클라우드 보안인증제도 추진경과

2018. 6. 28.

Contents

I. 클라우드 관련 정부 정책

1 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제정(1)

추진경과

- 2009년 "범정부 클라우드컴퓨팅 활성화 종합계획"의 일환으로 법안 준비
- 2012년 7월 입법예고, 8월 공청회
- 2013년 10월 법안 국회 제출
- 2015년 3월 3일 국회 본회의 통과, 3월 27일 **공포**
- 2015년 9월28일 **시행**

주요내용

- 정부의 **클라우드 육성 지원 근거 마련**
  - 기본계획 및 시행계획 수립/시행 사항 규정
  - 연구개발지원, 세제지원, 중소기업지원, 시범사업 등 산업 육성 지원 근거 마련
- 규제개선을 통한 **공공/민간의 클라우드 이용 활성화 근거 마련**
  - 공공기관의 민간 클라우드서비스 이용을 위해 노력하여야 한다는 정부의 노력 의무 규정
  - 민간의 인허가 요건으로 전산설비에 클라우드 서비스 포함
- 안전한 클라우드를 위한 **이용자 보호 근거 마련**
  - 개인정보관련사항은 "정보통신망법 " 및 "개인정보보호법 " 이 적용됨을 명시
  - 이용자 정보 오남용 방지를 위한 동의 없이 제3자 제공 금지 및 목적 외 이용금지

I. 클라우드 관련 정부 정책

1 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제정(2)

제20조

제20조(공공기관의 클라우드컴퓨팅 도입 촉진) ① 정부는 **공공기관이 업무를 위하여 클라우드컴퓨팅 서비스 제공자의 클라우드컴퓨팅서비스를 이용** 할 수 있도록 노력하여야 한다.

(취지) 정부는 공공기관이 업무를 위하여 클라우드컴퓨팅서비스 제공자의 클라우드컴퓨팅서비스를 이용할 수 있도록 노력(클라우드컴퓨팅 사업의 수요예보, 클라우드서비스 보안인증제 도입 등 수행) 하여야 한다고 규정하여 정부의 의무를 부과

제13조

제13조(클라우드컴퓨팅 사업의 수요예보) ① **국가기관등의 장은 연 1회 이상 소관 기관의 클라우드 컴퓨팅 사업의 수요정보를 과학기술정보통신부장관에게 제출**하여야 한다. ② 과학기술정보통신부장관은 제1항에 따라 접수된 클라우드 컴퓨팅 수요정보를 연 1회 이상 클라우드컴퓨팅서비스 제공자에게 공개하여야 한다. (이하생략)

구분	제출횟수	제출시기	제출절차	공개주체	공표시기	공개장소
수요예보	연1회	매년 10월31일	국가공공기관 등→행정안전부 장관→과학기술정보통신부장관	과학기술 정보통신부장관	제출 받은 날부터 30일 이내	과학기술정보통신부 인터넷 홈페이지 (보도자료 등)

KISA

I. 클라우드 보안인증 정부 정책

2 「클라우드컴퓨팅서비스 정보보호에 관한 기준」 고시('16.4.4)

목적

「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조 제2항에 따라 **클라우드컴퓨팅서비스의 안전성 및 신뢰성 향상에 필요한 정보보호 기준의 구체적인 내용을 정함**

주요내용

관리적·물리적·기술적 보호조치 및 공공기관용 추가 보호조치로 **총 14개 부문 117개 통제항목**으로 구성

구분	주요 조치내용
관리적 보호조치	정보보호정책 수립, 인적보안, 자산 관리, 서비스 공급망 관리, 침해사고 관리 등
기술적 보호조치	가상화 보안, 접근통제, 네트워크 보안, 데이터보안/암호화 등
물리적 보호조치	보안구역 지정, 물리적 접근제어, 장비 반출입 등 정보처리 시설 및 장비보호
공공기관용 추가 보호조치	도입 전산장비 안정성, 물리적 위치 및 분리, 검증필 암호화 기술 제공 등

정보보호 기준은 권고사항이지만, 침해사고, 정보유출사고 등이 발생한 경우 과실 유무를 판단하는 기준이 될 수 있고 이용자들이 서비스 이용계약을 체결 할 때 정보보호기준의 준수를 요구할 수 있으므로 클라우드서비스 제공자는 정보보호기준을 준수하기 위해 노력하여야 한다.

