2026 Vol. 2

Privacy Report

2026 개인정보 이슈 심층 분석 보고서

개인정보 유출과 랜섬웨어

KISA 한국인터넷진흥원

목차
Contents

1

대형 플랫폼의 접근권한 관리와 개인정보 유출 위험 대응

이정민 카카오엔터테인먼트 정보보호최고책임자

10

데이터 탈취형 랜섬웨어와 입증책임의 문제

채성희 법무법인 광장 변호사

17

개인정보 유출에 대한 CEO-CPO 책임과 예방투자

김홍선 김·장 법률사무소 고문

Privacy Report
2026 Vol. 2

대형 플랫폼의 접근권한 관리와 개인정보 유출 위험 대응

- 대형 플랫폼의 인적 계정과 서비스 계정을 중심으로 -

이정민
카카오엔터테인먼트 정보보호최고책임자

접근권한 관리만으로는 개인정보 유출을 막을 수 없습니다.
권한이 필요한 주체와 시스템을 제대로 파악하고 필요한 범위와 기간에 대한 통제가 이뤄진 상태에서 사용 내역을 확인하는 것이 중요합니다.
이러한 체계로 유출 가능성과 영향 범위를 줄이고 사고 발생 시 대응력을 높일 수 있습니다.

1. 대형 플랫폼의 권한 위험 요인

첫 번째, 대형 플랫폼 서비스는 다수의 비즈니스 파트너가 플랫폼 서비스 운영에 참여하며, 이용자와 파트너가 거의 상시로 양방향 접근을 합니다. 또한, 실시간 피드백과 빈번한 업데이트도 이어집니다. 이런 환경에서는 개인정보취급자, 서버 운영자, DBA, 개발자, CS 등의 다양한 담당자들도 여러 시스템을 오가며 작업을 합니다.
상시적인 운영과 잦은 변화가 있을수록 한 번 부여한 권한이 현재 업무와 계속 일치하는지 확인하기 어려워집니다.

두 번째, 계정이 탈취되지 않더라도 정상 계정의 관리가 소홀하면 사용 위험이 커질 수 있습니다. 업무 범위보다 과도한 권한, 종료 시점이 없는 임시 권한, 직무 변경 후에도 유지되는 권한 등이 이에 해당합니다.
따라서 "권한을 주었는가"만 확인하는 데 그치지 않고 "누가 어떤 목적으로 얼마 동안 사용하며, 그 필요성이 현재도 유지되는가"를 살펴야 합니다.

단계	주요 실패	관리 방안
요청	목적이 모호하거나 업무보다 넓은 범위를 요구	업무 불가능성·대체수단을 먼저 확인
승인	업무 담당자와 기술 담당자 사이의 정보 격차	역할을 나누되 보안정책 관점에서 최종 판단
사용	SSO·자동화 접속, 특권 사용, 대량 조회를 늦게 인지	사용자 알림·전수 감사·위험기반 탐지
연장	기간 미정, 반복 연장, 직무 변경 후 잔존 권한	짧게 부여하고 목적을 재확인한 뒤 연장

현행 개인정보 보호법은 수탁자에게 목적 외 처리 금지와 안전조치를 요구하고, 위탁자에게 교육과 처리 현황 점검 등 감독 의무를 부과합니다.
그러나 일회성 점검만으로는 상시적인 접근과 이상 사용 여부를 통제하거나 파악할 수 없습니다.
특히 회사의 직접 통제 범위를 벗어난 외부자는 계약이나 감독 의무와 별도로 실제 권한이 사용되는 시점에서의 통제가 이뤄져야 합니다.[1]

2. 업무 목적별 범위와 기간설정

이러한 권한 위험을 줄이려면 업무 목적을 실제 시스템이 통제할 수 있는 조건으로 바꿔야 합니다.
'고객 응대에 필요합니다'라는 설명만으로 전체 고객정보 조회권한을 부여해서는 안 되며, 담당 고객과 서비스, 필요한 개인정보 항목, 조회·수정·다운로드 등 허용 행위, 사용 기간을 구분해야 합니다.
또한 화면상에 정보가 가려져 있더라도 다운로드 파일이나 API 응답에 원문이 포함된다면 통제 실효성이 없습니다.

권한을 검토할 때에는 업무상 필요성과 함께 더 적은 개인정보로 같은 목적을 달성할 수 있는지 확인해야 하며, 개발·시험에는 실제 개인정보가 없는 합성 데이터를 우선 사용하고, 실제 데이터가 필요하면 필요성과 사용 범위를 별도로 검토해야 합니다.

고객 응대의 경우는 담당 건에 필요한 정보만 보여주는 방식을 적용할 수 있습니다.
역할별로 기본 조회권한을 정하더라도 담당 서비스, 처리 대상, 접속 환경에 따라 범위를 더 좁힐 수 있다면 이를 적용하는 것이 적절합니다.
이는 필요한 작업에 필요한 권한만 부여한다는 최소권한 원칙을 구체화하는 과정입니다.[3]

(1) 외부 인력에는 계약과 작업 환경에 따른 조건을 추가합니다

내부 인력과 외부 인력 모두에게 최소권한을 적용해야 하며, 외부 인력은 계약 기간, 소속 업체, 내부 업무 책임자, 접속 단말의 관리 여부를 추가로 확인해야 합니다.
개인정보 처리업무를 위탁하는 경우에는 재위탁 동의 여부와 실제 작업자 변경이 권한 현황에 반영되는지 살펴야 합니다.
업체명 등으로 만든 공용계정만 관리하면 담당자가 교체되어도 기존 접근이 남을 수 있습니다.[1], [2]

구분	허용 범위 기준	종료 및 재검토
외부 인력 공통 조건	개인별 식별, 승인된 접속 경로와 단말, 대상 시스템	계약·담당자 변경과 계정 관리 연동
직무별 표준권한	CS·개발·운영 등의 업무와 필요한 데이터·기능	업무 변경 시 재검토 및 정기적 권한 필요성 확인
임시·예외 권한	표준권한으로 처리할 수 없는 구체적 작업	목적·만료 시점 설정 및 연장 시 재승인

(2) 표준권한과 고위험 예외의 승인 절차를 구분합니다

업무 책임자는 필요성과 기간을 설명하고, 데이터·시스템 책임자는 이를 바탕으로 허용할 데이터와 기능을 판단해야 합니다. 이때 표준 범위의 요청은 정해진 승인권자가 처리하되, 대량 반출이나 운영환경 관리자 권한처럼 영향이 큰 요청과 정책 예외에는 보안 검토를 추가하는 방식이 효과적입니다. 따라서 보안정책에 따른 최종 판단을 개별 요청의 보안부서 직접 승인으로만 구현할 필요는 없으며, 승인 기준과 위임 범위를 명확히 해야 요청량이 많은 환경에서도 통제를 유지할 수 있습니다.

프로젝트 종료일이 불확실한 경우에도 임시 권한의 만료 시점은 정해야 합니다.
우선 업무 수행에 필요한 기간을 부여하되, 연장할 때에는 목적과 범위를 다시 확인해야 합니다. 같은 예외가 반복되면 표준권한이 실제 업무를 반영하는지 검토하되, 반복된다는 이유만으로 상시 권한으로 전환해서는 안 됩니다.
접근 검토에 관한 연구에서도 검토자가 업무 맥락을 이해하고 적절한 정보를 제공받는 것이 중요한 과제로 제시되고 있습니다.

3. 인적 계정과 특권 계정 변경 관리

권한은 발급 시점에 적절했더라도 담당 업무가 바뀌면 불필요해질 수 있습니다.
따라서 입사 시·직무 변경 시·퇴사 시와 계약 종료 등의 인사 변동 여부를 계정의 발급·변경·회수 절차와 연결해야 합니다. 개인정보취급자별 계정 발급과 업무 변경 시 접근권한의 변경·말소는 개인정보의 안전성 확보조치 기준에서도 요구하는 사항입니다.[2]

(1) 사용자를 식별하고 일반 업무와 관리자 작업을 분리합니다

특권 계정도 실제 사용자를 확인할 수 있어야 합니다. 일반 업무용 계정과 관리자용 계정을 분리하거나, 개인별 인증을 거쳐 제한된 시간만 관리자 권한을 활성화하는 방식을 적용할 수 있습니다. 시스템 제약으로 공용 관리자 계정을 사용해야 한다면 사용할 수 있는 이용자를 사전에 정하고, 사용 시에는 정당한 사유를 남기도록 해야 합니다. 이와 함께 개인별 인증과 사용 이력을 해당 작업에 연결하되, 업무 편의를 위한 상시 공유는 예외로 인정해서는 안 됩니다.

다중 요소 인증은 외부 접속과 관리자 접근에 우선 적용하고, 개인정보에 접근하는 인적 계정으로 점차 확대하는 것이 좋습니다. 다만 인증수단을 하나 더 추가하는 것만으로 모든 위험이 사라지는 것은 아니므로, 인증수단의 등록·복구 절차와 이미 발급된 세션의 차단도 함께 관리해야 합니다. 장애 대응용 긴급권한은 신속하게 사용할 수 있도록 사전 절차를 정하되, 사용 시 필요성과 사용자, 종료 시점을 기록하고 사후 작업 내용의 적절성을 검토해야 합니다.

