정보유출 조사

Digital Forensics-Based Trade Secret & Confidential Information Leakage Investigation

디지털포렌식 기반 기업비밀·정보유출 조사

HM COMPANY™

1. 기업비밀·산업기술 유출 현황

경찰청에 따르면 2025년 검거된 기술유출 범죄는 **179건**이며, 그중 **82.7%**가 내부 임직원에 의한 유출로 나타났습니다. 기업비밀 유출은 주로 회사 자료에 접근 권한을 가진 내부자에 의해 발생하며, **기업의 경쟁력 저하, 법적 분쟁, 재무적 손실**로 이어질 수 있습니다.

23.3조원

2020~2025.6
산업기술 유출 피해 추산

산업통상자원부·국정원(2026)

179건

2025년
기술유출 범죄 검거 건수

(전년 대비 45.5%↑)
경찰청(2025)

82.7%

2025년 기술유출 중
내부 임직원에 의한 유출 비율

경찰청(2025)

내부자 유출은 이직·퇴직 과정뿐 아니라 업무 편의, 재택·외근, 협력사 공유 등 일상적인 업무 환경에서도 발생할 수 있습니다. 대표적인 유출 경로로는 **USB 등 외부저장매체를 통한 반출, 개인 이메일·클라우드 전송, 상용 메신저 공유, 모바일 촬영**이 있습니다.

주요 기업비밀 유출 경로

유형	내용
외부저장매체	영업비밀 및 협력사 공동 개발 자료를 개인 USB 등 외부저장매체로 반출하는 행위
이메일	이직을 준비하며 차기 직장에서 활용할 목적으로 회사 업무자료를 개인 이메일로 전송하는 행위
클라우드	업무용 PC에서 개인 클라우드 계정에 접속하여 대외비 업무자료를 무단 업로드하는 행위
상용 메신저	전 직장 동료 또는 외부 관계자의 요청을 받고 고객사 연구 결과 정보를 상용 메신저로 전달하는 행위
모바일 기기	휴대전화·태블릿으로 회사 업무시스템 화면 또는 기업비밀 자료를 촬영하여 반출하는 행위

기업비밀 유출, 법적 책임이 무거워집니다

최근 법이 바뀌면서 기업비밀을 외부로 반출하는 행위에 대한 처벌이 크게 강화되었습니다. 고의로 영업비밀이나 산업기술을 유출하면 회사가 입은 실제 피해액의 **최대 5배**까지 배상해야 하며, 회사 자료를 무단으로 삭제하거나 훼손하는 것만으로도 **최대 징역 10년**의 형사처벌을 받을 수 있습니다.
(부정경쟁방지법 2024.8.21 · 산업기술보호법 2025.7.22 시행)

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

2-1. 정보유출 조사 방법론 — 외부저장매체 분석

외부저장매체는 연결되는 순간부터 시스템에 사용 흔적을 남깁니다.
연결, 사용, 파일 접근·복사 흔적이 Windows 시스템에 기록되며, 이를 종합 분석하여 자료 반출 정황을 확인합니다.

연결
USB · 외장 SSD · SD · MTP
장치 ID 및 Serial Number 식별

→

사용
폴더·파일 접근 및 실행 이력 확인
사용자 행위 타임라인 추적

→

유출
파일 복사 및 반출 흐름 분석
자료 반출 흐름 재구성

외부저장매체 분석 절차

1 데이터 수집·보존
쓰기 방지 장치 적용
Chain of Custody 유지

→

2 이미징 및 무결성 검증
비트 단위 저장매체 복제
SHA-256 해시값 산출

→

3 시스템 아티팩트 분석
레지스트리 및 시스템 로그 분석 및 사용 흔적 추출

→

4 상관분석 및 결과 보고
사용자 행위 타임라인 재구성
조사 결과 보고 및 대응 방안 제시

외부저장매체 주요 분석 항목

분석영역	내용
장치 식별	• 외부저장매체 **연결·해제 기록 확인** • 연결 이력이 확인된 외부저장매체의 **장치명, 시리얼 번호, 식별자** 등 확인 • 연결 이력이 있는 외부저장매체의 장치 정보를 **사내 관리대장과 대조**하여 인가 여부 확인
사용 흔적	• 외부저장매체에서 **생성 또는 접근한 폴더 이력** 확인 • 외부저장매체에서 **생성·실행된 파일 목록** 확인
유출 흔적	• 외부저장매체 **연결 시점 전후의 사용자 행위를 타임라인으로 재구성**하여 자료 반출 정황 분석 • 외부저장매체에서 생성·접근된 폴더·파일 중 **기업비밀 관련 데이터 선별**

