개인정보보호위원회 보도자료

보도시점 2025. 6. 12.(목) 12:00 (2025. 6. 12.(목) 석간) 배포 2025. 6. 11.(수) 18:50

개인정보위, 클라우드 분야 사전 실태점검 결과 발표

- 상위 3개 서비스인 AWS, Azure, NCP의 보호법상 안전조치기능 제공 현황 점검
- “추가설정 및 별도 솔루션 구독 등이 필요한 항목에 대해 개발문서(가이드, 설명서 등) 통해 명확히 안내”하도록 개선권고
- 국내 약 65만 이용사업자의 안전조치수준 제고 기대

개인정보보호위원회(위원장 고학수, 이하 ‘개인정보위’)는 6월 11일(수) 전체회의를 열어, 클라우드 서비스 제공사업자(Cloud Service Provider, 이하 ‘클라우드사업자’) 3개 사*에 대한 사전 실태점검** 결과를 발표하였다.

* 아마존(AWS), 마이크로소프트(Azure), 네이버클라우드(Naver Cloud Platform, 이하 ‘NCP’)

** **사전 실태점검** : 개인정보 보호 취약점을 선제적 점검하여 침해 위험을 사전에 예방하는 제도로, 법 위반 또는 개선 필요사항 발견 시 시정·개선권고(보호법 제63조의2)

< 점검 배경 및 대상 >

이번 실태점검은 클라우드를 기반으로 개인정보처리시스템을 운영하는 이용사업자(중소기업·스타트업·소상공인 포함, 이하 ‘이용사업자’)*들이 클라우드 상 안전조치 기능 미비로 인해 개인정보 보호법(이하 ‘보호법’) 위반 또는 개인정보 유출 위험에 노출되는 것을 선제적으로 예방하기 위해 진행되었다.

* 국내 약 65만 개 이용사업자가 이번 실태점검 대상인 3개 사의 클라우드 서비스를 사용 중

※ 가상서버(Virtual Machine) 및 데이터베이스(Database) 클라우드 서비스를 대상으로 이용사업자 관점에서 응용프로그램(예: 워드프레스(WordPress))을 구축하며 안전조치 기능 현황 점검

< 점검 결과 >

점검 결과, 점검대상 클라우드 서비스들은 보호법상 필수 안전조치 기능 자체는 제공하고 있었으나, ① 일부 기능의 경우 이용사업자가 **추가설정**을 해야 하거나, ② **별도 솔루션을 구독**해야만 하는 경우도 있어 이용사업자들에게 적극적인 안내가 필요하였다.

※ 클라우드 가상서버 및 데이터베이스 등은 개인정보가 아닌 일반적인 데이터 처리에도 활용되는 범용 서비스로, 개인정보 처리를 위한 안전조치 기능을 전부 기본 탑재하지는 않음

① 기본 안전조치 설정 외 추가 설정이 필요한 기능

보호법은 개인정보취급자에게 업무 수행에 필요한 최소한의 범위로 개인정보처리시스템의 접근권한을 차등 부여하고 접속계정을 공유하지 않을 것을 요구한다. 이를 위해 필요한 하위계정 발급 및 접근권한 설정 기능은 점검대상 클라우드 서비스들에서 기본 제공되는데, 이용사업자가 이 기능을 활용하려면 자사 담당자별로 하위계정을 발급하고 각기 접근권한을 부여하는 조치를 추가로 해야만 한다.

또한 보호법은 개인정보취급자가 개인정보처리시스템에 접속할 수 있는 범위를 인터넷 프로토콜(이하 '아이피') 주소 등으로 제한하고, 외부 인터넷에서 접속 시 아이디·비밀번호 이외의 안전한 인증수단(이하 '2차 인증')을 적용할 것을 요구한다. 점검 대상 서비스들은 접속 아이피 주소 대역 제한 기능을 기본으로 갖추고 있지만, 실제 이용사업자가 자사 환경에 맞게 허용·제한할 아이피 주소 대역을 추가로 설정해야만 한다. 2차 인증 기능의 경우 대개 기본 탑재되어 있으나, 일부 추가설정이 필요한 부분이 있어 이용사업자의 주의를 요한다.