(2) 기록의 완전성과 사람의 검토 범위를 구분합니다

대형 플랫폼에서는 권한 변경, 감사기능 해제, 대량 조회·반출 등 고위험 작업의 중요도를 검토에 반영하고, 그 외 활동에는 자동 점검과 정기 검토를 결합하는 방식이 적절합니다.
이때 검토자 스스로가 본인이 수행한 작업을 직접 검토하고 종결하지 않도록 수행과 검토를 분리해야 합니다.
사용내역 전체를 감사 대상으로 확보하되, 검토 범위와 주기는 위험의 크기나 중요도 및 법적 기준에 맞춰 정해야 합니다.

(3) 회수 요청이 실제 접근 차단으로 이어지는지 확인합니다

부서이동 시에는 이전 업무에 따른 권한을 재검토하고, 새 업무에 필요한 권한을 별도로 승인하는 것이 일반적입니다. 또한 인수인계에 필요한 기존 권한에도 종료일을 설정해야 합니다.
이전·신규 부서장의 확인이 지연된다는 이유로 기존 권한 전체를 별도 기간 없이 유지해서는 안 됩니다.
또한, 통합 로그인 계정을 정지했더라도 개별 시스템의 로컬 계정이나 별도로 발급한 토큰이 남을 수 있으므로, 회수 완료 여부는 통합 계정의 삭제 처리 상태만으로 판단해서는 안 됩니다.
대상 시스템에 회수가 실제로 반영되었는지, 다른 경로로 접근할 수 있는지까지 확인해야 합니다.

4. 서비스 계정 관리

서비스 계정은 애플리케이션이나 배치 작업이 다른 시스템에 접근할 때 사용하는 계정입니다.
이때 API 키, 인증서, 접근 토큰은 신원을 증명하거나 접근을 허용하는 자격증명으로 사용되는데 계정 하나에 여러 자격증명이 연결될 수 있으므로 계정 목록만으로는 실제 접근 경로를 파악하기 어렵습니다.
이처럼 사용자뿐 아니라 서비스와 애플리케이션의 신원도 접근 판단에 포함해야 한다는 점은 제로 트러스트 관련 NIST 지침에서도 중요하게 언급하고 있습니다.[5]

(1) 계정의 책임자와 실제 사용처를 연결합니다

각 계정에는 소유 부서와 운영 책임자, 담당자 부재 시 대체 책임자를 정해 담당자 한 명의 기억에 의존하거나 조직 개편 후 책임자가 사라지는 상태를 피해야 합니다. 사용하는 서비스, 업무 목적, 운영·개발 환경, 접근 대상과 허용 기능을 연결하고 자격증명별 발급·교체·만료일과 최종 사용일도 관리해야 합니다.
이 과정에서 소스코드 검사나 트래픽 분석만으로 모든 키를 발견했다고 판단해서는 안 되며 최근 호출이 없다는 이유만으로 미사용 상태라고 판단해서도 안 됩니다.
실제로 월말 배치나 재해복구용으로 사용이 거의 없는 계정일 수 있으므로 실행 주기와 서비스 의존 관계까지 확인해야 합니다.

(2) 장기 유효 키를 줄이고 서비스별로 권한을 나눕니다

장기 유효 키는 유출 후에도 계속 사용될 수 있고 여러 시스템에 복제되면 회수 대상을 찾기 어렵습니다. 이러한 위험을 줄이려면 지원되는 환경에서는 실행 중인 서비스의 신원을 확인해 짧은 유효기간의 자격증명을 발급하는 방식을 우선 검토해야 합니다.
고정 키가 필요한 경우에는 코드나 일반 설정 파일에 직접 넣지 않고 접근이 제한된 저장소에서 관리하되 키 자체가 로그나 오류 메시지에 남지 않도록 해야 합니다.
운영환경과 개발환경, 서로 다른 서비스가 같은 키를 공유하지 않도록 하고 필요한 API·데이터·기능으로 권한을 제한해야 합니다.
이와 함께 키의 교체 주기와 만료 정책을 노출 위험 및 시스템 지원 범위에 맞춰 정하되 노출이 의심되는 경우에는 정기 교체일까지 기다려서는 안 됩니다.[3], [5]

5. 개인정보 접근 및 이상 사용 탐지

정상적으로 로그인했다는 사실만으로 이후의 모든 데이터 접근이 정당해지는 것은 아닙니다. 계정 탈취뿐 아니라 정상 계정의 오남용도 확인하려면 접속 기록을 권한 변경, 개인정보 조회와 다운로드 기록에 연결해 사용 흐름을 살펴야 합니다.
이를 바탕으로 담당 범위를 벗어난 조회, 짧은 시간의 반복 다운로드, 권한 상승 직후의 대량 추출 등을 업무 목적과 비교하되 정상 업무에도 대량 처리가 있을 수 있으므로 조회량만으로 유출 또는 정상 여부를 단정해서는 안 됩니다.

(1) 접속 위험과 사용 위험에 맞춰 조치합니다

위험기반 인증은 사용자 신원, 단말 상태, 접속 환경 등을 바탕으로 추가 확인이 필요한지를 판단하는 방식입니다.
이를 구현할 때에는 정책 규칙이나 위험 점수 등을 선택할 수 있으나 어느 방식을 택하더라도 접속 위치나 내부 네트워크라는 이유만으로 신뢰를 부여하지 않고 제로 트러스트 관점으로 필요한 자원에 대한 접근을 판단해야 합니다.[4]

상황	우선 조치	판단 시 유의점
새 단말 등 추가 확인 대상 접속	추가 인증 및 사용자 활동 확인 요구	위치·단말 정보 하나만으로 공격 단정 금지
정상 인증 후 업무 범위 외 조회·반출	해당 행위 제한 및 승인된 업무 여부 확인	추가 인증 성공만으로 권한 필요성 인정 불가
자격증명 탈취·유출이 강하게 의심되는 정황	세션·키·반출 경로 차단 및 사고 대응 개시	사용자 응답 대기 중 위험한 접근 허용 금지

위험 점수가 높을수록 위험한 것으로 평가하는 모델에서는 조치 임계치를 낮추면 탐지 범위와 오탐이 함께 증가할 수 있으므로 정상 업무의 종류와 실제 조사 결과를 반영하여 임계치를 조정해야 합니다. 위험기반 인증 연구에서도 서비스 환경과 설정에 따라 보안성과 사용성이 달라질 수 있음을 보여주며, 다른 서비스의 수치나 가중치를 그대로 적용하기보다 정상 업무 차단과 탐지 누락을 함께 검증해야 합니다.[7]

(2) 사용자가 대응할 수 있는 알림을 제공합니다

모든 로그인 성공·실패를 같은 방식으로 알리면 중요한 경보가 묻힐 수 있으므로 새 단말이나 의심스러운 접속 등 확인이 필요한 사건을 선별해야 합니다.
로그인 알림 연구에서도 이러한 알림의 선별과 구체적인 대응 안내가 중요하게 다뤄집니다. 다만 사용자 알림은 탐지를 보완하는 수단이므로 응답이 없더라도 보안 조직의 확인과 대응은 진행되어야 합니다.[6]

(3) 로그와 탐지 결과도 보호 대상으로 관리합니다

접속기록은 책임 추적에 필요한 식별자·접속일시·접속지·처리 대상·수행업무 등을 남기되 비밀번호·토큰과 불필요한 개인정보 원문을 저장하지 않아야 합니다.
이렇게 수집한 기록은 법적 보관·점검 기준에 따라 관리하고, 이를 분석하는 화면에서도 직접 식별정보는 필요한 범위로 제한하여 원본 조회와 식별정보 연결 권한을 통제해야 합니다.[2]
탐지에 AI를 적용하는 경우에도 위험 점수만으로 업무 정당성을 판단해서는 안 되며 규칙 기반 점검과 실제 조사 결과를 먼저 확보해 AI 탐지 내역이 선별에 도움이 되는지 검증이 필요합니다. 이때 차단 근거와 해제 이력을 남겨 AI 탐지로 인해 업무가 중단된 경우에도 신속히 재검토할 수 있어야 합니다.

6. 유출 의심 시 접근 차단과 영향 검토

이상징후를 발견해도 관련 계정과 데이터를 확인하는 동안 접근이 계속되면 피해가 커질 수 있습니다. 이를 막으려면 접근권한 관리 체계에 평상시의 승인·회수뿐 아니라 사고 시 누가 무엇을 제한할지까지 포함해야 하며, 이와 같이 탐지, 대응, 복구를 위험관리와 연결하는 것은 NIST의 사고 대응 지침에서도 강조하는 방향입니다.[8]

(1) 위험한 접근을 제한하고 증거를 보존합니다

사고 대응 담당자는 최초 인지 시각, 의심 계정·자격증명, 대상 시스템, 확인된 행위를 기록하고 관련자에게 상황을 공유해야 합니다.

