정보보호 리스크 사전진단

Pre-Diagnostic Service for Corporate Information Security Risk

디지털 분석 기반의 기업비밀 유출 위험 사전진단

HM COMPANY™

1. 정보보호 리스크 진단의 필요성

최근 5년간 산업기술 유출 피해 규모가 약 23조원에 달하는 등 **기업비밀 유출**은 기업의 경쟁력과 존속 가능성을 위협하는 **핵심 리스크**로 확대되고 있습니다. 2025년 검거된 **기술유출 범죄 179건 중 82.7%**가 **내부 임직원에 의한 유출**로 나타나, 내부자 리스크 관리의 중요성이 더욱 커지고 있습니다.

23조원

2020~2024
산업기술 유출 피해 추산

국가정보원(2025)

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 기업비밀의 **개인 이메일 전송, 외부저장매체 무단 반출, 상용 메신저를 통한 고객정보 공유 등** 다양한 경로로 발생하고 있습니다. 보안 솔루션 도입이 일반화되었음에도 시스템 설정 오류, 예외 정책, 인가자의 우회 행위로 인한 유출 가능성은 여전히 존재합니다. 따라서, **사고 발생 전 위험 영역을 식별하고 보완**하는 **사전진단이 필요**합니다.

왜 정보보호 리스크 진단이 필요한가

기업비밀 유출 사고는 **보안 솔루션의 도입 여부**뿐 아니라, **보안 정책의 설계 수준과 임직원의 실제 준수 여부**에 따라 발생 가능성이 달라집니다. 보안 솔루션만으로는 정책 우회, 관리 사각지대 등에서 발생하는 유출 정황을 충분히 식별하기 어렵습니다.
HM COMPANY는 문서·데이터 관리실태, 보안 솔루션 실효성, 내부자 행위 리스크를 통합 분석하여 **기업비밀 유출 가능성을 사전에 식별**하고 실질적인 **개선 방안을 제시**합니다.

기업비밀 유출 경로 예시

유형	내용
이메일	이직을 준비하며 차기 직장에서 활용할 목적으로 회사 업무자료를 개인 이메일로 전송
클라우드	업무용 PC에서 개인 클라우드 계정에 접속해 대외비 업무자료를 무단 업로드
모바일 기기	휴대전화·태블릿으로 회사 업무시스템 화면 또는 기업비밀 자료를 촬영하여 무단 반출
상용 메신저	전 직장 동료의 요청을 받고 고객사 연구 결과 정보를 상용 메신저로 무단 전달
외부저장매체	영업비밀 및 협력사 공동 개발 자료를 개인 USB 등 외부저장매체로 무단 반출

2-1. 진단 방법론 — 문서·데이터 관리실태 진단

임직원이 보유·사용하는 문서, 이메일, 저장소 데이터가 **사내 보안 정책에 따라 관리되고 있는지** 사전에 진단합니다.
보안 정책을 우회하거나 회피한 정황까지 함께 분석하여 잠재적인 유출 위험을 식별합니다.

