



# LEGAL UPDATE

정보보호센터

Sep. 2024

## 클라우드컴퓨팅서비스 보안인증제도(CSAP)

ICT활용 패러다임이 변화하면서, IT 인프라를 자체적으로 구축하는 방식을 지나 클라우드 컴퓨팅을 활용하는 방식으로 점차 전환되었습니다. 이에 따라 클라우드 서비스의 안전성에 대한 우려가 제기되자 이를 해소하기 위해 국내에서는 2016년부터 클라우드 컴퓨팅 서비스 보안 인증제도(CSAP)를 시행하고 있습니다. CSAP 인증제도는 국가/공공기관에 안전한 서비스를 제공하기 위해 마련되었으며, IaaS, SaaS, DaaS 유형별로 각 상, 중, 하 등급으로 인증됩니다. 주요 보안인증기준으로는 정보보호정책 수립, 서비스 연속성 관리(관리적 보호조치), 물리적 보호구역 지정, 정보처리 시설 및 장비보호(물리적 보호조치), 가상화 보안, 접근통제(기술적 보호조치) 등이 있습니다. 현재까지 114건의 클라우드 서비스 보안인증이 유지되고 있으며, 이를 통해 이용자의 신뢰도와 정보보호 수준을 높이는데 기여하고 있습니다. 국내외 클라우드 서비스 제공자 및 클라우드 서비스 이용 기업들이 CSAP 인증제도를 잘 이해하고 이에 투자한다면 보다 더 안전한 클라우드 업무환경을 구축할 수 있을 것으로 기대됩니다.

### 1. 인증제도 도입배경

ICT 활용 패러다임이 정보 시스템을 자체적으로 구축하던 과거의 방식에서 민첩하고 유연한 서비스 제공을 가능케 하는 클라우드 컴퓨팅 방식으로 전환되고 있습니다. 클라우드 시스템은 기본적으로 서비스 이용량에 비례하여 비용을 지불하는 서비스로, 책임공유모델을 기반으로 SaaS(Software as a Service), PaaS(Platform as a Service), IaaS(Infrastructure as a Service)로 구분됩니다. 2010년부터 미국 등 주요국은 클라우드 우선적용정책을 추진하고 있으며, 우리나라의 경우 2015년 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」(이하 '클라우드컴퓨팅법')을 제정한 이래 3차례에 걸쳐 클라우드컴퓨팅 발전 기본계획을 수립·시행하며 클라우드 산업 육성에 노력하였습니다.

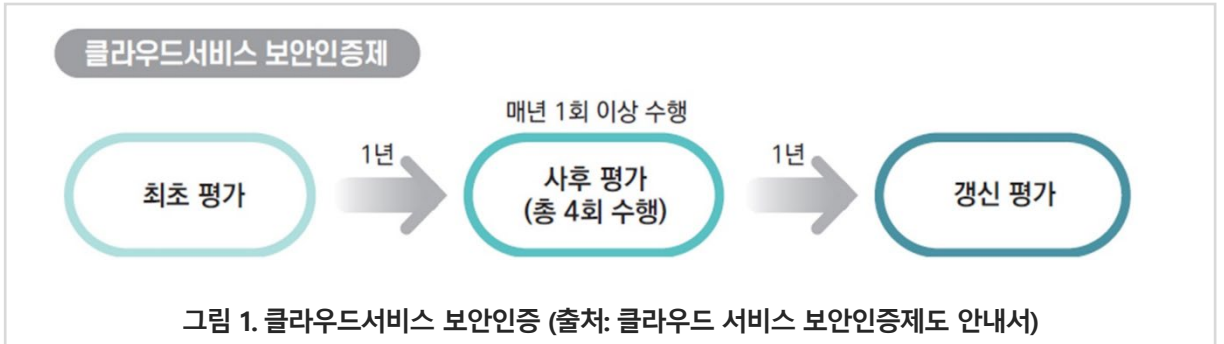
2016. 5.경 '클라우드컴퓨팅서비스 보안인증제도 안내서'가 처음으로 공개 및 시행되어 클라우드 컴퓨팅서비스(이하 '클라우드서비스') 기업에서 보안인증을 획득하기 시작하였고, 2022. 1. 11. 클라우드컴퓨팅법 제23조의2가 신설되어 클라우드서비스의 보안인증에 관한 법적 근거가 마련됨에 따라 클라우드서비스 사업자의 필수 요소로 자리잡았습니다.