KISA

Ⅱ. 보안인증제 개요

1 개요

정의

클라우드컴퓨팅서비스 사업자가 제공하는 서비스에 대해 **정보보호 기준의 준수여부 확인**을 인증 기관에 요청하는 경우 **인증기관이 이를 평가인증**하여 사용자들이 안심하고 클라우드서비스를 이용 할 수 있도록 지원하는 제도

목적 및 필요성

- 공공기관에게 안전성 및 신뢰성이 검증된 민간 클라우드서비스 공급
- 객관적이고 공정한 클라우드서비스 보안인증을 실시하여 이용자의 보안 우려를 해소하고 클라우드 서비스 경쟁력을 확보

기대효과

- 클라우드 서비스 제공자 관점
  - 객관적이고 공정한 클라우드서비스 보안 인증을 통해 **이용자 신뢰도 향상** 및 **제공자의 정보보호 수준 향상**
  - 클라우드서비스를 이용하는 공공기관의 **정보화 사업에 입찰 참여가 가능**
- 클라우드서비스 이용자(공공기관) 관점
  - 공공기관이 인증받은 클라우드서비스를 이용함으로써 **안전한 민간 클라우드서비스 이용 환경 조성 및 보안우려 해소를 통한 이용 활성화**

Ⅱ. 보안인증제 개요

2 추진근거

클라우드컴퓨팅 기본계획 (`15.11.10, 국무회의)

o (보안인증) 공공기관이 안전하게 민간 클라우드를 이용할 수 있도록 클라우드 보안인증제도 마련 (국정원·미래부·행자부, '15년)

* 공공기관 보안지침(국정원), 민간 클라우드 보안인증제도(미래부), 평가(KISA) 등 보안인증체계를 마련하고 인증실시('16년 ~)

클라우드 정보보호 고시 제7조 (정보보호 기준의 준수여부 확인)

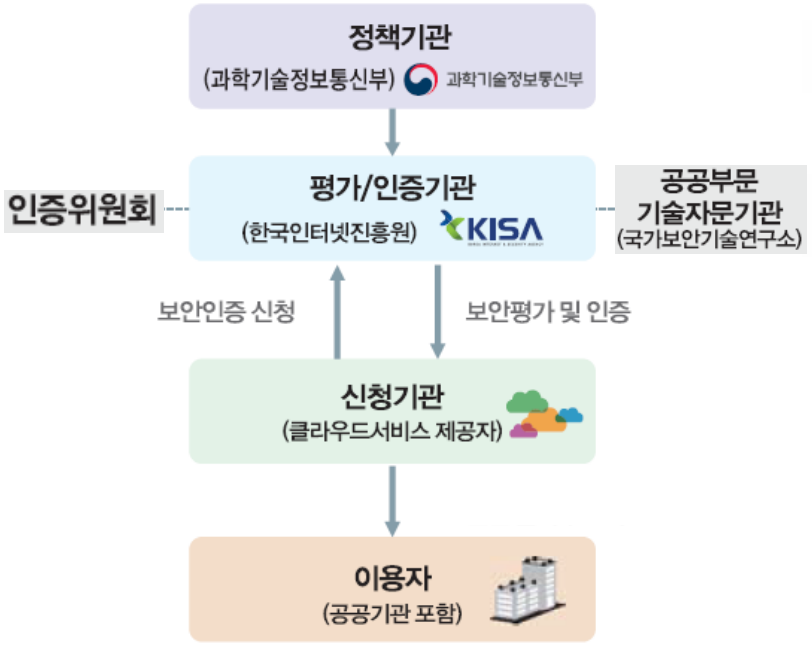
과학기술정보통신부장관은 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제5조에 따른 "기본계획"상의 "보안인증제" 시행을 위해 클라우드컴퓨팅서비스 제공자가 그 서비스가 이 기준을 준수하는지 확인을 요청한 경우에는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 "한국인터넷진흥원"의 장이 그 서비스를 조사 또는 시험·평가하여 인증 할 수 있다.