Q 회사 PC에 어떤 외부저장매체가 언제 연결되고 사용되었습니까?
A 장치 시리얼, 연결 시각, 해제 시각 등을 분석하고 사내 관리대장과 대조하여 비인가 외부저장매체 사용 정황을 식별합니다.

Q USB를 통해 어떤 파일이 반출되었는지 확인할 수 있습니까?
A 외부저장매체 연결 시점 전후의 사용자 행위를 **타임라인으로 재구성**하여 복사·실행된 파일을 특정하고, 기업비밀 관련 데이터를 선별합니다.

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

2-2. 정보유출 조사 방법론 — 이메일 분석

발송된 메일, 삭제된 메일, 자동 전달·외부 계정 전송 메일도 분석 가능한 흔적을 남길 수 있습니다.
로컬 메일 파일, 브라우저 캐시, 클라우드 및 계정 로그를 교차 분석하여 외부 전송 정황을 확인합니다.

주요 이메일 유출 유형

외부 개인 계정으로 전송
그룹웨어에서 Gmail, NAVER 등 개인 계정으로 포워딩

로컬 백업파일 외부 반출
PST, OST, EML 파일을 외부저장매체로 복사

외부망 접속 및 다운로드
OWA, VPN 등을 통한 우회 접속 및 다운로드

자동 전달 및 권한 위임
Outlook Rule, OAuth 권한 위임을 통한 지속적 유출 채널 설정

이메일 분석 절차

1 → 2 → 3 → 4

1. 이메일 데이터 수집·보존
메일박스 및 로컬 메일 파일 확보
Chain of Custody 유지

2. 이메일 복원·파싱
EML · PST · OST 분석
메일 송수신 이력 추출

3. 통합 교차분석
로컬 파일, 브라우저 기록, 클라우드 로그
통합 상관분석

4. 상관분석 및 결과 보고
이메일 송수신 및 외부 전송 흐름 재구성
조사 결과 보고 및 대응 방안 제시

이메일 주요 분석 항목

분석영역	내용
송수신 이력	• 이메일의 **발신자 · 수신자 · 일시 · 제목 · 본문 · 첨부파일** 확인 • 사내 메일 시스템 · 웹메일 · 로컬 백업 파일에서 **송수신 기록 추출**
삭제 메일 복구	• **삭제된 이메일 · 첨부파일** 복원 • 휴지통 비우기 · 완전 삭제 · 자동 정리 등 **은폐 시도 흔적** 확인
외부 전송 흔적	• 외부로 발송된 이메일 및 첨부파일 중 **기업비밀 관련 데이터 선별** • **자동 전달 규칙 · 위임 권한 설정** 등 지속적 유출 채널 식별 • 첨부파일의 해시값·메타데이터를 **사내 원본 문서와 대조**하여 동일 문서 여부 확인

Q 외부 계정으로 전송된 메일과 첨부파일은 무엇입니까?
A 사내 메일, 웹메일, **로컬 백업파일(PST·OST·EML)**을 통합 분석하여 외부 발송 메일과 첨부파일을 확인합니다.

Q 외부로 발송된 첨부파일이 사내 원본 문서와 동일한지 확인할 수 있습니까?
A 첨부파일의 **해시값과 메타데이터를 사내 원본 문서와 대조**하여 동일 자료 여부와 전송 정황을 확인합니다.

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

2-3. 정보유출 조사 방법론 — 웹·클라우드 분석

개인 클라우드에 업로드한 파일도 브라우저 기록, 동기화 폴더, 캐시, 계정 로그 등에 분석 가능한 흔적을 남길 수 있습니다.
브라우저 기록, 클라우드 동기화 흔적, 접속 로그를 교차 분석하여 외부 업로드 및 공유 정황을 확인합니다.