### 2. 클라우드컴퓨팅서비스 보안인증제도 (CSAP)

#### 가. 인증제도 개요

클라우드서비스 보안인증제도는 클라우드컴퓨팅법 제23조의2에 따라 클라우드서비스의 정보보호 수준의

향상 및 보장을 위하여 서비스에 대한 보안인증을 수행하는 제도로, 국가·공공기관에 안전하고 신뢰할 수 있는 서비스를 공급하고 이용자의 보안 우려를 해소하여 산업의 경쟁력을 확보하는데 기여합니다. 클라우드서비스 보안인증제를 처음으로 신청한 경우, 최초평가를 통해 인증을 취득하면 5년의 유효기간 안에 매년 보안인증기준을 준수하고 있는지 확인하기 위한 사후평가를 시행하며, 총 4회 수행 후 보안인증 유효기간(5년)이 만료되기 전에 연장을 원하는 경우 갱신평가가 이뤄집니다.



### 나. 인증 대상

‘클라우드컴퓨팅법’ 제20조에 따라 국가·공공기관 등은 업무를 위하여 클라우드서비스를 이용하되 노력해야 하고 이때 보안인증을 받은 클라우드서비스를 우선적으로 고려해야 합니다. 이에 따라 국가·공공기관 등의 업무를 위하여 클라우드서비스를 제공자하려는 자는 보안인증을 받아야 됩니다. 참고로 보안인증의 대상이 되는 클라우드서비스란 클라우드컴퓨팅 기술을 이용하여 정보시스템의 인프라, 응용프로그램, 개발환경 중 어느 하나 이상을 제공하는 서비스를 의미합니다(동법 시행령 제3조).

#### <관련법규(클라우드컴퓨팅법)>

제 20조(국가기관등의 클라우드컴퓨팅서비스 이용 촉진) ① 국가기관등은 업무를 위하여 클라우드컴퓨팅 서비스 제공자의 클라우드컴퓨팅서비스를 이용할 수 있도록 노력하여야 한다.

② 국가기관등은 제1항에 따른 클라우드컴퓨팅서비스 이용에 있어서 제23조의2제1항에 따른 보안인증을 받은 클라우드컴퓨팅서비스를 우선적으로 고려하여야 한다.

### 다. 인증 기준 및 현황

클라우드서비스 보안인증 범위에는 클라우드서비스에 포함되거나 관련 있는 자산(시스템, 설비, 시설 등), 조직, 지원서비스 등이 모두 포함됩니다. 인증 유형으로는 IaaS, SaaS, DaaS가 있으며, 2023. 1. 경 「클라우드컴퓨팅서비스 보안인증에 대한 고시」가 개정되면서 상, 중, 하 등급제가 도입되었습니다.

구분	내용	주요 내용
인증 유형 (관리적, 물리적, 기술적, 국가기관용 보호조치)	IaaS	- 서버, 저장장치, 네트워크 등을 제공하는 서비스 인증 - 총 14개분야 116개 통제항목으로 구성
	SaaS	- 응용프로그램 등 소프트웨어를 제공하는 서비스 인증 - 표준등급, 간편등급 - 11개 분야 31개 통제 항목
	DaaS	- 가상데스크톱 환경 제공하는 서비스 인증 - 14개 분야 11개 통제항목

구분	내용	주요 내용
인증 등급	상	-등급 정의만 되어 있음
	중	-등급 정의만 되어 있음
	하	-관리적, 기술적, 국가기관용 보호조치 (14개 분야 64개 통제 항목)
	하 (SaaS)	-관리적, 기술적, 국가기관용 보호조치 (11개 분야 30개 통제 항목)

클라우드서비스 보안인증기준은 크게 관리적, 물리적, 기술적 보호조치로 구분될 수 있으며, 일부 항목들은 ISMS인증 획득으로 대체할 수 있습니다.

