EQST insight

클라우드 서비스 보안인증제도(CSAP) 개편 동향

관제전략담당 노민철 수석

과학기술정보통신부는 지난 1 월 31 일 민간기업이 공공부문에 클라우드 서비스를 공급하기 위해 필요한 인증인 클라우드컴퓨팅 서비스 보안인증(CSAP[1]) 일부 개정안을 고시했으며, 현재 시행 중에 있다. 이는 2016 년 4 월에 「클라우드컴퓨팅서비스 정보보호에 관한 기준」이 고시된 이후 7 년이 되어가는 시점에서의 개정이다.

이번 개정안의 주요 내용은 공공부문 클라우드 보안인증 체계를 시스템 중요도에 따라 상·중·하 등급으로 나눠 각기 다른 보안 규제를 하겠다는 것이다. 특히 '하' 등급은 물리적 망분리 이외에 논리적 망분리까지 허용하는 것으로 보안 규제를 완화한다.

더욱이 오는 2025 년까지 추진될 행정·공공기관 정보시스템 클라우드 전환 사업이 상대적으로 덜 민감한 업무인 '하' 등급부터 시작될 것으로 보여, 국내와 해외 클라우드 서비스 사업자(CSP[2]) 간의 희비가 교차하고 있는 상황이다. 보안규제 완화가 제한된 공공 영역을 개방해 클라우드 시장 전반을 활성화하고 공공 서비스를 혁신하기 위한 결정이라지만, 해외 CSP 에 비해 상대적으로 경쟁력이 부족한 국내 CSP 가 경쟁에서 밀릴 수 있다는 우려도 제기되는 상황이다.

이번 헤드라인에서는 클라우드 서비스 보안인증제도가 개정된 배경과 국내/해외 클라우드 사업자(CSP)의 상황, 그리고 이번 개정안으로 변경된 관리/물리/기술적 보호조치 내용에 대해 살펴보고자 한다.

