개인정보보호위원회 보도자료

보도시점 배포 즉시 배포 2026. 6. 15.(월) 10:00

# 개인정보위, 클라우드·개발 협업도구 사용시 자격증명 관리 강화 당부

- 최근 자격증명 노출로 인한 개인정보 유출 사고 증가, 안전한 계정·권한관리 중요
- 깃허브(GitHub) 등 개발 협업도구에 접근키, 비밀번호, API 토큰 등 자격증명을 저장하지 않도록 관리 필요

개인정보보호위원회(위원장 송경희, 이하 '개인정보위')는 **클라우드 기반 서비스와 소프트웨어 개발 협업 환경이 확대**됨에 따라 접근키(Access Key), 인증토큰, API 키 등 **자격증명 정보의 중요성이 더욱 커지고 있다**고 밝혔다.

최근 국내외에서 개발 협업도구와 클라우드 환경에 저장된 자격증명이 외부에 노출되거나 탈취되어 개인정보가 유출되는 사고가 잇따라 발생하고 있다. 특히, 개발 과정에서 사용되는 **자격증명이 소스코드 저장소나 협업도구에 노출**될 경우 개인정보처리시스템, 데이터베이스, 클라우드 서비스 등에 대한 무단 접근으로 이어져 **대규모 개인정보 유출**이 발생할 수 있어 사업자의 각별한 주의가 요구된다.

깃허브(GitHub)* 등 개발 협업도구에 저장된 소스코드에서 클라우드 접근키 또는 API키와 같은 자격증명이 노출되는 사례가 확인되고 있다. 개발자가 관리 편의를 위해 소스코드에 자격증명 정보를 저장하는 경우, 공격자가 이를 악용하여 개인정보처리시스템에 접근할 수 있으므로 안전한 관리가 필요하다.

* 소프트웨어 코드 검토·배포, 프로젝트 공유 등 서비스 개발 관련 업무 협업도구

**< 자격증명 노출 또는 탈취로 개인정보가 유출된 국내 사례 >**

▶ (A사) 신원미상의 자가 스피어피싱 메일을 통해 깃허브 계정 접근권한을 확보한 후 AWS 접근키*를 획득하여 내부 데이터베이스에 저장된 개인정보 약 240만 건 열람

* AWS 접근키는 클라우드 자원에 접근할 수 있는 인증정보로, 부여된 권한 범위 내에서 서비스 운영 및 관리 가능

▶ (B사) 신원미상의 자가 깃허브에 평문으로 저장된 데이터베이스 접속정보를 확보하여 개인정보 약 42만 건을 유출

▶ (C사) 신원미상의 자가 깃허브에 노출된 AWS 접근키를 확보하여 개인정보 약 1천만건을 유출

▶ (D사) 신원미상의 자가 깃허브에 저장된 소스코드에 하드코딩 된 시스템 접근 자격증명(시크릿 키)이 노출되어 개인정보 유출

이에 개인정보위는 클라우드 환경 또는 개발 협업도구를 사용하는 사업자에게 다음과 같은 보호조치를 권고하였다.

○ 소스코드에 접근키, 비밀번호, API 키 등 **자격증명이 저장·노출되지 않도록 설정·관리**

○ 장기 자격증명 대신 일정 시간 이후 자동으로 만료되는 **임시 자격증명 사용**

※ (예) AWS IAM Role 기반 접근통제 체계는 일정 시간 동안만 유효한 임시 자격증명을 발급하여 운영 가능

○ 자격증명이 사용 가능한 **IP주소, 네트워크 구간 등을 제한**하여 외부에서의 무단 사용 방지

○ 데이터베이스, 클라우드 관리 콘솔 등 주요 시스템에 대해서는 **다중인증**(MFA, Multi Factor Authentication) **적용** 및 **최소권한 원칙**에 따른 **접근권한** 부여

○ **자격증명 사용 내역**을 **정기적**으로 **점검**하고, 불필요하거나 장기간 사용되지 않은 접근권한을 즉시 회수

**< 자격증명의 협업도구 저장 방지를 위한 사업자 조치(예시) >**

▶ 협업도구에서 자격증명 파일 또는 인증서 파일 등이 관리되지 않도록 **제외 설정**

※ 깃허브의 경우 .gitignore 파일에 인증서, 환경설정 파일(.env) 등을 등록하여 코드저장소 업로드 대상에서 제외 가능

▶ 기밀정보 **자동 탐지 도구***를 활용해, 코드저장소 업로드 전 자격증명 노출 여부를 점검

* 깃허브에서 제공하는 'Secret Scanning', 'Push Protection' 등 활용 가능

▶ 소프트웨어 엔지니어 대상 정기 교육 실시 및 코드 리뷰* 과정에서 하드코딩된 비밀번호, 접근키 등 자격증명 포함 여부 확인

* 개발한 코드가 서비스에 적용되기 전 안전성 관점에서 동료 엔지니어 상호간 검토하는 과정

▶ 자격증명 노출이 확인된 경우 해당 자격증명을 즉시 폐기하고 신규 자격증명으로 교체하는 등 신속한 대응 실시

양청삼 개인정보위 사무처장은 "클라우드 환경에서는 접근키, 데이터베이스 계정, API 키 등 자격증명 하나만으로도 중요 시스템에 접근할 수 있는 만큼, 안전한 계정·권한관리가 무엇보다 중요하다."라며, "사업자는 자격증명이 소스코드나 개발 협업도구에 저장되지 않도록 관리하고, 임시 자격증명 사용과 접근통제 강화를 통해 개인정보 유출사고를 예방해야 한다."라고 밝혔다.

아울러, "실수로 자격증명을 코드저장소에 업로드 한 경우 작업 공간에서 삭제하더라도 형상관리 이력에 해당 정보가 남을 수 있으므로, 즉시 해당 자격증명을 폐기하고 새로운 자격증명으로 교체 발급하는 등 신속한 조치를 취하는 것이 바람직하다."라고 강조하였다.


| 담당 부서 <총괄> | 예방조정심의관 사전실태점검과 | 책임자 | 과 장 | 김해숙 (02-2100-3060) |
|---|---|---|---|---|
| | | 담당자 | 사무관 | 서인숙 (02-2100-2482) |
| | | 담당자 | 사무관 | 전이루 (02-2100-2448) |