개인정보의 대량 조회나 외부 전송이 의심되면 해당 세션과 반출 기능을 제한하고 필요한 경우 계정 정지와 키 폐기를 진행해야 합니다.
이때 이미 발급된 세션과 토큰이 모두 무효화되는지는 반드시 확인해야 합니다.
상시 운영 서비스에서는 전체 시스템의 일괄 중단이 이용자 피해를 키울 수 있으므로 계정별, 권한별, 기능별, 서비스별 차단 수단을 각각 준비해야 합니다.
이러한 차단 조치와 함께 조사에 필요한 인증·조회·다운로드·권한 변경 로그를 보존하고 접근을 제한해 증거 보존과 추가 피해 방지를 병행해야 합니다.[8]

(2) 접근 가능한 범위와 실제 영향을 구분해 조사합니다

피해 범위를 조사할 때에는 계정이 접근할 수 있었던 개인정보와 실제 조회·변경·반출된 개인정보를 구분해야 합니다.
이를 위해 대상 정보의 항목과 정보주체 범위, 발생 기간, 외부 전송 여부를 확인하고 다른 서비스나 분석 저장소로 접근이 이어졌는지도 조사해야 합니다.
이렇게 확보한 조사 결과는 확인된 사실, 합리적으로 의심되는 범위, 아직 확인하지 못한 사항으로 나누어 구분해야 피해 범위를 정확하게 판단할 수 있습니다.
위탁업체가 관련된 경우에도 이러한 조사에 필요한 기록과 조치 현황을 요청하고 확보해야 하며 업체의 조사만 기다려서는 안 됩니다.

(3) 통지와 신고 판단을 조사 완료까지 미루지 않습니다

개인정보 유출 등을 알게 된 경우에는 해당 정보주체에게 지체 없이, 원칙적으로 72시간 이내에 통지해야 합니다. 여기서 법령의 '유출등'에는 분실·도난·유출뿐 아니라 위조·변조·훼손도 포함됩니다.
기관 신고는 별도의 요건에 따라 판단해야 하며 실제 유출 등이 발생했고 정보주체 1천 명 이상에 관한 경우, 민감정보·고유식별정보가 포함된 경우, 외부 불법 접근에 의한 경우 중 어느 하나에 해당하면 개인정보보호위원회 또는 한국인터넷진흥원에 원칙적으로 72시간 이내 신고해야 합니다.[9], [10]

한편 이번에 새롭게 추가된 사항으로 불법 접근으로 유출 등이 의심되지만 정보주체를 특정하기 곤란한 경우, 또는 제3자의 불법 거래 등 일부 유출 등이 확인되어 다른 정보주체의 유출 등 가능성도 인정되는 경우에는 유출 가능성 통지 요건을 검토해야 합니다. 이 요건에 해당하면 해당 불법 접근 또는 사실을 안 때부터 원칙적으로 72시간 이내에 가능성이 있는 모든 정보주체에게 통지해야 합니다.

7. 관리 책임과 성과지표의 개선 우선순위

접근권한 관리는 업무 필요성, 기술적 허용 범위와 보안정책을 함께 판단해야 하므로 업무 책임자는 목적과 기간을, 데이터·시스템 책임자는 허용 범위를 확인해야 합니다.

이러한 판단이 실제 처리로 이어지도록 운영 조직은 권한 처리 결과를 관리하고 보안 조직은 기준 수립, 고위험 예외 검토, 독립 점검을 맡는 방식으로 역할을 나눌 수 있습니다.
여기에 개인정보보호 담당 조직이 법적 의무와 사고 통지·신고를 함께 검토해야 하며 이 모든 역할은 조직 명칭보다 책임 기준에 따라 부여되는 것이 중요합니다.

(1) 통제의 존재보다 실제 적용 범위부터 확인합니다

개인별 계정이나 다중 요소 인증을 도입했다는 사실만으로 관리 수준이 충분하다고 판단할 수는 없습니다. 실제 적용 범위를 확인하려면 인적 계정은 관리자 화면과 외부 접속 등에 인증 통제가 빠져 있는지 살펴보고 서비스 계정은 신원 확인과 자격증명 관리를 별도로 점검해야 합니다.
점검과 개선의 순서는 개인정보가 집중된 시스템과 대량 반출 경로를 파악하는 데서 시작해 소유자 없는 계정, 불필요한 특권, 만료 없는 예외, 노출된 자격증명을 우선 정리하는 순으로 진행해야 합니다.
이 과정에서 기본 정책을 각 서비스가 실제로 이행하는지와 정책과 인증 시스템 장애 시의 처리 방식도 점검해야 합니다.
제로 트러스트는 이와 같이 접근 판단을 지속적으로 개선해 나가는 원칙으로 적용하는 것이 필요합니다.[4], [5]

(2) 보안성과 업무 영향을 같은 기준으로 점검합니다

지표	측정 방식	유의점
관리 현황의 완전성	소유자·목적·권한 범위가 확인된 대상 수 ÷ 식별된 전체 관리 대상 수	미등록 대상 발견 현황도 함께 관리
회수 처리 시간	인사·계약 변경 효력 발생 또는 서비스 사용 종료·폐기 결정부터 실제 차단 확인까지의 소요시간	계정 유형(인적·서비스) 및 시스템별 구분 분석
탐지 후 조치 시간	이상징후 접수부터 확인 및 필요한 차단까지의 시간	사고 유형·심각도 및 미처리 건 함께 검토
업무 영향	정상 업무가 제한된 건의 비율과 권한 승인 소요시간	신속성만을 위한 검토 수준 하향 금지

지표를 비교할 때에는 대상과 측정 기간을 고정하고 평균뿐 아니라 시스템별 편차도 확인해야 하며, 예외 권한 비율이나 경보 수가 줄었다는 사실만을 성과로 삼으면 필요한 예외와 미탐지가 가려질 수 있습니다.
지표 점검과 함께 권한 회수와 사고 대응 절차가 실제로 작동하는지도 모의훈련으로 검증이 필요합니다.

정리하자면 접근권한 관리의 성과는 불필요한 접근을 줄이고 잘못된 사용을 발견했을 때 영향 범위를 확인해 조치할 수 있는지로 평가해야 합니다.
이를 위해 대형 플랫폼은 사람과 서비스의 신원, 허용한 권한, 실제 사용 기록을 연결하고 업무가 바뀔 때마다 이를 갱신해야 하고, 이런 관리체계가 데이터 최소화, 안전한 개발과 운영, 사고 대응과 함께 작동할 때 개인정보 유출 가능성과 피해를 줄일 수 있다고 생각합니다.

참고문헌

법령·고시 적용 기준일은 2026년 9월 18일입니다. 일부 개정 조항은 부칙에 따라 시행 시점이 다릅니다.

[1] 개인정보 보호법 제26조 업무위탁에 따른 개인정보의 처리 제한.

[2] 개인정보보호위원회. 개인정보의 안전성 확보조치 기준. 고시 제2026-9호, 2026.7.1. 일부개정. 제5조·제8조 및 부칙.

[3] NIST. (2020). SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations.

[4] Rose, S. et al. (2020). NIST SP 800-207, Zero Trust Architecture.

[5] Chandramouli, R. & Butcher, Z. (2023). NIST SP 800-207A, A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments.

[6] Markert, P., Lassak, L., Golla, M. & Dürmuth, M. (2024). Understanding Users' Interaction with Login Notifications. CHI '24, Article 853.

[7] Wiefling, S. et al. (2023). Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service. ACM TOPS, 26(1), Article 6.

[8] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.

[9] 개인정보 보호법 제34조 개인정보 유출등의 통지·신고. 법률 제21445호, 2026.9.11. 시행.

[10] 개인정보 보호법 시행령 제39조, 제39조의2·제39조의3, 제40조. 대통령령 제36671호, 2026.9.11. 시행.

데이터 탈취형 랜섬웨어와 입증책임의 문제

채성희
법무법인 광장 변호사

1. 랜섬웨어의 개념 변화

전통적인 관점에서 랜섬웨어(Ransomware)는 주로 데이터의 가용성(availability) 침해에 초점이 맞춰져 있었다. 미국 CISA(Cybersecurity and Infrastructure Security Agency)는 랜섬웨어를 파일을 암호화한 후 복호화를 대가로 금전을 요구하는 악성코드라고 설명한 바 있다.[1] 그러나 2010년대 중반까지 암호화(encryption) 또는 잠금(locking)과 같은 한두 가지 행위에만 집중되던 랜섬웨어 공격 양상은 사이버 위협 환경이 급변함에 따라 다각적으로 진화하기 시작했다.