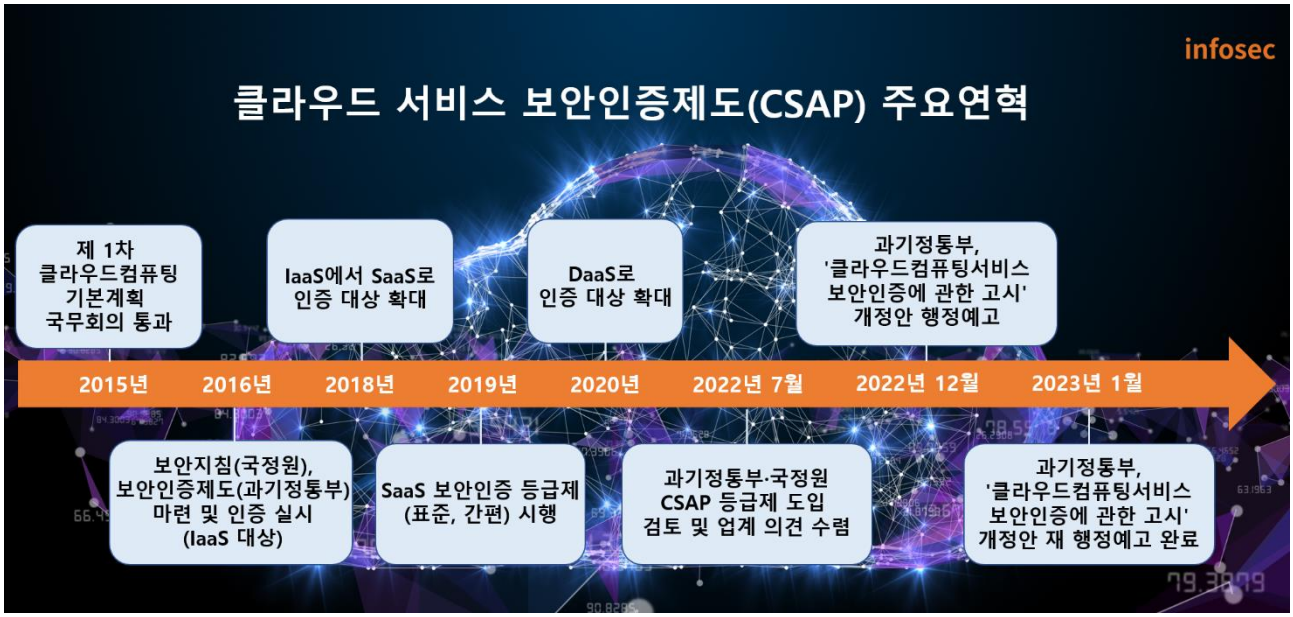
---

[1] 클라우드 서비스 제공자가 제공하는 서비스에 대해 『 클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률 』 제 23 조 제 2 항에 따라 정보보호 기준의 준수여부 확인을 인증기관이 평가·인증하여 이용자들이 안심하고 클라우드 서비스를 이용할 수 있도록 지원하는 제도

[2] CSP(Cloud Service Provider)는 공공 클라우드 인프라, 플랫폼 서비스를 제공하는 업체를 의미한다. CSP 는 자체 데이터센터를 구축해 다수의 물리 서버를 가상화해 제공하며 네트워크, 스토리지, 전력 등 서버 운영에 필요한 모든 것을 지원하고 있다. 대표적으로 아마존의 'AWS', 마이크로소프트의 'Azure', 구글의 'GCP' 등이며, 국내기업으로는 네이버클라우드, NHN 클라우드, KT 클라우드 등이 있다.

* 출처: 한국인터넷진흥원(KISA) 홈페이지

1. 클라우드 서비스 보안인증제도(CSAP) 개편 배경 및 경과



* 출처: 전자신문 기사(https://www.etnews.com/20230130000194) 이미지 재가공

그간 아마존웹서비스(AWS)나 마이크로소프트(MS), 구글 클라우드 등 해외 CSP 는 한국 시장 진입을 위해 클라우드 서비스 보안인증제도(CSAP)의 규제완화를 꾸준히 요청해왔다. 지난 2022 년 5 월 조 바이든 미국 대통령이 방한 후 주한미국상공회의소에서 과학기술정보통신부에 클라우드 서비스의 보안인증제도(CSAP) 와 논리적 망분리 허용에 관한 내용이 담긴 공문을 보냈다는 소식이 전해지기도 했다. 이후 국가정보원이 국내 CSP 로부터 클라우드 서비스 보안인증제도(CSAP)완화에 대한 의견을 마련하면서, 규제완화에 대한 세부내용이 발표되기 시작했다.

2022 년 6 월 과학기술정보통신부에서 'SW 산업의 질적 도약을 위한 국내 SW 기업의 성장 및 해외 진출 지원방안' 간담회를 열고 클라우드 서비스 보안인증제도(CSAP) 완화·개편 지시와 3 분기 내 보안인증제를 완화 계획을 알렸으며, 7 월에는 과학기술정보통신부에서 보안인증을 상·중·하 등급으로 세분화한 계획을 발표, 8 월에는 보안인증제 등급 및 완화 차등 적용을 공식화했다.

같은 해 11 월 과학기술정보통신부는 클라우드 보안인증 개편안 설명회를 개최하며 클라우드 보안인증 평가기관 지정계획, 인증평가 수수료의 부과 및 지원계획 등 고시 개정에 따른 주요 변경사항과 함께 기존의 보안인증 과정에서 기업이 부담을 호소했던 인증 평가 방식에 대한 개선 계획을 안내했다.

이러한 과정 중 보안인증과 관련하여 국내 CSP 와 회의를 진행하려 했지만 대다수의 업체들이 불참하였고, 도리어 국내 CSP 는 국정감사에서 정부가 추진하는 클라우드 서비스 보안인증제도 개편에 대해 '글로벌 추세 역행'이라고 비판하며 제도적 보완을 요구하기도 했다.