웹 접속
브라우저 · 웹메일 · 클라우드
접속 이력 및 계정 정보 식별

→

업로드 · 동기화
파일 전송 및 클라우드 동기화 이력
파일 이동 흐름 추적

→

외부 유출
개인 클라우드 보관 및 공유 링크 생성
외부 유출 흐름 재구성

웹·클라우드 분석 절차

1. **웹·클라우드 데이터 수집·보존**
   단말 및 계정 관련 자료 확보
   Chain of Custody 유지
2. **브라우저·캐시 복원 및 파싱**
   브라우저 기록 및 캐시 분석
   접속 및 파일 전송 이력 확인
3. **통합 교차분석**
   로컬 데이터, 클라우드 로그,
   계정 로그 통합 분석
4. **상관분석 및 결과 보고**
   업로드 및 공유 흐름 재구성
   조사 결과 보고 및 대응 방안 제시

웹·클라우드 주요 분석 항목

분석영역	내용
접속 및 계정 이력	• 브라우저 **방문 기록 · 검색어 · 다운로드 파일 목록** 분석 • 개인 클라우드 · 웹메일 · 웹하드 등 **외부 서비스 접속 이력 확인** • 외부 서비스 **로그인 계정, 접속 IP, 접속 일시** 확인
클라우드 업로드·동기화	• **클라우드 동기화 폴더 및 캐시** 분석(OneDrive, Google Drive, Dropbox 등) • 동기화 파일의 **업로드, 수정, 삭제 이력** 확인
유출 흔적	• 외부로 업로드·공유된 파일 중 **기업비밀 관련 데이터 선별** • **공유 링크 생성, 접근 권한 부여** 등 외부 유출 채널 식별 • 클라우드 파일을 **사내 원본 문서와 대조**하여 반출 여부 및 동일성 확인

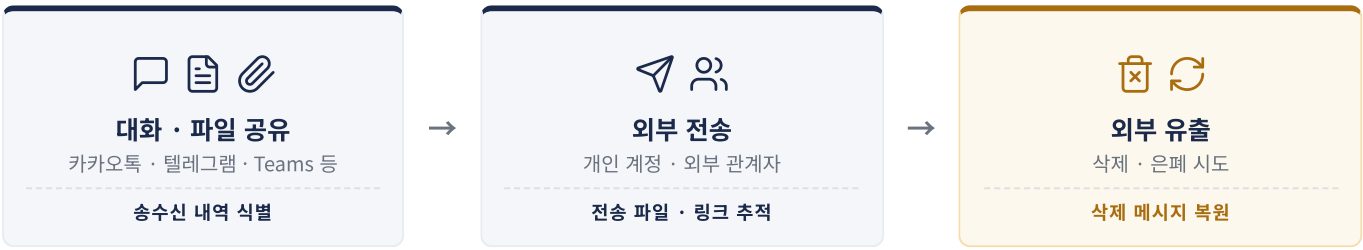
Q 사내 PC에서 웹메일·웹하드 등 외부 서비스 접속 흔적을 확인할 수 있습니까?
A 브라우저 방문 기록, 다운로드 목록, 외부 서비스 **로그인 계정, 접속 IP, 접속 일시**를 교차 분석하여 사외 자료 이동 정황을 식별합니다.

Q OneDrive·Google Drive 등 동기화 폴더에 남은 흔적도 분석할 수 있습니까?
A 동기화 폴더와 캐시에 남은 **업로드·수정·삭제 이력**을 복원하여 단말 기준으로 클라우드 자료 이동 흐름을 분석합니다.

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

2-4. 정보유출 조사 방법론 — 상용 메신저 분석

카카오톡 · 텔레그램 등 상용 메신저는 대화 한 번으로 자료가 외부로 전달되는 대표적 유출 경로입니다.
PC · 모바일에 남는 **대화 기록과 전송 파일 흔적**을 복원 · 분석하여 자료 유출 정황을 확인합니다.