Ⅱ. 보안인증제 개요

3 평가·인증 종류 및 체계

최초평가 ⟷ (1년) 사후평가 ⟷ (1년) 사후평가 ⟷ (1년) 갱신평가

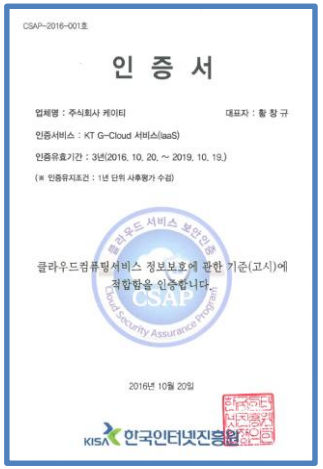
종류	내용
최초평가	클라우드서비스 보안인증을 처음 취득하기 위한 평가 (중요한 변경사항 발생시에도 최초평가 실시)
사후평가	인증 취득 후에도 지속적으로 클라우드서비스 보안 평가인증 기준을 준수하고 있는 확인하기 위한 평가 (연 1회 이상)
갱신평가	유효기간(3년) 만료일 이전에 유효기간 연장을 목적으로 하는 평가



구분	주요역할
정책기관 (과학기술정보통신부)	· 평가·인증 관련 법·제도 개선 및 정책 수립 · 평가/인증기관의 지정 및 감독
평가인증기관 (한국인터넷진흥원)	· 평가·인증 신청접수 · 평가·인증기준, 지침 개발 · 평가를 통한 인증업무 수행 · 인증서 발급 및 인증된 클라우드서비스 관리
인증위원회	· 평가결과를 통한 인증 심의·의결 · 인증취소의 타당성 심의 · 학계, 연구기관, 기술자문기관 등 클라우드 관련 전문가 5인 이상 10명 이내로 구성
기술자문기관 (국가보안기술연구소)	· 공공기관 민간 클라우드서비스 도입 보안기준 마련 · 국가·공공 클라우드 안전성 강화 대책 수립
신청기관 (클라우드사업자)	· IaaS, SaaS 등 클라우드서비스 제공 · 자체 보안 활동 정기 · 수시 수행

Ⅲ. 클라우드 보안인증서 발급 현황

인증 번호	업체(기관)명	인증범위	유효기간
CSAP-2016-001호	주식회사 케이티	KT G-Cloud 서비스(IaaS)	16-10-21 ~ 19-10-19
CSAP-2017-001호	Naver Bussiness Platform(주)	네이버클라우드 BIZ-G 서비스(IaaS)	17-02-24 ~ 20-02-23
CSAP-2017-002호	주식회사 가비아	가비아 G 클라우드 공공(IaaS)	17-05-11 ~ 20-05-10
CSAP-2017-003호	엔에이치엔터테인먼트㈜	G-토스트 클라우드 (IaaS)	17-12-15 ~ 20-12-14
CSAP-2018-001호	㈜엘지씨엔에스	LG G-Cloud (IaaS)	18-02-28 ~ 21-02.27


CSAP-2016-001호

인 증 서

업체명 : 주식회사 케이티 대표자 : 황 창 규

인증서비스 : KT G-Cloud 서비스(IaaS)

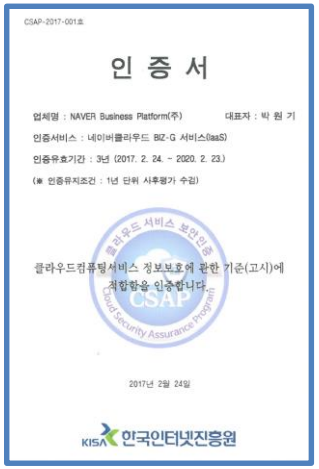
인증유효기간 : 3년(2016. 10. 20. ~ 2019. 10. 19.)