이러한 변화의 핵심 요인으로 기업들의 백업 및 복구 능력 향상으로 인해 전통적인 '암호화' 방식만으로는 공격자들의 협상력이 약화되었다는 점을 들 수 있을 것이다. 이에 따라 공격자들은 데이터 가용성을 마비시키는 데 그치지 않고, 기업의 민감 데이터를 외부로 유출하여 공개하겠다고 협박하는 전략을 취하게 되었다.[2]

이와 같은 공격 양상의 구조적 변화로 인해 기존의 단순한 유형 구분은 더 이상 적절하지 않게 되었으며, 유럽 ENISA(European Union Agency for Cybersecurity)는 랜섬웨어를 새롭게 정의하기에 이르렀다. ENISA는 랜섬웨어를 "공격자가 대상의 자산을 통제한 후 그 자산의 가용성(availability)과 기밀성(confidentiality)을 돌려주는 대가로 몸값을 요구하는 공격"으로 정의하였다.[2] 특히 ENISA는 랜섬웨어 공격에는 자산(assets), 행위(actions), 협박(blackmail)이 존재한다고 설명하며, 이러한 정의가 공격자가 데이터를 암호화(encrypt)하였는지 또는 탈취(steal)하였는지에 좌우되지 않는다고 명시하고 있다. 이 중 랜섬웨어의 핵심 행위를 Lock(잠금)·Encrypt(암호화)·Delete(삭제)·Steal(탈취)의 네 가지 LEDS로 분류하면서, 탈취는 공격자의 통제 아래로 데이터를 복사하는 행위를 의미한다고 설명한다. 데이터 탈취에는 인터넷을 통한 외부 반출(exfiltration)이 포함되며, 탈취가 반드시 암호화나 삭제를 수반하는 것은 아니다. 실제로 ENISA는 데이터 탈취가 증가하면서 데이터 암호화 없이 이루어지는 갈취(extortion without any data encryption)가 관찰되고 있음에 주목하였다.[3] 즉, 랜섬웨어로서 암호화를 수행하지 아니하더라도 탈취한 데이터를 공개·판매하겠다는 위협만으로 금전을 요구하는 유형(이하 "데이터 탈취형 랜섬웨어"라 한다)까지 랜섬웨어의 개념에 온전히 포섭되도록 변화하였다.

2. 데이터 탈취형 랜섬웨어의 진화 및 증가

피해 기업의 시스템과 데이터를 암호화하고 몸값을 요구하는 동시에, 피해 기업의 민감한 데이터를 외부로 반출하고 추가 협상 수단으로 공개 사이트에 게시하겠다고 위협하는, 이른바 이중 갈취(double extortion)는 앞서 설명한 바와 같이 2010년대 중반 이후 빈발하기 시작하였다. 2019년 말 Maze 랜섬웨어 그룹의 사례가 대표적이다.[4] 이처럼 데이터 탈취 및 공개 위협이 도입된 이후 갈취 수단 역시 다양해져 탈취 정보의 다크웹 경매, 언론 접촉을 통한 피해 사실 확산, 피해 기업이 복구를 시도할 경우 직접 전화하여 압박하는 행위 등이 추가되었다.[4]

이러한 데이터 탈취형 랜섬웨어 사고는 국내외를 불문하고 점점 그 발생 빈도 및 비율이 증가하는 추세이다. Google Threat Intelligence Group(GTIG)과 Mandiant의 2025년 분석에 따르면, 2025년에 Mandiant가 대응한 랜섬웨어 침해사고 중 약 77%에서 데이터 탈취가 확인되거나 의심되어 2024년(약 57%) 대비 크게 증가한 것으로 나타났다.[5] 국내 문헌에서도 데이터 탈취형 랜섬웨어의 확산세를 확인할 수 있다.

• 과기정통부와 KISA는 2024년 사이버위협을 분석하며, 고객정보를 빌미로 한 삼중 갈취를 주요 동향으로 지적하였다. 즉, 랜섬웨어가 기업 기밀자료 유출 및 공개 협박에 더해 피해 기업에 대한 DDoS까지 수행하는 "3중 갈취 전술"로 고도화되고 있다는 것이다. 아울러, 피해 기업의 협력사·고객 등 이해관계자에게 직접 접촉하여 추가 몸값을 요구하는 양상을 지적한 바 있다.[6]

• KISA는 Qilin 랜섬웨어 그룹이 국내 금융 IT 컨설팅·데이터 운영기업을 공격해 대규모 데이터 유출을 일으킨 후, 서버에 저장된 다수 자산운용사의 정보를 개별 피해사례로 분리하여 각각 별도로 협상을 시도한 실제 사례를 소개하였다. 당시 2025년 KISA에 신고된 랜섬웨어 감염 건수는 274건으로 전년(195건) 대비 증가하였다.[7]

• 2026년 상반기에는, KISA 신고·접수 기준 랜섬웨어 신고는 145건으로 전년 동기(82건) 대비 76.8% 급증하였으며, 과기정통부와 KISA는 '데이터 유출을 결합한 이중 갈취 확산'을 2026년 상반기 5대 핵심 사이버 위협 중 하나로 선정하였다.[8] 관련하여 공격자들은 시스템을 암호화하기 전에 중요 데이터를 외부로 빼낸 뒤 복호화 대가와 데이터 비공개 대가를 동시에 요구하고 있다.

이러한 동향과 관련하여 주목할 점은, 개인정보 자체가 공격자가 의도적으로 탐색하고 탈취하는 '갈취 자산'으로 변모하였다는 점이다. ENISA가 623건의 랜섬웨어 사건을 분석한 결과, 탈취된 데이터 중 58.2%에 건강정보(PHI), 여권번호·비자정보, 주소 등 GDPR 상 개인정보가 포함되어 있었다.[2] Mandiant의 조사에서도 공격자가 민감한 데이터를 수집하기 위해 해당 정보가 존재할 가능성이 높은 시스템을 직접 탐색(manual reconnaissance)한 증거가 확인되었다.[5] 이로 인해 피해는 시스템을 운영하는 기업에 그치지 않고, 포함된 개인정보의 주체인 고객·임직원·거래처 등 제3자에게까지 확산되고, 기업에 대하여는 개인정보 보호법에 따른 책임 문제를 발생시킨다.

3. 데이터 탈취형 랜섬웨어 사고의 특징 – 사고 조사 및 입증에 어려움을 야기하는 요소들

데이터 탈취형 랜섬웨어의 확산은 피해 규모의 확대뿐만 아니라, 사고 발생 여부와 피해 범위를 입증하고 파악하는 과정에서 구조적인 특수성과 어려움을 수반한다. 특히 암호화를 수반하지 않는 데이터 탈취형 랜섬웨어 사고는 종래의 개인정보 유출 사고뿐 아니라 암호화에 국한한 전통적인 랜섬웨어 사고와도 구분된다. 종래의 개인정보 유출 사고는 대개 유출 사실이나 흔적의 발견에서 출발하여 조사를 통해 경위와 범위를 확인해 가는 경우가 많고, 전통적인 랜섬웨어 사고에서는 개인정보 데이터베이스의 암호화 사실이 발견되면 적어도 개인정보의 훼손이 있었다는 점이 확인될 수 있다(2026. 9. 11.부터 시행된 개정 개인정보 보호법에서는 '훼손'도 '유출 등'에 포함되어 비로소 통지 및 신고의 대상이 되었고, 개정 전 법에서도 '훼손'은 과징금 부과 사유에는 해당하였다. 랜섬웨어에 의한 암호화도 이러한 '훼손'에 해당한다고 볼 수 있을 것이다). 이와 달리 암호화를 수반하지 않는 데이터 탈취형 랜섬웨어 사고에서는 훼손의 외형이 없고, 유출 여부와 범위에 관한 파악이 상당 부분 공격자의 주장에 의존하게 되므로 여러 가지 입증상의 어려움을 수반한다.

첫째, 공격자가 공개한 정보와 실제로 탈취한 정보가 일치하지 않는 특징이 있다. 공격자는 실제 데이터를 보유하고 있음을 증명하고 몸값을 압박하기 위해 탈취 데이터의 일부만 먼저 공개(partial leak)하거나, 협상 실패 시 전부를 공개하는 방식을 취한다. ENISA 분석에 따르면 전체 사건 중 62건(9.95%)에서 부분 공개가, 236건(37.88%)에서 전체 공개가 확인되었는데[2], 이는 공격자가 외부에 노출한 샘플 범위만으로는 실제 탈취된 개인정보의 전체 범위를 정확히 특정할 수 없음을 시사한다. 그런데 이러한 공격자의 주장은 블러핑일 수 있어서 공격자의 주장만으로 실제 유출 여부, 유출 항목 및 규모를 정확히 판단하기 어려운 것이다. 이러한 어려움은 데이터의 훼손(암호화)이 이루어지지 않는 데이터 탈취형 랜섬웨어 사고의 경우 더욱 가중된다.