문서·데이터 보유 현황 파악
문서 · 이메일 · 저장소
진단 대상 및 범위 식별

→

보안정책 부합성 분석
정책 준수 여부 및 우회 정황
잠재 위험 사전 식별

→

관리실태 진단 결과 정리
정책 미준수 항목 정리 및 보완 권고
개선방안 제시

진단 절차

1 **데이터 수집 · 보존**
매체 · 이메일 · 로그

→ 2 **분석 데이터 추출**
사용 흔적, 송수신 이력,
출력 및 정책 위반 정황

→ 3 **보안정책 대조**
사내 보안정책 기준 대비
준수·우회 여부 식별

→ 4 **진단 결과 보고**
관리실태 종합 정리
및 보완 권고

진단 항목

진단 영역	내용
외부저장매체	• USB, 외장 SSD, SD카드 등 외부저장매체의 **연결 및 사용 흔적** 진단 • 장치 정보를 **사내 관리대장과 대조**하여 인가 매체 여부 확인
이메일·메신저	• 이메일 **송수신 이력**을 분석하여 개인 계정 전송 및 자동 전달 규칙 설정 여부 진단 • 로컬 백업파일, 웹메일, 사내 메신저 등 다채널 송수신 흔적 통합 분석
인쇄·출력 흔적	• 인쇄 작업 로그 및 스풀 흔적을 분석하여 **대외비 문서 출력 정황** 진단 • 시간대, 문서 유형, 사용자별 인쇄량을 기준으로 이상 패턴 및 출력물 반출 가능성 평가
문서 정책 준수	• 대외비·기밀 분류, 보관기간, 접근권한 등 **문서 보안정책 준수 여부** 진단 • 문서 분류 누락, 권한 외 공유, 장기 미정리 등 **관리 사각지대 식별**
웹·클라우드	• 외부 클라우드 서비스 **접속 기록 및 동기화 흔적** 분석 • 웹 기반 파일 업로드·다운로드 이력 및 이상 패턴 진단

실제 사례

문서 정책 준수
보관기간을 초과한 개인정보 파일 잔존
직무 권한 범위를 벗어난 대외비 문서 보관

이메일·메신저
클라우드·이메일을 통한 **미인가 외부 전송**
사내 메신저 로그에 **고객정보 평문 저장**

외부저장매체
비인가 외부저장매체 연결 및 사용
외장 매체 내 **암호화 미적용 자료** 보관

2-2. 진단 방법론 — 보안 솔루션 실효성 진단

기업이 운영 중인 DLP, DRM, 방화벽, MDM 등 **보안 솔루션이 정책 설계 의도에 맞게 작동하고 있는지** 사전에 검증합니다.
정책 설정의 적정성, 우회 가능성, 로그 수집 및 탐지 수준까지 실제 데이터 기반으로 진단합니다.

보안 솔루션 운영 환경 파악
DLP · DRM · F/W · MDM
진단 대상 솔루션 식별

→

정책 우회 가능성 검증
정책 우회 정황 및 로그 누락 여부
통제 사각지대 사전 식별

→

솔루션 실효성 진단 결과 정리
통제 사각지대 목록화 및 보완 방안 제시
개선방안 제시

진단 절차

1 **솔루션 설정·정책 수집**
솔루션 정책·룰 확보
로그 수집 범위 확인

→ 2 **우회 정황 식별**
신종 유출 채널 및
인가자 행위 아티팩트 분석

→ 3 **통합 상관분석**
매체, 통신, 권한 정보
연계 통합 분석

→ 4 **진단 결과 보고**
솔루션 실효성 평가 및
보완 권고

진단 항목

진단 영역	내용
인가자 우회	• 인가된 저장매체를 이용한 **무단 반출** 및 인가 클라우드 계정의 **외부 동기화** • 사내 화이트리스트 도구, 예외 경로, 개인 노트 앱을 활용한 **우회 가능성 진단**
외부자 우회	• 사회공학을 통한 **자격증명 탈취**, 만료 권한 또는 위임 **권한 악용** 가능성 진단 • API Key, OAuth 토큰의 **외부 유출 가능성** 진단
신종 채널	• 생성형 AI 입력, 이미지 OCR 우회, VDI 스크린샷, 화면 재촬영 등 **신종 유출 채널** 진단 • AirDrop, Nearby Share, P2P 전송, 클라우드 공유 링크 첨부 등 **비정형 전송 경로** 진단
솔루션 회피	• 확장자 변경, 파일 구조 변환, 암호화, 분할, 압축, 인코딩을 통한 **탐지 회피 정황** 진단 • 보안 솔루션 예외 경로 내 영업비밀 저장 여부 확인

실제 사례

솔루션 회피
문서를 캡처한 뒤 **이미지로 변환**하여 보관
압축·암호화를 통한 DLP 탐지 정책 우회

신종 채널
AI 프롬프트에 **영업비밀 또는 대외비** 입력
클라우드 공유 링크로 외부 공유 및 동기화

인가자 우회
공유계정의 비인가 사용
퇴직자 계정 및 **권한 미회수**

2-3. 진단 방법론 — 정보보안 리스크 분석

개인정보뿐 아니라 영업비밀, 설계자료, 연구자료 등 기업 **핵심 데이터의 유출·훼손 위험을 종합적으로 진단**합니다.
임직원의 이상 행위 패턴과 협력사·외주 인력의 데이터 접근 흐름까지 분석하여, 정보자산이 실제 업무 환경에서 적정하게 보호되고 있는지 검증합니다.

