042 섀도 AI

Shadow AI

조직의 공식 승인이나 통제 없이 직원이 개인적으로 AI 도구를 사용하는 현상

- 생산성 향상을 위해 생성형 AI 등을 자율적으로 사용하면서, 보안·데이터 관리 사각지대를 발생시키는 조직 운영 리스크
- 단순히 통제와 차단의 대상으로만 보기보다, 조직 내 AI 사용 현황에 대한 가시적 확보와 관리·통제 체계 마련이 필요

섀도 AI의 개념

섀도 AI란 IT 부서 등 조직의 공식적인 승인이나 감독 없이, 조직 구성원이나 직원이 AI 도구나 애플리케이션을 개인적으로 사용하는 현상을 의미합니다. 업무 생산성 향상이나 반복 작업 자동화를 목적으로 ChatGPT와 같은 생성형 AI 서비스를 개인 계정으로 활용하는 경우가 대표적입니다. 조직이 인지하거나 승인하지 않은 상태에서 '그림자'처럼 활용된다는 점에서 '섀도 AI'라는 명칭이 붙었습니다. 이는 비인가 IT 기술 사용을 의미하는 '섀도 IT'와 유사하지만, AI가 데이터를 처리·학습하는 특성으로 인해 위험이 더 복잡하고 은밀하게 확대될 수 있다는 점에서 차이가 있습니다.

섀도 AI로 인한 피해

섀도 AI는 AI의 실무 활용 가치가 커질수록 빠르게 확산되고 있습니다. 그러나 이러한 비공식적 사용은 조직 차원의 보안 및 데이터 관리 위험을 크게 증가시킵니다. CISCO의 「2025 사이버보안 준비 지수」에 따르면, 전 세계 보안 리더의 83%는 섀도 AI 탐지에 자신이 없다고 응답했으며, 다수의 조직이 실제 사용 현황을 정확히 파악하지 못하고 있는 것으로 나타났습니다. 또한 주요 AI 서비스에 입력된 데이터 중 일부에 기업 내부 정보가 포함된 사례가 확인되었고, IBM의 「2025 데이터 유출 비용 보고서」는 섀도 AI 관련 사고가 탐지·대응에 더 많은 시간과 비용을 초래한다고 분석했습니다.

섀도 AI의 대응 방안

섀도 AI에 대응하기 위해서는 단순한 사용 금지보다 안전한 활용을 전제로 한 관리전략이 필요합니다. 매니지엔진의 조사에 따르면, IT 의사결정권자의 97%는 섀도 AI를 기업에 대한 심각한 위협으로 인식하고 있는 반면, 91%의 직원들은 섀도 AI 사용에 거의 위험이 없다고 인식하고 있는 것으로 나타났습니다. 이러한 인식 격차는 섀도 AI 관리의 또 다른 리스크 요인으로 지적됩니다. 전문가들은 섀도 AI를 통제와 차단의 대상으로만 보기보다, 조직의 공식 AI 활용 체계 안으로 안전하게 흡수·관리하는 접근이 중요하다고 강조하며, 이를 위해선 AI 활용 교육과 명확한 정책 정비가 필수적입니다.