제도소개

안전한 클라우드 컴퓨팅 서비스 정보보호 관리체계를 만들어갑니다.

인증제도

클라우드서비스 제공자가 제공하는 서비스에 대해「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제23조의2에 따라 정보보호 수준의 향상 및 보장을 위하여 보안인증기준에 적합한 클라우드컴퓨팅서비스에 대하여 보안인증을 수행하는 제도입니다.

보안인증의 표시는「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제23조의2조제3항에 따라 보안인증을 받은 클라우드컴퓨팅서비스에 대해 표시할 수 있습니다.
보안인증의 표시는「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행규칙」제4조에 따라 표시도안의 크기를 용도에 맞게 같은 배율로 조정할 수 있으며, 알아보기 쉽게 표시하여야 합니다.
표시도안의 색상 및 글씨체는 임의로 변경할 수 없습니다.

목적 및 필요성

- 국가·공공기관에게 안전성 및 신뢰성이 검증된 민간 클라우드서비스 공급
- 객관적이고 공정한 클라우드서비스 보안인증를 실시하여 이용자의 보안 우려를 해소하고, 클라우드서비스의 경쟁력 확보

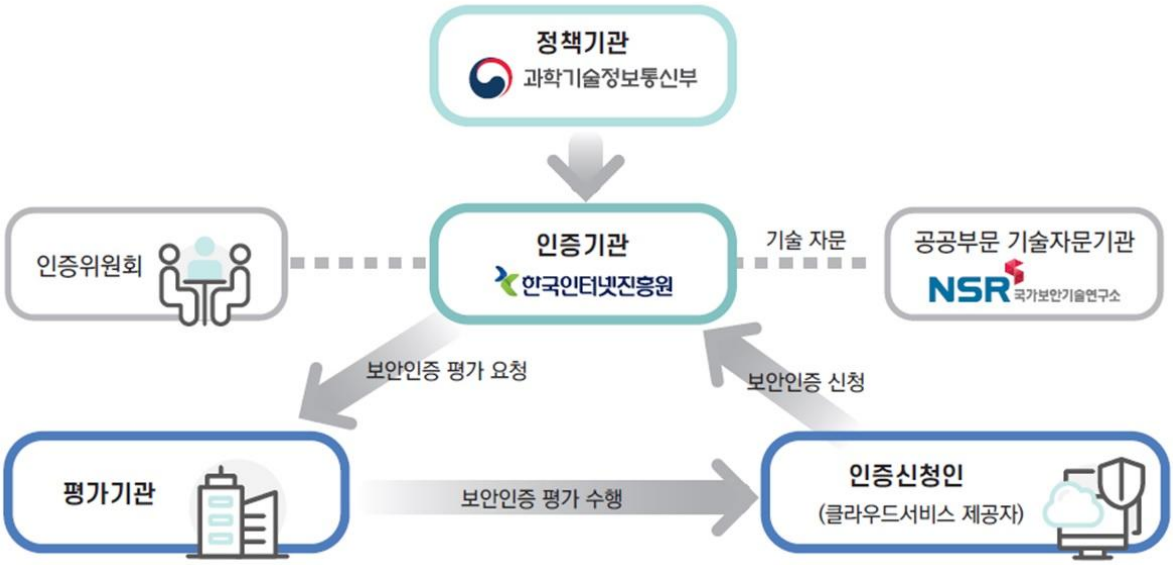
추진근거

- 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제5조에 의한「제1차 클라우드컴퓨팅 기본계획」(2015)에 따른 클라우드서비스 보안인증제도 시행
- 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제23조의2에 따라 보안인증에 관한 업무 수행