핵심 정보자산 식별
분류 · 중요도 · 보유 위치
진단 대상 자산 식별

→

유출 위험 사전 매핑
행위 · 흐름 · 유출 시나리오
잠재 리스크 평가

→

리스크 분석 결과 정리
개선 우선순위 및 보완 방안
개선방안 제시

진단 절차

1 **자산 식별**
핵심 데이터 분류
보유 위치 매핑

→ 2 **위험 매핑**
유출 경로 · 사각지대
시나리오 도출

→ 3 **행위 분석**
임직원 · 협력사
이상 행위 패턴

→ 4 **종합 진단**
리스크 우선순위
결과 보고·보완 권고

진단 항목

진단 영역	내용
핵심 데이터	• 영업비밀, 개인정보, 설계자료 등 **핵심 데이터 식별 및 보유 위치 매핑** • 데이터 분류 및 민감도 등급에 따른 **접근권한·보유기간 적정성** 진단
임직원 행위	• 접근, 다운로드, 전송 등 **사용자 이상 행위 패턴** 식별 • 퇴사 예정자 및 권한자의 **비정상 데이터 활용 정황** 사전 진단
협력사·외주	• 협력사·외주 인력의 **데이터 접근 및 반출 흐름** 진단 • 위탁계약 및 NDA 적용 범위와 실제 데이터 사용 정황 대조
사각지대	• 개인 단말, 원격 접속 등 **관리 사각지대 위험 평가** • 물리적 반출, 촬영, 출력 등 **비정형 유출 채널 리스크** 식별

실제 사례

협력사·외주
수탁사의 **위탁 계약 외 데이터 처리 및 접근**
NDA 적용 범위를 벗어난 정보 사용

임직원 행위
퇴직 예정자의 대량 파일 전송 정황
비업무시간 주요 폴더 접근 이력

사각지대
기밀자료 출력 후 물리적 반출
개인 **휴대전화 촬영**을 통한 자료 반출

3-1. 기업비밀 유출 사례 — 출력물을 통한 물리적 반출

사례 요약

3,700여장

***SOP 175건 · 국가핵심기술 2종**

C사 R&D 투자 자산 중 반출 시도된 출력 문서량

산업	바이오
유형	영업비밀·산업기술 물리적 반출 시도
주체	C사 전 직원 A씨 (본사 근무자)
기간	2022.12 행위 ~ 2025.7 판결
결과	**징역 3년 실형 선고** (미수 단계)

출처 매거진한경 magazine.hankyung.com/business/article/202507158148b

> 바이오 C사의 전 직원 A씨가 CDMO 표준작업지침서(SOP) 등 **영업비밀 175건, A4 약 3,700장을 열흘간 분산 출력**한 후 일부 문서를 은닉하여 반출하려다 **출문 게이트 검문 과정에서 적발**된 사례입니다.
> 외부 유출은 미수에 그쳤으나, 법원은 유출 시도 자체의 위험성을 인정하여 실형을 선고했습니다.

타임라인

직무 권한 보유
SOP · 국가핵심기술 175건
직무 권한으로 자료 접근

열흘간 분산 출력
A4 3,700여장 · 주말 회의실 활용
감사 임계 미도달

옷 속 300장 은닉
디지털 통제 회피
물리적 반출

현행범 체포
유출 미수
징역 3년 실형

탐지 실패 요인

- ✕ **디지털 통제 범위의 한계** — 출력물 기반 반출은 일반적인 파일 반출 통제 범위 밖에서 발생
- ✕ **출력 임계치 설정의 한계** — 일 단위 기준만 적용되어 분산 출력의 누적 이상치 미탐지
- ✕ **사전 경보 체계 부재** — 이상 출력 패턴을 사전에 탐지하지 못하고 출문 검문 단계에서 최종 적발