(※ 인증유지조건 : 1년 단위 사후평가 수검)

클라우드컴퓨팅서비스 정보보호에 관한 기준(고시)에 적합함을 인증합니다.

2016년 10월 20일

KISA 한국인터넷진흥원


CSAP-2017-001호

인 증 서

업체명 : NAVER Business Platform(주) 대표자 : 박 원 기

인증서비스 : 네이버클라우드 BIZ-G 서비스(IaaS)

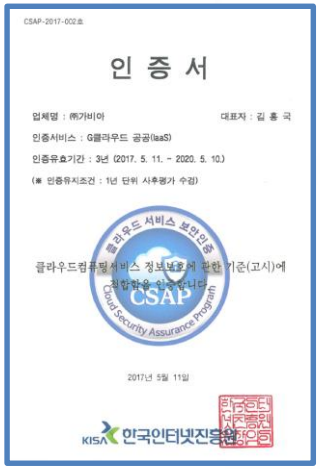
인증유효기간 : 3년 (2017. 2. 24. ~ 2020. 2. 23.)

(※ 인증유지조건 : 1년 단위 사후평가 수검)

클라우드컴퓨팅서비스 정보보호에 관한 기준(고시)에 적합함을 인증합니다.

2017년 2월 24일

KISA 한국인터넷진흥원


CSAP-2017-002호

인 증 서

업체명 : ㈜가비아 대표자 : 김 홍 국

인증서비스 : G클라우드 공공(IaaS)

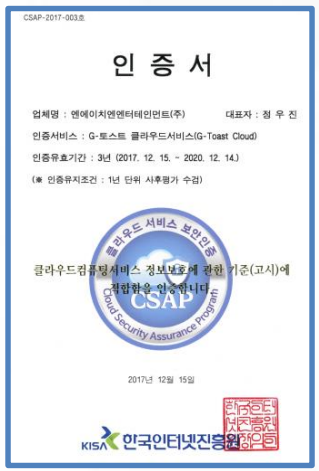
인증유효기간 : 3년 (2017. 5. 11. ~ 2020. 5. 10.)

(※ 인증유지조건 : 1년 단위 사후평가 수검)

클라우드컴퓨팅서비스 정보보호에 관한 기준(고시)에 적합함을 인증합니다.

2017년 5월 11일

KISA 한국인터넷진흥원


CSAP-2017-003호

인 증 서

업체명 : 엔에이치엔엔터테인먼트(주) 대표자 : 정 우 진

인증서비스 : G-토스트 클라우드서비스(G-Toast Cloud)

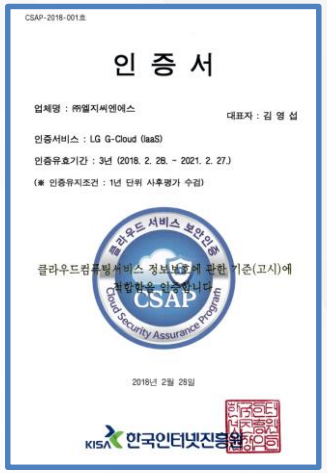
인증유효기간 : 3년 (2017. 12. 15. ~ 2020. 12. 14.)

(※ 인증유지조건 : 1년 단위 사후평가 수검)

클라우드컴퓨팅서비스 정보보호에 관한 기준(고시)에 적합함을 인증합니다.

2017년 12월 15일

KISA 한국인터넷진흥원


CSAP-2018-001호

인 증 서

업체명 : ㈜엘지씨엔에스 대표자 : 김 영 섭

인증서비스 : LG G-Cloud (IaaS)

인증유효기간 : 3년 (2018. 2. 28. ~ 2021. 2. 27.)

