조치 결정 › 05 종결·보고

변경 이력 자동 보존
변경 시점·사용자·내용 자동 기록

필터 및 CSV 내보내기
처리 상태·자회사·기간별 추출

사건 단위 첨부자료 보관
제보·조사 자료를 사건 단위 통합

그룹사 통합 관리
자회사·해외 법인까지 통합 관리

HYENA · Walnut

감사 조직이 직접 포렌식 분석을 수행할 수 있도록 지원하는 솔루션과, 비정형 데이터 검토 및 PC 카카오톡 분석을 지원하는 솔루션으로 구성됩니다.

HYENA

비정형 데이터 리뷰 플랫폼

문서·이메일·채팅·멀티미디어를 수집·처리·분류해
핵심 정보와 증거를 신속히 찾아냅니다.



HYENA eAudit · 프로젝트 인덱싱 관리

· dTSearch 기반 고급 검색·분석 엔진

· 데이터 시각화 및 패턴 인식

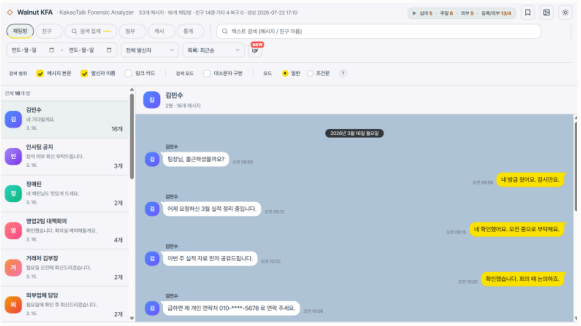
· 효율적인 팀 협업·검토 기능

· 사용자 정의 분류·태깅

Walnut

KakaoTalk Forensic Analyzer

암호화되어 저장된 PC 카카오톡 대화를
복호화하고 열람·검색·통계로 정리합니다.



Walnut KFA · 대화방 목록 · 조건식 검색

· 암호화 대화 데이터 복호화

· 삭제·회수 메시지 구분 표시

· 외부 전송 없는 로컬 처리

· 해시값·처리 이력 무결성 관리

2024.10.10 국내 주요 대기업·로펌과 리뷰 플랫폼 'HYENA' 공급 계약 체결 (서울신문) · 두 솔루션 모두 ADFS의 수행 경험을 바탕으로 개발했습니다.

V. 교육·컨설팅

Education & Consulting

조직이 직접 포렌식 역량을 갖출 수 있도록 교육 3과정과 컨설팅 3종을 운영합니다.

교육 과정

- 내부감사 포렌식 전문가 - 수집·분석 방법론 실무 과정
- AI 기반 내부감사 실무 - 데이터 기반 감사 적용 방법
- 기업 맞춤형 교육 - 조직 상황에 맞춘 과정 설계

컨설팅 서비스

- 디지털포렌식 LAB 구축 - 장비·SW 선정부터 절차 표준화
- KOLAS 인정 컨설팅 - 17025 기반 품질 체계 구축·심사 대응
- AI 윤리경영 컨설팅 - 활용 현황 진단과 가이드라인 수립

교육 수행 실적

- 기업 - 삼성·LG·신세계·GS·효성·KT·네이버·KB 등
- 공공기관·공기업 - 인천국제공항공사·한국수력원자력·한국전력 등
- 협회·기관 - 한국감사협회·흑자경영연구소·한국생산성본부 등

조직이 외부 의존도를 낮추고 자체 조사 역량을 갖추도록 교육 과정과 LAB 구축·인정 컨설팅을 함께 제공합니다.

교육 과정 · 컨설팅 서비스

2015년부터 감사인 대상 강연과 교육을 통해 실무 경험과 방법론을 공유해 왔으며, 조직이 자체 포렌식 역량을 갖추도록 지원합니다.

교육 과정

내부감사 포렌식 전문가 과정

디지털 증거를 다루는 감사 전문가 되기

증거 수집·분석 절차부터 감사 계획, 보고서 작성까지 실제 사례와 모의 실습으로 익힙니다. 수료증을 발급합니다.

AI 기반 내부감사 실무과정

AI로 배우는 내부감사, 실무편

엑셀 수작업 감사를 AI로 전환합니다. 이상거래 탐지부터 보고서 자동화까지 바로 적용하는 실무 과정입니다.

