

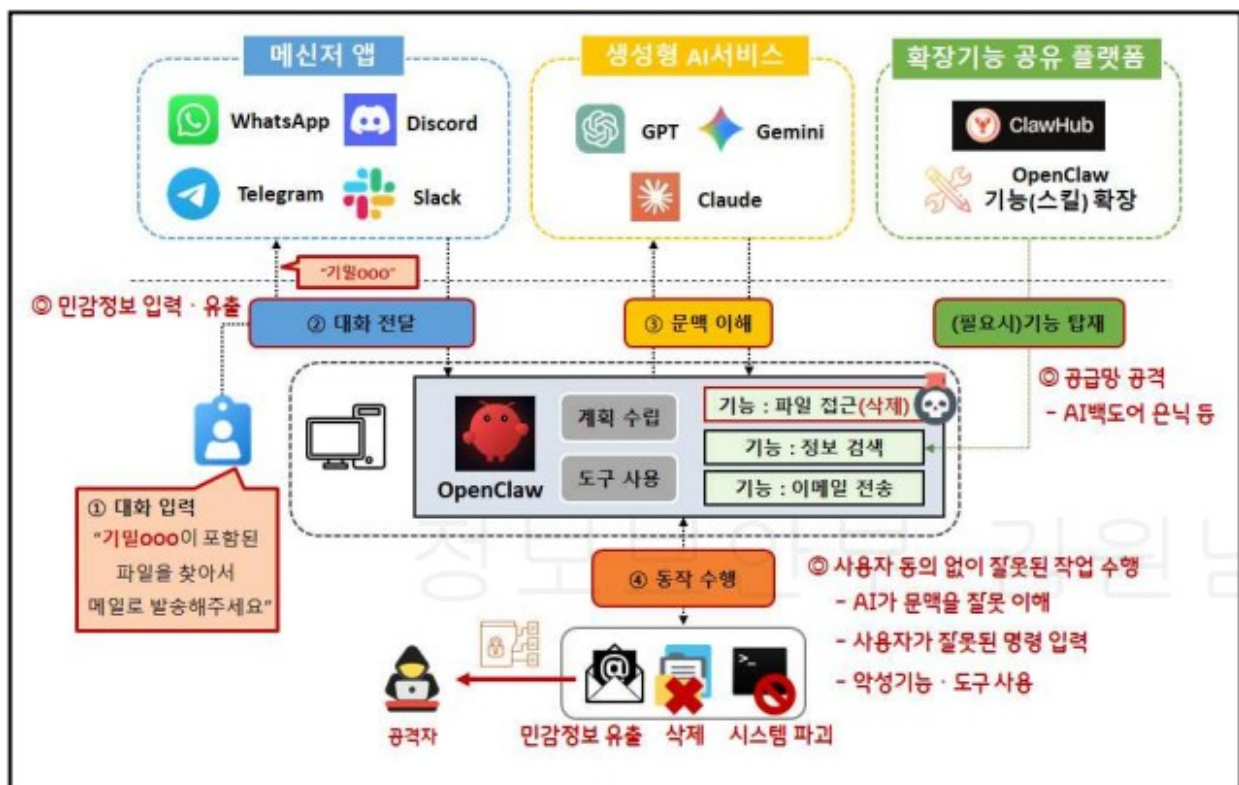
[보안권고문] 오픈클로(OpenClaw) 사용 주의 안내

‘오픈클로(OpenClaw)’ 활용 시 자료 유출, 파일 삭제 등 보안 취약요소가 발견

민감 정보 등이 저장된 업무용 PC에서는 사용 자제를 권고하며 업무와 무관한 개인 PC에서 사용 시 ‘파일 읽기만 가능하게 권한 부여’ 등

1 개요

최근 이슈되고 있는 오픈소스 AI 에이전트인 오픈클로(OpenClaw)¹⁾ 관련 취약요소가 발견



- (민감 정보 유출) 사용자 명령 프롬프트가 메신저 앱 및 생성형 AI서비스 등 (GPT 등)에 전달, 저장되어 내부 민감정보가 포함되어 있을 경우 유출 가능

※ 예시) 명령 프롬프트: 기밀문서 OOOOOO를 PC에서 찾아서 내 이메일 OOO@OOO.com으로 전송해줘

1) 오픈클로(OpenClaw) : 사용자 단말에 설치되어 브라우저, 메신저와 연계 동작하여 자동 업무를 처리하는 오픈 소스 기반 AI에이전트

- (사용자 동의 없이 작업 수행) 오픈클로가 파일삭제 및 내부 자료 외부 전송 등 가능
- (공급망 공격) 오픈클로가 기능확장(이메일 전송) 시 공유 플랫폼(클로허브 등)에 게시된 소스코드 활용 및 해당 소스코드에 백도어, 악성코드 은닉 가능
- (원격제어) 해커가 제작한 웹사이트에 방문 시 인증 토큰 탈취 및 방화벽 우회를 통한 제어권 탈취
- 이와 관련, 아래 권고 사항 실시 및 사이버 침해사고 등 특이사항 발생 시 즉시 경기교육사이버안전센터(031-240-6599, goeboan@korea.kr)로 신고

② 권고 사항

민감 정보가 포함된 업무용PC, 서버에서 오픈클로 사용 자제

업무와 무관한 개인용 PC에서 사용 시 **보안 설정, 대책 수립**하여 활용

- (보안 설정) 설정파일(openclaw.json)에 권한 제한 설정
 - ☞ 데이터를 임의로 수정, 삭제하지 못하도록 읽기 권한만 부여
 - ☞ 사용가능한 도구 목록 설정 및 위험도구 실행 시 사용자 승인
 - ☞ 외부 생성형 AI서비스 대신 로컬 AI모델 사용
- (보안 대책)
 - ☞ 메신저앱 대신 오픈클로에 직접 사용자 대화 입력
 - ☞ 불필요 기능 탑재 금지 및 기능 안전성 사전 확인
 - ☞ 별도 PC 혹은 도커 등 가상화 기술을 활용하여 격리하에 사용