보호인가 폐쇄인가: 미 의회가 문제 삼은 한국의 클라우드 제도

미 의회, 한국의 클라우드 규제 문제 공식 제기

3 월 3 일(현지시간), 미국 의회가 한국의 클라우드 보안 인증제도와 관련해 새로운 통상 이슈를 제기했다. 캐럴 밀러(Carroll Miller·공화·웨스트버지니아) 하원의원을 비롯한 의원들은 제이미슨 그리어(Jamieson Greer) 미국 무역대표부(USTR) 대사에게 서한을 보내 "한국이 미국 클라우드 서비스 제공업체에 대해 차별적인 조치를 취하고 있다"며 대응을 촉구했다.

핵심은 한국의 '클라우드 보안 인증제도(CSAP)'다. 이 제도는 공공기관이 민간 클라우드 서비스를 도입할 때 필수적으로 요구되는 보안 인증으로, 데이터 민감도에 따라 상·중·하 3 단계로 구분된다. 현재 외국계 클라우드 사업자는 '하' 등급까지만 인증을 받을 수 있어 공공부문 주요 서비스 시장 진입이 사실상 제한돼 있다.

국가정보원이 데이터 현지화 요건을 제도화하려는 움직임을 보이면서, 미국 클라우드 업체들이 한국 정부 기관에 서비스를 제공하기 어려워질 수 있다는 우려도 나온다. 미국의원들은 이러한 조치가 한미 자유무역협정(FTA)과 트럼프 행정부 시절 체결된 한미 전략적 무역·투자 협정의 원칙에 어긋난다고 지적했다.

한국의 공공 클라우드 시장은 네이버클라우드, KT 클라우드, NHN 클라우드 등 국내 사업자가 약 80~90%를 차지하고 있으며, AWS, Microsoft Azure, Google Cloud 등 글로벌 기업의 점유율은 10% 미만에 머물고 있다.

G20 국가들의 공공 클라우드 정책을 분석한 결과, 주요국의 대부분(15 개국 이상)은 공공부문 클라우드 시장의 절반 이상을 글로벌 서비스 제공업체가 차지하고 있다. 반면 한국은 중국, 러시아, 사우디아라비아 등과 함께 비교적 폐쇄적인 정책 기조를 유지하는 국가로 분류됐다. 특히 중·상등급 인증에 대한 높은 진입 장벽은 G20 중에서도 가장 제한적인 구조라는 평가다.

민간 부문은 이미 글로벌 클라우드 인증을 폭넓게 활용하고 있는 반면, 공공 부문이 국내 기업 중심으로만 운용되는 현 구조는 기술 생태계 전반의 경쟁력 제고를 제약하는 요인으로 작용한다. 정부의 공공조달 중심 제도를 통해 국내 클라우드 서비스

제공업체(CSP)의 시장 기반이 강화 되었지만, 이러한 보호 중심 설계가 중장기적으로 실제 해외 경쟁력 제고와 글로벌 시장 진출로 이어지고 있지는 않다.

공공조달 시장을 둘러싼 이러한 규제는 단기적으로 산업 보호 효과를 가져오지만, 장기적으로 글로벌 시장에서의 확장성과 경쟁력 확보에 불리하게 작용한다. 이 구조가 야기하는 외교적 마찰까지 고려하면 정책 수립 과정에서 개방성과 호환성 등 다양한 요소를 반영해야 한다는 점을 다시 상기시킨다.

Protection or Isolation: U.S. Congressional Concerns over Korea's Cloud Regulatory Framework

On March 3 (local time), members of the U.S. Congress formally expressed concerns over Korea's Cloud Security Assurance Program (CSAP), raising the issue as a potential trade barrier. Representative Carroll Miller (R–West Virginia) and other lawmakers sent a letter to U.S. Trade Representative Jamieson Greer, arguing that Korea's cloud security rules constitute *discriminatory treatment* against American cloud service providers and requesting an official response from the administration.

The CSAP is a mandatory framework governing the adoption of private cloud services by Korean public institutions. It categorizes data sensitivity into three levels—high, medium, and low—and currently limits foreign providers to certification at the lowest level. This effectively excludes global companies such as AWS, Microsoft Azure, and Google Cloud from competing in large-scale public-sector projects.

Additional concerns have emerged regarding the National Intelligence Service's initiative to institutionalize data localization requirements, which could further restrict foreign participation in government IT services. Lawmakers contend that these policies conflict with the principles of the Korea–U.S. Free Trade Agreement (KORUS FTA) and the bilateral Strategic Trade and Investment Framework agreed during the Trump administration.

Korea's public cloud market remains heavily domestic, with Naver Cloud, KT Cloud, and NHN Cloud holding an estimated 80–90 percent share. In contrast, foreign providers account for less than 10 percent. Comparative analysis of G20 economies shows that most major countries allow global providers to capture over half of the public-sector cloud market, whereas Korea maintains one of the most restrictive frameworks—alongside China, Russia, and Saudi Arabia.

While the private-sector cloud ecosystem in Korea increasingly adopts global standards and certifications, the public-sector procurement structure continues to favor domestic firms. This approach has supported local capacity building but has also limited incentives for innovation and hindered international competitiveness.

In the short term, these policies may deliver a degree of industrial protection. However, in the long run, they risk constraining Korea's ability to integrate with global digital supply chains and to expand its cloud industry beyond national borders. As diplomatic and trade sensitivities intensify, a recalibration of the regulatory framework may be needed—one that balances data sovereignty, market openness, and interoperability to sustain technological competitiveness and bilateral trust.