진단 방법론

HM COMPANY 분석 영역

- 출력 가능한 **핵심 자산의 관리 수준 점검** 및 사용자별 누적 **출력량 이상치 재구성**
- 프린트 로그를 일별·문서별·사용자별로 분석하여 **누적 출력 패턴의 이상 여부 탐지**
- **권한자의 비정상 열람 행위**와 핵심 문서 접근 시간대·빈도 이상치 분석
- 외부저장매체 연결 이력, 웹메일 전송, 클라우드 업로드 흔적 분석
- 퇴사 예정자의 접근 자료 인벤토리 확보 및 **사전 진단 체계 운영 여부 점검**

* SOP (Standard Operating Procedure): 제조·운영 과정의 표준 절차 문서
** CDMO: 의약품을 위탁받아 개발·제조하는 사업 모델

3-2. 정보유출 사례 — 아날로그 방식의 보안 통제 우회

사례 요약

192,088명

3년 2개월 미탐지

영업점 직원 12명에 의한 가맹점주 개인정보 장기 유출

산업	금융 · 카드
유형	개인정보 유출 (개인정보보호법)
주체	D사 영업점 직원 12명
기간	2022.3 ~ 2025.5 · 적발 2025.12
결과	**개인정보보호위원회 조사 착수** · 12명 징계

출처 경향신문 www.khan.co.kr/article/202512241411011

> 카드 D사의 영업점 **직원 12명이 약 3년 2개월간 가맹점주 19만 2,088명의 개인정보를 조회**한 뒤 카드 모집인에게 전달한 개인정보 유출 사례입니다.
> 파일 반출 방지 통제와 다운로드 차단이 작동하고 있었음에도, **모니터 촬영과 수기 전사 방식**으로 디지털 통제를 우회했습니다.
> 해당 사건은 내부 제보를 통해 적발되어 개인정보보호위원회 조사가 착수되었습니다.

타임라인

영업 실적 압박
12명 공모 시작
가맹점 DB 조회

모니터 촬영·수기
DLP 우회
아날로그 수법 활용

누적 192,088건
이상치 분석 부재로
장기 누적

내부 제보 적발
개보위 조사 착수
12명 징계 · 수사

탐지 실패 요인

- ✕ **아날로그 우회 채널의 통제 한계** — 촬영·수기 전사는 시스템 차단 범위 밖에서 발생
- ✕ **이상 조회 패턴 분석 체계 미흡** — 조회 이력은 존재했으나 이상행위 탐지 룰이 미흡
- ✕ **집합적 패턴 분석 부재** — 동일 대상 반복 조회, 특정 기간 집중 조회 등 집합 분석 미흡

진단 방법론

HM COMPANY 분석 영역

- 직원별 **개인정보 DB 조회 권한 범위 진단 및 권한** 적정성 평가
- DB 조회 이력에 대한 **임계치 설정 및 이상 패턴 탐지**
- **사용자별 누적 조회량** 통계 및 동일 직무군 대비 이상치 비교 분석
- 영업 실적 평가 시점과 개인정보 접근 패턴 간 **상관관계 분석**
- 부서·시점별 **개인정보 조회 패턴 비교 및 업무상 접근 필요성** 검토

3-3. 정보유출 사례 — 퇴사자 인증키 미회수

사례 요약

3,370만건

약 5개월간 미인지

대한민국 역대 최대 규모 개인정보 유출

산업	이커머스
유형	개인정보 유출 (개인정보보호법)
주체	E사 전 직원 (개발자)
기간	2025.06 ~ 2025.11 · 발표 2025.11
결과	**개인정보보호위원회 개선권고** · 경찰 수사

출처 한경비즈니스 magazine.hankyung.com/business/article/202512017037b

> 이커머스 E사의 전 직원이 **재직 중 발급받은 인증키를 이용해 퇴사 후에도 시스템에 접근**하고, 약 5개월간 **3,370만 건의 개인정보를 무단 유출**한 사례입니다. 퇴사 처리 과정에서 인증키 회수·폐기 절차가 정상적으로 이행되지 않아 통제 사각지대가 발생했습니다. 이후 개인정보보호위원회 개선권고, 경찰 수사 및 관계부처 신고 등 후속 조치가 진행되었습니다.