구분	주요 인증기준	주요 내용
관리적 보호조치	정보보호정책 및 인적 관리	-정보보호 정책 수립, 검토, 변경, 문서관리 -조직 구성, 역할 및 책임 부여
	서비스 연속성 관리	-자산관리, 침해사고 등 장애 대응, 서비스 가용성 관리
	준거성	-법 및 정책 준수와 보안감사
물리적 보호조치	물리적 보호구역	-보호구역 지정, 출입통제, 보호구역 내 작업
	정보처리 시설 및 장비보호	-시설 배치, 보호설비, 케이블 보호, 유지보수
기술적 보호조치	가상화 보안	-가상화 인프라 자원 관리 및 모니터, 가상환경 보안
	접근통제	-접근통제 정책 수립, 접근 권한 관리

클라우드서비스 보안인증제를 시행한 이래 국내에서 2016년부터 2024년까지 총 143건의 인증서가 발급되었으며, 24년 현재 114건의 인증서가 유지되고 있습니다. 해외 사업자 중에서는 AWS, 구글 등이 CSAP 인증을 받기 위해 평가 신청 작업을 개시한 것으로 알려져 있으며, 알리바바와 텐센트 등 중국 클라우드 사업자들도 인증 신청 여부를 고려하고 있는 것으로 알려져 있습니다.

### 3. 시사점

ICT 환경의 패러다임이 크게 변화한 것은 물론, 생성형 AI 서비스의 확대, 원격근무의 일상화, 화상회의 사용의 증가 등으로 인해 클라우드서비스의 활용이 지속적으로 늘어나고 있습니다. 이러한 상황에서도 일부 사업자들은 보안 우려로 인해 클라우드서비스 도입을 망설이기도 합니다. 클라우드서비스 보안인증제도는 이러한 클라우드서비스 활성화와 클라우드서비스 보안우려 해소라는 2가치 측면에서 중요한 의미를 갖습니다.

즉, 클라우드서비스 보안인증 기준을 충족하는 국내 클라우드서비스 기업들은 강화된 안전성을 바탕으로 글로벌 경쟁력을 강화할 수 있으며, 외국 기업들의 경우도 국가기관 등에 서비스를 제공하기 위해서는

클라우드서비스 보안인증을 받아야 하므로 넓은 의미에서 클라우드서비스 활성화를 통해 산업 전반의 성장에 긍정적 영향을 끼칠 수 있습니다. 더불어 클라우드서비스 보안인증을 취득한 서비스 제공자는 객관적이고 공정한 보안인증을 통해 이용자의 신뢰도를 높일 수 있으며, 서비스 이용자 입장에서는 인증받은 클라우드 서비스를 이용하여 보안우려를 해소할 수 있게 되는 것입니다.

법무법인(유한) 화우 정보보호센터는 오랜 경험과 축적된 노하우를 기반으로 기업 고객을 위한 최적의 솔루션을 안내해 드리고 있습니다. 정보보호 관련 법령의 해석 및 그 대응과 정보보호 기술적 자문(해킹 진단, 보안취약점) 등 포괄적인 올인원(All-in-One) 서비스를 제공하고 있습니다. 관련하여 문의사항이 있으신 경우 언제든지 화우에 연락하여 주시기 바랍니다.

## Contacts

### 이근우

T. (+82) 2 6003 7558

센터장/파트너변호사 E. [klee@yoonyang.com](mailto:klee@yoonyang.com)

### 정한근

T. (+82) 2 6003 7781

고문 E. [hkjung@yoonyang.com](mailto:hkjung@yoonyang.com)

### 이광욱

T. (+82) 2 6003 7535

파트너변호사 E. [kwlee@yoonyang.com](mailto:kwlee@yoonyang.com)

### 이수경

T. (+82) 2 6182 8132

파트너변호사 E. [sgyi@yoonyang.com](mailto:sgyi@yoonyang.com)

### 백재환

T. (+82) 2 6182 8366

전문위원 E. [jhb@yoonyang.com](mailto:jhb@yoonyang.com)

### 지재원

T. (+82) 2 6003 7568

연구위원 E. [jwji@yoonyang.com](mailto:jwji@yoonyang.com)