- **(접근권한 차등부여)** 하위계정 발급 및 계정별 권한설정 기능 제공
  → 이용사업자 담당자별 하위계정 발급 및 업무 수행에 필요최소한의 접근권한 부여 설정 필요
- **(권한설정내역 및 접속기록 보관)** 기록 보관기능 제공되나 미활성화된 부분 존재
  → 보호법상 보존의무 있는 기록에 대해 보관기능 활성화 설정 필요
- **(비인가 접근 제한(방화벽))** 아이피 주소 등 기반 접근제한 기능 제공
  → 허용 또는 차단할 아이피 주소(예: 이용사업자 사업장) 대역을 설정 필요
- **(2차 인증)** 아이디·비밀번호 이외의 인증수단 적용기능 제공
  → AWS·NCP의 경우 관리자 외 계정에 대해서는 추가설정 필요
- **(최대접속시간)** 일정시간(예: 3시간, 12시간) 미작업 시 자동 접속종료 기능 제공
  → Azure의 경우 마이크로소프트 계정에서 파생되어 기본 계정설정에 미탑재, 추가설정 필요

※ 클라우드사업자 콘솔·포털 내 안전조치 기능 기준(이하 같음)

② 별도 솔루션 서비스 구독 등이 필요한 기능

보호법은 개인정보처리시스템에 관하여, 개인정보취급자에게 접근권한을 부여한 기록(log)을 3년간 보존 및 개인정보취급자가 접속한 기록을 1년(일정 규모 이상 개인정보처리자는 2년)간 보존해야 하며, 이 접속기록을 평상시 및 공격을 받을 시를 비롯하여 상시 분석함으로써 개인정보 유출 시도(이상행위)를 탐지할 의무를 부여한다.

점검대상 클라우드 서비스들은 기록보존 기능 자체는 기본으로 제공하지만 보존 기간이 대개 수십 일 수준으로 단기에 그치고 있었다. 이용사업자가 1~3년의 보존의무를 이행하려면, 기록을 별도로 장기 보관하는 기능을 자체 구현하면서 필요한 별도 저장용량을 구입하거나, 또는 클라우드사업자가 제공하는 별도 기록 관리 솔루션을 구독해야 한다.

이상행위 탐지와 관련해서는, 기본적인 기능을 기본으로 제공하는 클라우드 사업자도 일부 있었으나, 실제 현장에서 필요로 하는 수준의 이상행위 탐지 시스템은 대개 별도 구독 솔루션으로 제공되고 있었다.

그 외, 암호 키 관리, 악성프로그램 방지 등 기능도 별도 솔루션으로 구독해야 하는 경우가 다수 있었다.

- **(권한설정내역 및 접속기록 보관)** 단기간(수십 일 수준) 보관 기능 기본 제공
  → 1~3년 의무보존 대상 기록에 대해 별도 저장용량 구입, 기록 관리 솔루션 구독 등 필요
- **(유출탐지·대응, 암호키관리, 악성프로그램탐지 등 보안기능)** 통상 별도 솔루션으로 보안기능 제공
  → 관련 기능을 제공하는 별도 솔루션 구독 등 필요

< 개선권고 >

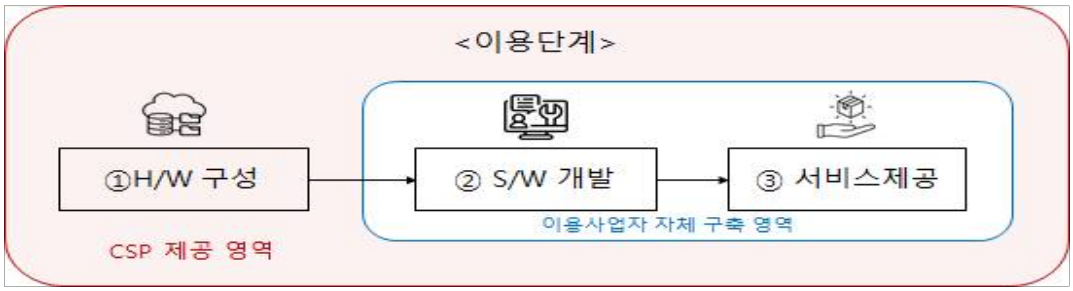
개인정보위는 클라우드사업자 3사를 대상으로 이들이 제공하는 안전조치 기능 중 **추가 설정 또는 별도 솔루션 구독이 필요한 기능의 존재 및 설정 방법**을 개발문서(가이드, 설명서 등)를 통해 이용사업자에게 명확히 **알릴 것을 개선권고**하는 한편, 타 클라우드 사업자 및 이용사업자들을 대상으로도 한국인터넷진흥원 등 전문기관과 함께 적극적으로 계도해 나갈 계획이다.