이후 2022 년 12 월 과학기술정보통신부는 「클라우드컴퓨팅 서비스 보안인증에 관한 고시」 일부 개정안 행정예고를 2023 년 1 월 18 일까지 하였고, 최종으로 2023 년 1 월 31 일에 「클라우드컴퓨팅 서비스 보안인증에 관한 고시」 (과학기술정보통신부 고시 제 2023-3 호)를 일부 개정하여 고시했다.

과학기술정보통신부가 밝힌 개정 이유는 "공공부문의 민간 클라우드 이용 활성화를 위해 국가기관 등의 시스템을 3 등급으로 구분하고 등급별로 차등화 된 보안인증기준을 적용하는 클라우드 보안인증 등급제 도입을 위해 필요한 사항을 정하기 위함"이라고 전했다.

2. 클라우드 서비스 보안인증제도(CSAP) 개정 사항

2023 년 1 월 31 일에 고시된 주요 개정내용은 크게 3 가지로 구분된다.

가. 기존 클라우드 보안인증의 등급제 신설(제 14 조 개정)

- 클라우드컴퓨팅 서비스의 정보보호 수준에 따라 보안인증 기준을 차등화해 적용하는 등급제(상등급, 중등급, 하등급) 시행 근거 마련

나. 보안인증 유형 및 등급에 따른 세부 점검항목을 공개(제 15 조 개정)

- 클라우드 보안인증 유형 및 등급에 따라 보안인증기준 내에서 세부 점검항목을 공개할 수 있는 근거 마련

다. 클라우드 보안인증의 등급화에 따른 보안조치 개정(별표 1, 2, 3, 4, 7)

- 관리적, 물리적, 기술적, 국가기관 등이 이용하는 클라우드컴퓨팅 서비스 보호조치 개정

개정된 클라우드 서비스 보안인증제도(CSAP)를 살펴보면

첫 번째, 「클라우드컴퓨팅 서비스 보안인증에 관한 고시」 제 14 조(보안인증 유형 및 등급)의 내용을 보면 클라우드컴퓨팅 서비스 보안인증 유형 4 가지와 3 개의 등급으로 나눈다.

보안인증의 유형은 다음과 같다.

〈표 1〉 보안인증 유형

구분	보안인증 유형
IaaS 인증	서버, 저장장치, 네트워크 등을 제공하는 서비스 인증
SaaS 인증	응용프로그램 등 소프트웨어를 제공하는 서비스 인증
PaaS 인증	응용프로그램 등 소프트웨어의 개발·배포·운영·관리 등을 위한 환경을 제공하는 서비스 인증
기타	위 3 가지의 서비스를 둘 이상 복합하는 서비스 인증

위 보안인증의 유형에 따라 보안인증 등급은 기존 IaaS, SaaS(표준등급), SasS(간편등급), PaaS 에서 개정 후 상, 중, 하로 구분한다.

〈표 2〉 보안등급별 평가기준

<table>
<tr><th>등급</th><th>시스템 등급 분류</th><th>평가기준</th></tr>
<tr><td>하</td><td>개인정보 미포함, 공개된 공공 데이터 운영 시스템</td><td>· 합리화: 물리적 망분리 → 논리적 망분리
- 국내 서비스형 소프트웨어(SaaS) 사업자가 공공시장에 신규 진입할 수 있도록 기존의 민간·공공 영역 간 물리적 분리 요건 완화
- 단 클라우드 시스템과 데이터의 물리적 위치는 국내한정</td></tr>
<tr><td rowspan="2">중</td><td>비공개 업무자료를 포함 또는 운영하는 시스템</td><td rowspan="2">· 현행 수준 유지
- 보안성을 담보한 네트워크 접근 허용
· 합리적 간소화
- 기존유형(IaaS, SaaS 표준, SaaS 간편) 통폐합 및 불필요 항목 삭제
- 이용 기관별 테이블 분리 기준 완화</td></tr>
<tr><td>중요도에 따라 행정내부업무 시스템도 포함 가능</td></tr>
<tr><td>상</td><td>민감정보 포함, 행정 내부업무 운영 시스템</td><td>· 보안 강화</td></tr>
</table>

2016 년부터 2023 년 2 월까지 클라우드 서비스 보안인증을 받아 국가기관에서 사용 가능한 시스템은 82 개로 IaaS 9 개, SaaS 표준 22 개, SaaS 간편 48 개, DaaS 3 개다.