둘째, 데이터 탈취 여부 및 범위를 사후적으로 확인하는 것 자체가 쉽지 않다. 여기에는 여러 측면이 있다: i) 랜섬웨어 공격자들이 사용하는 인프라는 웹사이트가 자주 업데이트되지 않거나, 공개된 유출 데이터 링크가 만료되거나, 데이터에 접근할 수 없거나, 웹사이트가 폐쇄되는 등 매우 불안정한 특성을 지닌다.[2] 이로 인해 피해 기업들은 실제 랜섬웨어 공격이 발생했는지, 그리고 구체적으로 어떤 파일이 외부로 탈취되었는지를 객관적으로 입증하고 확인하는 데 큰 어려움을 겪고 있으며, 공식적으로 드러난 통계와 사건은 빙산의 일각에 불과하다는 평가를 받고 있다.[2] ii) 일반 침해사고의 경우 침해자는 사고 발생 경로를 은폐하기 위한 로그의 대규모 삭제와 같이 조기 발견 가능성을 높이는 행동을 굳이 하지 않는 경향이 있다. 그러나 랜섬웨어의 경우 침해 사실을 알리는 것 자체가 목적이고 이를 굳이 은폐할 필요가 없으므로 관련 로그를 삭제하는 등 증거 파괴 행위가 빈번히 발생한다. 특히 기술적으로도, 랜섬웨어 실행 단계 중 시스템 복구 억제(Inhibition) 단계에서 이벤트 로그와 섀도우 카피를 중지하는 과정이 수반되고, 때로는 로그 파일 자체를 암호화하므로 포렌식에 필요한 흔적이 사라지는 결과가 발생하기도 한다.[2]

4. 데이터 탈취형 랜섬웨어 사고의 입증에 관한 문제점들

(1) 개인정보 보호법 제34조에 따른 통지·신고 시점의 혼선

개인정보 보호법 제34조 제1항 및 제4항은 개인정보처리자가 개인정보가 '유출등이 있음을 알게 되었을 때' 지체 없이 정보주체에 대한 통지 및 개인정보보호위원회 또는 KISA에 신고하도록 규정하고 있다. 그런데 데이터 암호화가 없는 데이터 탈취형 랜섬웨어 사고에서는 우선 '유출등이 있었음을 알게 되었을 때', 즉 통지 및 신고 의무의 기산점을 확정하기가 어렵다. 피해 회사 입장에서는 만일 공격자의 랜섬노트를 발견한 즉시 그에 따라 신고 및 통지를 수행할 경우, 실제로는 데이터 유출이 없었음에도 개인정보보호위원회의 조사 대상이 되는 한편 정보주체들의 신뢰를 상실하는 결과를 맞이할 수 있다. 그렇다고 하여 포렌식 및 공격자 대화 등을 통해 실제 유출 범위가 특정될 때까지 통지를 유예한다면, 그동안 앞서 살펴본 바와 같이 공격자가 로그를 완전히 파괴하여 유출 범위를 특정할 수 없게 되는 사태가 발생할 우려가 있다. 이 경우 개인정보처리자는 유출 사실을 확정할 수 없으므로, 법 제34조에 따른 통지·신고 의무 발생이 무한정 지연되는 문제가 발생한다.

물론 공격자가 다크웹에 탈취한 개인정보의 일부를 게시하거나 개인정보처리자에게 샘플 정보를 제공할 수 있고, 그 구성이 개인정보처리자의 데이터베이스와 일치한다면 그 일부에 대한 유출이 인정되고, 나머지에 대해서는 유출 가능성 통지(개인정보 보호법 제34조 제2항)를 수행하면 될 것이다.[9] 이를 참조하여 공격자로부터 유출이 주장되는 데이터를 충분한 분량으로 입수하고(특히 다크웹에 공개된 경우 앞서 언급한 바와 같이 인프라가 불안정하므로 조속히 샘플 데이터를 개인정보처리자의 영역으로 확보하여 두는 것이 필요하다), 공격자가 공개 내지 제공한 자료와 자사 데이터베이스의 일치 여부, 레코드의 최신성 여부, 내부 고유 식별자 포함 여부 등을 면밀히 비교 검토하고 다른 가능한 자료와 교차 검증함으로써 주장을 검증하는 단계가 필요할 것이다.

(2) 사고 발생 및 내용에 관한 입증책임

데이터 탈취형 랜섬웨어 사고는 개인정보 보호법상 개인정보의 유출에 해당하므로, 만일 개인정보처리자가 안전성 확보조치를 다하였음을 입증하지 않는 한 매출액의 최대 3%에 달하는 과징금이 부과될 수 있다(개인정보 보호법 제64조의2 제1항 제9호). 과징금 액수를 산정함에 있어서는 위반행위에 상응하는 비례성과 침해 예방에 대한 효과성이 확보될 수 있도록 위반행위의 내용 및 정도, 개인정보처리자가 처리하는 개인정보의 유형과 정보주체에게 미치는 영향, 개인정보가 유출등이 된 경우 위반행위와의 관련성 및 유출등의 규모와 같은 사항들을 고려하여야 한다(개인정보 보호법 제64조의2 제5항 제1호, 제5호). 이와 같이 과징금 부과 처분 사유의 기초사실이 되는 개인정보의 유출 발생에 관한 입증책임은 처분청인 개인정보보호위원회에 있다.[10] 또한, 개인정보 유출과 안전성 확보조치 간의 인과관계는 요구되지 아니하지만, '위반행위와의 관련성'을 과징금 액수 산정에 고려하여야 하고, 이는 위반행위의 중대성 판단의 요소이므로(개인정보 보호법 시행령 제60조의2 제7항, [별표 1의5]), 개인정보보호위원회로서는 위반행위의 중대성

판단을 정당화하기 위하여 최소한 유출과 안전성 확보조치 위반 간의 '관련성'은 입증할 수 있어야 할 것이다. 유출등이 의심되는 개인정보의 유형과 정보주체에게 미치는 영향, 유출등의 규모도 마찬가지이다.

이와 관련하여 가장 먼저 눈에 띄는 문제는, (다시 한번, 암호화가 된 경우는 유출등의 존재 및 내용에 관하여 비교적 입증이 용이하므로 암호화를 수반하지 않는 데이터 탈취만이 본고의 검토 대상임을 다시 한번 명확히 한다) 실제 유출 발생 여부, 사고의 정확한 규모, 탈취된 개인정보의 종류와 정보주체에 미치는 영향(민감정보 여부 등)을 입증하기 위한 근거자료가 존재하지 않거나, 존재하더라도 전체 사고 규모 중 일부에 국한하는 경우가 많다는 것이다. 이러한 상황에서 처분청이 실제로 공격자가 공개한 샘플 데이터만을 가지고 전체 데이터셋에 대하여 동일한 유출이 발생하였음을 전제로 사고의 중대성을 판단하고 과징금 액수를 산정한다면, 처분사유가 적정하였는지에 대한 문제가 발생할 수 있을 것이다.

나아가 랜섬웨어 실행 과정에서 앞서 살펴본 바와 같이 피해 시스템의 이벤트 로그 등 포렌식에 필요한 증거가 파괴되었다면, 공격자의 초기 침투 경로를 특정하기 어려워진다. 물론 개인정보처리자로서는 이벤트 로그가 없더라도 시스템의 설정이나 여러 가지 관리 기록 등을 통하여 안전성 확보조치를 이행하였음을 어느 정도 입증할 수 있겠으나, 결정적으로 침투 경로와 관련하여 안전성 확보조치 위반이 없었다는 점, 예컨대 침투가 알려지지 않은 취약점을 통하여 이루어졌다는 점을 입증할 수 없게 된다. 이러한 사정은 개인정보처리자의 의무 위반이 없음에 관한 유력한 정황이라는 점에서 그러한 입증 기회의 상실은 처리자에게 중대한 불이익이 될 수 있다. 더욱이 일단 침투가 이루어진 후 공격자에 의해 이벤트 로그가 삭제·암호화될 수 있었다는 사실 자체가, 삭제 내지 암호화된 이벤트 로그에 개인정보처리시스템에 대한 접속기록이 포함되어 있다면, 접속기록 보관 의무 위반(개인정보의 안전성 확보조치 기준 제8조 제3항)의 정황이 될 수 있을 것이다. 그런데 안전성 확보조치 이행과 유출 간의 인과관계를 요구하지 아니하고 다만 관련성을 과징금 액수 산정에 감안하도록 하고 있는 현행법 규정에 의하면, 실제로 침투 자체가 개인정보처리자의 의무위반과 무관하게 이루어졌더라도 이벤트 로그가 삭제된 이상 안전성 확보조치 위반이 인정되어 고액의 과징금을 부과받는 경우가 발생할 수 있는 것이다. 이로 인하여 개인정보처리자가 사실상 결과책임을 부담하게 되는 것은 아닌지 재고하여 볼 필요가 있어 보인다.

민사적으로도, 개인정보 보호법 제39조 제1항은 정보주체의 손해배상청구권과 관련하여 고의 또는 과실 없음에 대한 입증책임을 개인정보처리자에게 부과하고 있다. 이와 관련하여서도 위와 같은 이유로 개인정보처리자가 입증 불가로 인한 결과책임을 부담하는 결과가 발생할 우려가 있을 것이다. 이 조항은 개인정보 유출에 관한 개인정보처리자의 귀책사유를 정보주체가 입증하기 어렵기 때문에 입증책임을 전환한다는 취지의 규정인데, 과연 이와 같이 개인정보처리자의 결과책임을 인정하는 경우까지 의도 내지 용인하는 것이라고 해석함이 타당할지 의문이다.