이번 실태점검 및 후속 개선을 통해 클라우드를 활용하는 국내 다수 개인정보처리자들의 인식과 보호 수준이 향상될 것이 기대된다.

담당 부서 <총괄>	조사조정국 조사3팀	책임자	팀 장	전승재 (02-2100-3151)
		담당자	사무관	김문호 (02-2100-3158)
<공동>	한국인터넷진흥원 유출조사팀	책임자	팀 장	조형진 (061-820-2850)
		담당자	선 임	이광재 (061-820-2854)

참고 클라우드 서비스 기반 개인정보처리 시 책임영역 구분

○ 이용사업자가 클라우드 서비스를 이용하여 개인정보 처리시스템을 구축하는 과정은 다음과 같음



- ①이용사업자는 **CSP가 제공하는 콘솔**(AWS/NCP)·**포털**(Azure) 웹페이지를 통해 컴퓨팅 리소스(네트워크 대역, 서버 등 가상 하드웨어)를 **구독·설정**하여 인프라 구성

- ②가상서버 내부*에 원격접속하여 필요한 소프트웨어(예: 데이터베이스, 웹서버)를 설치하고 이를 기반으로 애플리케이션 자체구축

* 가상서버 내부는 이용사업자 자체구축 영역(참고: 자체구축 서버 내 작업과 동일)

※ 다만, **데이터베이스의 경우** 이용사업자 자체구축 대신 **CSP로부터 구독도 가능**(이때 로그 관리·분석·장기보관 등 부가기능 추가 구독 가능)

- ③자체구축 완료한 애플리케이션(웹·앱)을 통해 대고객 서비스 제공

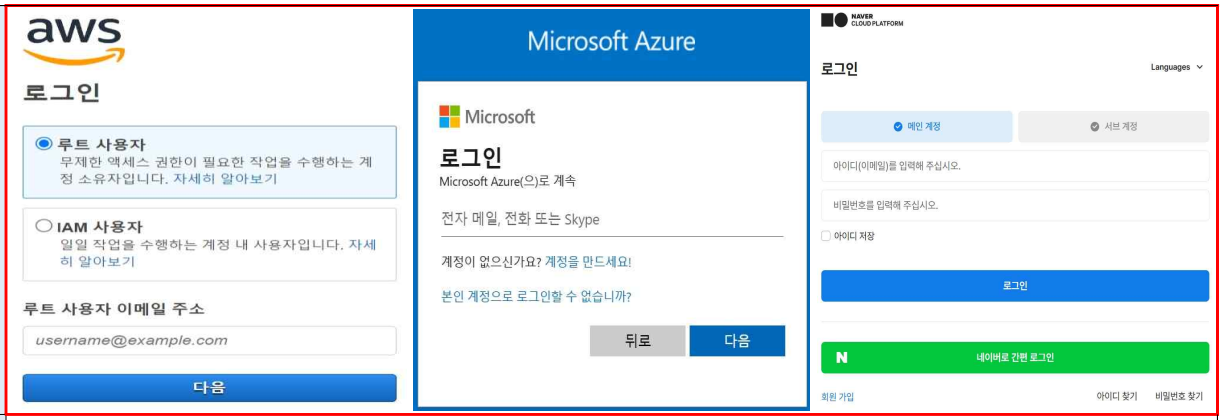
☞ 이용사업자 **구독 영역** 내 안전조치기능은 CSP **책임영역**(**본건 점검대상**) / 이용사업자 자체구축 영역 내 안전조치기능은 이용사업자 책임영역

