건의제목	클라우드 보안 인증 제도에 대한 규제 개혁		
규제 소관부처	과학기술정보통신부, 행정안전부		
건의자 (소속·직위·성명)	Business Software Alliance (Korea Country Manager, 김근)	연락처	+82 10 9137 5100 Geun@bsa.org

□ 건의내용

○ **(규제내용)** 『클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률』 및 행정안전부의 관련 지침에 따라, 공공기관 및 행정기관(이하 "공공기관")은 클라우드 보안 인증 제도(이하 'CSAP', 'Cloud Security Assurance Program')에 따라 인증된 클라우드 서비스 제공 업체가 제공하는 클라우드 서비스만 채택할 수 있음. CSAP에 따라, 클라우드 컴퓨터 서비스 제공 업체는 과학기술정보통신부(과기부)의 『클라우드 컴퓨팅 서비스 정보보호에 관한 기준 고시』의 규정을 기반으로 평가 및 인증됨

○ **(문제점)** CSAP은 보안상 이점이 없음에도 불구하고 글로벌 클라우드 서비스 제공업체에 기술적, 행정적 부담을 부과하여 시장 진출을 막는 요소로 작용하며, 그 결과 현재 CSAP을 획득한 글로벌 클라우드 서비스 제공 업체는 전무함. CSAP의 요구 사항 중 글로벌 표준에 부합하지 않는 과도한 요구 사항들은 다음과 같음

a) **물리적 망 분리:** 현재 CSAP의 물리적 망 분리 규정은 예외 없이 모든 공공 부분에 걸쳐 요구되고 있는 사항임. 일부 국가에서는 매우 민감한 일부 영역(국가 보안, 국방)에 한하여 물리적 또는 논리적 망 분리 요구하는 경우가 있으나, 공립 대학교 및 내부 통신과 같이 민감하지 않은(때로는 공개된) 데이터를 처리하는 워크로드와 기관까지 공공 부분 전반에 걸쳐 적용되는 경우는 거의 없음. 이처럼 획일적으로 적용되는 물리적 망 분리의 규정은 클라우드 보안을 강화하는데 도움이 되지 않을 뿐 아니라 멀티 테넌트(Multi-tenant) 클라우드 서비스의 규모의 경제와 최첨단 보안 기능인 클라우드 컴퓨팅

서비스의 주요 이점 또한 훼손함

b) **암호화:** 클라우드 서비스 제공업체가 공공기관에게 클라우드 서비스를 제공하기 위해서는 정부에서 허용한 알고리즘(예:ARIA, SEED)을 사용해야 함. 이러한 요구사항은 이미 국제적으로 인정된 표준을 충족하고 타 시장의 가장 민감한 상황에서도 허용되는 최첨단 암호화 알고리즘을 사용하는 여러 선도적인 클라우드 서비스 사업자들에게 비실용적인 요구사항임

c) **데이터 현지화:** 클라우드의 관리 시스템 및 데이터를 물리적으로 국내에 두도록 함. 이는 국외의 데이터센터에서 데이터를 저장/처리하는 많은 클라우드 서비스 제공업체에게 불필요한 장벽임. 경우에 따라, 해외에 위치한 데이터 센터를 활용하는 것이 데이터의 복제(Redundancy) 및 백업(Back-up)을 가능하도록 하며, 데이터 센터에 물리적 또는 사이버 공격이 발생한 경우에도 물리적으로 거리가 있는 원격 데이터 센터에 저장된 데이터를 사용하여 피해를 복구할 수 있게 됨

위 언급된 문제점들에 따른 결과는 다음과 같음

○ **국내 공공기관은 글로벌 클라우드 서비스 제공업체가 제공하는 첨단서비스 이용이 불가함** CSAP의 데이터 현지화 및 망 분리와 같은 다양한 요구사항들로 인해 글로벌 클라우드 서비스 제공 업체의 서비스가 더 나은 기능, 경쟁력 있는 가격, 더 높은 수준의 보안을 가졌음에도, 공공기관의 글로벌 클라우드 서비스를 활용을 막고 있음. 여러 글로벌 클라우드 서비스 제공 업체는 이미 사이버 보안 기능에 막대한 자원을 투자하고, 최신 사이버 위협에 대처하기 위해 클라우드 시스템의 보안 프로그램 및 제어를 지속적으로 업그레이드 하고 있음.