타임라인

인증키 보유
업무 권한으로
인증키 정상 발급

인증키 미회수
퇴사 처리 시
인증키 회수·폐기 누락

3,370만 건 유출
이상 접근 미인지로
장기 유출 누적

정부 조사 착수
개보위 개선권고
경찰 수사

탐지 실패 요인

- ✕ **퇴사 시점 권한·인증키 회수 점검 부재** — 퇴사 후에도 기존 인증키로 시스템 접근 가능
- ✕ **이상 접근 패턴 분석 체계 미흡** — 장기간 인증키 사용 이상 징후 미탐지
- ✕ **인증키 사용 이력 모니터링 부재** — 퇴사자 인증키 기반 토큰 발급 및 접근 이력 미추적

진단 방법론

HM COMPANY 분석 영역

- 핵심 시스템 **인증키·토큰의 발급, 회수, 재발급** 절차 운영 여부 진단
- **퇴사자 계정, 권한, 인증키, 토큰 회수** 체계 진단
- 개발자·관리자 **권한 보유자의 인증키 사용 이력 모니터링** 및 비정상 사용 탐지
- **API Key 및 인증 토큰의 외부 노출 여부** 진단
- 시간대, IP, 빈도 기준의 **이상 접근** 패턴 분석

4. 진단 절차 및 도입 효과

정보유출 발생 전 잠재 위험을 식별하기 위해 서버, PC, 외부저장매체, 이메일·메신저·클라우드 등 **주요 데이터 흐름을 통합 진단**합니다. 진단은 **사전 조사부터 대상자 심층 진단**까지 5단계로 진행됩니다.

진단 영역 및 분석 데이터

진단 영역	내용
서버 데이터	**유형** 기업 자체 서버 및 위탁 운영 데이터센터 **진단 채널** 이메일, 사내 메신저 **진단 데이터** 이메일 로그, 메신저 로그, 보안 솔루션 로그
PC 데이터	**유형** 업무용 PC 내 업무자료 및 사용자 행위 흔적 **진단 채널** 이메일, 외부저장매체, 클라우드, 프린트 **진단 데이터** OS 시스템 로그, 웹브라우저 사용 흔적, 메신저 로그, 클라우드 업로드 흔적

진단 절차

Step 1. 데이터 분석 | **Step 2. 심층 진단**

1. **사전 조사 및 진단 범위 정의**
2. **분석 데이터 수집**
3. **데이터 분석 및 위험 정황 식별**
4. **심층 진단 대상자 선정**
5. **대상자 심층 진단 및 개선안 도출**

도입 효과

기업비밀 유출 위험 사전 차단
서버·PC 데이터의 무단 반출 위험 식별

잠재 위험 영역 사전 식별
이메일·메신저·클라우드 기반 유출 경로 사전 점검

유출 가능 경로 식별
잠재 유출 경로 식별 및 보안정책 강화

데이터 기반 리스크 인사이트
이상 행위 패턴 분석을 통한 내부 위협 사전 인지

법적·규제 리스크 대응
관련 법규 준수 수준 점검 및 분쟁 예방

임직원 부정행위 리스크 식별
임직원 부정 정황 및 이상 행위 사전 인지

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		
디지털포렌식 서비스	정보유출 조사	IT 감사	컴플라이언스 리스크 진단	회계감사 외부전문가 조사	
정보보호 리스크 진단	KOLAS 공인시험성적서 발급		경영진단·내부감사	직장 내 괴롭힘 조사	PMA

Why HM COMPANY ADFS

15년+
디지털포렌식 기반
조사·진단 수행 경험

19,946+
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

HM COMPANY™

Pre-Diagnostic Service for Corporate Information Security Risk

Contact Us

박 재 현 상무

jaehyun.park@hmcom.co.kr

이 정 훈 수석

jeonghoon.lee@hmcom.co.kr

전화

02-6237-6213

기업 규모, 보안 환경, 진단 목적에 맞춰 최적의 정보보호 리스크 진단 범위와 수행 방안을 제안드립니다.

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