(※ 인증유지조건 : 1년 단위 사후평가 수검)

클라우드컴퓨팅서비스 정보보호에 관한 기준(고시)에 적합함을 인증합니다.

2018년 2월 28일

KISA 한국인터넷진흥원

Ⅳ. 클라우드 보안인증제 확대시행(IaaS → IaaS, SaaS)

1 추진 배경

보안성이 확보된
SaaS 육성 필요

▪ **중·소 사업자가 많은 SaaS 시장**

서비스 모델별 공급 현황 (단위 : 개)

구 분		사례수	IaaS	PaaS	SaaS
전 체		155	59	8	88
기업 규모	중견기업 이상	24	13	1	10
	중소기업	131	46	7	78

※출처(2017년 클라우드 산업 실태조사, NIPA, '16.12)

▪ **단일 IaaS 서비스 위에 다수 SaaS 서비스(3rd Party 등) 동작**

kt ucloud biz
DB VPN 모니터링 보안

NAVER CLOUD PLATFORM
DB 모니터링 보안 AI 분석

gabia.
방화벽 모니터링 로드밸런싱 보안

공공기관에서 안심하고 사용할 수 있는 SaaS 서비스 제공을 위한 보안인증제 확대 시행(IaaS → IaaS, SaaS)

KISA

Ⅳ. 클라우드 보안인증제 확대시행(IaaS → IaaS, SaaS)

1 추진배경

제도적 측면

- (해외) 선도국가는 SaaS 서비스 인증을 통해 ERP, CRM, 협업서비스등 다양한 서비스 정부기관 도입
- (국내) 보안성 검토
  - 사업자 : 납품 기관별 보안성 검토 대응 지원

사업적 측면

- 일부 사업자 이외, 아직 도입검토 단계

SaaS

- 일부 SaaS 사업자는 공공기관 납품의사 밝힘

※ 씨앗 등록 사업자 대상 조사

IaaS

- 자체개발, 파트너쉽을 통해 SaaS 제공예정
- 대부분 공공 확대 희망

공공기관 클라우드 도입 활성화

국내 중소 SaaS 기업 육성

SaaS 대상 클라우드 보안인증제 추진 필요

KISA

Ⅳ. 클라우드 보안인증제 확대시행(IaaS → IaaS, SaaS)

2 추진 경과

1) SaaS에 적합한 인증기준 및 평가방법론 마련(~'17.6월)

- (인증기준) 기존 IaaS 인증기준 대비 32% 감소(기존 117개→78개)
  - IaaS에 의존적인 물리적 보호조치 전체, 관리적 보호조치 일부 항목 삭제 등 완화
  - 다자간 계약관계, 이용자 데이터 흐름, SW개발 보안 등은 강화
- (평가방법론) IaaS 평가방법 기반 SaaS 사업자, 환경을 고려한 평가방법론 개발

2) SaaS 보안인증 시범 사업 수행(17.6월~11월)

가비아 (ERP, 그룹웨어)	▪ 클라우드 환경에서 업무 서비스(이메일, 게시판 등) 제공
인프라닉스 (시스템 모니터링)	▪ 클라우드 자원의 생성, 삭제, 운영 현황을 대시보드로 제공
지니언스 (NAC Cloud)	▪ 클라우드 단말들에 대한 네트워크 통제 등 보안기능 제공

서면/현장평가

소스코드 및 취약점 점검

모의침투 테스트

Ⅳ. 클라우드 보안인증제 확대시행(IaaS → IaaS, SaaS)