< 참고 : 접속 지점별 CSP/이용사업자 영역 구분 >

이용사업자 접속 지점		접속 수단 예	영역
콘솔·포털		CSP 제공 웹페이지	**CSP 제공 영역**
가상서버(VM)		이용사업자 터미널	이용사업자 자체구축 영역
DB	i) 가상서버 내 구축 시	이용사업자 터미널	이용사업자 자체구축 영역 (당해 가상서버 내 구축 시)
	ii) 콘솔·포털 내 구독 시	CSP 제공 웹페이지	**CSP 제공 영역** (별도 가상 DB서버 구독 시)
웹·앱 어플리케이션		이용사업자 터미널	이용사업자 자체구축 영역

< 점검대상 CSP 제공 영역 예시(붉은색 테두리 표시) >

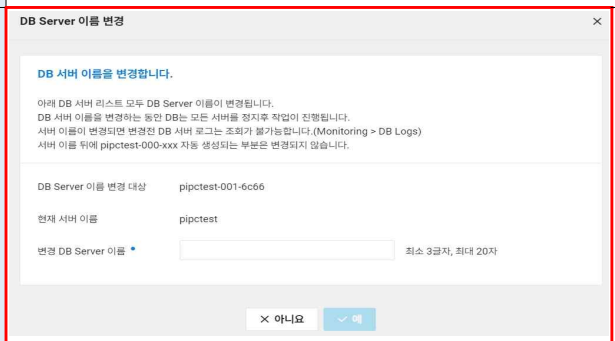
① Console



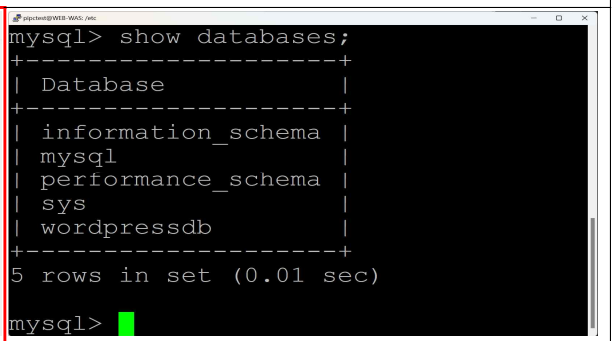
② Server

※ 터미널을 이용해 가상서버에 접속한 모습(이용사업자 자체서버 접속시와 동일)

③ DB

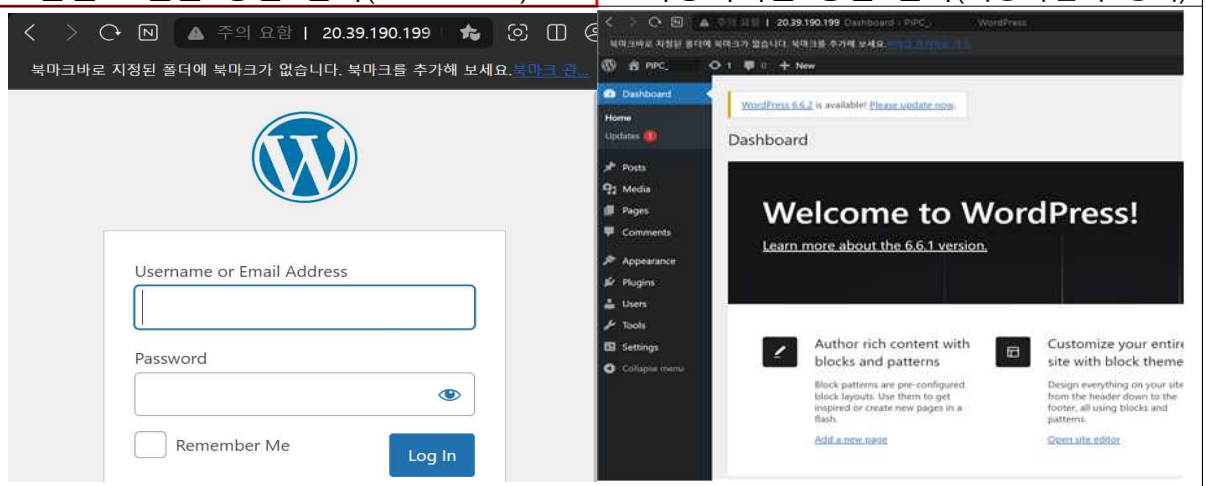


※ 콘솔·포털을 통한 접속(AWS·Azure)



※ 가상서버를 통한 접속(이용사업자 영역)

④ Application



※ 이용자에게 서비스되는 영역