보안인증체계

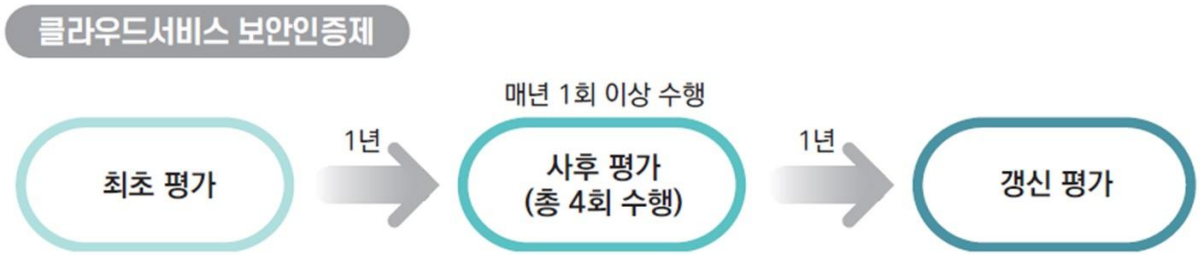
- 클라우드서비스 보안인증체계는 역할과 책임에 따라 정책기관, 인증/평가기관, 인증위원회, 기술자문기관, 인증신청인, 이용자로 구분합니다. 정책기관은 과학기술정보통신부, 인증기관은 한국

인터넷진흥원, 평가기관은 한국인터넷진흥원 및 과학기술정보통신부에서 지정한 기관, 공공부문 기술자문기관은 국가보안기술연구소에서 그 역할을 수행하고 있습니다.



- 정책기관 (과학기술정보통신부)
- 인증기관 (한국인터넷진흥원): 인증위원회 개최, 공공부문 기술자문기관 (국가보안기술연구소)에서 기술자문, 평가기관에게 보안인증 평가요청, 인증신청인 (클라우드서비스 제공자) 보안인증 신청
- 평가기관 : 인증신청인 (클라우드서비스 제공자)에게 보안인증 평가 수행
- 인증신청인 (클라우드서비스 제공자) : 인증기관 (한국인터넷진흥원)에게 보안인증 신청

보안인증 유형 등



- 클라우드서비스 보안인증제
  - 최초평가
  - 1년후 사후평가(총4회 수행, 매년 1회이상 수행)
  - 1년후 갱신평가

▶ 보안인증 유형

- 클라우드서비스 보안인증 유형은 **IaaS, SaaS, DaaS**가 있으며, 유효기간은 모두 5년입니다.
  ※ 기존 인증제도(IaaS, SaaS(표준등급, 간편등급), DaaS 등)는 상·중 등급 시행 전까지 인증 신청 가능

▶ 보안인증 등급

- 클라우드서비스 보안인증 등급은 **상·중·하**로 구분됩니다.
  ※ 하 등급은 고시에 반영되어 있으며, 상·중 등급은 추후 반영 예정

▶ 인증평가 종류

- **최초평가**는 처음으로 인증을 신청하거나, 인증범위에 중요한 변경이 있어 다시 인증을 신청한 때에 실시하는 평가입니다.
  ※ 최초평가를 통해 인증을 취득하면, 5년의 유효기간을 부여

- **사후평가**는 보안인증을 취득한 이후 지속적으로 클라우드서비스 보안인증기준을 준수하고 있는지 확인하기 위한 평가이며, 보안인증 유효기간(5년) 안에 매년 시행됩니다.

- **갱신평가**는 보안인증 유효기간(5년)이 만료되기 전에 클라우드서비스에 대한 보안인증의 연장을 원하는 경우에 실시하는 평가입니다.
  ※ 갱신평가를 통과하는 경우, 5년의 유효기간을 다시 부여

보안인증 범위

- 클라우드서비스 보안인증 범위는 클라우드서비스에 포함되거나 관련 있는 자산(시스템, 설비, 시설 등), 조직, 지원서비스 등을 모두 포함하여 설정합니다.
  ※ 클라우드서비스란 클라우드컴퓨팅법 시행령 제3조의 서비스를 의미

보안인증기준

▶ 기존 보안인증제도의 유형에 따른 보안인증기준은 다음과 같습니다.