상용 메신저 분석 절차



상용 메신저 주요 분석 항목

분석영역	내용
대화 내역	• PC · 모바일 메신저의 **송수신 대화 내용 복원** • **삭제된 메시지 · 대화방** 복원 시도 및 키워드 분석
전송 파일	• 메신저로 주고받은 **문서 · 이미지 · 압축파일 등 전송 파일 추출** • 전송 파일을 **사내 원본 문서와 대조**하여 기업비밀 관련 데이터 선별
계정 · 기기	• 사용 메신저 **계정 · 기기 · 로그인 이력** 식별 • PC · 모바일 동기화 및 외부 관계자와의 **대화 상관 분석**

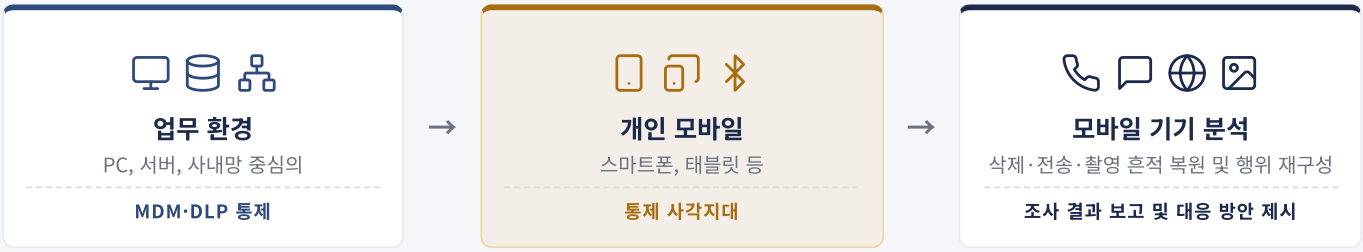
Q 메신저로 주고받은 대화와 파일을 확인할 수 있습니까?
A PC · 모바일에 저장된 메신저 로컬 데이터를 복원 · 분석하여 **송수신 대화와 전송 파일**을 추출하고, 기업비밀 관련 자료를 선별합니다.

Q 상대방이 삭제한 메시지도 복원됩니까?
A 단말에 남은 데이터베이스 영역을 분석하여 **삭제된 메시지 · 대화방의 복원**을 시도하며, 복원된 내역으로 유출 정황을 재구성합니다.

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

2-5. 정보유출 조사 방법론 — 모바일 기기 분석

개인 모바일 단말은 기업 보안 솔루션의 통제 범위 밖에서 활용되는 경우가 많아, 정보유출 조사에서 **중요한 분석 대상**입니다.
통화, 메시지, 미디어, 클라우드, 근접 무선 전송 기록 등을 분석하여 자료 촬영·전송·공유 정황을 확인합니다.



모바일 기기 분석 절차



모바일 기기 주요 분석 항목

분석영역	내용
통화	• 통화 이력 · 주소록 분석 • 녹음 파일 **STT**(Speech To Text) 변환 및 키워드 분석
메신저	• **메신저 로컬 DB 추출 및 복호화**(카카오톡, 텔레그램, WhatsApp 등) • SMS의 일시, 내용, 첨부파일 분석
웹 기록	• 웹 탐색 기록 · 다운로드 파일 분석 • **클라우드 동기화 캐시** 분석(iCloud, OneDrive, Google Drive 등)
미디어	• 갤러리 및 미디어 파일 목록 분석 • **OCR** 변환을 통해 촬영된 문서의 텍스트 추출 • **EXIF 메타데이터**(촬영 좌표, 시각, 기기 모델 등)를 분석하여 사내 촬영 여부 판단
기타	• 파일 시스템 및 앱 사용 흔적 분석 • **AirDrop, Quick Share, Nearby Share** 등 근접 무선 전송 이력 분석 • **생성형 AI 앱**(ChatGPT, Claude 등) 사용 및 프롬프트 입력 기록 분석 • **MDM 우회, 탈옥·루팅** 등 보안 통제 회피 정황 확인

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

3-1. 정보유출 사례 — 화장품 레시피 이직 유출

사례 요약

460억원

유출 레시피 기반 신제품 출시 후 경쟁사 B사의 1년 내 매출

반출 자료 기반 신제품 출시로 원 보유 기업의 시장 점유율 잠식

산업	화장품
유형	영업비밀 침해(부정경쟁방지법 위반)
주체	A사 전 R&D 연구원 2명
기간	2018 이직 ~ 2024.1 판결 확정
결과	**대법원 유죄 확정** · 개인 징역 6~10개월 선고

출처 EBN www.ebn.co.kr/news/articleView.html?idxno=1697206

> 화장품 A사의 R&D 연구원 2명이 경쟁사 B사로 이직하는 과정에서, 재직 중 **정당한 권한으로 접근했던 화장품 레시피 등 영업비밀**을 반출한 사례입니다.
> B사는 해당 자료를 기반으로 신제품을 출시해 **1년 내 약 460억원의 매출**을 기록했으며, 대법원은 2024년 1월 영업비밀 침해를 **유죄로 확정**했습니다.