5. 결론

이상에서 살펴본 바와 같이, 랜섬웨어의 개념은 데이터의 가용성 침해에서 기밀성 침해까지 포괄하는 방향으로 확장되었고, 이제는 암호화 없이 탈취한 데이터를 공개하겠다는 위협만으로 금전을 요구하는 데이터 탈취형 랜섬웨어가 주된 공격 양상으로 자리 잡아 가고 있다. 그러나 이러한 사고는 훼손의 외형 없이 유출 여부와 범위에 관한 판단을 상당 부분 공격자의 주장에 의존하게 하고, 공격 과정에서 포렌식에 필요한 증거까지 파괴되는 경우가 많다. 그 결과 개인정보처리자로서는 통지·신고 의무의 기산점을 확정하기 어렵고, 과징금 절차에서는 일부 샘플로부터 전체 유출이 추단되거나 의무 위반과 무관한 침투에 대해서도 사실상 결과책임을 지게 될 위험에 놓일 수 있다. 나아가 민사소송에서도 무과실의 입증이 불가능해짐에 따라 입증책임 전환 규정의 본래 취지를 넘어서는 책임을 부담할 우려가 있다.

따라서 실무적으로는 개인정보처리자가 공격자가 공개한 데이터를 조속히 확보하여 자사 데이터베이스와 교차 검증하고, 평소 안전성 확보조치의 이행 증거와 접속기록을 공격자가 시스템을 장악하더라도 보존되는 방식으로 축적해 두는 노력이 필요할 수 있다. 개인정보보호위원회로서는 입증되지 아니한 잠재적 피해가 아닌 실제 확인된 피해에 기초하여 위반행위의 중대성을 판단하였음을 명확히 입증할 수 있어야 하며, 유출과 위반행위와의 관련성 또한 보다 신중히 검토할 필요가 있겠다. 입법론적으로는 데이터 탈취형 랜섬웨어 사고의 특수성을 고려하여, 증거의 공백에 대한 책임이 어느 일방에게 일률적으로 전가되지 않도록 하는 제도적 보완을 검토할 필요가 있을 것이다.

참고문헌

[1] CISA, MS-ISAC, NSA & FBI. (2023). #StopRansomware Guide(Version 3.0, October 2023). p. 3.

[2] ENISA. (2022). ENISA Threat Landscape for Ransomware Attacks. pp. 8–10, 14, 18–22.

[3] ENISA. (2022). ENISA Threat Landscape 2022. p. 36.

[4] ENISA. (2021). ENISA Threat Landscape 2021. p. 25.

[5] Google Threat Intelligence Group. (2026). Ransomware Under Pressure: Tactics, Techniques, and Procedures in a Shifting Threat Landscape.

[6] 과학기술정보통신부·한국인터넷진흥원. (2024). 2025년 사이버 위협 전망. pp. 5–6.

[7] 과학기술정보통신부·한국인터넷진흥원. (2026). 25년 사이버 위협 하반기 동향 및 26년 전망. pp. 5, 13.

[8] 과학기술정보통신부·한국인터넷진흥원. (2026). 2026년 상반기 사이버 위협 동향 보고서. pp. 6, 14.

[9] 개인정보보호위원회. (2026). 개인정보 유출등 대응 안내서. 39면.

[10] 대법원 1984. 7. 24. 선고 84누124 판결.

개인정보 유출에 대한 CEO-CPO 책임과 예방투자

김홍선
김·장 법률사무소 고문

1. 프라이버시의 등장과 개인정보보호

미국은 개인의 자유와 인권을 중요한 가치로 삼고 탄생한 국가지만, 정작 미국 연방헌법에는 프라이버시(Privacy)라는 단어가 단 한 번도 등장하지 않는다. 프라이버시를 독립적인 법적 권리로 처음 체계화한 것은 1890년 〈하버드 로 리뷰(Harvard Law Review)〉에 게재된 '프라이버시에 대한 권리(The Right to Privacy)'라는 논문이다.[1] 글을 쓴 주인공은 보스턴에서 활동하던 새뮤얼 워렌과 루이스 브랜다이스 변호사다.

이 글이 나온 배경에는 카메라와 황색 언론이 있다. 1888년 코닥이 내놓은 휴대용 카메라는 오늘날의 스마트폰에 버금가는 혁신의 아이콘이었다. 그런데 바로 이 문명의 기기가 문제를 일으켰다. 누구나 손쉽게 사진을 찍을 수 있게 되자, 사교계 인사들의 사생활이 가십 신문의 좋은 먹잇감이 된 것이다. 워렌과 브랜다이스는 새로운 기술과 언론의 관행이 개인의 사적 영역을 침범하는 현실에 주목했다. 브랜다이스는 훗날 연방 대법관이 되어 미국 프라이버시 보호를 옹호하는 중요한 반대의견을 남겨서 미국 프라이버시 법리의 초석이 되는 판례를 만들어냈다.

신기술은 새로운 사회적 개념을 만들어낸다. 디지털 혁명도 예외가 아니다. 그중 하나가 디지털로 저장된 개인정보를 보호해야 한다는 데이터 프라이버시(Data Privacy)다. 기업이 개인정보를 수집한 목적을 벗어나 부적절하게 활용하거나, 관리 부실로 개인정보가 외부에 노출되어서는 안 된다는 개념이다.

디지털 데이터는 일반 물체와 특성이 다르다. 값비싼 보석을 도둑맞으면 보석은 주인의 손에서 사라진다. 그러나 디지털 정보를 탈취하는 공격자는 원본은 그대로 둔 채 복제해 간다. 디지털 정보에는 이전(transfer)이 아니라 복제(copy)가 일어날 뿐이다. 이를 경제학에서는 '비경합성(non-rival)'이라고 한다.

따라서, 개인정보가 유출되었다고 해서 데이터베이스나 파일 안의 정보가 사라지지 않는다. 정보를 도둑맞고도 소유자가 이를 한참 동안 알아채지 못하는 이유가 여기에 있다. 정보의 유출 여부는 주로 데이터에 접근한 시스템의 로그 기록을 통해 확인된다. 개인정보보호가 시스템과 네트워크를 보호하는 사이버보안과 밀접할 수밖에 없는 이유다.

필자가 은행에서 10년간 최고정보보호책임자(CISO), 개인정보보호책임자(CPO), 신용정보관리·보호인의 역할을 함께 수행할 수 있었던 것도 이처럼 개인정보보호와 사이버보안이 긴밀하게 연결되어 있기 때문이다. 은행이 보유한 개인정보와 신용정보는 대부분 디지털 공간에 존재한다. 사이버보안과 개인정보보호는 서로 다른 법적 목적과 책무를 갖지만, 보안 통제와 개인정보 유출 방지는 한 배를 타고 있는 셈이다.

AI의 확산은 여기에 새로운 과제를 더한다. 기존의 무단 접근과 정보유출 위험에 더해 프롬프트 인젝션, 데이터 오염, 모델 응답을 분석해 학습 데이터를 역추출하는 공격 등 위협의 양상이 전혀 다르다. RAG로 연결된 문서, 벡터 데이터베이스, 외부 도구와 AI 에이전트에 제공한 접근권한까지 관리 대상이 넓어진다. 따라서, 패킷과 로그 분석, 접근권한 통제를 중심으로 방어해 온 기존 보안팀의 역량만으로는 한계가 있다. 어떤 정보가 어떤 경로로 학습과 추론에 쓰이는지, 즉 데이터 파이프라인과 데이터 거버넌스가 핵심 통제 대상이 되므로 CPO의 역할도 더욱 전문화될 수밖에 없다.

문제는 개인정보보호가 특정 부서만의 문제가 아니라는 점이다. CPO는 현업의 데이터를 직접 다루지 않으며, 조직의 예산과 인력을 배분할 권한도 없다. 그러므로 CPO의 권한과 책임이 세밀하게 정의되어야 하며, 무엇보다 현업 부서와의 역할 분담과 조직 전체의 거버넌스 체계 안에서 제자리를 찾아야 한다.

2. 견제와 협력의 3선 방어체제

2020년 데이터 3법(개인정보보호법, 신용정보법, 정보통신망법)이 개정되면서 개인정보 규제 환경에 큰 변화가 일어났다. 이 개정은 가명정보를 도입해 데이터 활용의 가능성을 열었지만, 기업에는 그에 걸맞은 책임 체계가 요구되었다.

당시 은행에서는 전사적인 개인정보 및 신용정보 거버넌스를 전면적으로 재편하는 험난한 여정이 시작되었다. 데이터를 다루는 모든 프로세스를 세부적으로 재수립하고, 각 부서의 R&R(역할과 책임)과 데이터 오너쉽(ownership)을 명문화해야 했다. 개인정보를 수집하는 순간부터 저장, 활용, 제공, 분리 보관, 파기에 이르기까지 누가 어떤 권한을 갖고, 그에 따른 책임은 누구에게 있는지 명확하게 정의해야 했다.

과정은 결코 순탄치 않았다. 어떤 부서도 새로운 책임을 떠안고 싶어 하지 않는 것은 어쩌면 조직의 본능이다. 필자는 현업 부서장들을 지속적으로 만나 설득했다.