악의적인 사이버 행위자의 능력이 발전함에 따라, 정부는 새로운 사이버 위협을 처리할 수 있는 최고의 기술을 보유하고 있는지 확인해 볼 필요가

있음. 위에 명시한 문제점으로 인해 효과적인 사이버 보안 솔루션을 개발한 기업이 CSAP을 획득하지 못해 시장에서 사라지게 된다면, 한국의 공공기관은 최첨단 사이버 보안을 제공할 수 없는 제한적이고 비용 가중화 된 선택권만 가지게 될 것임

○ 국내 SaaS(Software as a Service) 제공업체의 시장 참여 기회가 상실됨. 많은 국내 SaaS 제공 업체는 서비스를 제공할 때 글로벌 클라우드 서비스 제공 업체의 클라우드 인프라에 크게 의존하고 있음. 다만, CSAP의 요구사항으로 국내 SaaS 제공 업체도 한국의 공공기관 클라우드 서비스 시장에 진출할 수 없는 상황이며, 국내 SaaS 제공 업체의 기회 박탈은 국내 클라우드 서비스 산업의 성장과 발전을 저해 할 것임

○ 비용이 증가하고 및 보안이 약화됨. CSAP의 요구 사항은 실질적인 보안상 이점 없이 클라우드 서비스 제공 업체 및 SaaS 제공 업체의 비용을 증가시키고 경우에 따라서 보안을 약화시킴. 예시는 다음과 같음

a) 외부 공인 평가자가 심사하고 국제적으로 인정된 표준을 기반으로 하는 인증을 인정하는 대신, CSAP은 기존 인증에 대한 부가 및 중복 검증을 요구함. 따라서 검증 과정에서 클라우드 서비스 제공 업체에 추가적인 비용이 부과되고 서비스 채택 절차가 지연됨

b) 데이터 현지화의 요건은 클라우드 서비스 제공 업체가 해외 데이터 센터를 사용하여 중요한 데이터의 복제 및 백업 작업을 수행하지 못하게 함. 또한 최고의 기능과 가장 안전한 솔루션을 제공하는 회사 대신, 데이터 현지화 요구 사항을 가장 잘 준수하는 회사에 과도한 가치를 부여하여 사이버 보안 솔루션 시장을 왜곡함

c) 클라우드 서비스 제공 업체가 이미 널리 채택하고 있는 최첨단 암호화 알고리즘이 아닌 국내/정부에서 허용한 암호와 알고리즘(예: ARIA, SEED)만 사용하도록 요구하는 것은 글로벌 사이버 보안 환경의 파편화를 심화 시킴. 이는 규정 준수 비용을 증가시키는 동시에 조직이 동급 최고의 암호화 기술을 사용하지 못하게 하고 국제적으로 공인된 다른 표준을 사용하는 시스템 간 상호 운용상 문제를 야기함. 특히,

이러한 규정은 정부가 양자 컴퓨터로 전환함에 따라 문제가 될 가능성이 농후함

※ (해외사례) 미국 FedRAMP

FedRAMP (Federal Risk and Authorization Management Program)는 미국 연방 정부의 클라우드 서비스 채택 및 사용에 있어서, 비용 효율이 높고, 리스크 기반의 접근 방식을 제공하기 위해 만들어 졌음. FedRAMP는 연방 정보의 보안 및 보호를 중점으로, 기관들이 최신 클라우드 기술을 사용할 수 있도록 지원하고 있으며, 클라우드 서비스 오퍼링(CSO)을 낮은 영향 등급, 보통 영향 등급, 높은 영향 등급으로 분류함. 보안 등급은 FIPS(Federal Information Processing Standard) 이러한 리스크 기반의 접근 방식으로 미국 정부 기관들은 클라우드 서비스에 대해 광범위한 선택권을 가지게 되었으며, 미국 기업이 아닌 6개의 클라우드 서비스 제공업체가 높은 등급의 클라우드 서비스를 제공할 수 있는 인증을 받게 되었음

199에 따른 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)의 세 가지 보안 목표에 따라 분류됨
특히, FedRAMP는 높은 영향 수준 등급에 대해서만 데이터 현지화를 요구하고 있음. 따라서 이 등급에 한에 공공기관들은 계약에 따라 특정 위치에 데이터를 저장하도록 요구할 수 있으나, 높은 영향 수준 등급에서도 물리적 망 분리는 필수 요건이 아니며, 이는 물리적 망 분리가 반드시 더 안전한 시스템으로 이어지는 것은 아니라는 미국의 견해를 반영한 것임

중간 등급과 낮은 등급의 경우, 미국 정부의 접근 방식은 민간 기업의 접근 방식과 유사하며, 이는 데이터와 기업에 미칠 잠재적 영향을 고려하여 단순성, 현지화 또는 보안 제어 보완을 통해 기업이 더 나은 서비스를 제공할 수 있는가를 고려하는 리스크 기반의 결정을 내리는 것을 의미함