타임라인

정당한 접근 권한 보유
자외선 차단제 레시피
직무상 정당한 열람

B사로 이직
레시피 등 영업비밀 반출
내부 탐지 실패

B사 제품 출시
유출 레시피 기반 제품 출시
시장 점유율 잠식

대법원 유죄 확정
A사 시장 점유율 잠식
개인 징역 6~10개월 선고

탐지 실패 요인

- ✕ **정상 권한에 가려진 이상 행위** — 업무상 접근 가능한 자료였기 때문에 단순 열람만으로는 유출 위험을 식별하기 어려움
- ✕ **퇴사·이직 전후 점검 부재** — 핵심 파일의 저장, 복사, 다운로드, 삭제 흐름이 시간순으로 분석되지 않음
- ✕ **외부 반출 경로 확인 미흡** — 클라우드, 이메일, 메신저, USB 등 외부 이동 흔적을 종합적으로 확인하지 못함

조사 방법론

접근·복사 이력 재구성
퇴직자가 어떤 자료에 언제 접근하고 복사했는지 시간순으로 재구성합니다.

자료 유출 흔적 분석
메신저, 이메일, 클라우드 등을 통한 외부 전송 및 반출 흔적을 분석합니다.

반출 로그 종합 분석
USB, 인쇄, 외부저장매체 등을 통한 자료 반출 여부를 종합 검증합니다.

권한 흐름·행위 시퀀스 분석
정당한 열람부터 복사, 저장, 외부 전송까지 이어진 행위 흐름을 추적합니다.

비정상 행위 식별
평소 업무 패턴과 다른 야간·주말 접근, 대량 열람, 비정상 다운로드 등을 식별합니다.

삭제 데이터 복원
이직 직전 삭제되거나 정리된 파일, 메일, 메시지를 디지털포렌식 기법으로 복원합니다.

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

3-2. 정보유출 사례 — 차량 성능시험 자료 유출

사례 요약

4년+

유출 시점부터 적발까지

외부 클라우드·메일에 자료가 장기간 보관되었으나 미탐지

산업	자동차 (제조)
유형	영업비밀 침해(부정경쟁방지법 위반) 및 업무상 배임
주체	C사 전 차량 성능시험 연구원
기간	2020.12 유출 ~ 2025.5 판결
결과	**징역 1년 6개월 선고 및 법정구속**

출처 경기신문 www.kgnews.co.kr/news/article.html?no=846563

> C사 남양연구소의 전 연구원이 **2020년 12월 퇴직 직전** 차량 성능시험 기술자료와 엔진 개발 노하우 등을 **개인 네이버 클라우드에 업로드**하고 **본인 이메일 계정으로 전송**하여 외부 반출한 사례입니다.

타임라인

정당한 접근 권한 보유
차량 성능시험 자료
직무상 정당한 열람

클라우드·이메일 반출
개인 클라우드 업로드
본인 이메일 전송

외부 보관
클라우드·메일 보관
외부 활용 가능 상태로 장기 보관

법원 유죄 판결
부정경쟁방지법·업무상 배임
징역 1년 6개월 선고 및 법정구속

탐지 실패 요인

- ✕ **외부 채널 통제 한계** — 개인 클라우드와 외부 이메일은 DLP·매체제어 정책의 통제 범위를 벗어나거나 예외가 적용되어 유출 통로로 활용될 수 있음
- ✕ **정상 권한에 가려진 유출 정황** — 업무상 접근 가능한 자료였기 때문에 단순 열람만으로는 유출 위험을 판단하기 어려움
- ✕ **퇴직 시점 활동 분석 부재** — 퇴직 직전 클라우드 업로드, 이메일 전송 등 시점 기반 이상 행위를 모니터링하는 체계 미흡

조사 방법론

외부 채널 이력 검증
개인 클라우드 업로드 및 외부 이메일 전송 이력을 추적합니다.