"개인정보보호 부서에서는 여러분의 데이터를 직접 관리하지 않습니다. 데이터를 직접 관리하지 않는 조직 혼자서 어떻게 모든 사고를 예방하고 책임질 수 있겠습니까? 개인정보를 실제로 수집하고, 저장하고, 활용하고, 파기하는 것은 각 현업 부서입니다. 여러분이 안전하고 효율적으로 업무를 수행할 수 있도록 정책과 가이드라인을 마련하고, 필요한 인프라를 적극적으로 지원하겠습니다. 그러나, 데이터의 실제 운영과 그에 따른 위험을 관리하는 일차적인 책임은 현업이 가져야 합니다."

이 길고 지난했던 여정의 하이라이트는, 개인정보 프로세스의 오너쉽을 가진 각 현업 부서장(1선)들이 자신의 역할과 책임이 명확히 규정된 문서에 직접 서명한 순간이었다. 데이터의 생성부터 파기까지 실무를 담당하는 부서가 제1방어선이 되어 스스로 책임을 지고, CPO(2선)는 그들이 안전하게 달릴 수 있도록 정책과 가이드라인을 설계하고 제대로 운영되는지 모니터링하는 방어체계가 비로소 완성되었다. 서명된 문서를 CEO에게 보여드리며 거대한 산을 하나 넘은 느낌이었다.

권한과 책임의 불일치를 바로잡고, 견제와 균형을 통해 기업의 리스크를 근본적으로 줄이는 것. 이것이 보안과 데이터 거버넌스를 지탱하는 '3선 방어모델(Three Lines of Defense)'의 본질이다.[2]

모델의 원리는 분명하다. 개인정보를 수집·활용하는 현업과 이를 처리하는 IT 운영조직은 자신이 수행하는 업무의 위험을 직접 관리하는 제1선이다. CPO와 위험관리·준법감시·정보보호의 감독 기능은 전문지식을 바탕으로 기준을 마련하고, 현업의 통제를 지원·모니터링하며 필요한 경우 이의를 제기하는 제2선이다. 그리고 이들로부터 독립된 제3방어선(내부감사)이 1선과 2선의 거버넌스와 내부통제가 제대로 작동하는지 객관적으로 검증한다.

통제의 설계와 운영을 두 번에 걸쳐 교차 검증하고, 책임을 구분하면서도 서로 협력하고 견제하는 구조다. 방어선을 명확히 구분해야 각자의 책임 소재가 분명해지고, 사각지대를 보완할 수 있다. 견제와 협력이라는 강력한 톱니바퀴는 수많은 개인정보처리 프로세스 전반에 맞물려 돌아가야 한다.

리스크 관리가 업의 본질인 금융에서는 3선 방어체계가 감독 기준에 깊이 반영되어 있다.[3] 은행의 자본 적정성을 규정하는 바젤II 협약(2004)은 기존의 신용 리스크, 시장 리스크에 운영 리스크(Operational Risk)를 더해 3대 리스크의 틀을 완성했다. 운영 리스크는 '부적절하거나 실패한 내부 프로세스, 인력 및 시스템, 또는 외부 사건으로 인해 손실이 발생할 위험'을 뜻한다.[4] 사실상 조직 안에서 일어날 수 있는 모든 위험한 상황이 여기에 해당한다. 화재, 강도, 시스템 장애, 횡령, 사기가 그렇고, 정보유출도 마찬가지다.

2선의 견제가 실질적이려면 독립적인 판단과 그 판단을 실행에 옮길 수 있는 '통제 권한'이 뒷받침되어야 한다. 1선에 치명적인 문제가 방치되어 있을 경우, 2선은 해당 서비스의 개시를 보류하거나 중단을 요구하고 이를 경영진에 직보할 수 있어야 한다. 일종의 '킬 스위치(Kill-switch)'라고 할 수 있다. 과연 지금 CPO에게 그러한 권한이 주어져 있는가?

그러나 이러한 체계도 CEO의 리더쉽 없이는 제대로 작동하기 어렵다. 개인정보보호는 부서 간 이해관계가 충돌하고, 때로는 비즈니스의 편의성과 비용 문제까지 수반하기 때문이다. CPO가 아무리 좋은 정책을 만들어도 현업이 따르지 않거나 필요한 인력과 예산이 확보되지 않는다면 실효성을 기대하기 어렵다. 개인정보를 여러 조직이 함께 사용하는데 CPO 조직이 모든 책임을 지는 것도 비합리적이다. 조직 전체의 자원과 우선순위를 조정할 수 있는 CEO의 역할이 중요해지는 이유다.

3. CEO의 미션

흔히 정보유출 방지는 기술적으로 어려운 영역이라 비전문가가 이해하기 힘들고, 그래서 책임을 지기도 어렵다고 한다. 물론 모든 기술의 세부 사항을 이해하는 것은 쉽지 않다. 하지만 현장에서 간과하는 훨씬 더 중요한 본질이 있다. 개인정보보호와 사이버보안은 기술의 문제이기 이전에 결국 '조직문화와 예산'의 문제라는 점이다. 바로 이 대목에 이사회와 경영진이 귀를 기울여야 한다.

개인정보 유출사고의 상당수는 알려진 취약점을 제때 조치하지 못한 데서 시작된다. 보안취약점을 진단해서 찾아내는 것은 2선인 보안 부서의 역할이다. 그러나 정작 거대한 병목은 취약점을 찾은 뒤에 발생한다. 발견된 취약점을 분석하고 패치하는 작업은 보안팀이 아니라 IT 개발·운영팀의 책무다. 오탐(false-positives)을 걸러내고 서비스에 미치는 영향을 평가해야 하며, 변경 작업의 내용과 근거도 기록해야 한다. 취약점을 발견하는 것과 그것을 해결하는 것은 전혀 다른 업무다.

조직 간의 협조를 구하는 과정은 더 험난하다. 해당 서비스를 주관하는 현업 부서와 일정을 조율해야 하고, 대고객 서비스를 일시 중단해야 된다면 사전에 고객에게 공지해 양해를 구해야 한다. 장애로 인한 서비스 중단을 줄이기 위해 패치 작업은 대부분 모두가 잠든 야간이나 주말에 진행한다. 불필요한 개인정보 파기나 접근권한 회수도 마찬가지다. 발견은 2선이 하지만, 조치는 1선의 일손을 필요로 한다.

그렇다면, 어떻게 해야 하는가? 늘어나는 업무 부하를 감당할 수 있도록 IT 인력을 확충하고, 수작업을 줄이기 위한 자동화에 투자해야 한다. 결국 인력과 예산의 문제다.

그러나 경영진은 이런 현장의 실상을 모르는 경우가 많다. 그렇지 않아도 IT 예산이 크다는 이유로 비용절감 압박을 받는 상황에서, IT 부서가 보안 패치를 위한 인력보강을 요청하기는 쉽지 않다. CEO와 이사회가 예산과 인력이라는 고리를 풀어주지 않는다면, 아무리 첨단 솔루션으로 수만 개의 취약점을 찾아내더라도 실제 조치는 지연된다. 결국 진단 실적은 늘어나지만 실제 위험은 줄어들지 않는 상황이 된다.

무기만 좋다고 군대가 강해지는 것은 아니다. 군대는 일사불란하게 움직일 수 있는 규율과 수송·보급 같은 병참 인프라를 바탕으로, 적절한 전략에 따라 움직인다. 개인정보 방어체계도 솔루션 구매만으로 완성되지 않는다. 제품이 업무 프로세스에 녹아 있어야 하고, 운영하는 사람들이 잘 써야 하며, 무엇보다 개인정보가 흐르는 생애주기가 정책에 따라 빈틈없이 설계되어야 한다.

비즈니스의 전략과 우선순위를 정하고, 적절한 예산과 인적 자원을 할당하는 것은 일개 부서에서 결정할 수 있는 사안이 아니다. CEO는 각 부서의 책임과 권한을 명확히 하고, 필요한 인적·물적 자원을 배분하며, 이해관계가 충돌할 때 경영적 결단을 내려야 한다. 이사회는 경영진이 적절한 위험관리체계를 갖추고 이를 효과적으로 운영하는지 감독해야 한다. CPO는 중요한 위험과 개선 현황을 경영진과 이사회가 이해할 수 있는 언어로 보고해야 한다.

CEO와 이사회가 개인정보보호의 책임을 진다는 것은 조직의 최상위 책임자라는 선언적 의미에 그치지 않는다. 개인정보보호 책무는 세밀하게 정의되어야 한다. CEO가 책임질 영역, 각 부서장의

역할, 그리고 CPO의 권한과 책임이 명확히 구분되고 상호 견제되어야 한다. 이를 위해서는 조직 전반에 걸쳐 개인정보보호 리스크를 관리하는 투명하고 명확한 프로세스가 구축되어야 한다. 이러한 인력과 자원, 프로세스를 총괄하는 것이 CEO다.