기업 맞춤형 포렌식 교육

우리 회사에 맞춘 보안 교육

인원·수준·업종에 맞춰 커리큘럼을 설계합니다. 담당자 심화 과정부터 전 임직원 기본 교육까지 제공합니다.

컨설팅 서비스

조직 맞춤형 디지털포렌식 LAB 구축

- 수집·분석 장비 및 SW 선정
- 격리 분석 환경·무결성 체계 설계
- 분석 절차 및 품질관리 체계 수립

국제공인 시험기관 인정 컨설팅

- ISO/IEC 17025 기반 절차 표준화
- 시험원·기술책임자 자격 요건 준비
- 품질 보증 체계 구축 및 심사 대응

AI 윤리경영 컨설팅

- AI 활용 현황 및 리스크 진단
- 기업 맞춤형 AI 윤리 가이드라인
- 내부 통제·모니터링 체계 연계

교육 수행 대상 - 삼성·LG·신세계·GS·효성·KT·네이버·KB·현대카드 / 인천국제공항공사·한국수력원자력·한국전력·코레일 / 한국감사협회·한국생산성본부

VI. 수행 실적 및 문의

Track Record & Contact

금융·제조·유통·의료·공공 등 다양한 산업에서 조사·진단을 수행해 왔습니다. 상담 및 맞춤 견적은 무료로 제공됩니다.

주요 수행 실적

- 산업별 수행 - 제조 · 금융 · 의료 · 유통
- 2011년 설립 이후 상시 협업 관계 유지
- 사건 규모·유형에 관계없이 초기 쟁점부터 상담

신뢰의 근거

- 국가 연구·구축 과제 - 경찰청·IITP·콘텐츠진흥원 등 참여
- 기업·공공기관·협회 대상 교육 수행 실적 보유
- 디지털포렌식 분야 KOLAS 민간 최초 인정

의뢰부터 결과까지

- 상담 문의 → 범위 협의·NDA → 증거 확보
- 정밀 분석·보고서 작성 → 법정 제출 등 사후 지원
- 상담 및 맞춤 견적은 무료로 제공

산업별 수행 사례와 국가 연구·구축 과제 참여 실적을 근거로 제시하며, 상담과 견적은 무료입니다.

주요 수행 실적

금융, 제조, 의료, 유통 등 다양한 산업의 감사·컴플라이언스 조직과 함께해 왔습니다.

업체	분류	기간	내용
H 카드	금융	2011.10 ~ 현재	내부감사 Co-Sourcing
H 카드	금융	2012.07 ~ 현재	협력업체 개인정보·정보보안 리스크 진단
W 반도체	제조	2025.07 ~ 2025.09	임직원 부정행위 조사 및 사실관계 분석
H 보험	금융	2024.12 ~ 2025.01	법인카드·골프회원권 사용 적정성 조사
H 바이오	의료	2023.10 ~ 2023.12	임원 부정행위 의혹 조사 및 검토
B 헬스케어	의료	2023.06 ~ 2023.09	자사 임직원 개인정보 관리실태 진단
L 반도체	제조	2023.05 ~ 2023.08	첨단기술·영업비밀 유출 리스크 진단
O 화학	제조	2022.11 ~ 2023.03	임직원 부정행위 조사
H 모터	제조	2022.06 ~ 2022.08	제품 설계도 등 영업비밀 유출 리스크 진단
L 에너지	제조	2022.02 ~ 2022.05	정보유출 및 부정위험 조사·진단
L 전자	제조	2022.02 ~ 2022.04	고객 개인정보 관리체계 진단 및 컨설팅
H 제철	제조	2021.12 ~ 2022.06	회계장부 등 영업비밀 유출 진단
M 유업	유통	2021.08 ~ 2021.11	보유 고객정보 관리실태 진단
E 유통	유통	2021.05 ~ 2021.06	협력업체 개인정보 관리실태 진단

산업별 분포 · 수행 실적 14건 기준

7
제조
반도체·화학·자동차 에너지·전자·제철

3
금융
카드·보험

2
의료
바이오·헬스케어

2
유통
유업·유통

수행 서비스 유형

부정행위 조사
임직원·임원 부정행위 조사, 법인카드·골프회원권 적정성

영업비밀 유출 진단
첨단기술·설계도·회계장부 등 유출 리스크 진단

개인정보 관리실태 진단
자사 임직원·협력업체·고객 개인정보 관리체계

상시 협업
내부감사 Co-Sourcing, 협력업체 리스크 진단 (2011~)

모든 사건은 비밀유지서약(NDA)을 체결하고 진행했으며, 고객사 보호를 위해 이니셜로 표기합니다.