사용자 행위 이상치 분석
퇴직 직전 비정상 다운로드, 업로드, 이메일 전송 패턴을 식별합니다.

통신·관계 상관분석
외부 수신처, IP, 이메일 계정의 동시 활동과 연관성을 추적합니다.

단말 디지털포렌식
PC·노트북에서 외부 전송 흔적과 잔존 데이터를 분석합니다.

삭제·은폐 행위 분석
휴지통 비우기, 완전삭제, 파일명 변경 등 은폐 시도 흔적을 분석합니다.

증거 패키지 산출
법적 대응에 활용할 수 있도록 무결성이 보존된 증거 자료를 정리합니다.

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

3-3. 정보유출 사례 — 디스플레이 양산기술 모바일 촬영 유출

사례 요약

5조원

광저우 OLED 양산공정 관련 투자 규모

핵심기술이 스마트폰 촬영 방식으로 해외 경쟁업체에 유출

산업	디스플레이 제조 · 국가핵심기술
유형	산업기술 유출 및 영업비밀 침해(산업기술보호법·부정경쟁방지법 위반)
주체	E사 전 OLED 양산기술 팀장 및 재직자 3명 공모
기간	2020 이직 ~ 2024.8 기소
결과	**2명 구속기소 및 1명 불구속기소**

출처 머니투데이 www.mt.co.kr/industry/2024/08/21/2024082016585664112

> E사 광저우 공장에서 20년 이상 OLED 연구를 담당한 **팀장급 핵심인재**가 2020년 중국 디스플레이 업체로 이직하면서, **OLED 양산 설계도면 등 핵심기술을 스마트폰으로 촬영**해 유출한 사례입니다.
> 이직 이후에도 **E사 재직자 3명과 공모**해 추가 유출이 이루어졌으며, 2024년 8월 서울중앙지검은 산업기술보호법 및 부정경쟁방지법 위반 혐의로 **2명을 구속기소하고 1명을 불구속기소**했습니다.

타임라인

핵심기술 접근 권한자
광저우 OLED 양산기술 직무상 핵심기술 접근

스마트폰 촬영 반출
OLED 양산 설계도면 **모바일 촬영을 통한 반출**

재직자와 공모
E사 재직자 3명과 공모 **추가 유출 정황 지속**

검찰 기소
2명 구속기소 1명 불구속기소

탐지 실패 요인

- ✕ **물리 촬영 통제 한계** — 스마트폰 촬영은 DLP·매체제어 등 디지털 통제 범위를 벗어나 사내 시스템 로그만으로는 식별이 어려움
- ✕ **핵심인재의 정상 권한 접근** — 팀장급 핵심인재의 도면 열람은 정상 업무로 보일 수 있어 이상행위 탐지에서 누락될 가능성이 있음
- ✕ **이직 시점 및 공모 정황 분석 부재** — 이직 전후 재직자와의 통신, 공동 자료 접근, 동시 활동 패턴을 분석하는 체계가 미흡

조사 방법론

- 외부 채널 이력 검증 — **모바일 데이터 외부 전송 및 클라우드 동기화 흔적 추적**
- 사용자 행위 이상치 분석 — **이직 시점 전후 비정상 출입, 자료 접근, 촬영 가능 정황 식별**
- 통신·관계 상관분석 — **재직자와의 동시 통신, 자료 공유, 공모 정황 재구성**
- 모바일 디지털포렌식 — **개인 스마트폰 갤러리, 메신저, EXIF 메타데이터 복원 및 분석**

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

4. 정보유출 조사 절차 및 도입 효과

서버, PC, 외부저장매체, 모바일 기기, 이메일·메신저·클라우드 등 주요 유출 경로를 통합 분석하여 정보유출 정황과 반출 경로를 확인합니다. 조사는 사전 조사부터 대상자 심층 조사까지 5단계로 진행됩니다.