이러한 책임은 이제 법률에도 명시되었다. 2026년 9월 11일 시행된 개정 개인정보보호법은 사업주 또는 대표자에게 개인정보 보호에 필요한 전문인력과 예산을 지원하는 등 총괄적인 관리조치를 할 의무를 명시했다. CPO의 독립적인 업무 수행을 강화하고 대표자와 이사회에 정기적으로 보고하도록 했으며, 매출액 1,800억 원 초과 등 일정 규모 이상의 기업은 CPO를 지정·변경·해제할 때 이사회 의결을 거쳐 개인정보보호위원회에 신고해야 한다.[5]

주목할 부분은 예방투자에 대한 제도적 평가다. 개정법은 반복적이거나 고의 또는 중과실이 수반된 중대한 위반행위에 대한 제재를 강화했다. 반면 예산·인력·설비에 대한 투자의 규모와 지속성, 대표자의 책임 이행 정도, CPO 중심 보호체계의 운영 수준 등을 따져 고의·중과실이 아닌 한 과징금을 최대 40%까지 감경할 수 있게 했다. 사고가 발생한 뒤 책임자를 문책하는 것보다 사고를 예방하기 위한 인력과 시스템에 미리 투자하도록 유도하는 취지다. 예방투자는 이제 선의가 아니라 경영 판단의 문제다.

내부통제에 대한 경영진의 법적 책임도 무거워지고 있다. 대법원은 2021년 11월 11일 판결에서 회사의 규모와 영업 성격, 법적 위험 등에 비추어 높은 위험이 예상되는 경우, 대표이사가 합리적인 내부통제시스템을 구축하고 정상적으로 작동하도록 노력해야 한다는 취지의 법리를 제시했다.[6] 업무를 담당 이사들에게 분장했다는 사실만으로 대표이사의 감시의무가 사라지는 것은 아니라는 의미다.

금융권에서는 2024년 시행된 금융회사지배구조법에 따라, 임원별 내부통제 책임 범위를 문서로 확정하는 '책무구조도'가 은행·금융지주부터 단계적으로 도입되고 있다.[7] 이제 책임의 구조를 설계하고, 운영하고, 견제하는 선진 경영체제로 나아가야 한다.

4. 경영의 원칙

ISMS-P 인증을 받은 기업에서도 개인정보 유출사고가 잇따르자, 인증제도의 실효성에 대한 논란이 일었다. 여기서 드러나는 것은 기업 경영 현장에서 종종 목적(Purpose)과 목표(Objective)를 혼동하는 현상이다.

ISMS-P 인증은 사이버보안과 개인정보보호의 훌륭한 목표다. 인증을 준비하면서 자산과 개인정보처리 업무를 식별하고, 정책과 절차를 정비하며, 보안 통제의 수준을 점검할 수 있다. 문제는 인증을 빨리 받으려고 그 범위를 일부 영역으로 한정하거나, 일시적인 체크리스트 통과에만 집중한다는 것이다. 인증이라는 목표에만 급급하다 보면, 고객정보를 잘 지켜 고객의 신뢰를 얻는다는 본연의 목적을 놓칠 수 있다.

초연결환경에서는 공격자가 어디로 침투해 올지 알기 어렵고, 운영을 하다 보면 설계대로 통제가 작동하지 않기도 한다. 그래서 방어체계에 대한 설계도 중요하지만, 운영상의 실효성(Operational Effectiveness)이 더 중요한 지표다.

규제 역시 같은 함정에 빠질 수 있다. 체크리스트는 최소한의 보안기준을 일관되게 강제한다는 점에서 유용한 출발점이다. 그러나 체크리스트는 본질적으로 '무엇을 갖추었는가'를 묻지, '실제로 안전한가'를 보장하지 못한다. 악의를 가진 해커나 내부자는 체크리스트가 다루지 못하는 빈틈을 노린다. 그래서, 글로벌 규제는 기업이 스스로 위험을 평가해 통제를 설계하고, 그 실효성을 입증하도록 요구하는 리스크기반 책임성(accountability)의 원칙으로 옮겨가고 있다. 형식적인 준수를 넘어 실질적인 안전으로 목적을 명확히 설정해야 한다.

어느 기업에서는 매년 새로운 보안인증을 받는 것을 KPI로 세운다고 한다. 물론 인증을 취득하는 과정에서 보안 수준이 높아질 수는 있지만, 그만큼 인력과 자원이 정작 필요한 업무에서 빠져나간다. 경영이란 한정된 자원 속에서 최선의 결과를 끌어내는 예술인데, 목표가 목적을 앞지르면 기업 전체의 리스크 균형이 무너질 수 있다.

개인정보를 보호해야 하는 진정한 목적은 무엇인가? 개인정보보호는 기업이 고객과 맺은 엄중한 약속이다. 기업이 이 약속을 지키는 것은 고객과 주주, 나아가 사회에 대한 기업의 책무다. 이 목적을 잊은 채 솔루션 도입과 인증 획득이라는 단기 목표에만 매몰되면, 정작 유출사고가 났을 때 스스로를 '운이 없는 피해자'로 여기는 착각에 빠질 수 있다. 최고경영진과 이사회가 개인정보보호 본연의 목적을 확고하게 붙들 때, 비로소 기업의 가치를 지킬 수 있다.

5. 결론

개인정보보호는 조직 전체가 리스크 관리의 틀 안에서 풀어가야 할 의제다. 결코 특정 부서 또는 개인이 전담할 이슈가 아니다. 모든 기업이 반드시 3선 방어체제를 그대로 도입해야 한다는 것은 아니다. 조직의 규모와 업의 특성에 따라 부담스러울 수도 있다. 그러나 적어도 프로세스와 오너쉽, 견제와 검증 절차가 갖춰져야 통제 수준을 높일 수 있다. 사람은 실수할 수 있고, 운영하다 실패할 경우는 다양하다. 전체 조직의 극히 일부인 CPO 부서 직원들의 개인기에 기업의 생존을 맡길 수 있겠는가?

개인정보보호는 CPO 한 사람에게 책임을 맡긴다고 해결되는 문제가 아니다. 현업은 자신이 다루는 데이터에 책임을 지고, CPO는 전사적인 보호체계를 설계하고 감독하며, 내부감사는 그 실효성을 독립적으로 검증해야 한다. 그리고 CEO는 이 모든 조직이 제 역할을 할 수 있도록 권한과 자원을 부여하고 부서 간 갈등을 조정해야 한다. 책임을 분담한다는 것은 책임을 떠넘기는 일이 아니라 조직 전체가 책임을 실제로 이행하도록 만드는 일이고, CEO는 그 결과에 대해 경영 차원의 책임을 져야 한다. 개정 개인정보보호법이 대표자의 책임과 예방투자에 대한 과징금 감경을 함께 규정한 것도 같은 맥락이다.

AI와 복잡한 비즈니스 생태계는 개인정보가 이동하고 활용되는 범위를 더욱 넓히고 있다. 공격자의 수법 역시 프론티어 AI를 활용하며 빠르게 진화하고 있다. 이런 시대에 안전조치와 체크리스트에만 의존하는 정보유출 방어체계로는 한계가 있다. 먼저 개인정보보호가 조직 전체의 문제임을 인식하고, 모든 구성원이 참여하는 체계를 갖춰야 한다. 그러려면 CPO의 권한과 책임이 세밀하게 정의되어야 하며, 무엇보다 조직의 자원과 우선순위를 총괄적으로 결정하는 최고경영자(CEO)의 책임과 역할이 분명해야 한다.

참고문헌

1. Warren & Brandeis, “The Right to Privacy,” Harvard Law Review 4(5), 1890. https://www.brandeis.edu/library/archives/exhibits/ldb-100/career/privacy.shtml

2. The Institute of Internal Auditors, “Statement of Position – Three Lines Model”, IIA는 2020년 ‘Three Lines of Defense’를 ‘Three Lines Model’로 개정했음. https://www.theiia.org/en/resources/statements-of-position

3. Basel Committee, Corporate Governance Principles for Banks (2015), 현행 통합 지침 CGO10. https://www.bis.org/committees/bcbs/basel-consolidated-guidelines/module/cgo/10

4. Basel Committee, Operational Risk, Basel Framework ORR10 https://www.bis.org/committees/bcbs/basel-consolidated-guidelines/module/orr/10

5. 개인정보보호위원회, 「개인정보 유출 사전예방·피해구제 강화를 위한 개인정보 보호법·시행령·고시, 9월 11일부터 시행」, 2026.9.10. https://pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=12459

6. 대법원 2021. 11. 11. 선고 2017다222368판결 “회사에 관한 소송” https://www.law.go.kr/LSW/precInfoP.do?precSeq=219783

7. 금융위원회, 「지배구조법 시행령 개정안 국무회의 통과」, 2024.6.11. https://www.fsc.go.kr/po010104/82422

Privacy Report
2026 개인정보 이슈
심층 분석 보고서

『2026 개인정보 이슈 심층 분석 보고서』는
개인정보보호위원회 출연금으로 수행한
사업의 결과물입니다.

한국인터넷진흥원의 승인 없이 본 보고서의 무단전재나
복제를 금하며, 인용 출처 『2026 개인정보 이슈 심층 분석
보고서』를 밝혀주시기 바랍니다.

본 보고서의 내용은
한국인터넷진흥원의 공식 견해가 아님을 알려드립니다.

발행

발행일 2026년 10월

발행처 한국인터넷진흥원 개인정보예방팀
전라남도 나주시 진흥길 9

Privacy Report

2026 개인정보 이슈 심층 분석 보고서

2026 Vol. 2

KISA 한국인터넷진흥원