〈표 3〉 연도별 클라우드 서비스 보안인증 시스템 현황

연도	계	2016 년	2017 년	2018 년	2019 년	2020 년	2021 년	2022 년	2023 년
현황	82	1	3	2	8	8	23	26	11

자세한 현황은 국가정보원 소속 국가사이버안보센터[3] 와 한국인터넷진흥원(KISA)[4] 에서 확인 가능하다.

[3] 국가정보보안기본지침(2023.1.31 부).
https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=InstructionGuide_main&nttId=18590&pageIndex=1

[4] 클라우드 보안인증제 연도별 인증서 발급현황. https://isms.kisa.or.kr/main/csap/issue/

두 번째, 제 15 조(보안인증기준)는 클라우드컴퓨팅 서비스 보안인증제도(CSAP) 항목을 14 개 통제항목과 117 개 평가항목으로 분류했다. 관리적/물리적/기술적 보호조치(별표 1~3)를 위한 14 개 통제항목과 106 개 평가항목을 적용한다.

〈표 4〉 관리적/물리적/기술적 분야별 통제항목 및 평가항목 현황

구분	통제항목	평가항목 수	하적용수
관리적	정보보호 정책 및 조직	5	2
	인적보안	11	2
	자산관리	10	3
	서비스공급망관리	4	2
	침해사고관리	7	6
	서비스연속성관리	7	5
	준거성	4	2
	소계	48	22
물리적	물리적 보호구역	5	2
	정보처리시설 및 장비보호	6	-
	소계	11	2
기술적	가상화보안	10	6
	접근통제	9	9
	네트워크 보안	6	5
	데이터보호 및 암호화	10	3
	시스템개발 및 도입보안	12	6
	소계	47	29
14 개 분야 총계		106	53

또한, 행정기관 및 공공기관에게 클라우드컴퓨팅 서비스를 제공하려는 경우 국가기관 등이 이용하는 클라우드컴퓨팅 서비스 보호조치(별표 4)는 1 개 분야 11 개 평가항목을 적용하는 것이다.

〈표 5〉 공공기관 보안요구사항 통제항목 및 평가항목 현황

구분	통제항목	평가항목 수	하적용수
공공기관 보안요구 사항	관리적보호조치	4	4
	물리적보호조치	2	2
	기술적보호조치	5	5
	소계	11	11

세부 점검항목은 한국인터넷진흥원 홈페이지에 공개되어 있다.

마지막으로 클라우드 보안인증의 등급화에 따른 관리적/물리적/기술적 보호조치를 위한 평가항목이 일부 변경됐다.

특히, 국가기관 등이 이용하는 클라우드컴퓨팅 서비스 보호조치와 관련하여, 물리적 보호조치 내 물리적 위치 및 영역 분리 통제항목에 상·중·하 등급이 모두 적용되는 부분에 가장 논란이 많다. 클라우드 시스템, 백업 시스템 및 데이터와 이를 위한 관리·운영 인력의 물리적 위치 기준 충족을 위해서는 데이터센터가 국내에 위치해야 하고, CC 인증은 국가정보원이 주관하는 공통평가기준을 통과해야 한다.

망분리는 기존에 적용했던 물리적 망분리를 상·중등급에 적용하고, 하등급만 적용하도록 하여 일반 이용자용 클라우드컴퓨팅 서비스 영역과 물리적 또는 논리적 망분리가 가능하다.

3. 클라우드 서비스 보안인증제도(CSAP) 개편에 따른 국내/해외 CSP 의 상황

공정거래위원회에 의하면 2021 년 민간 시장의 해외 클라우드 비중이 이미 73% (AWS 62.1%, Azure 12%) 이상을 차지하고 있다. 이번 보안인증제도 개편으로 클라우드 시장이 개방될 경우 외국 기업의 독과점 행태가 공공시장으로 확대될 수 있다는 예측이 나오고 있어, 국내 CSP(네이버, KT, NHN)의 입장은 매우 부정적이다. 이와 함께 규모가 큰 해외 기업들이 국내 시장을 장악하고 데이터 주권 역시 심각하게 훼손될 것이란 우려의 목소리가 나오고 있다.