데이터 유출 경로 및 주요 분석 대상

분석영역	내용
서버 데이터	유형: 기업 자체 서버 및 위탁 운영 데이터센터 유출 경로: 이메일, 사내 메신저 분석 대상: 이메일 로그, 메신저 로그, 보안 솔루션 로그
PC 데이터	유형: 업무용 PC 및 개인 휴대전화 내 업무 관련 파일 유출 경로: 이메일, 외부저장매체, 클라우드, 프린트, 모바일 촬영 분석 대상: OS 시스템 로그, 웹브라우저 기록, 메신저 로그, 클라우드 업로드 이력

기업비밀 유출 조사 절차

Step 1. 기초 데이터 분석 | **Step 2. 대상자 심층 조사**

1. **사전 조사 및 범위 정의**
2. **분석 데이터 수집**
3. **데이터 분석**
   기업비밀 유출 정황 식별
4. **심층 조사 대상자 선정**
5. **대상자 심층 조사**
   인터뷰 및 디지털포렌식 분석

도입 효과

기업비밀 유출 피해 최소화
서버·PC 데이터
무단 반출 정황 확인 및 대응

신속한 사고 원인 파악
이메일·메신저·클라우드
유출 경로 신속 확인 및 조치

유출 경로 및 반출 자료 식별
실제·잠재 유출 경로 식별
→ 보안정책 개선

데이터 기반 조사 인사이트
유출 경향과 원인 분석
→ 내부 위협 요인 식별

법적 대응 근거 확보
관련 법규 및 증거 절차 준수
분쟁 대응 근거 확보

임직원 부정행위 리스크 식별
임직원 부정 정황 확인
및 법적 조치 지원

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

5. HM Company 주요 수행 역량 및 실적

HM Company는 2011년 설립 이후 디지털포렌식 전문성을 기반으로 정보유출 조사, 개인정보·정보보호 리스크 진단, IT 감사, 내부감사 등 기업 리스크 대응 서비스를 수행해 왔습니다.

ADFS 본부	RAS 본부	AI MARU 본부
디지털포렌식 서비스	컴플라이언스 리스크 진단	리걸테크: 수사·증거 분석 AI
정보유출 조사 / IT 감사	회계감사 외부전문가 조사	에듀테크: AI 학습 도구
정보보호 리스크 진단	경영진단·내부감사	LLM 오케스트레이션 / RAG
KOLAS 공인시험성적서 발급	직장 내 괴롭힘 조사 / PMA	데이터 어노테이션 플랫폼 LEAP

Why HM COMPANY ADFS

15년+
디지털포렌식 기반
조사·진단 수행 경험

20,397+
누적 디지털포렌식
증거물 처리 경험

KOLAS
민간 최초 디지털포렌식 분야
KOLAS 공인시험기관 인정 보유

NDA
보안서약 체결 및
데이터 안전 폐기 체계 운영

주요 수행 실적

분야	주요 수행 실적
금융	내부감사 자료 검토 및 Co-Sourcing
금융	협력업체 개인정보 및 정보보안 리스크 진단
금융	법인카드 및 골프회원권 사용 적정성 조사
제조	임직원 부정행위 조사 및 사실관계 분석
제조	첨단기술 및 영업비밀 유출 리스크 진단
제조	제품 설계도 등 영업비밀 파일 유출 리스크 진단
제조	회계장부 등 영업비밀 유출 진단
제조	정보유출 및 부정위험 조사·진단
의료·헬스케어	임직원 개인정보 관리실태 진단
의료·헬스케어	임원 부정행위 의혹 조사 및 검토
유통	보유 고객정보 관리실태 진단
유통	협력업체 개인정보 관리실태 진단
법률 사건 지원	디지털 증거 확보, 선별 추출, 전처리, 검색 가능한 검토 환경 구성

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

HM COMPANY™

Tech DNA & Trade Secret Leakage Diagnostic Service

Contact Us

박 재 현 상무

jaehyun.park@hmcom.co.kr

이 정 훈 수석

jeonghoon.lee@hmcom.co.kr

ADFS본부

02-6237-6213

대표전화

02-6237-6233

본부 소개서

QR코드를 스캔하여
본부 소개서 PDF를 확인하세요.

기업비밀 유출 조사 상담 및 맞춤 견적 안내
기업비밀 유출이 의심되는 경우 상담을 통해
조사 범위와 대응 방향을 신속하게 안내드립니다.

hmcom.co.kr
hmadfs.com
서울특별시 서초구 효령로70길 36-9, 와이엘타워 2층, 3층

© 2026 HM Company™ | ADFS. All Rights Reserved