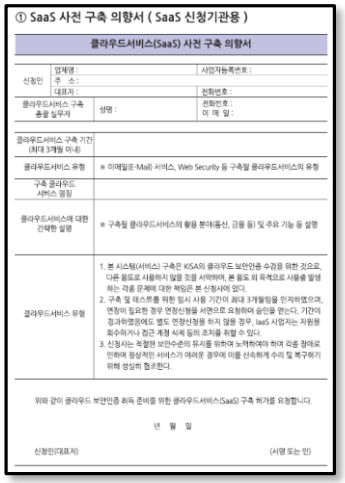
2 추진 경과

3) SaaS 사업자 및 유관기관 간담회 개최('18.1월~5월)

- 보안서비스 평가, 형상관리 등을 위한 평가기관(CC인증, GS인증 등) 협의(~'18.4월)
- 공공기관이 이용 가능한 SaaS 유형 발굴을 위한 관계기관 협의('18.5월)
- SaaS 사전 구축, 인증 수요 등을 의견수렴을 위한 사업자 간담회 개최('18.5.23)

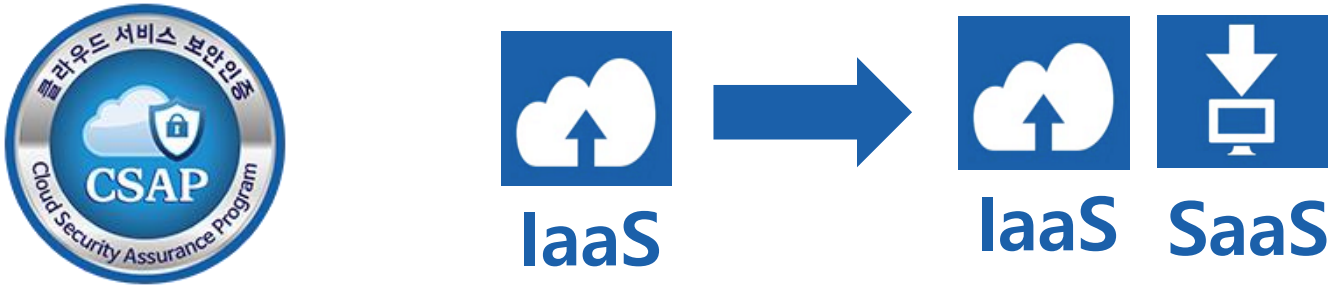
4) 클라우드 보안인증 안내서 개정(IaaS·SaaS 통합본)(~'18.6월)

- SaaS 인증 기준 및 평가 방법 추가
- 재해복구(DR)센터 구축 기준 추가
- SaaS 평가·인증 관련 양식 추가
  - SaaS 사전 구축 의향서, 예비점검 체크리스트, 지원서비스 등록신청서, 보안기능변경 영향분석서 등
- 사후관리(분기별) 절차 개선
  - 사후관리 절차(지원서비스 관리, 형상관리 등) 추가
  - 사후관리 제출서류 목록화 등



V. 기타

클라우드 보안인증제 확대 시행 예정



SaaS 보안인증 관련 유의사항

- ✓ SaaS 신청 시 인증받지 않은 IaaS 인프라를 사용할 경우, SaaS 서비스 관련 모든 인프라는 IaaS 인증기준 기반 점검 예정(즉, SaaS 서비스 : SaaS 인증기준 기반 점검, 인증받지 않은 IaaS 인프라 : IaaS 인증기준 기반 점검)
- ✓ 보안인증에서 제외되는 SaaS 유형

  ※ Private, Hybrid 전용으로 구축된 SaaS, 인증기준(취약점 점검 불가 등)에 미달하는 SaaS, 이용자 가상머신상에 구축하는 설치형 SaaS 등
- ✓ 보안인증 취득 후 지속적인 평가·인증기준 준수와 유지할 책임은 취득기관에 있음
- ✓ 서면/현장 평가, 취약점 점검 및 침투테스트 시 관련 조직 및 담당자의 유기적인 협조와 노력 필요

  ※ 평가 시 인증준비 미흡, 요청사항 대응 미흡, 중요 부적합 사항 미 조치 등의 사유로 철수 및 중단 가능

KISA

Internet On, Security In!

감사합니다