기존 보안인증에 물리적 망분리 요건으로 인해 해외 CSP 가 국내에 진입하지 못했는데, 개정안에 "하"등급과 기존 통제항목 중 61 개의 항목에서 예외 처리가 되어 외국계 기업의 공공부문 진출이 가시화되고 있다. 이로 인해 공공시장마저 잠식당할 우려가 있어 상·중·하 등급 시행시기를 동시에 맞춰줄 것을 요구하고 있다.

반면 국내 클라우드 서비스(CSP)의 입장과 다르게 클라우드 관리서비스(MSP)[5] 측은 중립적이다. 국내에 진출한 해외 글로벌 CSP 기업들이 국내 시장에서 고객과 직거래하기보다 MSP 를 통한 거래를 적극 활용하는 것으로 조사되었기 때문이다. 따라서 메가존클라우드, 베스핀글로벌 등의 주요 국내 MSP 사업자들은 아마존, 구글 등과 협업을 통해 사업 확대의 기회를 얻을 수 있어 내부로는 찬성을 주장하면서 외부적으로는 신중한 모습을 보이고 있다. 한편, 중소기업이 많은 SaaS 관련 업체들은 해외 CSP 기업들이 시장에 참여할 경우 사업 기회가 늘어날 것으로 예상돼 기대감이 높아지고 있다.

[5] MSP (Managed Service Provider)는 클라우드 도입을 위한 컨설팅부터 전환, 구축, 운영, 유지보수 서비스까지 클라우드 사업 전반을 담당하는 클라우드 관리서비스 제공사다. CSP 가 제공하는 다양한 서비스와 고객 요구에 따라 효과적인 서비스 구성안을 적용하고, 적용된 클라우드 인프라가 24 시간, 365 일 안전하게 운영될 수 있도록 관리를 돕는다. 국내 대표적인 기업으로 베스핀글로벌, 메가존클라우드, GS 네오텍 등이 있다.

4. 맺음말

지금까지 보안인증제에 대한 배경과 앞으로 변경되는 내용을 살펴보았다.

과학기술정보통신부는 클라우드 서비스 보안인증제도(CSAP) 고시 이후 상·중 등급은 별도 기준을 마련한 후 시행할 방침이다. 다만 상·중 등급 시행 전까지 종전 고시에 따라 보안인증 유형 및 등급(IaaS, SaaS 표준, SaaS 간편 등)에 대해 인증을 신청할 수 있고, 기존 SaaS 간편인증은 하 등급 인증을 받은 것으로 인정할 수 있다.

정부에서는 규제 완화로 공공영역에서 민간 클라우드 시장이 형성되고, 전반적인 수요가 확대될 것으로 기대하고 있으나, 클라우드 서비스(CSP), 클라우드 관리서비스(MSP), 서비스형 소프트웨어(SaaS)는 엇갈린 입장 차이를 보이고 있다. 특히 이미 민간시장을 장악한 해외 CSP 들이 공공시장마저 장악해 국내 클라우드 서비스 업체의 경쟁력이 위축될 것이라는 우려 속 국내 CSP 업체의 반발이 예상되고 있다. 반면, 해외 CSP 는 미국 정부를 통해 상·중 등급도 완화해 줄 것을 지속적으로 요청하고 있는 것으로 알려졌다.

공공 데이터 주권을 훼손할 수 있다는 우려도 존재한다. 클라우드 서비스를 위한 시스템 및 데이터의 물리적 저장 위치를 국내로 한정하고 있지만, 백업 데이터 체계 등을 통해 해외로 데이터가 유출될 수 있다는 우려가 있기 때문이다. 데이터 주권 확보와 신뢰받고 안정된 서비스를 제공할 수 있도록 정부와 CSP 업체가 의견 조율에 최선을 다해 주길 바란다.