- IaaS 보안인증은 관리적·물리적·기술적 보호조치 및 공공기관용 추가 보호조치로 총 14개 분야 116개 통제항목으로 구성
- SaaS 표준등급 인증은 관리적·기술적 및 공공기관용 추가 보호조치로 총 13개 분야 79개 통제항목으로 구성
- SaaS 간편등급 인증은 관리적·기술적 및 공공기관용 추가 보호조치로 총 11개 분야 31개 통제항목으로 구성
- DaaS 인증은 관리적·물리적·기술적 및 공공기관용 추가 보호조치로 총 14개 분야 110개 통제항목으로 구성

▶ 등급제 시행에 따른 보안인증기준은 다음과 같습니다.

- 하등급 인증은 관리적·기술적 및 공공기관용 추가 보호조치로 총 14개 분야 64개 통제항목으로 구성
- 하등급 SaaS 인증은 관리적·기술적 및 공공기관용 추가 보호조치로 총 11개 분야 30개 통제항목으로 구성

심사종류							
통제 분야	**통제 항목**	**통제항목 수**					
		IaaS	**SaaS**		**DaaS**	**하등급**	**하등급 SaaS**
			표준	**간편**			
1. 정보보호 정책 및 조직	1.1. 정보보호 정책	3	3	1	3	1	-
	1.2. 정보보호 조직	2	2	1	2	1	1
2. 인적보안	2.1. 내부인력 보안	5	4	1	4	1	1
	2.2. 외부인력 보안	3	-	-	3	-	-
	2.3. 정보보호 교육	3	1	1	1	1	1
3. 자산관리	3.1. 자산 식별 및 분류	3	1	-	3	2	-
	3.2. 자산 변경관리	3	1	-	3	-	-
	3.3. 위험관리	4	1	-	4	1	-
4. 서비스 공급망 관리	4.1. 공급망 관리정책	2	2	-	2	1	-
	4.2. 공급망 변경관리	2	1	-	2	1	-
5. 침해사고관리	5.1. 침해사고 대응 절차 및 체계	3	3	1	3	3	1

심사종류							
통제 분야	**통제 항목**	**통제항목 수**					
		IaaS	**SaaS**		**DaaS**	**하등급**	**하등급 SaaS**
			표준	**간편**			
	5.2. 침해사고 대응	2	2	1	2	2	1
	5.3. 사후관리	2	2	-	2	1	-
6. 서비스 연속성 관리	6.1. 장애대응	4	4	1	4	4	1
	6.2. 서비스 가용성	3	2	1	3	1	1
7. 준거성	7.1. 법 및 정책 준수	2	1	1	2	1	1
	7.2. 보안 감사	2	2	-	2	1	-
8. 물리적 보안	8.1. 물리적 보호구역	5	-	-	5	2	-
	8.2. 정보처리 시설 및 장비보호	6	-	-	6	-	-
9. 가상화 보안	9.1. 가상화 인프라	6	2	1	5	5	1
	9.2. 가상 환경	4	4	-	2	1	-
10. 접근통제	10.1. 접근통제 정책	2	2	1	2	2	1
	10.2. 접근권한 관리	3	3	-	3	3	-
	10.3. 사용자 식별 및 인증	4	4	3	4	4	3

심사종류							
통제 분야	**통제 항목**	**통제항목 수**					
		IaaS	**SaaS**		**DaaS**	**하등급**	**하등급 SaaS**
			표준	**간편**			
11. 네트워크 보안	11.1. 네트워크 보안	6	5	2	6	5	2
12. 데이터 보호 및 암호화	12.1. 데이터 보호	6	6	2	6	2	1
	12.2. 매체 보안	2	-	-	2	-	-
	12.3. 암호화	2	2	2	2	1	1
13. 시스템 개발 및 도입 보안	13.1. 시스템 분석 및 설계	5	5	1	5	3	1
	13.2. 구현 및 시험	4	4	1	4	3	1
	13.3. 외주 개발 보안	1	1	-	1	-	-
	13.4. 시스템 도입 보안	2	-	-	2	-	-
14. 국가기관등의 보안요구사항	14.1. 관리적 보호조치	4	4	4	4	4	4
	14.2. 물리적 보호조치	2	2	2	2	2	2
	14.3. 기술적 보호조치	4	3	3	4	5	5
총계		116	79	31	110	64	30