○ (개선방안) 공공 부분을 영향 및 보안 요구사항에 따라 세분화하고, 각 보안 분류에 따라 요구사항을 조정하는 CSAP의 규제 개혁이 필요함

a) BSA는 과학기술정보통신부와 행정안전부가 FedRAMP와 유사한 접근 방식을 채택하고 각 공공 기관의 기능과 처리하는 데이터의 민감도를 고려하여, CSAP에서 보안 등급을 구별하는 방식을 도입하는 것을 권장함. 이러한 리스크 기반 접근 방식은 공공 기관이 보안 요구에 가장 적합한 클라우드 서비스를 조달 할 수 있는 유연성을 제공하여, 공공 부분 내에서 클라우드 채택을 촉진하는데 기여할 것임. 이는 또한 클라우드 서비스 제공 업체가 보다 효과적이고 효율적인 보안 솔루션을 개발하도록 장려할 것임

b) 이와 관련하여, 정부는, 특히 민감도가 낮은 공공기관의 경우, 보안 강화에 거의 도움이 되지 않으며 상용 클라우드가 제공하는 보안 및 복원력 이점을 감소시키는 물리적 네트워크 분리 요구 사항(14.2.1)과 암호화 알고리즘 요구 사항(14.3.1)을 폐지할 것을 권고함. 이러한 조항들은 공공 부문에서 양자 컴퓨팅으로 전환할 수 있는 동급 최고의 암호화 기술 사용하는데 있어 방해 요소로 작용함

c) 또한 미국 국립표준기술연구소 (National Institute of Standards and Technologies, NIST)등 국제적으로 인증된 표준 (예:ISO 9000 및 27000 시리즈)과 BSA Framework for Secure Software과 같은 업계 모범 사례에 따라 개발 및 관리 되는 소프트웨어의 조달을 허용해야 함

관련법규	- 전자정부법 - 『클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률』
건의성격	■ 신규 건의 □ 반복 건의

붙임1 관련 법령

□ 『클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률』

제5조(기본계획 및 시행계획의 수립) ① 과학기술정보통신부장관은 클라우드컴퓨팅의 발전과 이용 촉진 및 이용자 보호와 관련된 중앙행정기관(이하 "관계 중앙행정기관"이라 한다)의 클라우드컴퓨팅 관련 계획과 시책 등을 종합하여 3년마다 기본계획(이하 "기본계획"이라 한다)을 수립하고 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제7조에 따른 정보통신 전략위원회의 심의를 거쳐 확정하여야 한다.

제20조(국가기관등의 클라우드컴퓨팅서비스 이용 촉진) ① 국가기관등은 업무를 위하여 클라우드컴퓨팅서비스 제공자의 클라우드컴퓨팅서비스를 이용할 수 있도록 노력하여야 한다. <개정 2022. 1. 11.> ② 국가기관등은 제1항에 따른 클라우드컴퓨팅서비스 이용에 있어서 제23조의2제1항에 따른 보안인증을 받은 클라우드컴퓨팅서비스를 우선적으로 고려하여야 한다.

□ 『행정기관 및 공공기관의 클라우드컴퓨팅서비스 이용 기준 및 안전성 확보 등에 관한 고시 』

제7조(안전성 기준) ① 행정기관등의 장이 클라우드컴퓨팅서비스를 이용하는 경우에는 국가정보원장이 수립한 「국가 정보보안 기본지침」을 준수해야 한다.

② 행정기관등의 장이 클라우드컴퓨팅서비스를 이용하는 경우에는 과학기술정보통신부장관이 고시하는 「클라우드컴퓨팅서비스 정보보호에 관한 기준」 제7조에 따라 인증(이하 "보안인증"이라 한다)된 클라우드컴퓨팅서비스를 우선 고려해야 한다.

③ 행정기관등의 장이 제2항에도 불구하고 보안인증되지 않은 클라우드컴퓨팅서비스를 이용하고자 하는 경우에는 국가정보원장과 사전에 협의를 거쳐 이용할 수 있다.

④ 「초·중등교육법」 제2조 및 「고등교육법」 제2조에 따른 학교의 장이 교육 현장에서 교육목적으로 이용하는 정보시스템에 대해서는 제2항 및 제3항을 적용하지 않을 수 있다.

⑤ 행정기관등의 장은 제1항 및 제2항 이외에 클라우드컴퓨팅서비스를 이용하는 업무의 특성 등을 고려하여 보안요건을 추가하여 적용할 수 있다.

☐ 『클라우드 컴퓨팅 서비스 정보보호에 관한 기준 고시』

제7조(정보보호 기준의 준수여부 확인) 과학기술정보통신부장관은 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제5조에 따른 "기본계획"(2015년 12월 7일 확정, 정보통신전략위원회) 상의 "보안인증제" 시행을 위해 클라우드컴퓨팅서비스 제공자가 그 서비스가 이 기준을 준수하는지 확인을 요청한 경우에는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 "한국인터넷진흥원"의 장이 그 서비스를 조사 또는 시험·평가하여 인증 할 수 있다.