신뢰의 근거

고객사, 교육 수행기관, 국가 연구·구축 과제 세 축으로 본부의 수행 역량을 뒷받침합니다

교육 수행 기관

기업

삼성 · LG · 신세계 · GS · 효성 · KT · 네이버 · KB · 현대카드 등

공공기관 · 공기업

인천국제공항공사 · 한국수력원자력 · 한국전력 · 코레일 등

협회 및 기타 기관

한국감사협회 · 흑자경영연구소 · 한국생산성본부 등

※ 디지털 데이터 수집·분석 방법론 교육 수행 기준

국가 연구 · 구축 과제

경찰청

AI 기반 범죄수사 시스템 구축 사업 수주

IITP

디지털증거 증명력 제고를 위한 인과관계 추론 과제

한국콘텐츠진흥원

클라우드 기반 증거수집 관련 과제 수주

중소벤처기업부

중소기업 기술보호 디지털포렌식 지원단 선정

국가기술표준원

디지털포렌식 분야 KOLAS
국제공인시험기관 인정 (민간 최초)

한림대학교

포렌식 연구센터 공동 설립 · 산학협력

국내 최초 온라인 내부감사 경진대회를 한국감사협회와 공동 개최하고 있으며, TV 드라마 「감사합니다」 자문을 수행했습니다.

의뢰부터 결과까지

사건 규모와 유형에 관계없이 초기 쟁점 검토부터 증거 확보·보존 방향까지 상담해 드립니다. 상담 및 맞춤 견적은 무료입니다.

STEP 01 상담 문의	STEP 02 범위 협의·NDA	STEP 03 증거 확보	STEP 04 분석 · 보고	STEP 05 사후 지원
사건 개요와 쟁점 확인 온라인 · 이메일 · 전화	조사 범위 · 일정 · 비용 협의 보안서약 체결	현장 출동 · 이미징 해시값 검증 · CoC 기록	정밀 분석 · 타임라인 재구성 분석 보고서 작성	법정 제출 지원 전문가 의견 정리

지금 상담이 필요한 상황

- 핵심 인력의 퇴사·이직이 예정되어 있거나 이미 진행된 경우
- 기업비밀·개인정보 유출 정황이 포착된 경우
- 법원의 자료보전명령 또는 전문가 사실조사 결정을 통보받은 경우
- 민·형사 소송에서 디지털 증거 제출이 요구되는 경우
- 감독기관 점검·조사 대응을 위한 객관적 증빙이 필요한 경우
- 사고 발생 전 선제적 리스크 진단을 검토하는 경우

주요 산출물

분석 보고서

법정 제출용 전문 보고서.
발견사항·원인·영향도 및 개선 방향

해시값 검증 확인서

SHA-256 해시값을 이용해 원본과 사본의 동일성·무결성 확인을 지원하는 문서

Chain of Custody 이력서

증거 인계·인수 및 이동·보관 연속 기록

KOLAS 공인시험성적서

인정범위 내 항목의 공인시험 결과 (KT1050)

포렌식 파트너십 프로그램 - 법무법인·법률사무소 대상 NDA 체결 후 전담 전문가를 지정하고, 긴급 증거보전과 제출 자료의 신속 검토를 우선 지원합니다.

CONTACT US

디지털 증거가 필요한 순간

초기 상담부터 함께합니다

사건 규모와 유형에 관계없이 초기 쟁점 검토부터 증거 확보·보존 방향까지 신속히 상담해 드립니다.
디지털포렌식 서비스 상담 및 맞춤 견적을 무료로 제공합니다.

본부장

박재현 상무

jaehyun.park@hmcom.co.kr

조사·진단 실무총괄

이정훈 수석

Jeonghoon.lee@hmcom.co.kr

hmcom.co.kr | hmadfs.com | office@hmcom.co.kr | 02-6237-6213

서울특별시 서초구 효령로70길 36-9, 와이엘타워 2·3층

© 2026 HM Company™ | ADFS. All Rights Reserved.